COL334 Major

Viraj Agashe

TOTAL POINTS

33 / 40

QUESTION 1

1 1.a **3 / 3**

✓ **+ 1 pts** **Correct packet sequence**

1,3,2,5,7,9,4,6,11,8,10,12

or 1,2,3,4,5,7,9,6,8,11,10,12

✓ **+ 1 pts** **correct delay calculation**

0,2,0,5,0,5,1,4,0,3,0,3 or 1,3,1,6,1,6,2,5,1,4,1,4

or

0,1,1,2,1,5,2,3,1,3,1,3 or 1,2,2,3,2,6,3,4,2,4,2,4

✓ **+ 1 pts** **average delay = 23/11 or 34/11 or 23/12 or 35/12**

+ 0.5 pts minor mistake in any of the above steps

+ 0 pts Incorrect

QUESTION 2

2 1.b **4 / 4**

✓ **+ 2 pts** **Correct packet sequence**

1,2,4,3,6,8,5,10,12,7,9,11 or 2,4,1,6,3,8,5,10,12,7,9,11

or 2,4,3,6,7,8,9,10,12,11,5,1 or

1,2,4,7,6,8,9,10,12,11,5,3

or 2,1,4,6,3,5,8,7,10,9,12,11 or 1,2,4,3,6,5,8,7,10,12,9,11

✓ **+ 1 pts** **correct delay calculation**

0,1,2,1,3,2,6,0,5,0,3,0

or

1,2,3,2,4,3,7,1,6,1,4,1

✓ **+ 1 pts** **Average delay = 23/11 or 23/12 or 34/11 or 35/12**

+ 0.5 pts minor mistake in any of the above step

+ 0 pts incorrect

QUESTION 3

3 1.c **3 / 3**

✓ **+ 1 pts** **Why NAT in today's world(any one point)**

✓ **+ 1 pts** **Why NAT temporary solution?(any 1 point)**

✓ **+ 1 pts** **Will NAT stay? no marks without a valid reason.**

+ 0 pts otherwise

QUESTION 4

4 2a **4 / 4**

✓ **+ 4 pts** **Correct initial and final routing table**

- 1 pts calculation and computation step incorrect/incomplete/not shown

+ 0 pts Not attempted/incorrect

QUESTION 5

5 2b **2 / 2**

✓ **+ 2 pts** **correct answer and explanation**

+ 0 pts not attempted/Incorrect answer

+ 1 pts Partially correct answer

QUESTION 6

6 2c **3 / 3**

✓ **+ 1 pts** **How control plane under logical centralized? (SDN concept, remote controller)**

✓ **+ 0.5 pts** **In such case- Separate devices**

✓ **+ 0.75 pts** **Any 1 advantage**

✓ **+ 0.75 pts** **Any 1 disadvantage**

+ 0 pts Incorrect/not attempted

QUESTION 7

7 3a **0.5 / 5**

+ 1.5 pts Correctly detecting when the collision happens

Explanation:

we assume both transmit at equal speeds. So, collision happens somewhere in the mid,i.e,

245/2 = 122.50-bit times

+ **1.5 pts** Correct usage of the jamming signal.

Explanation:

Both A and B send and alert each other that a collision has occurred after
245 + 10 = 255-bit times.
next transmission will happen at 255+245 = 500 bit times

+ **2 pts** Reporting the correct packet starting for both A and B.

Explanation:

Since there is only one collision let's assume A takes k=0 and B takes k=1 in the CSMA/CD algorithm.
So, the frame from A starts at 500 bit-time and reaches B at 500+245+300=1045-bit times.
while B will start to send its frame at 1046-bit times.

+ **0 pts** wrong

+ 0.5 Point adjustment

values have to be written.

QUESTION 8

8 3b **1.5 / 3**

+ **3 pts** Correct

✓ **+ 1 pts Partially Correct/Correct Idea**

+ **0 pts** Incorrect/Unattempted

+ **1 pts** Correct Expression but steps not shown/are unclear.

