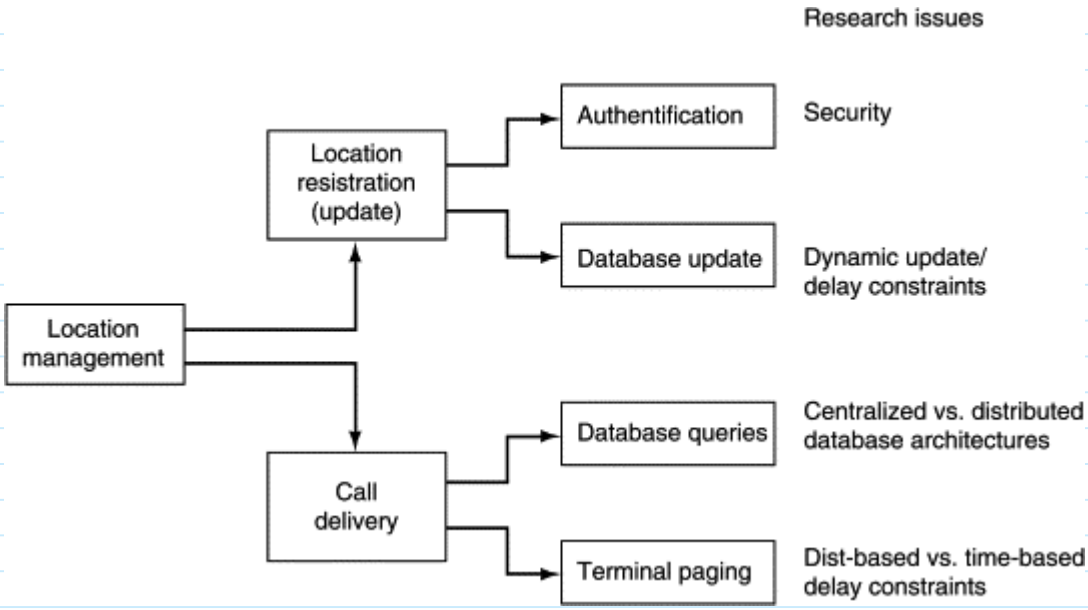
Mobile computing

25 June 2023 08:19

Location Management in mobile computing

Location management in mobile computing refers to the process of determining and tracking the geographic location of a mobile device, such as a smartphone or tablet, within a cellular network or other wireless communication system. It involves techniques and protocols that enable mobile devices to stay connected and seamlessly transition between different network cells or access points while maintaining continuous network connectivity.

1. Location management is a two-stage process: The first stage involves discovering the current attachment point of the mobile user for call delivery. This stage focuses on determining the location of the user within the network.
2. The second stage of location management is call delivery, which involves routing calls and messages to the mobile user based on their current location.
3. Location management protocols are responsible for querying and storing information in location databases. These databases store the necessary information to track and locate mobile users within the network.
4. Paging signals are used in location management to locate the mobile user within the network. These signals are sent to the last known location area or tracking area of the user to prompt a response.
5. Key research areas in location management include the design of efficient database architectures to reduce query traffic. This focuses on optimizing the storage and retrieval of location information.
6. Streamlining location update signaling is another important research area. It aims to minimize the signaling overhead associated with updating the location of mobile users as they move within the network.
7. Terminal paging schemes are also a key focus of research in location management. These schemes aim to improve the efficiency and accuracy of locating mobile users through paging signals.
8. Location management research issues, including security concerns, are associated with their respective location management operations, as depicted in Figure 8. This indicates the relationship between research topics and their practical implementation.
9. Location management issues are not protocol dependent and can be applied to various mobile networks. The principles and techniques can be utilized in different network architectures to address database, signaling, and paging challenges.



some key concepts related to location management in mobile computing:

1. **Cell Towers and Base Stations:** Mobile networks are divided into cells, each served by a cell tower or base station. These towers or stations transmit and receive signals to communicate with mobile devices within their coverage area.
2. **Location Area (LA):** A location area is a group of cells in a cellular network. The network tracks the location of a mobile device at the location area level, which allows for efficient tracking and management.
3. **Tracking Area (TA):** A tracking area is a smaller subset of a location area. It represents an even smaller area within which a mobile device can move without requiring an update of its location to the network. This helps reduce the signaling overhead associated with location updates.
4. **Location Update:** When a mobile device moves from one location area or tracking area to another, it needs to update its current location to the network. This update is typically triggered by the device or initiated by the network through periodic signaling messages.
5. **Paging:** Paging is the process by which the network locates a mobile device when there is an incoming call or message for that device. The network sends a paging message to the last known location area or tracking area of the device, and if the device is within that area, it responds accordingly.
6. **Handover (Handoff):** Handover is the process of transferring an ongoing call or data session from one cell to another as a mobile device moves between cells. Handover can be initiated by the network or the mobile device itself, ensuring uninterrupted connectivity during movement.
7. **Location-Based Services (LBS):** Location-based services leverage the location information of mobile devices to provide customized services based on the user's current geographic position. Examples include navigation apps, location-based advertising, and geographically targeted information services.

