**Vehicular Ad-Hoc Networks(VANETs)-CSL 7310**

**Quiz-1** Name: Roll:

Q.1 Which of the following does not constitute a key difference between VANET and MANET? Understanding these differences is crucial for designing and optimizing network protocols. Each type of network has unique characteristics that affect its performance and applications.

a. The high relative speed of mobile node
b. Limited Redundancy
**c. Self-Organizing**
d. Rapid topology changes

**Answer: c. Self-Organizing**

Both VANETs and MANETs are self-organizing networks, so this characteristic does not differentiate them. The other options, including the high relative speed of mobile nodes, limited redundancy, and rapid topology changes, highlight distinctions between the two types of networks.

Q.2 When evaluating VANET systems, it's important to identify their core needs. Which of the following is a key requirement of VANET? Addressing this requirement is essential for ensuring the effective operation of the network. Understanding these requirements helps in optimizing VANET performance and functionality.

a. Mobility
b. Scalability
c. Fairness
**d. All of the above**

**Answer: d. All of the above**

Q.3 What is Routing in VANET?

I. Convention, or standard, controls how nodes decide how to route packets between computing devices.
II. Packet communication between nodes either directly or through intermediate nodes without fixed infrastructure.

a. Only I
b. Only II
**c. Both I and II**
d. Neither I nor II

**Answer: c. Both I and II**

Q.4 To grasp the unique features of VANET, it's important to identify their specific attributes. Which of the following is a characteristic of VANET? Recognizing these characteristics helps us understand how VANET operates and interacts with its environment. Each feature is crucial in defining the network's functionality and performance.

a. Static Topology
b. Wired communication
c. Fixed infrastructure
**d. Mobility Modeling and Prediction**

**Answer: d. Mobility Modeling and Prediction**

Q.5. +2

Q.6 Select the correct option for VANET characteristics

I. Topology: Variable, Nodes join and leave the network very frequently
II. Connection life: short, depending on the road infrastructure condition
III. Connectivity: Permanent, end to end connectivity assured
IV. RSU provides connectivity between two vehicle nodes.

   a. All the options are correct
   b. Only I, II and III
   **c. Only I, II and IV**
   d. Only I, II

**Answer c. Only I, II, and IV**

Q.7 To fully appreciate the functionality of VANET, it's useful to explore its specific applications. Which of the following represents a driver-oriented application of VANET? Understanding these applications reveals how VANET enhances driving experiences and improves road safety. Each application plays a significant role in providing real-time assistance and information to drivers.

a. Incident management and collision avoidance
b. Tourist information
c. Packet route selection
**d. Road traffic and safety information**

**Answer: d. Road traffic and safety information**

Q.8. +2

Q.9 Which of the following is not a communication technology used in VANET

a. Dedicated Short-Range Communication
b. Wireless Access to Vehicular Environment
c. IEEE 802.11p
**d. None of the above**

**Answer: d. None of the above**

Q.10 How is VANET utilized when an accident occurs at a road junction, and information is broadcast to nearby vehicles?

a. VANET updates the vehicle's navigation system with alternative routes.
b. VANET sends traffic violation alerts to nearby drivers.
**c. VANET broadcasts information about the accident to nearby vehicles, helping to alert drivers to potential hazards and improve road safety quickly.**
d. VANET adjusts the traffic lights at the junction to manage vehicle flow.

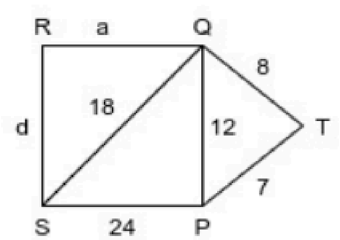
**Answer: c. VANET broadcasts information about the accident to nearby vehicles, helping to alert drivers to potential hazards and improve road safety quickly.**

# Vehicular Ad-Hoc Networks(VANETs)-CSL 7310

**Quiz-2** Name: Roll:

**Marks: 15** **Time-: 45 Min.Total**

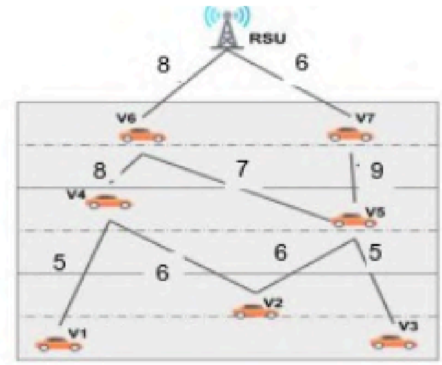
**Q. 1.** **[2]**




Using the Dijkstra algorithm, the lowest cost path from P to S is PQRS and second lowest cost path from P to S is PS. Find the possible values of (a + d). What is the minimum cost required to travel from P to S for the maximum value of (a+d)?

**a+d<=12,24**

**Q. 2** **[1]**




Using the Dijkstra algorithm, find which vehicle (V1,V2,V3) is nearest to the RSU? Also select the path from RSU to the nearest vehicle.
Note: All weighted links are continuous.

**A)** V1, RSU - V6 - V4 - V1

**B)** V2, RSU - V6 - V4 - V2

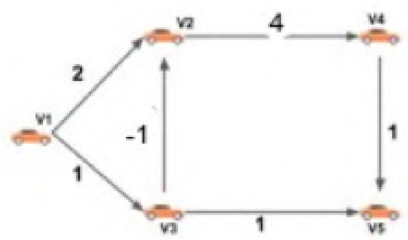
**C)** V2, RSU - V6 - V5 - V2

**D)** V3, RSU - V6 - V5 - V3

**E)** V3, RSU - V7 - V5 - V3

Last two options are correct

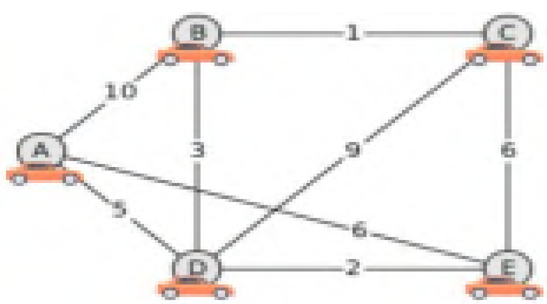
**Q.3** **[1]**




Find the minimum cost from V1 to V4, using the Bellman-ford algorithm? Note: All given lines connecting the units are connected.

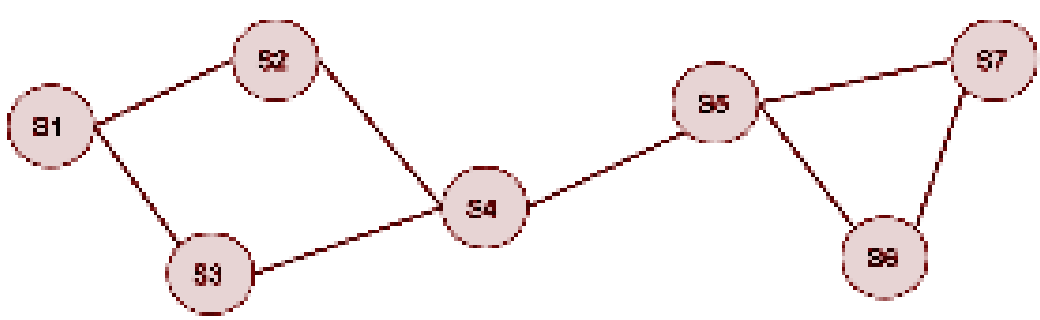
The shortest path between V1 and V4 is V1 - V3 - V2 - V4