+ 0.5 Point adjustment

1 data transmitted per unit time

QUESTION 9

9 3c **2 / 2**

✓ **+ 1 pts Explained why ARP query is sent in a broadcast frame (the destination MAC address is not known, hence everyone is to be asked)**

✓ **+ 1 pts Explained why the response is directed to a specific MAC (the source address is now known from the query, so a broadcast would be wasteful)**

+ **0 pts** Incorrect/Unattempted

QUESTION 10

10 4a **2 / 2**

+ **0 pts** incorrect answer(if answer is yes)

+ **1 pts** Answer is No, but partially correct explanation

✓ **+ 2 pts Answer is No, and correct explaination**

QUESTION 11

11 4b **3 / 3**

+ **0 pts** Totally Incorrect answer

+ **1.5 pts** Correct explanation of how message reaches but without explaining the role of HSS,MME or gateway routers in it or incorrect explanation of some part or some missing detail

✓ **+ 3 pts All parts included**

- 0.5 pts for frivolous regrade request

QUESTION 12

12 4c **2 / 3**

✓ **+ 1 pts Fully correct for confidentiality**

+ **0.5 pts** Partially correct for confidentiality

+ **1 pts** Fully correct for authentication

✓ **+ 0.5 pts Partially correct for authentication**

+ **1 pts** Correct example Provided(for both confidentiality and authentication)

✓ **+ 0.5 pts Partially correct example or lacks explanation**

+ **0 pts** Wrong answer

PKI is used for authentication by sigining a message with own private key which will be only decrypted by his "public key". You are discussing authenticity of this "public key" instead of what is asked. Still partial marks.

QUESTION 13

13 4d **3 / 3**

✓ **+ 1 pts Correct definition of attack**

✓ **+ 0.5 pts Correct example explaining working of attack**

✓ **+ 1.5 pts Correct Prevention technique with role of**

CA

+ **0.5 pts** Only prevention (CA role not mentioned)
+ **0 pts** No attempt

Indian Institute of Technology Delhi
Department of Computer Science and Engineering
COL334/672: Computer Networks
Major Examination, Diwali 2022

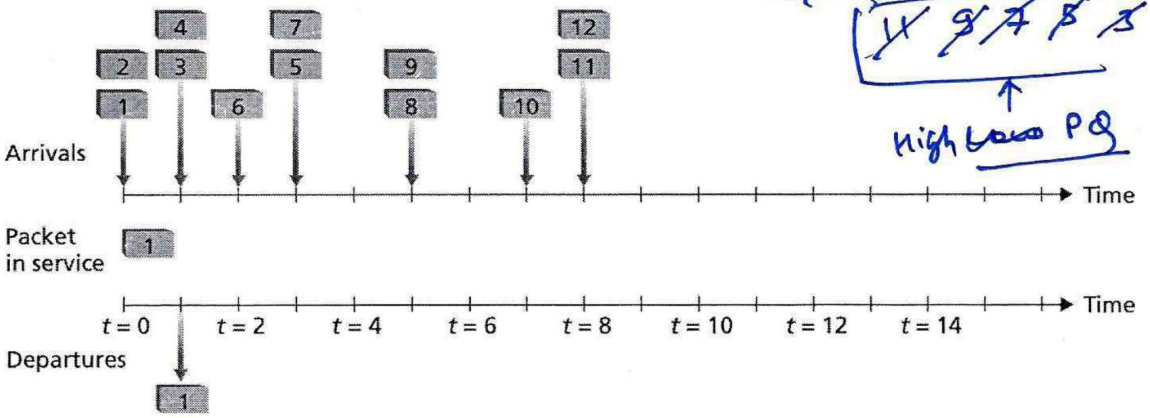
Full Marks: 40 **Time: 2 hours**

Name VIRAJ AGASHE **Entry Number** 2020CS10567

Answer the questions on the space provided
Be precise in your answers, and state any assumptions made

Question 1 [3+4+3 = 10 marks]

(a) Consider the following packet arrival pattern in a router. Assume that the router follows a priority-based scheduling policy where odd-numbered packets are high priority, and even-numbered packets are low priority. If only one packet can be transmitted during one timeslot, indicate the time at which packets 2 through 12 each leave the queue. What is the average delay between a packet's arrival and the beginning of the slot in which it is transmitted? Show the computation steps.