Location Based Services in mobile computing

- Location-Based Services (LBS) in mobile computing refer to services that utilize the geographical location of a mobile device or user to provide customized and relevant information, content, or functionality.
- LBS leverage the capabilities of mobile devices, such as GPS, Wi-Fi, cellular network triangulation, and other positioning technologies, to determine the user's location accurately.
- Location-Based Services enhance the functionality and personalization of mobile computing by utilizing the location information of mobile devices or users.
- These services offer a wide range of applications, including navigation, local search, advertising, social networking, proximity-based services, tracking, emergency services, and augmented reality.

Location-based services can be broken into the following distinct categories:

Pull. The application user initiates the location-based service processes. One example of a query-based location-based service is a user checking a mobile map application, such as Waze, to find the nearest automated teller machine. Some location-based services also enable users to check in to restaurants, concerts or sporting events using apps such as Foursquare, Yelp or Google Maps.

Push. The application initiates the location process based on a trigger or at regular intervals. The application then presents the user or device with relevant information based on their geographic location. Proximity-based marketing is a push-based location-based service example. Here, a user is sent an advertisement or coupon after the application proactively identifies that person as being near a specific retail outlet.

Here are some key points about Location-Based Services:

1. **Geolocation:** LBS rely on geolocation techniques to determine the precise or approximate location of a mobile device or user. This can include GPS (Global Positioning System), Wi-Fi positioning, cell tower triangulation, IP address mapping, or a combination of these methods.
2. **Navigation and Maps:** One of the most common applications of LBS is navigation and maps. Mobile devices can provide turn-by-turn directions, real-time traffic information, nearby points of interest (POI), and route optimization based on the user's current location.
3. **Local Search and Discovery:** LBS enable users to find local businesses, restaurants, services, and attractions based on their location. Users can search for specific categories, read reviews, view ratings, and get directions to the desired location.
4. **Location-Based Advertising:** LBS can be used to deliver targeted advertisements based on the user's current or past locations. Advertisers can deliver relevant ads to users in specific geographical areas, increasing the likelihood of reaching a relevant audience.
5. **Geotagging and Social Networking:** LBS allow users to attach location information, known as geotags, to their social media posts, photos, or status updates. This enables social networking platforms to provide location-specific features such as check-ins, location-based recommendations, and sharing location-related experiences with friends.
6. **Proximity-Based Services:** LBS can trigger notifications, offers, or alerts when a user enters or exits a predefined geographical area or when they are in close proximity to a specific location. This can include notifications about nearby sales, discounts, events, or reminders.
7. **Tracking and Fleet Management:** LBS can be utilized for tracking the location

and movement of vehicles, assets, or people. This is particularly useful for logistics, fleet management, personal safety, and monitoring applications.

8. **Emergency Services:** LBS play a critical role in emergency situations by providing emergency services with accurate location information for quick response and assistance. Emergency calls (like 911) can automatically transmit the caller's location to facilitate efficient emergency services.
9. **Augmented Reality (AR) and Gaming:** LBS can be integrated with augmented reality applications and location-based gaming, where virtual elements are superimposed on the real world based on the user's location. This creates immersive and interactive experiences that blend virtual content with the physical environment.

Automatically Locating Mobile Uses in mobile cpmputing

In the context of mobile computing, automatically locating mobile users can have several applications and benefits. Here are a few scenarios where automatic mobile user location can be useful:

1. **Location-based Services**: Mobile apps and services can utilize a user's location to provide personalized and context-aware experiences. For example, location-based advertising, navigation apps, local business recommendations, or emergency services can use the user's location to offer relevant information and functionality.
2. **Fleet Management:** Companies with a fleet of vehicles or mobile assets can use automatic mobile user location to track and manage their resources effectively. It helps optimize routes, monitor vehicle status, and provide real-time updates to customers about the estimated arrival time.
3. **Social Networking:** Location-based social networking applications allow users to connect with people nearby or share their current location with friends. Automatic mobile user location enables these features and enhances the social experience by facilitating local meetups, event planning, or discovering nearby points of interest.
4. **Safety and Security:** In emergency situations, such as natural disasters or personal distress, automatic mobile user location can be crucial for locating individuals in need of assistance. Emergency services can leverage this information to provide timely help and reduce response times.
5. **Geotagging and Content Localization:** Mobile devices with automatic location detection can automatically add geotags to photos, videos, or social media posts, enabling users to share their experiences with location context. Content localization, such as displaying information in the user's preferred language or adapting the content based on the user's location, is also possible using automatic mobile user location.
6. **Analytics and Business Insights:** Organizations can analyze aggregated and anonymized location data to gain insights into consumer behavior, foot traffic patterns, or urban planning. This information can be used to optimize business strategies, improve city infrastructure, or make data-driven decisions.

Locating and Organizing Services in mobile computing

Locating and organizing services in mobile computing involves the use of mobile applications and

technologies to help users discover, access, and manage various services conveniently.

Locating Services:

- In mobile computing, locating and organizing services refers to the process of finding and managing different services available through mobile applications.
- These services can include a wide range of offerings, such as transportation, food delivery, entertainment, financial transactions, healthcare, and more.
- Locating services involves utilizing various techniques to identify and present relevant service options to users based on their location, preferences, and needs.
- This can be achieved through location-based services (LBS) that utilize GPS, Wi-Fi positioning, or cellular network information to determine the user's location accurately.
- LBS applications can then provide location-specific recommendations and enable users to find nearby services easily.