**Q.4** Find the shortest path from A to C using the Bellman-ford algorithm. **[1]**

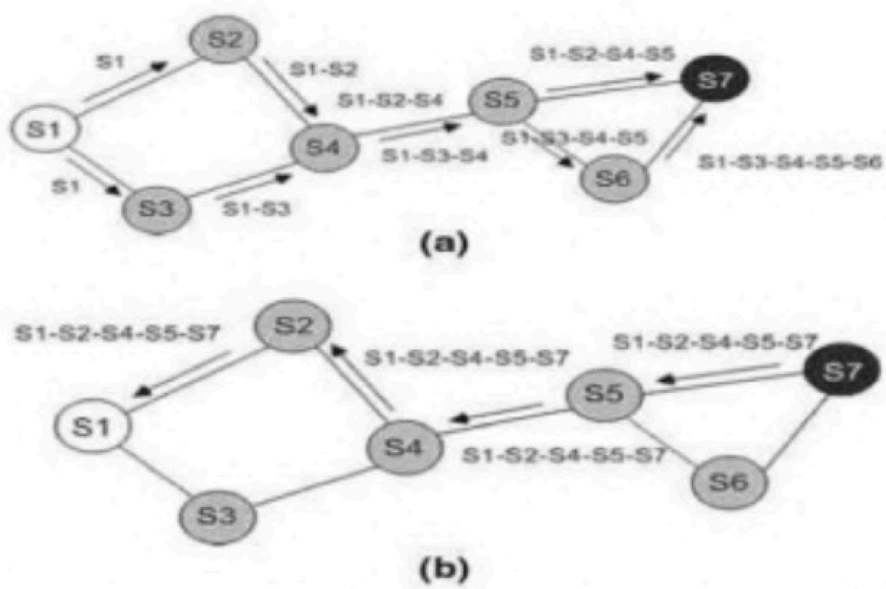



Shortest paths starting from A is A—D—B—C, distance 9

**Q.5** Find the shortest route from S1 to S7 using the Dynamic source routing (DSR) algorithm. **[5]**

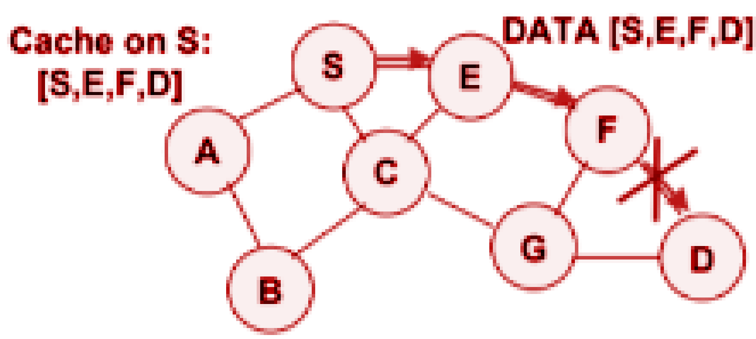


A.5 S1 - S2 - S4 - S5 - S7 OR S1 - S3 - S4 - S5 - S7
DSR route



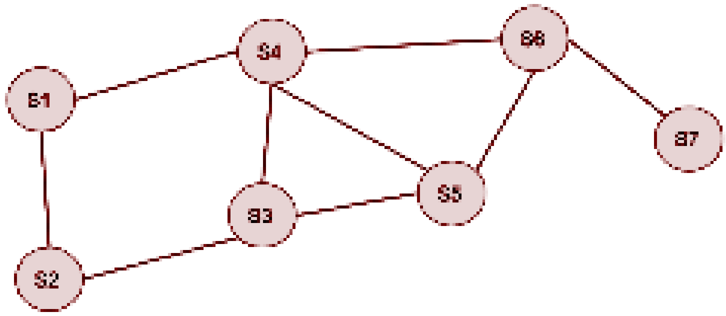

(a) Route Discovery (b) Using route record to send the route reply

**Q.6** In the following figure, a path is established from S to D. During data transmission, a link between nodes F and D is broken. How does the DSR protocol handle this problem? **[2]**




when the link between nodes F and D is broken, the DSR protocol handles the problem by generating and propagating a Route Error (RERR) message, updating route caches to invalidate the broken path, and potentially initiating a new route discovery to establish an alternative path from S to D.

**Q. 7** Find the route from S1 to S7 using the AODV algorithm. **[1]**




S1-S4-S6-S7

**Q.8** The handling of congestion is better in AODV than in DSR. Justify your answer. **[2]**

Certainly! Here are the key points summarized:

1. Routing Mechanism:
   - AODV: Uses routing tables with next-hop information, allowing quick route changes during congestion.
   - DSR: Uses source routing, where the full route is included in each packet, leading to larger overhead.

2. Route Adaptability:
   - AODV: Can dynamically discover and switch to alternate routes with minimal overhead.
   - DSR: Relies on cached routes or new discovery, but packet overhead can slow down the process in congested networks.

3. Control Overhead:
   - AODV: Lower control overhead, as it only updates routes when necessary.
   - DSR: Higher overhead due to carrying entire routes in each packet.

4. Scalability:
   - AODV: Scales better in larger, congested networks by efficiently managing routing tables.
   - DSR: Less efficient in large or congested networks due to increased packet size and processing.

5. Congestion Handling:
   - AODV: More effective at avoiding and managing congestion through quick route adjustments.
   - DSR: Slower and less efficient in handling congestion due to its routing method.

Overall, AODV is better at handling congestion compared to DSR due to its more efficient routing strategy and lower overhead.

[redacted]

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

**Indian Institute of Technology Jodhpur**

Vehicular Ad-Hoc Networks (CSL7310)

Instructor: Dr. Debasis Das

Quiz 3: VANET Security

19th October 2024

Time: 30 mins.

Maximum Marks: 20

Name and Roll no.: ______

- Attempt all the questions and solve them in the given spaces, no extra sheet will be given
- Write properly to justify your answer, multiple answers will not be considered
- Caught in any illicit activity will result in ZERO marks
- It is a closed book exam and mobile phones are not allowed, not even for calculations

1. Using the Playfair matrix, decrypt "UZTBDLGZPN".

Go Above

| | | | | |
|---|---|---|---|---|
| M | F | H | I/J | K |
| U | N | O | P | Q |
| Z | V | W | X | Y |
| E | L | A | R | G |
| D | S | T | B | C |

Go Left

Exchange

Exchange

Go Left

Explanation.

Figure 1: Figure for Q1

**Solution:** UZ TB DL GZ PN

MU ST SE EY OU

After Decryption the plaintext is : MUST SEE YOU — Ans

2. Find integers $x$ such that, $7x \equiv 6 (mod\ 5)$ and $9x \equiv 8 (mod\ 7)$.

**Solution:** $a.b \equiv 1 (\mod n)$ — Explanation

$7 \times 3 = 21$ then $21 \bmod 5 = 1 \Rightarrow 3$ — Ans

$9 \times 4 = 36$ then $36 \bmod 7 = 1 \Rightarrow 4$ — Ans

3. Bob wants to digitally sign a very small message using his RSA private key. His public key parameters are n=33 and e=3. Given his private exponent d=7, if the hash of his message is h=2, what is the digital signature s of the hash?

Explanation

**Solution:** $S \equiv h^d \bmod n$ ; $h = 2, d = 7, n = 33$ ; $S = 2^7 \bmod 33$

$S = 128 \bmod 33 = 29$ — Ans

$33 \overline{)128} 3$, $99$, $29$

4. Assume that source S and destination D are connected through n intermediate routers labeled R. Determine how often each packet has to visit the network layer and the data link layer during transmission from S to D.

**Solution:** S — $R_1$ — $R_2$ ..... $R_n$ — D

Explanation

For N/W Layer : 2 (for Source & Destination) + n (for n routers)

For Data Layer : 2 (for Source & Destination) + 2× n (for n routers)



So, N/W Layer : 2+n packets.

Data Layer : 2+(2×n) packets — Ans

THE OTHERSIDE OF SILENCE

The Decrypted Message is: THE OTHER SIDE OF SILENCE



5. Given Cipher text "YMJTYMJWXNIJTKXNQJSHJ", the message is encrypted by Caesar cipher and k=5. Try to decrypt the message. (Start A = 0)

**Solution:**

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

C = Y M J T Y M J W X N I J T K X N Q J S H J

− K: 24 12 9 19 24 12 9 22 23 13 8 9 19 10 23 13 16 9 18 7 9

mod 26: −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5 −5

for P = 19 7 4 14 19 7 4 17 18 8 3 4 14 5 18 8 11 4 13 2 4

Explanation or, 5 left shifts. (visible)

6. Using Vigenere cipher, encrypt the word "EXAM" using the Key "DONE" (Start $A = 0$).

**Solution:** M = E X A M
4 23 0 12

K = D O N E
3 14 13 4

7 37 13 16

So, 7 11 13 16 → C = HLNQ —— Ans

[(M + K) mod 26 = C]

37 mod 26 = 11

Explanation

7. State which is active or passive attack: Denial of Service, Traffic analysis, The release of message content, and Modification of messages.

**Solution:** Active → Denial of Service, Modification of message

Passive → Traffic analysis, The release of message content

can modify message

observes mostly

8. Describe any four properties of a Hash function.

**Solution:** Pre-Image (one-way) Resistance, Second Pre-image Resistance, Collision Resistance, Efficiency, Fixed Output size; Deterministic; Fast Computation; Avalanche Effect; and their Definition (any four) → Correct one

9. $17 + 27$ in $Z_{14}$ is? And, the Multiplicative inverse of 3 in $Z_{10}$ is?

**Solution:** 17+27 in $Z_{14}$ is 44 mod 14 = 2 ∴ Ans is 2 —— Ans

multiplicative inverse of 3 in $Z_{10}$ is $3 \times x \equiv 1 \bmod 10 \rightarrow 3 \times 7 \equiv 1 \bmod 10$. ∴ Ans is 7 —— Ans

10. With the permutation cipher, obtain the ciphertext from "YTHESEASHORE".

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{pmatrix}$$

Figure 2: Figure for Q10

**Solution:** $\pi \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{pmatrix}$

Exchange in Explanation

Y T H E S E     A S H O R E
1 2 3 4 5 6     1 2 3 4 5 6

H S Y E E T     H R A E O S
3 5 1 6 4 2     3 5 1 6 4 2

End of the exam

∴ The cipher text is: HSYEETHRAEOS

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

**Indian Institute of Technology Jodhpur**

Vehicular Ad-Hoc Networks (CSL7310)

Instructor: Dr. Debasis Das

Quiz 4: VANET Miscellaneous

Nov 16, 2024

Time: 30 mins. Maximum Marks: 20

Name and Roll no.: ____________________

- Attempt all the questions and solve them in the given spaces; no extra sheet will be given
- Write properly to **justify your answer**; multiple answers will not be considered
- Caught in any illicit activity will result in ZERO marks
- It is a closed book exam and mobile phones are not allowed, not even for calculations

1. You want to design a decision system for a smart city solution in which the vehicle's data will be used to predict its running condition, such as remaining fuel/charge, emissions, engine load etc. The users do not wish to share the data with any stakeholder. Name the specific paradigm which is more suitable for this. [Hint: Training without sharing data] **[1.5]**

   **Solution:** Federated Learning - the data produced by multiple nodes or clients is not shared with the server. Server initiates a model instance and local trainings are performed at each node.

2. In a data-driven anomaly detection system, which is a common way to represent the anomalous points? **[1]**

   A. Normal instances with a class label

   B. Outliers

   C. Unseen instances

   D. Centroid of all instances

3. In autonomous driving assistance systems (ADAS), which is the most cost-effective way to detect objects and calculate their distance from them? Cost includes deployment cost, hardware cost, computation cost, and consumed time. Write proper justification. **[1.5]**

   A. 3D LiDAR sensor and point cloud estimation

   B. Simple Ultrasound sensor

   C. Monocular depth estimation using an ordinary camera

   D. Heterogeneous sensor fusion (camera, LiDAR etc. working together)

   **Solution:** The main tradeoff is between (B) and (C). A simple ultrasound sensor will be substandard in performance as it cannot detect multiple objects and their attributes at a time. (C) is a suitable option as a monocular depth estimation algorithm can estimate different objects, their attributes and distance from the car.