Low PQ

High PQ

Ans. Assuming that packets cannot be sent immediately when received

PACKET	IN TIME	OUT TIME
2	0	3
3	1	2
4	1	7
5	3	4
6	2	8
7	3	5
8	5	10
9	5	6
10	7	11
11	8	9
12	8	12

Average Delay

Packet 1 : $\Delta t_1 = 1$

$\Delta t_2 = 3$

$\Delta t_3 = 1$

$\Delta t_4 = 6$

$\Delta t_5 = 1$

$\Delta t_6 = 6$

$\Delta t_7 = 2$

$\Delta t_8 = 5$

$\Delta t_9 = 1$

$\Delta t_{10} = 4$

$\Delta t_{11} = 1$

$\Delta t_{12} = 4$

$$\therefore \text{Avg time delay} = \frac{\sum \Delta t_i}{\sum i} = \frac{35}{12}$$

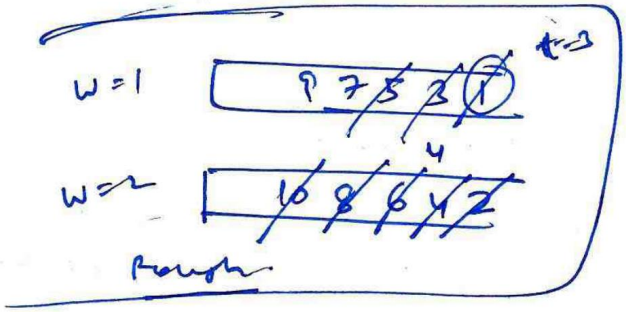
$$= 2.916 \text{ s.}$$

(b) Consider the same packet arrival pattern as shown in the previous figure. However, instead of priority-based, now assume that the router is following a weighted fair queueing (WFQ) scheduling policy. Further assume that odd-numbered packets are from Class 1 having WFQ weight of 1, and even-numbered packets are from Class 2 having WFQ weight of 2. Indicate which packet will go into service at each time slot. What is the average delay between a packet's arrival and its departure in this scheme? Show the steps clearly.

Sol.

w=1 11 9 7 5 3 1

w=2 10 8 6 4 2



Pack	In	Out
1	0	3
2	0	1
3	1	5
4	1	2
5	3	7
6	2	4
7	3	10
8	5	6
9	5	11
10	7	8
11	8	12
12	8	9

Delays

$\Delta t_1 = 3$
$\Delta t_2 = 1$
$\Delta t_3 = 4$
$\Delta t_4 = 1$
$\Delta t_5 = 4$
$\Delta t_6 = 2$
$\Delta t_7 = 7$
$\Delta t_8 = 1$
$\Delta t_9 = 6$
$\Delta t_{10} = 1$
$\Delta t_{11} = 4$
$\Delta t_{12} = 1$

Avg. delay

$$= \frac{\sum \Delta t_i}{\sum t_i} = \frac{35}{12}$$

Assumption:

1. Start with packets with WFQ = 2
2. If no packets in WFQ = 2 queue, send packet from WFQ = 1 queue.

(c) What is the need for Network Address Translation (NAT) in today's internet? Why was NAT considered to be a temporary solution? Do you think NAT will stay in operation in foreseeable future? Why?