Organizing Services:

- Organizing services entails providing users with tools and features to manage their interactions with different services efficiently.
- This can include functionalities like personalized service lists, favorites or bookmarks, user reviews and ratings, service comparisons, booking or reservation capabilities, and notifications or alerts for updates or promotions.

- ## Mobile Application Role:
  - Leverage mobile GPS, mapping services, and real-time data for seamless access.
  - Enable users to search, view, book, track, and interact with services.
  - Integrate multiple services into platforms or super-apps for a unified experience.

- ## Benefits:
  - Enhance user convenience and accessibility to services on the go.
  - Empower users to make informed decisions based on personalized recommendations.
  - Streamline service discovery, management, and transactions.
  - Optimize the overall mobile experience for users.

Issues and Future Directions

Location management in mobile computing presents its own set of challenges and potential future directions. Here are some key issues and future directions in mobile computing location management:

Issues:

1. **Accuracy and Precision:** Ensuring accurate and precise location information remains a challenge, especially in complex environments like urban areas or indoors where GPS signals may be weak or obstructed. Addressing this issue

involves exploring alternative location determination methods, such as combining multiple positioning technologies or improving the infrastructure for better location accuracy.

2. **Privacy Concerns:** Location data is highly sensitive and raises privacy concerns. Users may be reluctant to share their location information due to privacy risks. Future directions involve implementing robust privacy frameworks, user-controlled consent mechanisms, and anonymization techniques to protect location data and address privacy concerns.
3. **Energy Efficiency:** Continuous location tracking can consume significant battery power, affecting the overall device performance and user experience. Future directions involve developing energy-efficient location tracking algorithms and optimization techniques to minimize the energy consumption associated with location management.
4. **Context Awareness:** Location information is most valuable when combined with contextual data. Future directions involve leveraging other sensor data, such as accelerometer, gyroscope, or ambient sensors, to enhance location-based services and provide more context-aware experiences. This includes incorporating machine learning algorithms to analyze and interpret contextual data in real-time.
5. **Indoor Positioning:** Locating mobile users accurately indoors remains a challenge due to the limitations of GPS and other traditional positioning methods. Future directions involve exploring technologies like Bluetooth Low Energy (BLE) beacons, Wi-Fi fingerprinting, magnetic field sensing, or ultrasonic positioning to improve indoor positioning capabilities and enable location-based services within buildings.

Future Directions:

1. **Hybrid Positioning Technologies:** Future directions in location management involve combining multiple positioning technologies to provide more accurate and reliable location information. This includes integrating GPS, Wi-Fi, Bluetooth, and other technologies to create hybrid positioning systems that can seamlessly switch between different methods based on the environment and user requirements.
2. **Edge Computing for Location Processing**: Leveraging edge computing capabilities can reduce latency and improve real-time location processing. Future directions involve deploying location processing algorithms and services at the edge of the network, enabling faster and more efficient location management without relying heavily on centralized cloud infrastructure.
3. **Improved Location-Based Services:** Future directions involve developing more sophisticated and personalized location-based services. This includes leveraging artificial intelligence and machine learning techniques to analyze large amounts of location data, provide personalized recommendations, and anticipate user needs based on historical location patterns.
4. **Privacy-Preserving Location Services:** Future directions in location management involve designing location-based services that prioritize user privacy. This includes techniques such as differential privacy, secure multiparty computation, and homomorphic encryption to enable location-based services without compromising user privacy.
5. **Integration with IoT and Smart Environments:** The integration of location management with IoT and smart environments presents exciting future directions. This involves leveraging location data to enable seamless interaction between mobile devices and IoT devices, creating intelligent and context-aware environments that adapt based on user location and preferences.

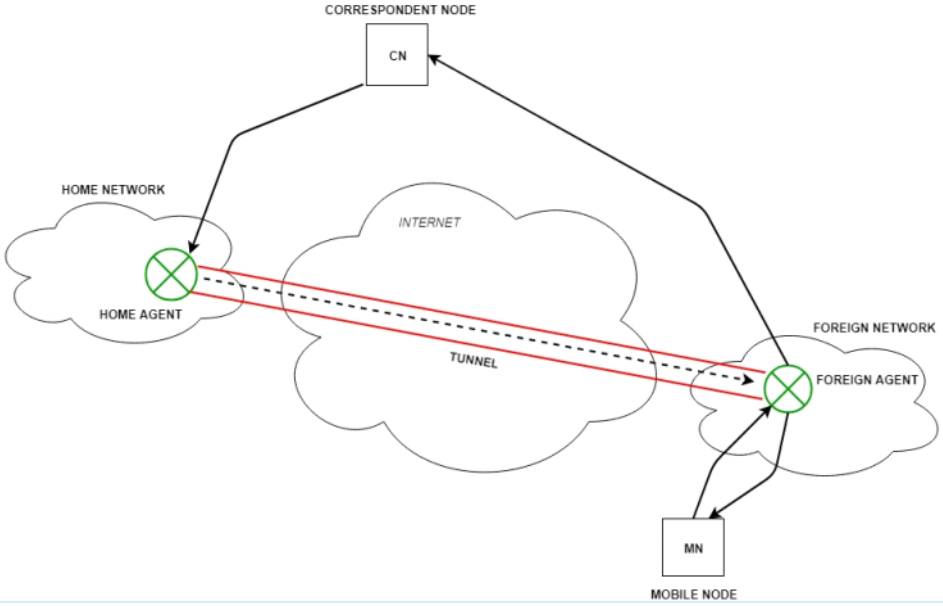
Mobile IP

Mobile IP (Internet Protocol) is a protocol that enables mobile devices to maintain continuous network connectivity while moving between different IP networks. It allows mobile devices, such as smartphones or tablets, to keep the same IP address and maintain ongoing sessions with other devices or servers, even as they change their point of attachment to the network.