4. Which technique is primarily used in the MAC layer of VANETs to prioritize safety messages over regular data? **[1]**

   A. TDMA (Time Division Multiple Access)

B. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

C. CDMA (Code Division Multiple Access)

D. FDMA (Frequency Division Multiple Access)

5. What is the typical maximum transmission range of a vehicle in a VANET using IEEE 802.11p on the 5.9 GHz band? **[1]**

   A. 50 meters

   B. 500 meters

   C. 100 meters

   D. 1 km

6. What is the maximum data rate supported by IEEE 802.11p in the 5.9 GHz band for vehicular communication? [ WAVE standard ] **[1]**

   A. 27 Mbps

   B. 54 Mbps

   C. 100 Mbps

   D. 1 Gbps

7. Which of the following modulation schemes is used in the Physical layer of IEEE 802.11p for VANETs? **[1]**

   A. BPSK (Binary Phase Shift Keying)

   B. QPSK (Quadrature Phase Shift Keying)

   C. 64-QAM (64 Quadrature Amplitude Modulation)

   D. OFDM (Orthogonal Frequency Division Multiplexing)

8. What are any two challenges faced by the Physical layer in VANETs due to the urban environment? **[2]**

   **Solution:** - Signal Propagation Issues (Multipath Fading, Shadowing, Path Loss); - High Node Mobility; - Co-channel Interference; - Limited Line-of-Sight (LOS); - Scalability; - High Power Consumption, etc.

9. In a VANET scenario, two vehicles are communicating over a wireless channel. The maximum transmission range of each vehicle is 100 meters. If the vehicle speed is 20 m/s, calculate the time it takes for the two vehicles to move out of range of each other. [Formula: Time to move out of range = ( Range / Relative Speed Range ) ] **[2]**
   +2

10. In a VANET using IEEE 802.11p, the data rate for a 64-QAM (Quadrature Amplitude Modulation) with 20 MHz bandwidth is given as 54 Mbps. Calculate the symbol rate (baud rate) for this communication. [Formula: Symbol rate = ( Data Rate / Bits per symbol ) ] **[2]**

**Solution:** Bits per symbol for 64-QAM = $2^6$ *bits per symbol* = 6 *bits per symbol*
Data rate = 54 *Mbps* = 54 *X* $10^6$ *bits per second*
Symbol rate (baud rate) = Data Rate / Bits per symbol
= 54 *X* $10^6$ *bits per second* / 6 *bits per symbol* = 9 *X* $10^6$ *symbols per second*
= 9 *Msymbols/sec* = 9 *megabaud* **(Ans.)**

11. In the Random Waypoint Mobility Model, what is the significance of the "pause time"? **[1]**
    A. It determines the vehicle's speed when moving
    B. It specifies how long a vehicle will stay at its destination before starting again
    C. It defines the vehicle's maximum travel distance
    D. It models the road network layout
12. Which of the following mobility models is specifically designed to simulate vehicular networks in cities with grid-like street patterns? **[1]**
    A. Random Waypoint Model
    B. Gauss-Markov Model
    C. Manhattan Mobility Model
    D. Freeway Mobility Model
13. What is a major limitation of the Random Walk Mobility Model in VANET simulations? **[1]**
    A. It doesn't account for road networks or traffic regulations
    B. It results in predictable vehicle paths
    C. It requires high computational resources
    D. It only works for rural environments
14. What is the key characteristic of the Gauss-Markov Mobility Model in VANETs? **[1]**
    A. It models vehicle movement as completely random
    B. It uses a random walk process to simulate vehicle behaviour
    C. It introduces correlation in vehicle velocity to simulate more realistic movement
    D. It assumes vehicles follow fixed paths along roads
15. A VANET system uses ECDSA (Elliptic Curve Digital Signature Algorithm) to sign messages. The message size is 512 bits, and the signature size is 256 bits. The transmission rate is 2 Mbps. Calculate the total size of each signed message and determine the time needed to transmit one signed message. [Formula: Transmission Time = Total Message size / Rate of transmission] **[2]**

**Solution:** Total message size = Message size + Signature size = 512 + 256 = 768 bits

Transmission rate = 2 Mbps = 2,000,000 bits per second

Transmission time = Total message size / Transmission rate = $768/2,000,000$
= 0.000384 *seconds* = 0.384 *milliseconds*

**Total size of each signed message: 768 bits**
**Transmission time: 0.384 milliseconds**

# Indian Institute of Technology, Jodhpur

## CSL7310:Vehicular Ad Hoc Networks

## Sample Paper, AY 2024-25

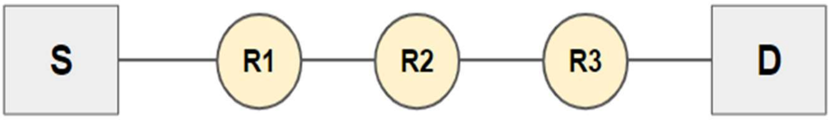
Q.1 If vehicle X is at point P and Vehicle Y is at point Q at timestamp T. Both Vehicles are moving in opposite directions and generate a signal to communicate with each other continuously. The interference generated by the signal is **2**

a. Positive
b. Negative
c. Either Positive or Negative
d. Both Positive and Negative

Q.2 Which of the following is not a characteristic of Vehicular Ad Hoc Network (VANET)? **2**

a. Multi-hop routing
b. Infrastructure-less
c. Long range wireless transmission
d. None of the mentioned

Q.3 Assume that source S and destination D are connected through three intermediate routers labeled R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D. **2**



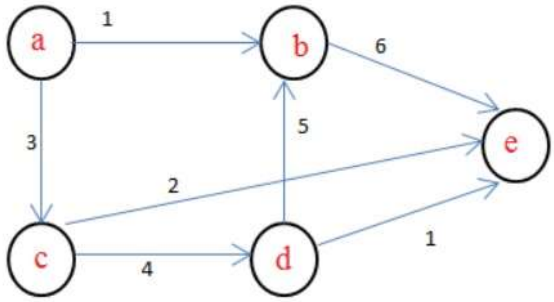

a. Network layer – 5 times and Data link layer – 8 times
b. Network layer – 5 times and Data link layer – 5 times
c. Network layer – 4 times and Data link layer – 7 times
d. Network layer – 5 times and Data link layer – 5 times

Q.4 Select the correct option for VANET characteristics **2**

I. Topology: Variable Nodes join and leave the network very frequently.
II. Connection life: short, depending on the road infrastructure condition.
III. Connectivity: Permanent, end to end connectivity assured
IV. RSU provides connectivity between two vehicle nodes.

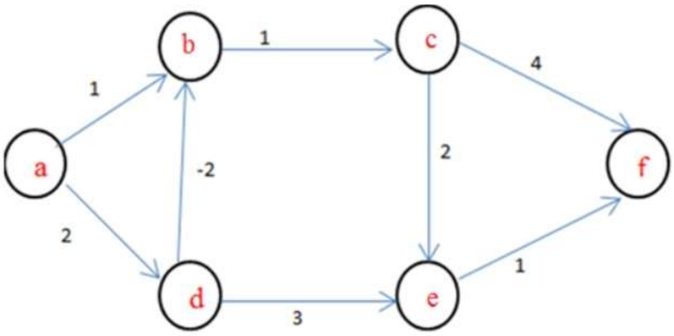
a. All the options are correct
b. Only I, II and III
c. Only I, II and IV
d. Only I, II

Q.5 Determine the shortest path using Dijkstra's algorithm to reach vertex 'e' from 'a' if 'a' is the source vertex. **2**




a. a-c-e
b. a-e-c
c. a-b-e
d. a-c-d-e

Q.6 Identify the path that has the minimum cost using Bellman-ford algorithm to travel from node 'a' to node 'f'. **2**




a. a-b-c-e-f
b. a-d-b-c-e-f
c. a-b-c-f
d. a-d-e-f

Q.7 Write down the important parameters with proper justification that reduce the communication establishment time between Vehicle-to-Vehicle and Vehicle-to-RSU. **6**

Q.8 Suppose we remove smart objects from the Internet of Vehicles. So will both VANET and Internet of Vehicle (IoV) be the same, or will there still be any difference between the VANET and IoV? Explain it with proper justification. **6**

Q.9 Given is an ad-hoc network which has initially the following topology (figure 3): **10**

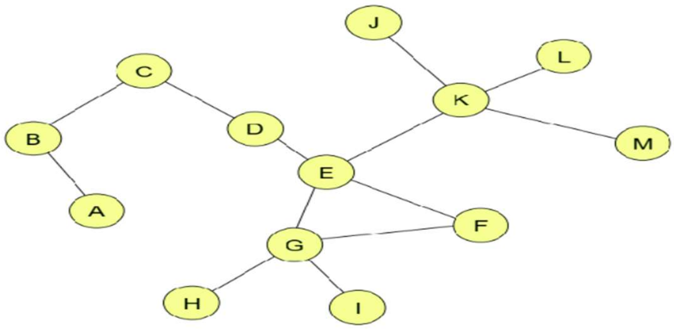



Figure 3: Ad-hoc network

Connected nodes are in transmission range and can forward messages along the edges. For routing, dynamic Source Routing (DSR) should be used. The caches of all nodes are empty. Now, D wants to send some packets to H. Give the sequence of messages exchanged for finding a path (also the “unnecessary” messages). For each message, describe sender, receiver, and the list of used nodes as written in the header by the routing? protocol. Assume that the paths are symmetrical. What happens if the connection between E and G breaks down?

