1. (10 points.) In the regional registration scheme or the pointer forwarding scheme for mobility management, the best regional area size expressed in terms of the number of boundary crossings is a function of the ratio of the call arrival rate to the user’s mobility rate, CMR. Do you expect a large or small regional area size when CMR is low? Give reasons.

**Ans:** When CMR is low, we expect a large regional area size because when CMR is low the user mobility rate is higher than the call arrival rate, so the cost due to frequent mobility update can be reduced by keeping the regional area size large. The cost for search would be high when the regional area size is large, but because the call arrival rate is low compared with the user’s mobility rate, this cost is small.
2. (10 points.) For each pair of algorithms given below, circle the one that you think would perform better than the other under the condition specified. No need to explain your answer.

(a) Lazy caching vs. \(\sqrt{\text{eager caching under high CMR}}\)
(b) Pure distance-based vs. \(\sqrt{\text{local anchor under high CMR}}\)
(c) Forwarding vs. \(\sqrt{\text{pure movement-based under low CMR}}\)
(d) \(\sqrt{\text{Fully distributed vs. dynamic anchor under high SMR}}\)
(e) Static anchor vs. \(\sqrt{\text{centralized under high CMR}}\)
3. (a) (5 points.) Describe a protocol that can dynamically determine whether or not to cache the location of a MU at a VLR.

**Ans:** The working set protocol can determine whether or not to cache the location of a MU at a VLR dynamically. Under this protocol, the working set of a mobile user $m$ is the set of VLRs that cache location information about $m$. A sliding window of length $T$ is maintained by the system. When a new operation occurs, the working set membership is dynamically maintained as follows:

- If the operation is a search operation from $VLR_i$ and if $VLR_i$ is not in the working set and $\alpha \times \lambda_i > \beta \times \sigma$ then add $VLR_i$ to the working set.
- If the operation is an update operation, then evaluate all the VLRs in the working set. If $\alpha \times \lambda_i < \beta \times \sigma$ then delete $VLR_i$ from the working set.

(b) (5 points.) Describe a protocol that can dynamically determine whether or not to cache a data item at a mobile host.

**Ans:** A dynamic sliding-window allocation scheme $SW[k]$ can dynamically determine whether or not to cache a data item at a mobile host. Under this protocol, the system maintains the last $k$ relevant operations and makes the allocation or deallocation decision after each relevant operation as follows:

- If the data item is not cached at the mobile node and if the window has more $rm$ operations than $ws$ operations, then allocate the data item at the mobile node.
- If the data item is cached at the mobile node and if the window has more $ws$ operations than $rm$ operations, then deallocate the data item from the mobile node.
4. (5 points.) Name three basic data and index organization techniques for wireless data broadcast. Suppose that we process a read transaction with selective tuning and data pre-declaration. Rank the three techniques in terms of the average access time and the average tuning time needed. Give reasons.

**Ans:** Three well known techniques are (a) access-time optimization without indexing; (b) tuning-time optimization with the index broadcast at the beginning of each broadcast; (c) \((1,m)\) indexing with the index being broadcast \(m\) times in each broadcast cycle.

In terms of access time, technique (a) is better than (b) which in turn is better than (c) because with indexing, clients have to wait till the beginning of the next broadcast, even if the required data is just in front of them. With \((1,m)\) indexing, clients have to wait a longer time (because they are \(m\) indexes instead of one index) on average before the first item comes around.

In terms of tuning time, technique (a) is the worst because the tuning time is the same as the access time; techniques (b) and (c) are tied for optimality for tuning time because the average tuning time to find the first index and subsequently to obtain all data items is about the same with pre-declaration.

5. (5 points.) Discuss the advantages and disadvantages of stateful cache invalidation schemes. Discuss qualitatively under the stateful approach how you can possibly estimate the average query response time, when given a set of parameter values characterizing the workload and operational environments.

**Ans:**

The advantages of the stateful approach are short query delay (if the cache content is updated, the query delay essentially is zero) and that the MH can disconnect arbitrarily and get sync with the proxy (agent) upon reconnection. The disadvantages are non-scalability (cannot handle a large population) and relatively high overhead for the server to maintain information about the cache content of the clients.

The query delay under the stateful scheme can be obtained by estimating the cache miss probability and the round-trip response time needed to communicate with the server per query amid the downlink traffic generated by invalidation report broadcast by the server and uplink traffic generated by queries that could not be answered locally. Then the average query delay can be computed as the product of cache miss probability and response time.
6. (10 points.) Assume that a 2 out of 3 majority voting scheme is used to reach result consensus and to tolerate link and sensor faults as described in paper [P8]. Assume that the network topology is shown above with TTL=3. As in [P8], let \( p \) be the data fault probability of each link and \( q \) be the fault probability of each node. Give an expression for the reliability that a sensor reading is transmitted correctly from the source node (labeled as A) to the sink node (labeled as D). Assume that all paths with TTL \( \leq 3 \) from A to D occur with equal probability. For the reliability expression, there is no need to do algebra to simplify the expression.