Mobile IP operates based on the concept of an IP tunneling mechanism. When a mobile device moves to a new network, it registers with a home network or home agent, which maintains its original IP address. The home agent acts as an intermediary for routing packets to and from the mobile device. When a packet is sent to the mobile device's IP address, it is intercepted by the home agent and tunneled to the current location of the device.

Mobile IP involves several key components:

1. **Mobile Node (MN):** The mobile device that is moving and changing its point of attachment to the network.
2. **Home Agent (HA):** The home agent is a router located in the home network of the mobile device. It maintains the home address of the mobile device and forwards packets to the current location of the mobile device.
3. **Foreign Agent (FA):** The foreign agent is a router in the visited network, where the mobile device is currently connected. It assists in forwarding packets to the mobile device and notifies the home agent about the device's presence in the visited network.
4. **Care-of Address (CoA):** The care-of address is the temporary IP address assigned to the mobile device in the visited network. It serves as the current location address of the mobile device.



Working:

1. The correspondent node sends data packets to the mobile node with the correspondent node's address as the source and the mobile node's home address as the destination.

2. The data packets reach the home agent because the mobile node is currently not in its home network; it has moved to a foreign network.
3. The foreign agent sends the care-of-address (CoA) to the home agent, indicating where all the packets should be forwarded.
4. A tunnel is established between the home agent and the foreign agent using a process called tunneling. Tunneling creates a virtual pipe for the packets between the tunnel entry (home agent) and the endpoint (foreign agent).
5. The home agent encapsulates the data packets into new packets, where the source address is the home address, and the destination address is the care-of-address. These encapsulated packets are sent through the tunnel to the foreign agent.
6. On the other side of the tunnel, the foreign agent receives the encapsulated packets, decapsulates them by removing the outer packet headers, and sends the original data packets to the mobile node.
7. The mobile node, upon receiving the data packets, generates a reply and sends it back to the foreign agent.
8. The foreign agent, having the knowledge of the mobile node's CoA, directly sends the reply to the correspondent node without involving the home agent.

Key Mechanisms in Mobile IP:

1. **Agent Discovery:**
   - Agents periodically broadcast agent advertisement messages to announce their presence.
   - The mobile node receives these messages and determines whether it is in the home network or a foreign network based on the source of the message.
2. **Agent Registration:**
   - After discovering the foreign agent, the mobile node sends a registration request (RREQ) to the foreign agent.
   - The foreign agent forwards the registration request to the home agent, including the care-of-address.
   - The home agent responds with a registration reply (RREP), which is sent back to the foreign agent.
   - The foreign agent then forwards the registration reply to the mobile node, completing the registration process.
3. **Tunneling:**
   - Tunneling establishes a virtual pipe, or tunnel, for packets between a tunnel entry (home agent) and an endpoint (foreign agent).
   - It involves encapsulating packets in a new header for forwarding via the tunnel.
   - In Mobile IP, tunneling is used to forward IP datagrams from the home agent to the care-of-address.
   - The home agent encapsulates packets with the source address as the home address and the destination address as the care-of-address.

Route Optimization in Mobile IP:

- The route optimization adds a conceptual data structure, the binding cache, to the correspondent node.
- The binding cache contains bindings for the mobile node’s home

address and its current care-of-address.

- Every time the home agent receives an IP datagram that is destined to a mobile node currently away from the home network, it sends a binding update to the correspondent node to update the information in the correspondent node's binding cache.
- After this, the correspondent node can directly tunnel packets to the mobile node. Mobile IP is provided by the network providers.

Comparison of TCP and Wireless

TCP (Transmission Control Protocol) and wireless networks are two distinct concepts that play important roles in computer networking. Here's a comparison of TCP and wireless networks:

TCP:

1. **Protocol:** TCP is a transport layer protocol that provides reliable, connection-oriented communication between devices over an IP network.
2. **Reliability:** TCP ensures reliable data delivery by using acknowledgment mechanisms, retransmission of lost packets, and flow control.
3. **Connection-oriented:** TCP establishes a connection between the sender and receiver before data transmission, ensuring orderly and error-free communication.
4. **Error detection and correction:** TCP includes mechanisms for error detection and correction using checksums and sequence numbers.
5. **Congestion control:** TCP employs congestion control mechanisms to avoid network congestion and ensure fair sharing of network resources.
6. **Suitable for wired networks:** TCP is widely used in wired networks, such as Ethernet, where the connection is stable and reliable.