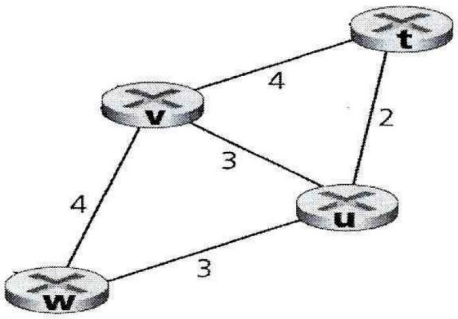
Ans. The need for NAT is that IPv4 addresses are only 32 bits long, which is not sufficient to assign a unique IP address to all the devices in the world (ran out of IPs in 2011 or so). Therefore, NAT, which allows devices of a subnet to share the same IP for the outside world, is used so that IPs can be reused inside the subnetwork.

NAT is considered as a temporary solution as IPv6 has begun to be adopted which is 128 bits long and enough to assign a unique IP to each sand grain. Further, there are some issues with NAT : It modifies the transport layer attributes like the port nos etc. which violates end-to-end agreements, and is not supposed to access those.

In the foreseeable future, NAT is likely to stay, as only 30% of devices accessing Google use IPv6 addresses as of 2019. The adoption of IPv6 completely will take a lot of time. Further NAT also provides some advantages like network security (outside world does not know exact IP address). Changing NAT would take a lot of structural changes to internet. In the long term, NAT may be discontinued but it is here to stay for now.

Question 2 [4+2+3 =9 marks]

(a) Consider the network shown in the figure below and assume that each node initially knows the costs to each of its neighbors. Consider the distance-vector algorithm and compute the distance table entries at each node. Show the computation steps.



Initial tables. ($t = 0$)

t	
v	4
u	2

v	
w	4
t	4
u	3

w	
v	4
u	3

u	
v	3
w	3
~~t~~	~~2~~

Now, all nodes send their own estimates to other nodes.

We update the distances as,

$$d_x(y) = \min_{\forall u \in N(x)} \left(d_x(u) + d_u(y) \right)$$

∴ For t:

$d_t(v) = \min(4, 3+2) = 4$

$d_t(u) = \min(2, 4+3) = 2$

$d_t(w) = \min(4+4, 2+3) = 5$

So on for other tables.

For v

$d_v(t) = \min(4, 3+2) = 4$

$d_v(u) = \min(3, 4+2, 4+3) = 3$

$d_v(w) = \min(4, 3+3) = 4$

So we get,

t	
v	4
u	2
w	5

v	
w	4
u	3
t	4

w	
v	4
u	3
t	5

u	
v	3
w	3
t	2

More steps at back.

In the next iteration, note that.

For t

$d_t(v) = \min(4, 3+2) = 4$

$d_t(u) = \min(2, 4+3) = 2$

$d_t(w) = \min(4+4, 2+3) = 5$

For v, u ⇒ All adjacent costs not changed, other costs greater.

For w

$d_w(t) = \min(5, 3+2, 4+4) = 5$

~~Rest are adjacent~~ Others adjacent, other costs greater.

No update.

So, these are converged

Complete steps for step 1

$d_u(w) = \min(3, 3+4) = 3$

$d_u(v) = \min(3, 2+4, 3+4) = 3$

$d_u(t) = \min(3+4, 2) = 2$

$d_w(v) = \min(4, 2+3) = 4$

$d_w(u) = \min(3, 3+4) = 3$

$d_w(t) = \min(2+3, 4+4) = 5$

(b) Assume that the nodes in the figure are connected to other nodes in the network (not explicitly shown). Give link-cost change for the links (u,t) and (u,w) such that node v will inform its neighbors of new paths as a result of executing the distance-vector algorithm.

Ans. ① If the link cost (u,t) becomes <1 (say 0.5), then exists a shorter path from v→t of length 3.5 compared to v→t link (4).

v→u→t

So there will be a change.

So, $c(u,t) = 0.5$ from $c(u,t) = 2$, $\Delta c(u,t) = -1.5$

② If link cost (u,w) becomes <1 (say 0.5), then again ∃ a shorter (v→w) path which is v→u→w of length 3.5 compared to 4.

$\therefore c(u,t) = 0.5$ from $c(u,t) = 3$.