**Ans:** There are 3 paths satisfying TTL \( \leq 3 \), namely, \( P_1: A \rightarrow E \rightarrow D \), \( P_2: A \rightarrow E \rightarrow C \rightarrow D \), and \( P_3: A \rightarrow B \rightarrow C \rightarrow D \). The fault probability of the first path is \( Q_{P_1} = A = 1 - (1 - q)(1 - p)^2 \) as derived in [P8]. The fault probability of each of the other two paths is the same, i.e., \( Q_{P_2} = Q_{P_3} = B = 1 - (1 - q)^2(1 - p)^3 \). The sink will take the three results returned from the source and perform voting so the system fails when at least two out of three return faulty results. So as derived in [P8], the failure probability of the system is \( Q_{P_1,P_2,P_3} = AB^2 + A(1 - B)B + AB(1 - B) + (1 - A)B^2 \). The system reliability is \( 1 - Q_{P_1,P_2,P_3} \).

**Alternative Ans:** The reliability of the first path is \( R_1 = (1 - q)(1 - p)^2 \) as derived in [P8]. The reliability of each of the other two paths is the same, i.e., \( R_2 = R_3 = (1 - q)^2(1 - p)^3 \). The sink will take the three results returned from the source and perform voting so the system works when at least two out of three return non-faulty readings. So the reliability of the system is given by \( R_1R_2R_3 + R_1(1 - R_2)R_3 + R_1R_2(1 - R_3) + (1 - R_1)R_2R_3 \).
7. (10 points.) Suppose a query requires 3 clusters to return sensor readings instead of involving all clusters. Also suppose that only 2 sensors in a cluster will return readings to the cluster head for data aggregation. In addition, for fault tolerance, $m_p$ disjoint paths will be used to return aggregate data from a cluster head to the processing center. Give an expression for the energy spent as a function of the probability of a sensor becoming a cluster head (i.e., $p$) based on the formulation given in paper [P9]. Note: the $m_p$ paths used for returning the aggregate data from a cluster head to the processing center is not based on hop-by-hop data delivery as discussed in paper [P10]. You only need to consider this problem using the formulation given in paper [P9].

**Ans:**

$$
\frac{3 \times p(1-p) \lambda}{r(p \lambda)^{3/2}} + \frac{3 \times 0.765 m_p a}{r}
$$

Note: the average number of sensors in a cluster is $1/p$ including the cluster head and $(1 - p)/p$ excluding the cluster head. The answer above is based on $1/p$ as the average number of sensors in a cluster.

The first expression accounts for energy spent by sensors in three clusters. The second expression accounts for energy spent by 3 CHs relaying data to the PC each through $m_p$ paths.
8. (10 points.) WEP in 802.11 is vulnerable to collision attacks and forgery attacks. Discuss these attacks and comment on the specific security properties (confidentiality, integrity, authentication, non-repudiation) that have been violated because of these attacks. Comment very briefly on specific measures or methods taken by 802.11i to deal with these attacks.

**Ans:** Collision attacks in WEP refer to keystream attacks, that is, once a packet is successfully decrypted, the attacker can recover the keystream by $RC4(k,IV) = P \oplus C$, so the attacker can use it to decrypt packets with same IV. Once the attacker collects all $2^{24}$ known keystreams for $2^{24}$ IV values (by storing $2^{24}$ plaintext/ciphertext in a decryption dictionary on disk), any packet can be decrypted. Since there are only 24 bits for IV, there are only $2^{24}$ IV choices and collisions are guaranteed to occur after several hours to several days. Collision attacks will cause confidentiality property to be violated. The measure taken in 802.11i is to use 48-bit IV and specify that IV be updated with every packet. A new base key is generated when IV reaches its maximum. Further in TKIP (an encryption algorithm supported by 802.11i), a per-packet key derived from the base key is used to encrypt a packet.

CRC attacks in WEP refer to attacks by which the attacker alters bits in the encrypted message and CRC-32 without knowing plaintext. It causes integrity property to be violated. The measure taken in 802.11i to use a new Message Integrity Code (MIC) utilizing a cryptographically secure hash makes changing data impossible.
9. (10 points.) In centralized group key management, a binary key tree may be maintained by a key server based on the LKH algorithm. A key tree shown above represents a state in which there are 6 members, M1-M6, in the group. Starting from this state, show the content of a broadcast message (using the format as shown in the lecture slide set) broadcast by the server in response to:

(a) An existing member M5 leaving the group
(b) A new member M7 joining the group

Comment on why backward secrecy and forward secrecy requirements would be satisfied by your broadcast message in these two cases.