Wireless Networks:

1. **Medium:** Wireless networks use wireless communication technologies, such as Wi-Fi, cellular networks (3G, 4G, 5G), and satellite communications, to transmit data without physical cables.
2. **Mobility:** Wireless networks provide mobility, allowing devices to connect and communicate while on the move.
3. **Signal interference and loss:** Wireless networks are susceptible to signal interference, obstacles, and environmental factors that can degrade the quality of the wireless connection.
4. **Limited bandwidth:** Wireless networks typically have lower bandwidth compared to wired networks, which can affect data transmission speeds.
5. **Connectivity limitations:** Wireless networks may have coverage limitations or dead zones where the signal strength is weak or unavailable.
6. **Multiple access technologies:** Wireless networks use various access technologies like CDMA, OFDMA, or TDMA to enable multiple devices to share the available bandwidth.
7. **Security concerns:** Wireless networks may be more vulnerable to unauthorized access or data interception, requiring additional security measures such as encryption and authentication.

Transaction Management

A transaction processing system allows application programmers to concentrate on writing code that will allow users to perform transactions simultaneously without bothering about what other users may be doing with their transactions at the same time:

- It manages the concurrent processing of transactions.
- It enables the sharing of data.
- It ensures the integrity of data.

Issues in Transaction Processing

Database applications are normally structured into transactions. The transaction is a type of operation that makes sure that database does not change into an inconsistent state to disrupt the transactions.

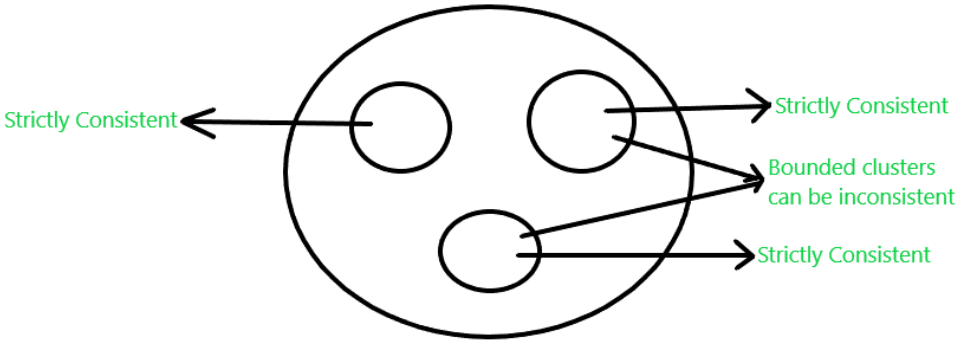
One important aim in the design of any database system is to maximize the number of transactions that can be active at a time. DBMS ensures serializability using ACID constraints:

- Atomicity
- Consistency
- Isolation
- Durability

ACID properties have been redefined to support transactions in the mobile environment are:

Atomicity Relaxation: Mobile Host is allowed to submit pieces of the transaction from different cells according to the movement. It requires the ability to break a transaction into many sub-transactions that can be concurrently executed.

Consistency Relaxation: The database is logically partitioned into “clusters” based on some attributes. Data in the same cluster must be strictly consistent. Although the bounded degree of inconsistency is tolerated among the clusters.



The above figure describes three clusters inside a bounded region.

Isolation Relaxation: The intermediate results of a transaction can be observed by other concurrent transactions. For example, if T1 is a

transaction process and T2 is another transaction process then T1 should not be visible to T2.

T1	
	T2

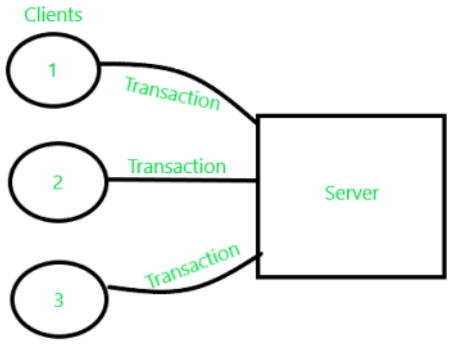
T1 and T2 are two transaction processes where the operation of T1 is not seen by T2.

Durability Relaxation: A disconnected Mobile Host can only commit a transaction locally if this transaction does not conflict with other transactions executed on the same HOST while HOST was disconnected.

Transaction Processing Environment

1. Centralized Environment: Single user system executes all the transactions.

2. Client Server Environment: Transaction and transaction initiation are done by the server and client respectively. Many clients can send transactions to servers simultaneously.



3. Distributed Environment: Data is distributed over a network. The transaction can occur fully on a node or partially on a different node.

4. Mobile Environment: Special type of distributed environment can accommodate user movements while processing transactions.

Issues in Mobile Environment

- **User Movement:** Tracking users, and data recovery are complicated. LOG location determination is complex.
- **Disconnections:** There may be temporary disconnections due to noise, fading of signal, handoff, etc. If there are planned disconnections, then the mobile user can perform some operations by downloading data beforehand. It can be referred to as data hoarding. Another way to deal with disconnection is by migrating transaction processing to a non-mobile computer. One more approach is maintaining proxy agents at MSS(Mobile Satellite Service). The process includes representing Mobile Host(MH) during its absence and participating in communication and finally handing over control to MH as it reappears.
- **Poor Communication Media-** Bandwidth allocated to mobile users could be very low. Interference from other traffic, noise, etc may corrupt data. MH

tends to disconnect from the network whenever there is no data to send or receive in the near future.

- **Processing Power-** With a less powerful CPU, database server operation is difficult.
- **Memory-** Memory availability is limited.
- **Battery Power-** Like memory, battery power is also limited.
- **User Interface-** It should be designed keeping in mind resource restrictions.
- **Security-** Chances of data theft and unauthorized access increases while MH moves from one cell to another.