.

Q.10 In the Following figure a path is established from S2 to S7. In the established path shown in figure 4 a link is broken between node S6 and S7. If Dynamic Source Routing (DSR) protocol is used for the transmission. Explain how the DSR protocol handles this issue? Consider S2 as source and S7 as destination. **6**

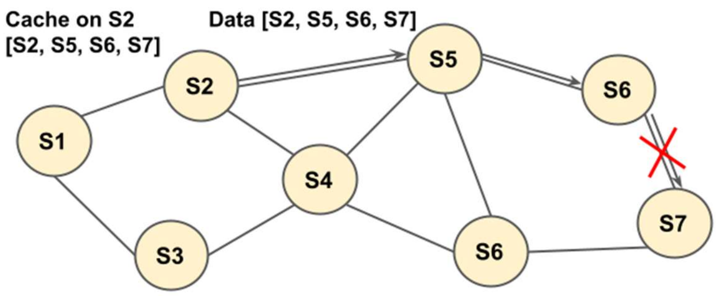



Figure 4: Vehicular Ad Hoc Network using DSR routing algorithm

Indian Institute of Technology Jodhpur
Department of Computer Science and Engineering
Vehicular Ad-Hoc Networks (CSL7310)
Instructor : Dr. Debasis Das
MAJOR EXAM (Fall 2024)

November 23, 2024

SOLUTIONS

SOLUTIONS

Instruction for MCQs/MSQs: Add justification to your correct options, or else that answer will not be considered.

1. Assume that source S and destination D are connected through three intermediate routers labeled R. Determine how often each packet has to visit the network layer and the data link layer during transmission from S to D. **[2]**

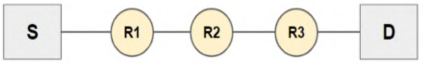



Figure 1: Figure for Q1

   A. Network layer – 5 times and Data link layer – 8 times.
   B. Network layer – 5 times and Data link layer – 5 times.
   C. Network layer – 4 times and Data link layer – 7 times.
   D. Network layer – 5 times and Data link layer – 9 times.

2. Select the correct option for VANET characteristics. **[2]**
   1. **Topology:** Variable Nodes join and leave the network very frequently.
   2. **Connection life:** short, depending on the road infrastructure condition.
   3. **Connectivity:** Permanent, end-to-end connectivity assured.
   4. RSU provides connectivity between two vehicle nodes.

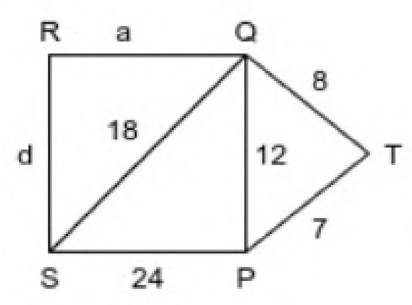
   A. All the options are correct.
   B. Only 1, 2 and 3 are correct.
   C. Only 1, 2 and 4 are correct.
   D. Only 1 and 2 are correct.

3. How does candidate coordination work in Opportunistic Routing? **[2]**
   A. Candidates independently decide whether to forward packets without communication.
   B. Candidates communicate to determine which should forward the packet based on priority.
   C. The source node dictates which candidate forwards the packet.
   D. Candidates randomly choose whether to forward or discard packets.

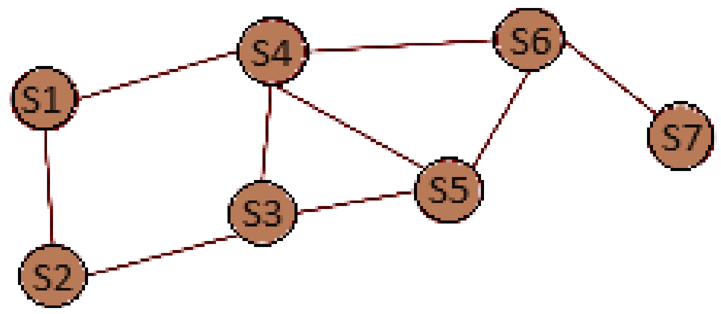
   In Opportunistic Routing (OR), candidate coordination works by having the potential forwarders communicate to decide which candidate will forward the packet based on a predefined priority system. This coordination ensures that only one candidate forwards the packet, preventing duplication of transmissions and improving efficiency. The candidates' priorities are usually determined by factors like distance to the destination or link quality.

4. Using the Dijkstra algorithm, the lowest cost path from P to S in PQRS (Figure 2.(a)) and the second lowest cost path from P to S is PS. Find the possible values of (a+d). What is the minimum cost to travel from P to S for the maximum value of (a+d)? **[2]**
   **Solution :**
   a+d $\leq$ 12,24

5. Find the route from S1 to S7 using the AODV algorithm (Figure 2.(b)). **[2]**




(a) Figure for Q4




(b) Figure for Q5

Figure 2: Figures for Q4 and Q5

   **Solution :**
   S1-S4-S6-S7.

6. Find integers $x$ such that, $7x \equiv 6(mod\ 5)$ and $9x \equiv 8(mod\ 7)$. (Show all the stepwise calculations) **[2]**
   **Solution :**
   $a \cdot b \equiv 1 \pmod{n}$.
   $7\ X\ 3 = 21\ then\ 21\ mod\ 5 = 1$ for $7x \equiv 6(mod\ 5)$ Ans is 3
   $9\ X\ 4 = 36\ then\ 36\ mod\ 7 = 1$ for $9x \equiv 8(mod\ 7)$ Ans is 4

7. Bob wants to digitally sign a very small message using his RSA private key. His public key parameters are n=33 and e=3. Given his private exponent d=7, if the hash of his message is h=2, what is the digital signature s of the hash? **[2]**
   **Solution :**
   $s \equiv h^d \pmod{n}. Given,\ h = 2;\ d = 7;\ n = 33.\ So,\ s == \equiv 2^7 \pmod{33}$
   $s \equiv 128 \pmod{33} = 29$...Ans

8. You want to design a decision system for a smart city solution in which the vehicle's data will be used to predict its running condition, such as remaining fuel/charge, emissions, engine load etc. The users do not wish to share the data with any stakeholder. Name the specific paradigm which is more suitable for this. [Hint: Training without sharing data] **[2]**
   **Solution :**
   Federated Learning - the data produced by multiple nodes or clients is not shared with the server. The server initiates a model instance, and local training is performed at each node.

9. Which technique is primarily used in the MAC layer of VANETs to prioritize safety messages over regular data? **[2]**

A. TDMA (Time Division Multiple Access)

B. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

C. CDMA (Code Division Multiple Access)

D. FDMA (Frequency Division Multiple Access)

10. What is the typical maximum transmission range of a vehicle in a VANET using IEEE 802.11p on the 5.9 GHz band? **[2]**

A. 50 meters

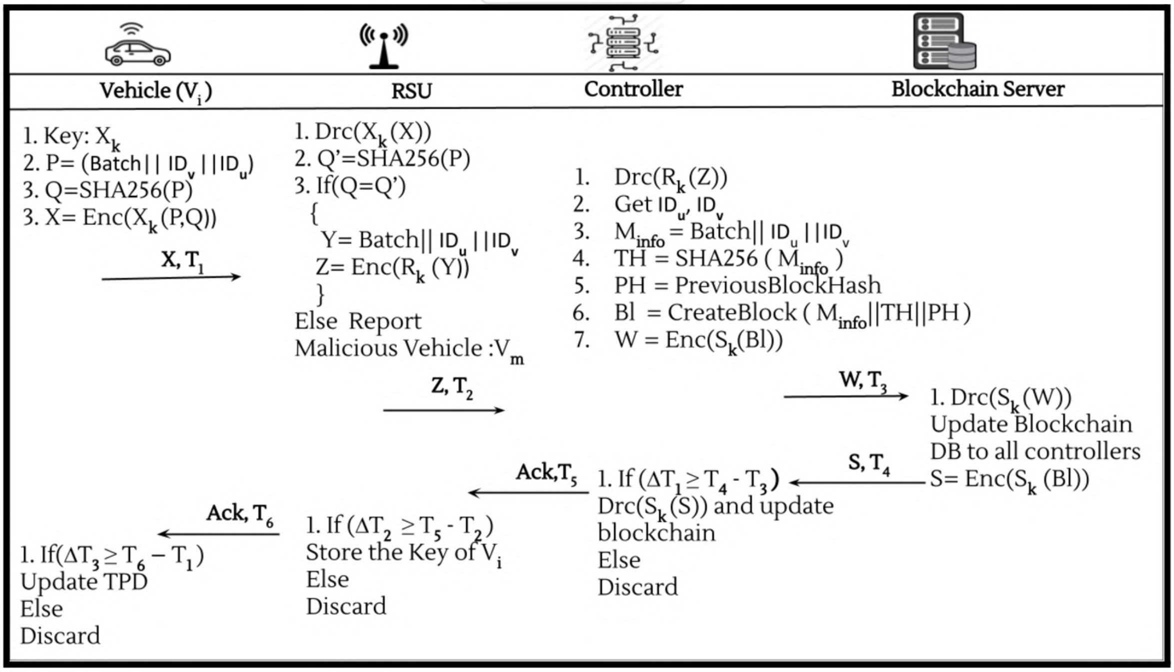
B. 500 meters

C. 100 meters

D. 1 km

11. Figure 3 shows the communication in VANET. Analyze the figure and answer the following. In 3b, Table 1 represents the execution time required to calculate the cryptographic functions and Table 2 represents the priority and size of different types of messages. The channel capacity is 2 Mbps. Note: Except for all these messages, the size required to store a variable is 1 byte. The priority is high to low from top to bottom in the table.