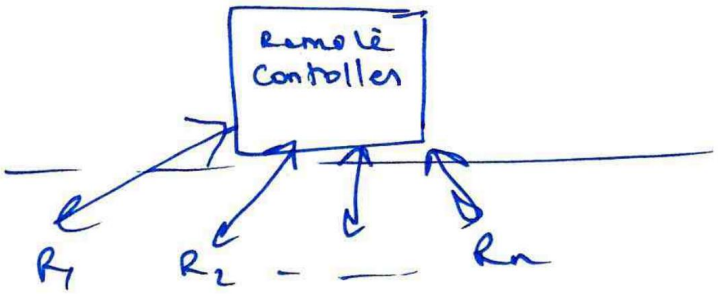
$\Delta c(u,t) = -2.5$.

Disadvantages

1. Single controller can be a point of failure (single point of failure) compared to distributed routing.
2. Requires structural changes in internet, may be expensive & infeasible.

(c) How can a control plane be under logically centralized control? In such cases, are the data and control planes implemented within the same device or in separate devices? What are the advantages and disadvantages in such approach? Precisely explain your answer.

Ans. A control plane can be under logically centralized control in the case of Software defined networking (SDN). In this case, there is a central server (SDN) in the control plane which has a complete view of the network and on the basis of congestion data, etc. it can control the routing tables of the routers by running a centralized algorithm & loading the routing tables into the routers.



Usually, the control plane is implemented in a separate device called the remote controller. If it is implemented in the routers, it would not be possible to have a complete picture of the network.

Advantages:

1. Via SDN, we can get a complete network picture. and routing can take into account the network congestion, etc.
2. Less dependant on routers — if routers malfunctions etc. it does not impact the network too much.
3. Routing can be done in such a way so as to balance the loads. Can prevent network oscillations like in link state routing.
4. Allows for more complex functionalities in the form of APIs, i.e. make routing/networking "smarter". (PTO) →
5. SDN is open source ⇒ Better algorithms.

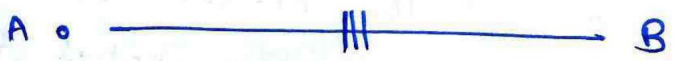
Dis

Question 3 [5+3+2 = 10 marks]

(a) Two nodes A and B are on a 10 Mbps broadcast channel, and the propagation delay between them is 245 bit times. Suppose A and B start sending Ethernet frames at the same time, the frames collide, and then A and B choose different values of K in the CSMA/CD *backoff* algorithm. Assuming no other nodes to be active, when can A and B retransmit the frames? Suppose the frame size is 300 bits and the jam signal is 10 bits. Show all computation steps. [Hint: *In CSMA/CD, a node waits K·512 bit times before sensing the channel again*]

Sol. Suppose both A, B start broadcast at $t = 0$.

Then



Collision

Packet/frame size $= f$

$r_1 = 10$ Mbps.

$p_1 = 245$ bit time

Jam size $= j$

Time till collision:

$$T_{coll} = \frac{f}{r_1} + \frac{p_1}{2}$$

$\frac{p_1}{2}$: Half of propogation time.

~~Final when~~

Time to send JAM signal:

$$T_{jam} = \frac{j}{r_1} + p_1$$

Backoff time.

Suppose the chosen values of K are K_1, K_2.