Data Dissemination in mobile computing

1. Data dissemination involves distributing statistical or other types of data to end-users, which can be in the form of audio, video, or other data services.
2. Various methods are used to release data to the public, including electronic formats, CD-ROMs, and paper publications such as PDF files containing aggregated data.
3. Mobile devices play a role in receiving the disseminated data and can select, tune, and cache the required data items for use in application programs.
4. Non-proprietary open systems using internet protocols have become the most popular method for data dissemination, allowing data to be made available in standard open formats.
5. Communication infrastructures are utilized to disseminate data across interconnected networks, enabling data to be accessed and exchanged.
6. Some organizations choose to use proprietary databases for data dissemination to protect sovereignty and copyright. This requires specific software for end-users to access the data, as it is not open in common formats.
7. Proprietary data formats involve converting the data into a specific format and providing specially designed software to users for data viewing and manipulation.

key points about data dissemination in mobile computing:

1. **Broadcast and Multicast:** Broadcasting and multicasting are commonly used techniques for data dissemination in mobile computing. Broadcasting involves sending data to all devices within the network, while multicasting allows data to be sent to a specific group of devices that subscribe to the multicast group.
2. **Publish-Subscribe Model:** The publish-subscribe model is widely used in mobile computing for data dissemination. In this model, data publishers publish information, and interested mobile devices subscribe to specific topics or content types. When new data becomes available, the publisher notifies the subscribed devices, ensuring efficient and targeted data dissemination.

3. **Content Caching and Prefetching:** To enhance data dissemination in mobile computing, content caching and prefetching techniques are employed. Caching involves storing frequently accessed data at strategic locations within the network, allowing mobile devices to retrieve the data locally instead of fetching it from the original source. Prefetching anticipates the data needs of mobile devices based on their behavior and proactively delivers relevant data in advance.
4. **Adaptive Data Dissemination:** Mobile computing environments are dynamic, and network conditions may vary. Adaptive data dissemination techniques adjust data delivery strategies based on factors such as device location, network connectivity, and resource availability. These techniques ensure optimal data dissemination by adapting to changing mobile conditions.
5. **Quality of Service (QoS) Considerations:** Data dissemination in mobile computing involves considering QoS requirements. Different data types may have specific QoS needs, such as real-time data requiring low latency and high reliability. QoS-aware data dissemination techniques prioritize and allocate network resources accordingly to meet these requirements.
6. **Energy Efficiency:** Energy efficiency is a critical consideration in data dissemination for mobile devices, as they have limited battery resources. Energy-efficient techniques, such as data compression, selective data transmission, and duty cycling, are employed to minimize energy consumption during data dissemination.
7. **Security and Privacy:** Data dissemination in mobile computing must address security and privacy concerns. Encryption, authentication, and access control mechanisms are implemented to ensure data confidentiality and integrity. Privacy-preserving techniques are used to protect sensitive user information during data dissemination.
8. **Network Infrastructure Support:** Efficient data dissemination in mobile computing often relies on an underlying network infrastructure, such as cellular networks or Wi-Fi access points. These infrastructures provide the necessary connectivity and coverage to deliver data to mobile devices efficiently.

Cache Consistency

Cache consistency in mobile computing refers to the synchronization and maintenance of data consistency between cached copies of data and the original source of data in a distributed mobile environment. It ensures that mobile devices accessing cached data receive accurate and up-to-date information.

Here are some key points about cache consistency in mobile computing:

1. **Data Replication:** Caching involves creating copies of data items in multiple caches distributed across the mobile network. Data replication improves data availability and reduces access latency by bringing data closer to mobile devices.
2. **Cache Invalidation:** Cache invalidation is the process of detecting and removing stale or outdated data from the cache. It occurs when the original data is updated or modified. Cache invalidation ensures that mobile devices retrieve the most recent version of data.
    1. **Cache Invalidation Techniques:** Different cache invalidation techniques are used to maintain cache consistency. These

techniques include:
a. Write-Through: In write-through invalidation, updates made to the original data source are immediately propagated to the caches, ensuring that caches always hold the most recent data.
b. Write-Invalidate: In write-invalidate invalidation, when the original data is updated, a notification is sent to the affected caches, instructing them to invalidate their copies of the data.
c. Time-to-Live (TTL): In TTL-based invalidation, each cached data item is assigned a time-to-live value, indicating how long the data remains valid in the cache. After the TTL expires, the data is considered stale and is invalidated.

3. **Cache Coherency Protocols:** Cache coherency protocols ensure that multiple caches holding copies of the same data remain consistent with each other and with the original data source. These protocols define rules and mechanisms for maintaining consistency during cache updates, data invalidation, and data access.
4. **Consistency Models:** Consistency models define the level of consistency guaranteed by cache systems. Common consistency models include strong consistency, weak consistency, and eventual consistency. The choice of the consistency model depends on the application requirements and trade-offs between performance and data accuracy.
5. **Network Latency and Disconnections:** In mobile computing, network latency and frequent disconnections pose challenges to cache consistency. Delayed updates and intermittent connectivity may result in inconsistencies between cached data and the source. Mechanisms like cache synchronization and conflict resolution are employed to handle these challenges.
6. **Conflict Resolution:** Conflicts may arise when multiple mobile devices concurrently access and update cached data. Conflict resolution mechanisms resolve conflicts by applying specific rules or policies, such as last write wins or merging conflicting updates.