- How much time will it take to propagate all these messages (i.e., from M1 to M4), including all the computation and communication costs ? **[4]**
  **Solution :**
  Number of Concatenation (8),SHA-256 (3), Encryption (4), Decryption (4) required for single message. Time required for concatenation (0.00120), SHA-256 (0.02490), Encryption (6.136), and Decryption (7.336).
  Total computation time required for single message (0.00120 + 0.02490 + 6.13600 + 7.33600 = 13.49810ms).
  Total computation time required for four messages (13.49810 * 4 = 53.9924ms).
  Total communication time= $(35*8*6)(s)/(2*10^6)$ = 0.00084 s =0.84 ms.
  Total time = 53.9924 ms + 0.84 ms = 54.8324 ms.
- If an accident happens on a badly conditioned construction road,
  - How many messages must be communicated, and what time will it take to transmit from vehicle to controller ? **[4]**
    **Solution :**
    Number of Concatenation (4), SHA-256 (2), Encryption (2), and Decryption (1) required for a single message.
    Time required for concatenation (0.00060), SHA-256 (0.01660), Encryption (3.068), and Decryption (1.834).
    The total computation time required for a single message (0.00060 + 0.01660 + 3.068 + 1.834 = 4.91920ms).
    Total computation time required for three/two messages (4.91920 * 3 = 14.75760ms).
    Total communication time= $(30*8*2)(s)/(2*10^6)$ = 0.00024 s =0.24 ms . Total time = 14.75760 ms + 0.24 ms = 14.99760
  - Which type of message will be transmitted first, and why ? **[2]**
    **Solution :**
    Accident M1 due to high priority.




(a) Figure for Q11

**Table1**

| Cryptographic function | ET (in MS) |
|---|---|
| AES encryption ($Enc(S_k(x))$ | 1.534 |
| AES Decryption ($Drc(S_k(x))$ | 1.834 |
| SHA256 | 0.0083 |
| XOR | 0.00012 |
| Concatenation | 0.00015 |

**Table2**

| Types of messages | Size (in bytes) | Priority |
|---|---|---|
| Accident M1 | 2 Byte | 1 |
| Traffic Jam M2 | 5 Byte | 2 |
| Bad Road M3 | 10 Byte | 3 |
| Construction site M4 | 18 Byte | 4 |

Where, ET: Execution Time, MS: milliseconds

(b) Tables for Q11

Figure 3: Diagram for Q11

12. Given is an ad-hoc network that initially has the following topology in Figure 4. Connected nodes are in transmission range and can forward messages along the edges. For routing, dynamic Source Routing (DSR) should be used. The caches of all nodes are empty. Now, D wants to send some packets to H. Give the sequence of messages exchanged for finding a path (also the "unnecessary" messages). For each message, please describe sender, receiver, and the list of used nodes as written in the header by the routing protocol. Assume that the paths are symmetrical. What happens if the connection between E and G breaks down? **[6]**

**Solution :**

The following steps are followed in DSR:

RREQ from source to destination and RREP from destination to sender sends data on the established path. Consider (sender, receiver, list of used nodes) format for each message. The messages are flooded to every neighbor.

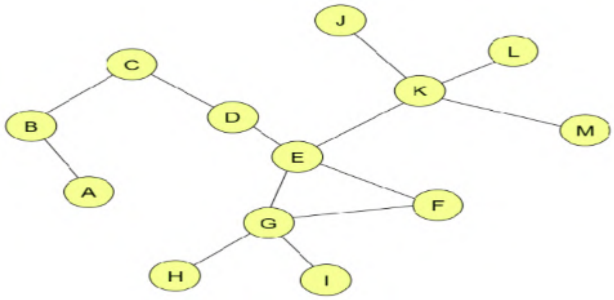



Figure 4: Ad-Hoc Network (For Question 12).

Step 1: RREQ: (D,C,Nil), (D,E,Nil).
Step 2: RREQ: (E,G,E), (E,D,E), (E,F,E), (E,K,E), (C,B,C), (C,D,C).
Step 3: RREQ: (G,H,EG), (G,I,EG), (B,A,CB), (B,C,CB), (D,C,CD), (D,E,CD), (F,E,EF), (F,G,EF).
H receives the first RREQ from D. H sends RREP on path HGED by extracting the headers attached to the received message. D receives RREP with H as its source and starts sending data.
If the link between E and G breaks, a RERR message is sent to the sender, and source D will attempt to reestablish the connection through the three steps outlined above.

13. A government agency is implementing a digital signature system using the RSA algorithm to secure communications. Each document must be signed using RSA, with a hash function employed to secure the integrity of the message before it is signed. The digital signature system utilizes a 2048-bit RSA key and SHA-256 for hashing. During an audit, it was discovered that due to a software flaw, the entropy used for generating the random keys in the RSA algorithm was severely compromised, effectively reducing the strength of the keys. Assume the effective strength of the keys was reduced to that of a 256-bit RSA key. The agency needs to assess the potential impact and require remedial actions based on this. (Entropy: a measure of the randomness or unpredictability of data)
**Details**

- Number of documents signed per day: 1000 documents.
- Days affected by the compromised keys: 100 days.
- The average size of each document: 2 MB.
- Hash Function Time for SHA-256 per MB: 0.05 seconds.
- RSA Signing Time for 2048-bit key per operation: 0.1 seconds.
- RSA Signing Time for 256-bit key per operation due to software flaw: 0.02 seconds.

**Problems**

- Calculate the total data processed under the compromised system. **[3]**
  **Solution :**
  Total Data Processed: Each document is 2 MB, and 1000 documents are processed daily for 100 days. Total Data = 1000 documents/day * 2 MB/document * 100 days = 200,000 MB = 200 GB

- Determine the time spent on hashing and signing documents with compromised keys. **[3]**

  **Solution :**

  Hashing Time: Each MB takes 0.05 seconds to hash, so each document takes 2 MB * 0.05s/MB = 0.1s. Therefore, for all documents: Total Hashing Time = 1000 documents/day * 0.1s/document * 100 days = 10,000 seconds.

  Signing Time with Compromised Keys: Each signing operation takes 0.02 seconds with the compromised 256-bit key, so, Total Signing Time = 1000 documents/day * 0.02 s/document * 100 days = 2,000 seconds

  Total Time = Total Hashing Time + Total Signing Time = 10,000 s+ 2,000 s= 12,000 s.

- Evaluate the security implications if an adversary can break the encryption of a 256-bit RSA key, which is significantly easier than breaking a 2048-bit RSA key. **[2]**

  **Solution :**

  Security Implications: Breaking a 256-bit RSA key is computationally feasible with modern technology, unlike a 2048-bit RSA key, which is considered secure against all feasible attack methods. The reduction in key strength means all documents signed during the affected period are vulnerable to forgery and decryption by adversaries, potentially exposing sensitive government communications to unauthorized access and manipulation.

14. Suppose a group of six vehicles (A, B, C, D, E, F) are deployed in a region with varying distances between them. The vehicles have communication devices to exchange routing information and dynamically update their routing tables using the Bellman-Ford algorithm. The initial distances (costs) between the vehicles are represented as follows (a negative cost represents a route with a beneficial aspect, such as a tailwind): A to B: 4 km, A to C: -2 km, B to C: 3 km, B to D: 2 km, C to B: 1 km, C to E: 2 km, D to E: -1 km, D to F: -3 km, E to D: 3 km, and E to F: 2 km. Assume all pairs of vehicles not directly connected have an initial infinity distance. Determine the shortest paths from vehicle A to all other vehicles in the network using the Bellman-Ford algorithm after three iterations. **[6]**

    **Solution :**

    Each vehicle initializes its distance value. For vehicle A, the distance to itself is 0, and the distance to all other vehicles is infinity, except where direct links exist.

    **Initial distances:**

    - A: [A: 0, B: 4, C: -2, D: $\infty$, E: $\infty$, F: $\infty$]
    - B, C, D, E, F initialize similarly based on direct links.

    **Iteration 1:** Update each vehicle's distance based on the Bellman-Ford relaxation process. Updated distances after Iteration 1:

    - A: [A: 0, B: -1, C: -2, D:3, E:0, F:2]
    - Adjustments reflect other vehicles.

    **Iteration 2 :** Updated distances after Iteration 2:
    A: [A: 0, B:-1, C: -2, D: 1, E: 0, F: -2]

    **Iteration 3 :** Refine distances to D and F using paths through E and others. Final distances after Iteration 3:
    A: [A: 0, B:-1, C: -2, D: 1, E: 0, F: -2]

    After three iterations of the Bellman-Ford algorithm, the shortest paths from vehicle A to the other vehicles in the VANET are as follows :

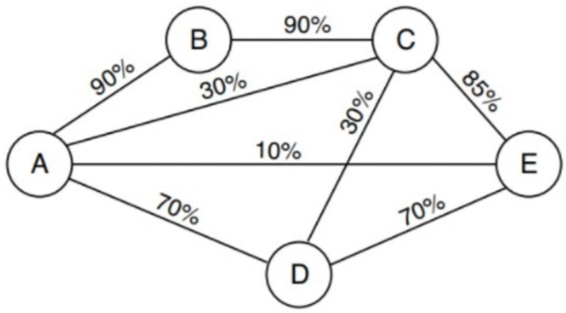



Figure 5: Graph representing the VANET network, where A, B, C, D, and E are the nodes. The value on the link represents the link probability.

- To B:-1km
- To C: -2 km
- To D: 1 km
- To E: 0 km
- To F: -2 km

This scenario highlights how the Bellman-Ford algorithm effectively handles dynamic changes and even negative weights in routing for VANETs.