whichever of K_1, K_2 is minimum., say K_1. Then,

A can start retransmitting after a time,

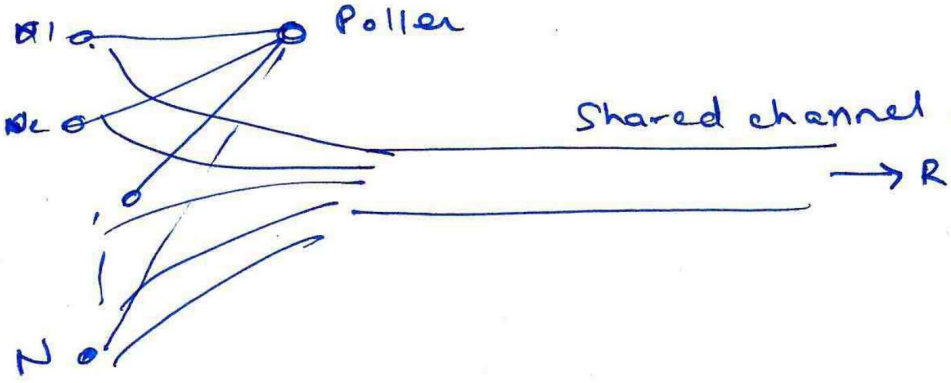
$$T_{coll} + T_{jam} + K_1 \cdot 512$$

B can start retransmitting after time,

$$T_{coll} + T_{jam} + K_1 \cdot 512 + \left(\frac{f}{r_1} + p_1\right)$$

if $< K_2 \cdot 512$

(b) Consider a broadcast channel with N nodes and a transmission rate of R bps which uses polling for medium access. Suppose the amount of time from when a node completes transmission until the subsequent node is permitted to transmit (the polling delay) is d. Further assume that within a polling round, a given node is allowed to transmit at most M bits. What would be the maximum throughput of this broadcast channel?



Suppose the i^{th} node is polled and it is ready to send. Then,

Time to send M bits = M/R.

Polling delay = d.

$\therefore$ Throughput = $\frac{\text{Actual sent data}}{\text{Potentially could have been sent}}$

Max possible data sent in $\frac{M}{R} + d$ time

$$= \frac{M}{R \cdot \left(\frac{M}{R} + d\right)}$$

$$\text{max throughput} = \frac{M}{M + dR} = \boxed{\frac{1}{1 + \frac{dR}{M}}}$$

(c) Why is an ARP query sent within a broadcast frame? Why is an ARP response sent within a frame with a specific destination MAC address?

Sol. ① An ARP query is sent as a broadcast because although we know the IP address of the receiver, we do not know their MAC address, and receiver could be any node connected to the shared channel. So, ARP broadcast is needed so that All nodes on the channel get the request & the one whose IP matches the query can respond.

② ARP broadcast contains the MAC address of the sender. So the receiver of the ARP broadcast already knows the MAC address of the sender & therefore can directly set the destination to be the specific MAC address of the broadcaster.

broadcastes.

Question 4 [2+3+3+3 = 11 marks]

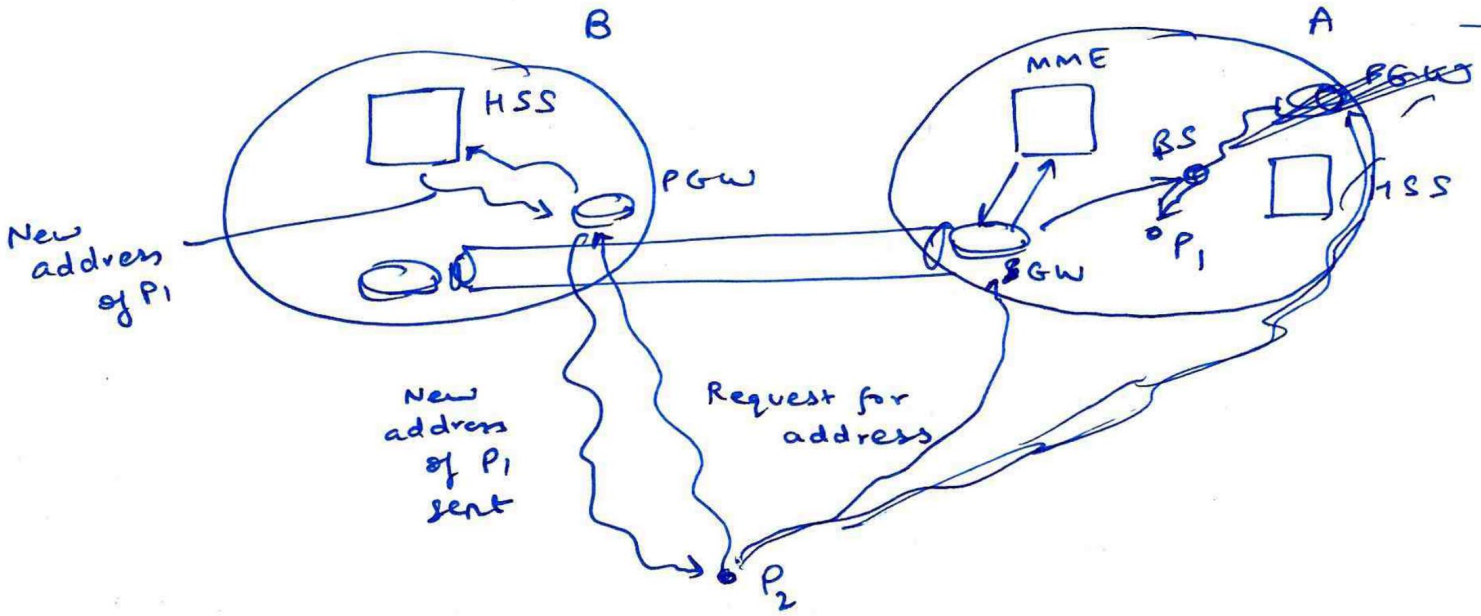
(a) Suppose the IEEE 802.11 RTS and CTS frames were as long as the standard DATA and ACK frames. Would there be any advantage to using the CTS and RTS frames? Why or why not?