Mobile database

A Mobile database is a database that can be connected to a mobile computing device over a mobile network (or wireless network). Here the client and the server have wireless connections. In today's world, mobile computing is growing very rapidly, and it is huge potential in the field of the database. It will be applicable on different-different devices like android based mobile databases, iOS based mobile databases, etc. Common examples of databases are Couch base Lite, Object Box, etc.

Features of Mobile database :

Here, we will discuss the features of the mobile database as follows.

- A cache is maintained to hold frequent and transactions so that they are not lost due to connection failure.

- As the use of laptops, mobile and PDAs is increasing to reside in the mobile system.
- Mobile databases are physically separate from the central database server.
- Mobile databases resided on mobile devices.
- Mobile databases are capable of communicating with a central database server or other mobile clients from remote sites.
- With the help of a mobile database, mobile users must be able to work without a wireless connection due to poor or even non-existent connections (disconnected).
- A mobile database is used to analyze and manipulate data on mobile devices.

Mobile Database typically involves three parties :

1. **Fixed Hosts –**
   It performs the transactions and data management functions with the help of database servers.

2. **Mobiles Units –**
   These are portable computers that move around a geographical region that includes the cellular network that these units use to communicate to base stations.

3. **Base Stations –**
   These are two-way radios installation in fixed locations, that pass communication with the mobile units to and from the fixed hosts.

Limitations :

Here, we will discuss the limitation of mobile databases as follows.

- It has Limited wireless bandwidth.
- In the mobile database, Wireless communication speed.
- It required Unlimited battery power to access.
- It is Less secured.
- It is Hard to make theft-proof.

Mobile Database Research Directions

Research in mobile databases focuses on addressing the unique challenges and requirements associated with managing data in mobile computing environments. Here are some research directions in the field of mobile databases:

1. **Data Management for Mobile Applications:** Research is needed to develop efficient data management techniques for mobile applications. This includes designing lightweight data models, query processing algorithms, and transaction management mechanisms that are tailored to the limited resources and intermittent connectivity of mobile devices.

2. **Context-Aware Data Management**: Context-awareness is a crucial aspect of mobile computing. Research is exploring techniques to capture, manage, and utilize contextual information (e.g., location, time, user preferences) to enhance data management in mobile databases. This involves context-aware data modeling, adaptive query processing, and personalized data delivery.

3. **Energy-Efficient Data Management:** Energy efficiency is a critical concern in

mobile computing due to limited battery life. Research is focused on developing energy-aware techniques for data storage, retrieval, and processing. This includes energy-efficient indexing, caching, compression, and query optimization strategies to minimize energy consumption in mobile devices.

4. **Data Synchronization and Replication:** Mobile devices frequently operate in disconnected or weakly connected environments. Research is exploring efficient techniques for data synchronization and replication, ensuring that data updates are propagated reliably and consistently across distributed mobile databases once connectivity is restored.

5. **Data Security and Privacy:** Mobile devices often contain sensitive data, making security and privacy paramount. Research is investigating techniques for secure data storage, secure data transmission, access control, and privacy-preserving data management in mobile databases. This includes encryption, authentication, anonymization, and data obfuscation methods.

6. **Mobile Cloud Databases:** Mobile devices can leverage cloud resources for data storage and processing. Research is focusing on integrating mobile devices with cloud databases, enabling offloading of data and computation-intensive tasks to the cloud. This includes data partitioning, load balancing, and query optimization techniques for efficient utilization of cloud resources.

7. **Mobile Edge Computing:** Mobile edge computing brings computation and data storage closer to the mobile devices at the network edge. Research is exploring how to leverage edge computing infrastructure for efficient data management in mobile databases. This includes edge caching, distributed query processing, and edge-assisted data analytics.

8. **Data Dissemination and Sharing:** Mobile devices often need to share data with other devices or users. Research is investigating efficient data dissemination and sharing mechanisms in mobile databases. This includes peer-to-peer data sharing, data broadcasting, and content-based data routing techniques.

9. **Mobile Database Performance Evaluation:** Evaluating the performance of mobile databases is crucial for understanding their limitations and identifying areas for improvement. Research is focused on developing benchmarks, metrics, and simulation models to assess the performance of mobile database systems under various workloads, network conditions, and data management strategies.

Security Fault Tolerance for Mobile N/W.

Security fault tolerance for mobile networks refers to the ability of a mobile network to maintain its security posture and functionality even in the presence of security breaches or faults. It involves designing and implementing mechanisms that can detect, respond to, and recover from security incidents, ensuring the continuity and resilience of the network.
Here are some key aspects of security fault tolerance in mobile networks:

1. **Intrusion Detection Systems (IDS):** Deploying IDSs in mobile networks can help detect unauthorized activities or attacks. IDSs monitor network traffic, analyze patterns, and raise alerts when suspicious behavior is detected. By promptly identifying security breaches, network administrators can take appropriate actions to mitigate the impact.

2. **Intrusion Prevention Systems (IPS):** IPSs complement IDSs by not only detecting security breaches but also actively preventing them. IPSs can block malicious traffic, apply access control policies, and enforce security measures in real-time to maintain the network's security posture.