15. Calculate the Expected Transmission Count (ETX) of the network shown in Figure 5 using opportunistic routing. In Figure 5, node B is the source, and D is the destination node. The Value on the link represents the delivery ratios of the link, i.e., the success probability of a single transmission over the link. **[5] Solution :**
To calculate the Expected Transmission Count (ETX) using opportunistic routing for the VANET network where B is the source and D is the destination, we need to determine the most efficient use of paths and the combination of transmissions required for successful packet delivery. Here are the steps involved:
Identifying Paths from B to D: Two-hop Path: B $\rightarrow$ A $\rightarrow$ D (90% from B to A, and 70% from A to D). Three-hop Path via E: B $\rightarrow$ C $\rightarrow$ E $\rightarrow$ D (90% from B to C, 85% from C to E, and 70% from E to D).
Calculating Success Probabilities for Each Path:
B $\rightarrow$ A $\rightarrow$ D: $0.90 \times 0.70 = 0.63$ and B $\rightarrow$ C $\rightarrow$ E $\rightarrow$ D: $0.90 \times 0.85 \times 0.70 = 0.5355$.
Calculating ETX for Each Path: ETX is calculated as the reciprocal of the success probability of a path. B $\rightarrow$ A $\rightarrow$ D: $ETX = \frac{1}{0.63} \approx 1.59$. B $\rightarrow$ A $\rightarrow$ E $\rightarrow$ D: $ETX = \frac{1}{0.5355} \approx 1.87$
Applying Opportunistic Routing: Opportunistic routing leverages multiple paths to minimize the ETX. This approach takes advantage of the best available route or a combination of routes to lower the overall transmission count. The correct path is 1.59.

16. Assume that you have developed a decision system $M$ for vehicle's predictive maintenance that is capable of telling if a vehicle needs maintenance ($y = 1$) or not ($y = 0$) based on the current conditions of the vehicle given as $x$. A valid counterfactual of a data point $x$ is defined as a data point $x_{cf}$ which the same decision model $M$ will classify into another class, i.e. $M(x) = y$, $M(x_{cf}) = \hat{y}$ and $y \neq \hat{y}$, which means it can say a 'what-if' scenario when the vehicle does

not require maintenance. A good counterfactual $x_{cf}$ will have the bare minimum difference between the individual feature values of $x$. Let the system $M$ be capable of classifying as well as producing a valid counterfactual of a given input. Given the current input vehicle condition $x = [3, 5, 1.7, 4.5, 2.1]$ to $M$, the decision of $M$ is $M(x) = 1$. Also, it produces two valid counterfactuals $x_1 = [3.1, 5.6, 2, 7, 8]$ and $x_2 = [4, 1, 3, 2.7, 2]$ where $M(x_1) = 0$ and $M(x_2) = 0$. Which one of the following is a better counterfactual option for the user ? Use Mean Absolute Error for comparison : $MAE(x, \hat{x}) = \frac{1}{n} \sum_i (|x_i - \hat{x}_i|)$. **[5]**

**Solution :**

Original input : $x = [3, 5, 1.7, 4.5, 2.1]$
Counterfactuals : $x_1 = [3.1, 5.6, 2, 7, 8]$ and $x_2 = [4, 1, 3, 2.7, 2]$

$MAE(x, x_1) = \frac{1}{5} \times (|3 - 3.1| + |5 - 5.6| + |1.7 - 2| + |4.5 - 7| + |2.1 - 8|) = 1.88$
$MAE(x, x_2) = \frac{1}{5} \times (|3 - 4| + |5 - 1| + |1.7 - 3| + |4.5 - 2.7| + |2.1 - 2|) = \mathbf{1.64}$

$x_2$ is suitable.

17. You are designing an advanced machine learning algorithm with distributed framework (like federated learning) for a smart city decision system. As a prototype, you have two clients ($K = 2$) and the dataset size is 50 ($n = 50$). You split the dataset into two clients as $n_1 = 35$ and $n_2 = 15$. Now, the clients and the server independently initialize the model with weight vectors as follows,

$\mathbf{w_1} = [1.31, 0.29, 1.57, -2.19]$,
$\mathbf{w_2} = [2.17, 1.91, -1.25, -0.39]$,
$\mathbf{w}_g = [2.19, 4.52, 3.14, 1.04]$

The clients train their own local models with learning rate $\eta = 0.1$ and they get the gradient updates as follows,

$\nabla_\mathbf{1} = [0.05, 0.04, -0.14, 0.15]$,
$\nabla_\mathbf{2} = [0.04, 0.56, -0.12, 0.33]$

You wish to apply two different aggregation algorithms - FedAvg and FedProx and compare the updated weights with the global model trained independently. After training the global model independently, you get the updated weights as $W'_s = [1.55, 0.8, 0.7, -1.7]$.

The computation models are as follows,

For FedAvg,
$\mathbf{w}' = \mathbf{w} - \eta \cdot \nabla$
$\mathbf{w}'_g = \sum_k \left( \frac{n_k}{n} \cdot \mathbf{w}_k \right), \forall k \in [1, K]$

For FedProx,
$\mathbf{w}' = \mathbf{w} - \eta \cdot [\nabla + \mu \cdot (\mathbf{w} - \mathbf{w}_g)]$
$\mathbf{w}'_g = \sum_k \left( \frac{n_k}{n} \cdot \mathbf{w}_k \right), \forall k \in [1, K]$

Question 17 continues on the next page. . .

**a)** Compute the final weights after aggregating the updated weights using FedAvg. Perform one iteration of client weight updates. **[6]**

**b)** Compute the final weights after aggregating the updated weights using FedProx. Perform one iteration of client weight update. Take $\mu = 0.1$. **[10]**

**c)** Comment on which method has yielded the weights closer to the one found by training the global model independently. Use MAE for comparison : $MAE(x, \hat{x}) = \frac{1}{n}\sum_i(|x_i - \hat{x}_i|)$. [4]

**Solution :**

(a) Using FedAvg, client updates are as follows,

$$\mathbf{w_1'} = \mathbf{w_1} - \eta \cdot \nabla_1 = \begin{bmatrix} 1.31 \\ 0.29 \\ 1.57 \\ -2.19 \end{bmatrix} - 0.1 \times \begin{bmatrix} 0.05 \\ 0.04 \\ -0.14 \\ 0.15 \end{bmatrix} = \begin{bmatrix} 1.305 \\ 0.286 \\ 1.584 \\ -2.205 \end{bmatrix}$$

$$\mathbf{w_2'} = \mathbf{w_2} - \eta \cdot \nabla_2 = \begin{bmatrix} 2.17 \\ 1.91 \\ -1.25 \\ -0.39 \end{bmatrix} - 0.1 \times \begin{bmatrix} 0.04 \\ 0.56 \\ -0.12 \\ 0.33 \end{bmatrix} = \begin{bmatrix} 2.166 \\ 1.854 \\ -1.238 \\ -0.423 \end{bmatrix}$$

From question, $n_1 = 35$ and $n_2 = 15$ for two clients, therefore the aggregated global model weights would be,

$$\mathbf{w}_g' = \frac{n_1}{n} \cdot \mathbf{w}_1 + \frac{n_2}{n} \cdot \mathbf{w}_2 = \frac{35}{50} \times \begin{bmatrix} 1.305 \\ 0.286 \\ 1.584 \\ -2.205 \end{bmatrix} + \frac{15}{50} \times \begin{bmatrix} 2.166 \\ 1.854 \\ -1.238 \\ -0.423 \end{bmatrix} = \begin{bmatrix} \mathbf{1.5633} \\ \mathbf{0.7564} \\ \mathbf{0.7374} \\ \mathbf{-1.6704} \end{bmatrix} = \mathbf{w}_{\text{fedavg}}$$

(b) Using FedProx, client updates are as follows,

$$\mathbf{w_1}' = \mathbf{w_1} - \eta \cdot [\nabla_1 + \mu \cdot (\mathbf{w_1} - \mathbf{w}_g)]$$
$$= \begin{bmatrix} 1.31 \\ 0.29 \\ 1.57 \\ -2.19 \end{bmatrix} - 0.1 \times \{ \begin{bmatrix} 0.05 \\ 0.04 \\ -0.14 \\ 0.15 \end{bmatrix} + 0.1 \times ( \begin{bmatrix} 1.31 \\ 0.29 \\ 1.57 \\ -2.19 \end{bmatrix} - \begin{bmatrix} 2.19 \\ 4.52 \\ 3.14 \\ 1.04 \end{bmatrix} )\} = \begin{bmatrix} 1.3138 \\ 0.3283 \\ 1.5997 \\ -2.1727 \end{bmatrix}$$

$$\mathbf{w_2}' = \mathbf{w_2} - \eta \cdot [\nabla_2 + \mu \cdot (\mathbf{w_2} - \mathbf{w}_g)]$$
$$= \begin{bmatrix} 2.17 \\ 1.91 \\ -1.25 \\ -0.39 \end{bmatrix} - 0.1 \times \{ \begin{bmatrix} 0.04 \\ 0.56 \\ -0.12 \\ 0.33 \end{bmatrix} + 0.1 \times ( \begin{bmatrix} 2.17 \\ 1.91 \\ -1.25 \\ -0.39 \end{bmatrix} - \begin{bmatrix} 2.19 \\ 4.52 \\ 3.14 \\ 1.04 \end{bmatrix} )\} = \begin{bmatrix} 2.1662 \\ 1.8801 \\ -1.1941 \\ -0.4087 \end{bmatrix}$$