Ans. No, there would be no advantage of this.
This is because the main advantage of small RTS / CTS packets is that in a scenario like hidden terminal, the sender gets to know quite quickly if the RTS packets have collided due to them being short (small in size).

If the RTS size ~ Message (DATA) size : The sender may get to know after a long delay that RTS packet has collided. Then they again have to wait for an exponential time (backoff).

↳ This would increase network delays a lot.
It would have been the same if the sender would have sent packet directly rather than RTS. We would have saved the time of sending RTS packet & its collisions. So, no advantage of keeping RTS/CTS. if they are large.

(b) You travel to an area with coverage from a cellular operator A, but your sim is registered with operator B. If one of your contacts sends you a sms while you are traveling, how would the message be delivered to your phone? Assume Direct Routing is used.



Figure

(Explanation →)

Suppose I am P_1 & person sending SMS is P_2.

The message would be delivered as follows:

1. The MME of network operator A would have informed HSS of op. B of my new location. ~~BS~~.
   (due to tie-up between op. A & op B)

2. P_2 would ask my HSS (operator B's HSS) of my new address.

3. Operator B's HSS would inform P_2 of my new address (IP) which is ~~present~~ present in the network area of A.

4. Since direct routing is used, P_2 would now send the SMS (destined for my IMSI) and address ~~as the new base station (BS)~~ as the new network address (of the gateway router of A's network)

5. The PDN Gateway Router (PGW) would receive the request & through the MME, would forward/route it to the base station P_1 is connected to.

   which stores the BS I am connected to.

6. Finally the BS sends the message to P_1 via wireless downstream transmission.

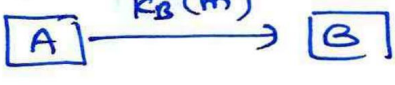
(c) How is Public Key Cryptography used for both confidentiality and authentication? Explain using an example.

Ans. Confidentiality:

Suppose I want to send a confidential message m. to a person B.

Person B sends me their public key (which is available to everyone).

Then, I encrypt m using their public key, i.e. $K_B^+(m)$ & send this to B.



K_B^+ → Public
K_B^- → Private

Only B can decrypt this message using their private key by applying it to the recvd. message, i.e.

$$K_B^-(K_B^+(m)) = m$$

Since the private key is very hard to find given the public key, public key cryptography is secure & can be used for confidentiality.

Authentication.