Ans:

(a) \{K'_3\}K_4, \{K'_2\}K'_6, \{K'_2\}K_3, \{K'_1\}K'_4, \{K'_1\}K_9

(b) The answer varies depending on the spot to insert the new member. Assume that the new member is inserted under M3 and that a new key is created (not broadcast) for the new member. Then the broadcast message would be: \{K'_{10}\}K_{10}, \{K'_9\}K_{12}, \{K'_9\}K'_{10}, \{K'_1\}K'_5, \{K'_1\}K_2

Forward secrecy is satisfied in (a) because the leaving member would not have the new key after the rekey; backward secrecy is not an issue in case (a).

Backward secrecy is satisfied in (b) because the new member would not have the old key after the rekey; forward secrecy is not an issue in case (b).
10. (10 points.) Suppose that 4 nodes shown above are involved in the execution of a contributory group key protocol based on Diffie-Hellman key exchange. Assume that there are all within radio range so they are fully connected. Ignore collision and assume that DH key exchange can occur in pairs simultaneously. Design a contributory group key protocol that would allow a group key to be established using the least amount of time.

(a) Describe your protocol. Give details about which nodes are doing Diffie-Hellman key exchange in your protocol.

(b) Give an expression for the group key established as a function of $p$, $g$, $S_1$, $S_2$, $S_3$ and $S_4$, where $p$ is a large prime number, $q$ is an integer, and $S_1$, $S_2$, $S_3$ and $S_4$ are random numbers selected by nodes 1, 2, 3 and 4, respectively.

(c) Exactly how many messages would be needed for these 4 nodes to finally agree on a secret key? Count every message.

Ans:

(a) In the first round, a key is established between node 1 and node 2 ($g^{S_1 S_2 \mod p}$) and a key is established between node 3 and node 4 ($g^{S_3 S_4 \mod p}$). Using the “key” established in the first round as a random number, in the 2nd round a key is established between node 1 and node 3 ($g^{(g^{S_1 S_2 \mod p})(g^{S_3 S_4 \mod p}) \mod p}$) and a key is established between node 2 and node 4 ($g^{(g^{S_1 S_2 \mod p})(g^{S_3 S_4 \mod p}) \mod p}$). This key would be the secret key established using the least amount of time.

(b) $g^{(g^{S_1 S_2 \mod p})(g^{S_3 S_4 \mod p}) \mod p}$.

(c) A total of 8 messages will be required because 4 messages are required in each round. (Note: each DH key exchange between two nodes takes two messages.)
11. (10 points.) $\mu TESLA$ is a protocol that allows a server to broadcast packets to receivers in intervals such that a packet broadcast in interval $i$, $i > 0$, contains a MAC (Message Authentication Code) calculated using key $K_i$. Keys are related to each other by a one-way function $F$ such that $K_i = F(K_{i+1})$ with $K_0$ being known to all receivers initially. $\mu TESLA$ delays disclosing $K_i$ at interval $i + \delta$, that is, $K_i$ is broadcast by the server after a delay of $\delta$ intervals. Consider a broadcast scenario as shown above. Suppose that $\delta = 2$ and that during an interval, at most three packets will be broadcast by the server. Briefly (3 lines per answer at most) answer the following questions:

(a) What’s the minimum receiver buffer size (in terms of the number of data packets the buffer can hold) if the receiver wants to be able to tolerate 3 consecutive MAC key losses. Explain your answer.

(b) According to $\mu TESLA$ when will $K_3$ be disclosed? When the receiver receives $K_3$, how does it know $K_3$ is valid?

(c) If $K_3$ received is proven valid, which packet(s) could be authenticated by the receiver? What is the procedure for doing authentication? Suppose that all data packets broadcast by the server are received by the receiver in order.

Ans:

(a) A buffer size of 9-packet is needed without any key loss to hold 6 unauthenticated packets received in the past two intervals and 3 authenticated packets received in the current interval. To tolerate three consecutive key losses, an additional buffer space to hold 9 unauthenticated packets is needed. Thus, a total of 18-packet buffer space is needed.

(b) $K_3$ will be disclosed in interval 5. The receiver can check if $F(K_3) = K_2$ if $K_2$ has been proven valid, or it can check if $F(F(K_3)) = K_1$ if $K_1$ has been proven valid, or it can check if $F(F(F(K_3))) = K_0$ if neither $K_2$ nor $K_1$ is known to be valid.

(c) Key $K_3$ is used to compute the MAC of $P_4$ and $P_5$ received during interval 3. If MACs agree, then $P_4$ and $P_5$ are authenticated and delivered to the client application.