From question, $n_1 = 35$ and $n_2 = 15$ for two clients, therefore the aggregated global model weights would be,

$$\mathbf{w}_g' = \frac{n_1}{n} \cdot \mathbf{w}_1 + \frac{n_2}{n} \cdot \mathbf{w}_2$$
$$= \frac{35}{50} \times \begin{bmatrix} 1.3138 \\ 0.3283 \\ 1.5997 \\ -2.1727 \end{bmatrix} + \frac{15}{50} \times \begin{bmatrix} 2.1662 \\ 1.8801 \\ -1.1941 \\ -0.4087 \end{bmatrix} = \begin{bmatrix} \mathbf{1.5695} \\ \mathbf{0.7938} \\ \mathbf{0.7615} \\ \mathbf{-1.6435} \end{bmatrix} \mathbf{w}_{\text{fedprox}}$$

(c) After training the global model independently, we obtained $W_s'$

Question 17 continues on the next page. . .

$$MAE(W_s', \mathbf{w}_{\text{fedavg}}) = \frac{1}{4} \times \sum \left| \begin{bmatrix} 1.55 \\ 0.8 \\ 0.7 \\ -1.7 \end{bmatrix} - \begin{bmatrix} 1.5633 \\ 0.7564 \\ 0.7374 \\ -1.6704 \end{bmatrix} \right| = \mathbf{0.0309}$$

$$MAE(W_s', \mathbf{w}_{\text{fedprox}}) = \frac{1}{4} \times \sum \left| \begin{bmatrix} 1.55 \\ 0.8 \\ 0.7 \\ -1.7 \end{bmatrix} - \begin{bmatrix} 1.5695 \\ 0.7938 \\ 0.7615 \\ -1.6435 \end{bmatrix} \right| = 0.03592$$

Using **FedAvg**, we have obtained weights closer to $W_s'$ (weights of the model after training independently).

Department of CSE
**Indian Institute of Technology Jodhpur**
Vehicular Ad-Hoc Networks (CSL7310)
Instructor : Dr. Debasis Das
MINOR EXAM (Fall 2024)

Dtd : Sept 21, 2024

SOLUTIONS SOLUTIONS

1. What is the primary advantage of Opportunistic Routing (OR) over traditional unipath routing in wireless networks? **[1]**

   A. It reduces the overall network size.

   B. It utilizes multiple potential forwarders to increase delivery reliability.

   C. It simplifies the routing process by using a single path.

   D. It eliminates the need for any coordination among nodes.

   Opportunistic Routing (OR) in Vehicular Ad-hoc Networks (VANETs) improves delivery reliability by using multiple candidate forwarders to forward data packets. This allows the selection of the best forwarder dynamically, based on real-time network conditions, improving performance in highly dynamic environments like VANETs compared to traditional unipath routing.

2. Which of the following is not a characteristic of Vehicular Ad Hoc Network (VANET)? **[1]**

   A. Multi-hop routing.

   B. Infrastructure-less.

   C. Long-range wireless transmission.

   D. None of the mentioned.

3. Assume that source S and destination D are connected through three intermediate routers labeled R. Determine how often each packet has to visit the network layer and the data link layer during transmission from S to D. **[1]**

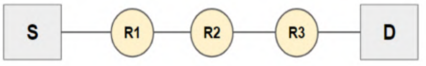



Figure 1: Figure for Q3

   A. Network layer – 5 times and Data link layer – 8 times.

   B. Network layer – 5 times and Data link layer – 5 times.

   C. Network layer – 4 times and Data link layer – 7 times.

   D. Network layer – 5 times and Data link layer – 5 times.

4. Select the correct option for VANET characteristics. **[1]**

   1. Topology: Variable Nodes join and leave the network very frequently.
   2. Connection life: short, depending on the road infrastructure condition.
   3. Connectivity: Permanent, end-to-end connectivity assured.

Question 4 continues on the next page. . .

4. RSU provides connectivity between two vehicle nodes.
   - A. All the options are correct.
   - B. Only 1, 2 and 3 are correct.
   - C. Only 1, 2 and 4 are correct.
   - D. Only 1 and 2 are correct.

5. In the context of OR, what does the term 'Candidate Set' (CS) refer to ? **[1]**
   - A. A group of nodes that are permanently assigned to forward packets.
   - B. A collection of nodes selected as potential forwarders for a packet.
   - C. A fixed path chosen before transmission begins.
   - D. A method for measuring link quality.

   In Opportunistic Routing (OR), the "Candidate Set" (CS) refers to a group of nodes that are selected as potential forwarders for a packet. These nodes are prioritized based on factors such as their proximity to the destination or the quality of the links, and any of them may forward the packet, depending on the network conditions at the time of transmission. This dynamic approach enhances the robustness and reliability of packet delivery.

6. Identify the path that has the minimum cost using Bellman-ford algorithm to travel from node 'a' to node 'f'. **[1]**

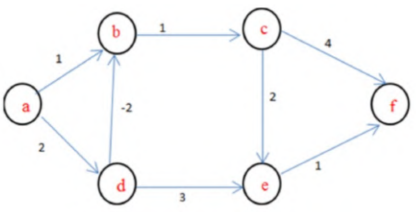



Figure 2: Figure for Q6

   - A. a-b-c-e-f
   - B. a-d-b-c-e-f
   - C. a-b-c-f
   - D. a-d-e-f

7. What is a significant drawback of using End-to-End metrics in Opportunistic Routing protocols ? **[1]**
   - A. They provide too much local information.
   - B. They can lead to increased overhead due to computation costs.
   - C. They do not consider link quality.
   - D. They simplify candidate selection.

   A significant drawback of using End-to-End metrics in Opportunistic Routing (OR) protocols is that they can introduce increased overhead due to the computational cost involved in estimating the entire path's quality, rather than just local link information. This can slow down the process and require more resources, making them less efficient in highly dynamic networks like Vehicular Ad-hoc Networks (VANETs).

8. How does candidate coordination work in Opportunistic Routing ? **[1]**

   A. Candidates independently decide whether to forward packets without communication.

   B. Candidates communicate to determine which should forward the packet based on priority.

   C. The source node dictates which candidate forwards the packet.

   D. Candidates randomly choose whether to forward or discard packets.

   In Opportunistic Routing (OR), candidate coordination works by having the potential forwarders communicate to decide which candidate will forward the packet based on a predefined priority system. This coordination ensures that only one candidate forwards the packet, preventing duplication of transmissions and improving efficiency. The candidates' priorities are usually determined by factors like distance to the destination or link quality.

9. What is the primary challenge addressed by routing protocols in Vehicular Ad Hoc Networks (VANETs) ? **[1]**

   A. Encryption and security.

   B. Network scalability.

   C. Network scalability.

   D. Data compression.

10. Which of the following routing protocols is specifically designed for Vehicular Ad Hoc Networks (VANETs) to efficiently manage fast-moving vehicles in urban environments ? **[1]**

    A. Dynamic Source Routing (DSR).

    B. Ad Hoc On-Demand Distance Vector Routing (AODV).

    C. Optimized Link State Routing (OLSR).

    D. Vehicular Ad hoc Network Routing (VANETR).

11. Consider a section of a highway with multiple vehicles equipped with Vehicular Ad Hoc Network (VANET) capabilities. The vehicles use a Distance Vector Routing protocol to communicate and navigate effectively by updating their routing tables based on the distance vectors received from their neighbors. Five vehicles, A, B, C, D, and E, are positioned along a straight section of the highway at various distances from each other. The distances between them are given as follows: A to B: 5 km, B to C: 3 km, C to D: 4 km, D to E: 2 km, A to D: 12 km (direct link due to visibility), B to E: 10 km (direct link due to visibility). Each vehicle only knows the distance to its immediate neighbors and any direct links it can establish due to line of sight or previous arrangements. They need to calculate the shortest paths to all other vehicles using the distance vector routing algorithm. Calculate the shortest path from vehicle A to all other vehicles after two rounds of updates. Assume each vehicle only exchanges information with its direct neighbors during an update round. **[5]**

    **Initial Setup:** Each vehicle constructs an initial distance vector based on its direct neighbors. Initially, the vehicles know only the distances to their direct neighbors or assume infinity where no direct link exists.
    **Initial distance vectors:**

    - A: [A:0, B:5, C:infinity, D:12, E:infinity]

- B: [A:5, B:0, C:3, D:infinity, E:10]
- C: [A:infinity, B:3, C:0, D:4, E:infinity]
- D: [A:12, B:infinity, C:4, D:0, E:2]
- E: [A:infinity, B:10, C:infinity, D:2, E:0]

**First Round of Updates:** Each vehicle updates its table based on the information received from its neighbors.

- A updates from B and D:
  A to C through B: 5 + 3 = 8 (New route discovered)
  A to E through D: 12 + 2 = 14 (New route discovered)
- B updates from A, C, and E:
  B to D through C: 3 + 4 = 7 (New route discovered)
- C updates from B and D:
  C to A through B: 3 + 5 = 8
  C to E through D: 4 + 2 = 6 (New route discovered)
- D and E update from their neighbors but find no shorter paths than already known.

**Second Round of Updates:** A now knows A to E through B,C, and D: 5 + 7 + 2= 14 (Better route through B,C,D)
**After two rounds, updated distance vectors:**

- A[A:0, B:5, C:8, D:12, E:14]
- B[A:5, B:0, C:3, D:7, E:9]
- C[A:8, B:3, C:0, D:4, E:6]
- D[A:12, B:7, C:4, D:0, E:2]
- E[A:14, B:9, C:6, D:2, E:0]

After two rounds of updates using the Distance Vector Routing protocol, vehicle A has calculated the shortest paths to all other vehicles in the network. The paths are as follows:

- To B: 5 km
- To C: 8 km
- To D: 12 km
- To E: 14 km

12. Suppose a group of six vehicles (A, B, C, D, E, F) are deployed in a region with varying distances between them. The vehicles have communication devices to exchange routing information and dynamically update their routing tables using the Bellman-Ford algorithm. The initial distances (costs) between the vehicles are represented as follows (a negative cost represents a route with a beneficial aspect, such as a tailwind): A to B: 4 km, A to C: -2 km, B to C: 3 km, B to D: 2 km, C to B: 1 km, C to E: 2 km, D to E: -1 km, D to F: -3 km, E to D: 3 km, and E to F: 2 km. Assume all pairs of vehicles not directly connected have an initial infinity distance. Determine the shortest paths from vehicle A to all other vehicles in the network using the Bellman-Ford algorithm after three iterations. **[5]**

**Initial distances:**

- A: [A: 0, B: 4, C: -2, D: $\infty$, E: $\infty$, F: $\infty$]
- B, C, D, E, F initialize similarly based on direct links.