For authenticating if a person is really who they claim to be, we centrally register the public key with an authority. The authority signs a public key using their own private key and makes their public key available. This signed key is a certificate. So, when B shares their public key, they share this certificate instead, which A can decrypt using the publically available authority key.

Using this certificate, they can know exactly who the key belongs to and therefore can be used for authentication.

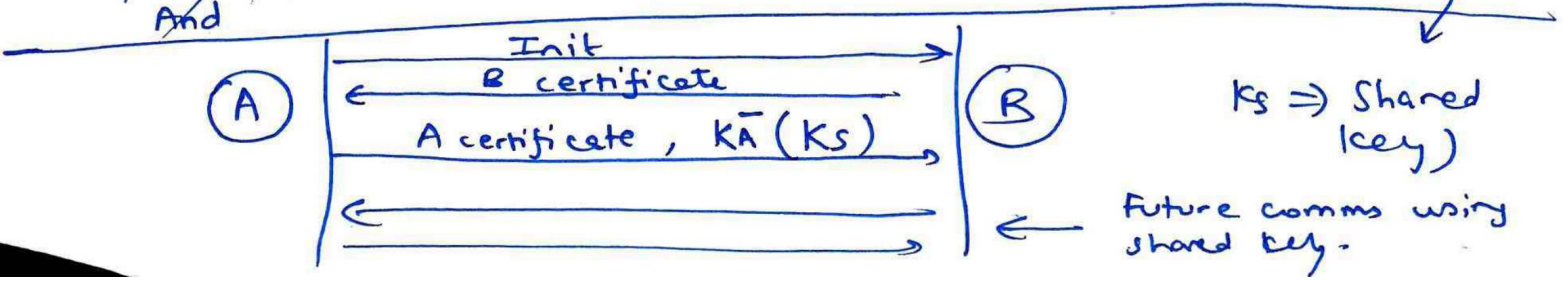
Example: First, A & B exchange the certificates. Along with the certificate, A also sends a key encrypted using B's public key ⇒ This will serve as a shared key in future. Now shared key ensures confidentiality while the certificate exchange ensured authentication.

We can give the example as follows:

1. Suppose A wants to send message m. Then, A can send their certificate and ask B for their certificate. B first checks if A's certificate is valid. Then B sends their own certificate which A can verify. Authentication complete.

2. Now, A can simply encrypt m using B's public key (from the decrypted certificate) & send $K_B^+(m)$ to B.

And,



(d) What is man-in-the-middle attack? How can one prevent it? Explain your answer with an example.

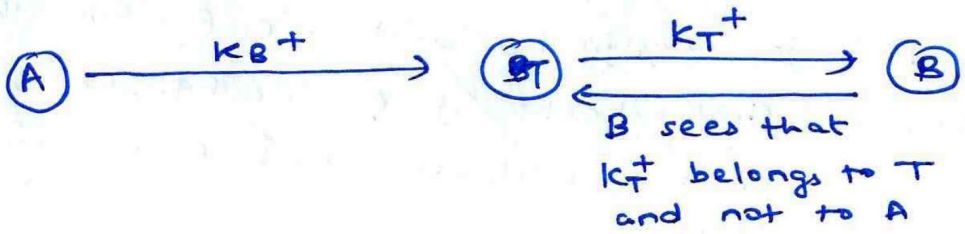
Ans. Man in the middle attack is when an intruder is able to join in a conversation and pretends to be one of the

parties communicating, eg. T pretends to be B for A, and A for B.

So, T can send messages to B using T's own keys (K_T^+ and K_T^-) rather than B. A has no way of knowing if A is communicating with B or T!

We can prevent MiM attacks by certification of the public keys by a central authority, which ensures that each key set is associated with an identity. This is achieved by digitally signing the public key of a user with CA's own pvt. key. To verify, one can simply decrypt using CA's own public key.

In the above example,



When B wants to send A a message m, B first asks for T's public key. Now, T sends its certificate for K_T^+, but now B knows K_T^+ does not belong to A and can terminate the transmission.