**Iteration 1 :** Update each vehicle's distance based on the Bellman-Ford relaxation process. Updated distances after Iteration 1:

- A: [A: 0, B: -1, C: -2, D:3, E:0, F:2]
- Adjustments reflect other vehicles.

**Iteration 2 :** Updated distances after Iteration 2:
A: [A: 0, B:-1, C: -2, D: 1, E: 0, F: -2]
**Iteration 3 :** Refine distances to D and F using paths through E and others. Final distances after Iteration 3:
A: [A: 0, B:-1, C: -2, D: 1, E: 0, F: -2]
After three iterations of the Bellman-Ford algorithm, the shortest paths from vehicle A to the other vehicles in the VANET are as follows :

- To B:-1km
- To C: -2 km
- To D: 1 km
- To E: 0 km
- To F: -2 km

This scenario highlights how the Bellman-Ford algorithm effectively handles dynamic changes and even negative weights in routing for VANETs.

13. In a Vehicular Ad Hoc Network (VANET) where vehicles frequently change positions and network topology updates dynamically, which routing protocol between Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV) would better handle rapid topological changes and why? Consider their operational mechanisms, strengths, and weaknesses in your analysis. **[5]**

Comparison of DSR and AODV

**Dynamic Source Routing (DSR) :**

- **Operational Mechanism:** DSR utilizes a route discovery mechanism where the source node floods a route request packet across the network until it reaches the destination. The route is then established based on the path that the packet traveled. DSR maintains a route cache that allows it to react quickly to topological changes using alternative cached routes.
- **Strengths:** Using route caching in DSR can significantly reduce the need for frequent route discoveries, which is advantageous in a dynamic environment as it offers faster route adjustments without the overhead of route rediscovery.
- **Weaknesses:** The main drawback of DSR is the overhead associated with maintaining large route caches in each node, especially in a dense network. Also, the entire route is included in the packet header, which can increase the packet size and, consequently, the overhead.

**Ad Hoc On-Demand Distance Vector (AODV) :**

- **Operational Mechanism :** AODV also starts with a route discovery process but utilizes routing tables with one entry per destination rather than source routing. It updates its routes through routing tables at each node, with nodes forwarding packets to the next hop as per the routing table entries.
- **Strengths :** AODV uses sequence numbers to ensure the freshness of routing information, thus avoiding loops and reducing the likelihood of using stale routes. It also features local route recovery, which can be quicker than global route rediscovery processes.
- **Weaknesses :** The main disadvantage of AODV in a highly dynamic network like a VANET is the latency involved in discovering new routes and the overhead of maintaining routing tables and sequence numbers, which can slow down its adaptation to rapid topology changes.

14. The campus is divided into three zones with the following nodes (shuttles) and paths: **Zone 1: Nodes A, B, C** (A to B: 3 minutes, A to C: 6 minutes, B to C: 2 minutes), **Zone 2: Nodes D, E** (D to E: 4 minutes) **Zone 3: Nodes F, G, H** (F to G: 5 minutes, F to H: 7 minutes, G to H: 3 minutes). Each node within a zone can communicate directly or via other nodes in the same zone, but communication between zones is handled by designated gateway nodes A for Zone 1, D for Zone 2, and F for Zone 3. At the start of a typical day, the network begins operation without any prior routing information. Calculate the shortest paths within each zone using IARP after the initial setup and routing information exchange. Consider the performance of IARP in managing intra-zone routing updates and maintaining efficient local route discovery. **[5]**

Students may opt any shortest path algorithm for Intra Zone communication.
**STEP 1 :**
Initial Routing Information Exchange within Zones: Each node in a zone shares its direct connectivity information with other nodes in the same zone. Using IARP, the nodes will calculate the shortest path to every other node within their zone using Dijkstra's algorithm:

- **Zone 1 :**
  - Node A: Starts with direct routes, A-B (3 min) and A-C (6 min). A discovers A-C via B: A to B to C = 3 + 2 = 5 minutes (updated path)
  - Node B: Starts with B-A (3 min) and B-C (2 min)
  - Node C: Starts with C-A (6 min) and C-B (2 min). C updates C-A via B: C to B to A = 2 + 3 = 5 minutes (updated path)
- **Zone 2 :**
  - Node D: Directly connected to E, D-E (4 min)
  - Node E: Directly connected to D, E-D (4 min)
- **Zone 3 :**
  - Node F: Starts with direct routes, F-G (5 min) and F-H (7 min)
  - Node G: Starts with G-F (5 min) and G-H (3 min)
  - Node H: Starts with H-F (7 min) and H-G (3 min)
  - H updates H-F via G: H to G to F = 3 + 5 = 8 minutes (though direct path remains optimal)

**STEP 2 :**
Conclusion of Initial Routing Establishment. After the initial exchange of routing tables and application of Dijkstra's algorithm :

- **Zone 1 Shortest Paths :**
  - A to B = 3 minutes
  - A to C = 5 minutes (optimized through B)
  - B to C = 2 minutes
  - B to A = 3 minutes
  - C to A = 5 minutes (optimized through B)
  - C to B = 2 minutes
- **Zone 2 Shortest Paths :**
  - D to E = 4 minutes
  - E to D = 4 minutes
- **Zone 3 Shortest Paths :**
  - F to G = 5 minutes
  - F to H = 7 minutes
  - G to H = 3 minutes
  - G to F = 5 minutes
  - H to G = 3 minutes
  - H to F = 7 minutes

The IARP effectively maintains routing efficiency within zones by ensuring that each node is aware of the shortest paths to all other nodes in its zone without the overhead of handling external zone routing data. This localized routing knowledge reduces routing overhead, speeds up route discovery, and maintains high levels of network performance in densely populated vehicular networks such as those in a busy university campus setting.

15. In a Vehicular Ad-hoc Network (VANET) setup with Zone Routing Protocol (ZRP), assume the zone radius is set up to **3 hops**. Each node has an average of **5 neighbours within their 1 hop range**. The network consists of 80 nodes. If a node initiates a route discovery process using Inter-ZRP (IERP), and each border node (at the edge of the zone) sends a route request to its neighbours, **calculate the number of nodes outside the 3-hop zone**. Assume the network is densely connected; for simplicity, no node outside the zone has already been queried. Also, you must recall Intra-ZRP and how to reach unique nodes at each hope (here, 5/3 would be the unique factor of neighbours with every hope, consider the floor value). **[5]**

Zone radius=3 hops; Each node has 5 neighbours on average; Total network nodes = 80; No overlap in query nodes outside the zone.

- **Step 1 :** Calculating the number of nodes within 3 hop zones (Intra-ZRP)
  - At hop 1: The node has 5 direct neighbours
  - At hop 2: Every 5 neighbours has 5 neighbours on average. However, there will be some overlap. As the unique factor is given as 5/3 here, so is the number of new nodes = 5×the unique neighbours (factors) = $5 \times 5/3 = 8$ unique nodes at 2 hops

Therefore the total number of nodes within the 3hop zone (Intra-Zone) is: = 1 (Source ) + 5 (1 hop neighbours) + 8 (2 hop unique neighbours) + 13 (3 hop unique neighbours) = 27 nodes/Considerable: 26 Nodes (Without Source Node)

- **Step 2 :** Determine the number of nodes outside the 3-hop zone (Inter-Zone Routing): Total number of nodes 80; nodes in the intra-zone → 27 or, 26; So, the number of nodes outside the zone (for which IERP is needed): Total number of nodes - Nodes in the intra-zone = 80 - 27 = 53 or, 80 - 26 = 54

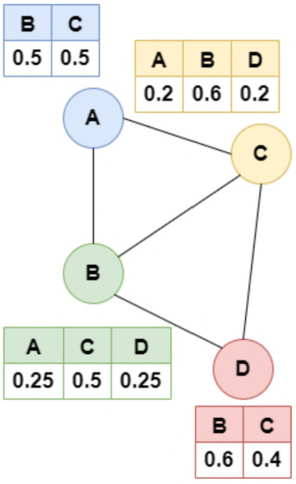



Figure 3: Figure for Q16

16. Let's say there is a unicast forwarding algorithm to calculate the path cost among two nodes, I and J, which is equal to $(1 - \text{Weight}_I(J))$, being $\text{Weight}_I(J)$, the weight J has on the table of I. After the cost calculation of all the paths, the smallest calculated value is the adopted path to deliver the packet. The figure illustrates the path cost. Find out the path with the least cost to deliver a packet from A to D using the protocol. (Consider all the four probable paths: ABD, ACD, ABCD and ACBD, to calculate the cost and get the lowest cost among them). **[5]**

Cost of the Paths:
ABD = (1 - 0.5) [A to B] + (1 - 0.25) [B to D] = 1.25
ACD = (1 - 0.5 ) [A to C] + (1 - 0.2 ) [C to D] = 1.3
ABCD = (1 - 0.5 ) [A to B] + (1 - 0.5) [B to C] + (1 - 0.2) [C to D] = 1.8
ACBD = (1 - 0.5 ) [A to C] + (1 - 0.6) [C to B] + (1 - 0.25) [B to D] = 1.65
So the least cost path among the four is ABD = 1.25