3. **Redundancy and Backup Systems:** Mobile networks should have redundancy and backup mechanisms in place to ensure fault tolerance. This includes redundant network components, backup servers, and distributed data storage to minimize the impact of security incidents. Redundancy helps maintain network availability and functionality even if certain components are compromised.

4. **Disaster Recovery Planning:** Mobile networks should have comprehensive disaster recovery plans that outline procedures for responding to security incidents, such as data breaches or network disruptions. These plans define roles, responsibilities, and communication channels to facilitate effective incident response, containment, and recovery.

5. **Encryption and Secure Communication:** Strong encryption mechanisms should be employed to secure data transmission and communication in mobile networks. Encryption helps protect data confidentiality and integrity, preventing unauthorized access or tampering of sensitive information.

6. **Access Control and Authentication:** Robust access control mechanisms and user authentication protocols should be implemented to ensure that only authorized users can access network resources. This includes password-based authentication, two-factor authentication, and role-based access control (RBAC) to enforce security policies.

7. **Security Monitoring and Logging:** Mobile networks should have robust monitoring and logging mechanisms in place to track and record security-related events. Monitoring tools can provide real-time visibility into network activities, while log files capture critical information for forensic analysis and post-incident investigations.

8. **Incident Response and Recovery:** Mobile networks should have well-defined incident response procedures to handle security incidents promptly and effectively. This involves isolating compromised systems, patching vulnerabilities, restoring services from backups, and conducting thorough investigations to understand the root cause of the incident.

9. **Security Auditing and Testing:** Regular security auditing and penetration testing help identify vulnerabilities and weaknesses in mobile networks. By conducting comprehensive assessments, network administrators can proactively address security flaws, apply necessary patches and updates, and improve the overall security posture.

10. **Security Awareness and Training:** Mobile network users and administrators should receive adequate security awareness and training to understand potential threats, best practices, and response procedures. Educating users about secure behavior and promoting a security-conscious culture is essential for maintaining security fault tolerance.

Introduction of Mobile Ad hoc

Network (MANET)

Mobile Adhoc Network (MANET) is a wireless network made up of a collection of mobile nodes connected wirelessly and free of any fixed infrastructure. It is self-configuring and self-healing. MANET provides a lot of benefits, but it also has several drawbacks that need to be fixed. Researchers are always trying to make MANET's features better in order to get over these constraints. Future advancements in new technology and methodologies might make MANET a dependable and effective wireless network.

- MANET stands for Mobile Adhoc Network, also known as a wireless Adhoc network or Adhoc wireless network.
- MANET consists of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without a fixed infrastructure.
- MANET nodes are free to move randomly, resulting in a frequently changing network topology.
- Each node in MANET behaves as a router, forwarding traffic to other specified nodes in the network.
- MANET can operate in a standalone fashion or be part of a larger internet.
- MANET forms a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes.
- The main challenge in MANET is to equip each device with the ability to continuously maintain the information required for proper traffic routing.
- MANETs were prevalent from 2000 to 2015 and typically operate at radio frequencies ranging from 30MHz to 5GHz.
- MANETs have various applications in areas such as road safety, environmental sensing, home automation, healthcare, disaster rescue operations, defense (air/land/navy), weapons, robotics, etc.

Characteristics of MANET –

- **Dynamic Topologies:**
  Network topology which is typically multihop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.
- **Bandwidth constrained, variable capacity links:**
  Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to a wired network
- **Autonomous Behavior:**
  Each node can act as a host and router, which shows its autonomous behavior.
- **Energy Constrained Operation:**
  As some or all the nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized by less memory, power, and lightweight features.
- **Limited Security:**
  Wireless networks are more prone to security threats. A centralized firewall is absent due to the distributed nature of the operation for security, routing, and host configuration.
- **Less Human Intervention:**
  They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

Pros and Cons of MANET –

Pros:

1. Separation from central network administration.
2. Each node can play both the roles ie. of router and host showing autonomous nature.

3. Self-configuring and self-healing nodes do not require human intervention.
4. Highly scalable and suits the expansion of more network hub.

Cons:

1. Resources are limited due to various constraints like noise, interference conditions, etc.
2. Lack of authorization facilities.
3. More prone to attacks due to limited physical security.
4. High latency i.e. There is a huge delay in the transfer of data between two sleeping nodes.

Advantages:

Flexibility: MANETs are highly flexible, as they can be easily deployed in various environments and can be adapted to different applications and scenarios. This makes them ideal for use in emergency situations or military operations, where there may not be a pre-existing network infrastructure.

Scalability: MANETs can easily scale to accommodate a large number of nodes, making them suitable for large-scale deployments. They can also handle dynamic changes in network topology, such as the addition or removal of nodes.

Cost-effective: Since MANETs do not require any centralized infrastructure, they are often more cost-effective than traditional wired or wireless networks. They can also be used to extend the range of existing networks without the need for additional infrastructure.

Rapid Deployment: MANETs can be rapidly deployed in areas where infrastructure is not available, such as disaster zones or rural areas.

Disadvantages:

Security: MANETs are vulnerable to security threats, such as attacks by malicious nodes, eavesdropping, and data interception. Since the network is decentralized, there is no central authority to ensure the security of the network.

Reliability: MANETs are less reliable than traditional networks, as they are subject to interference, signal attenuation, and other environmental factors that can affect the quality of the connection.

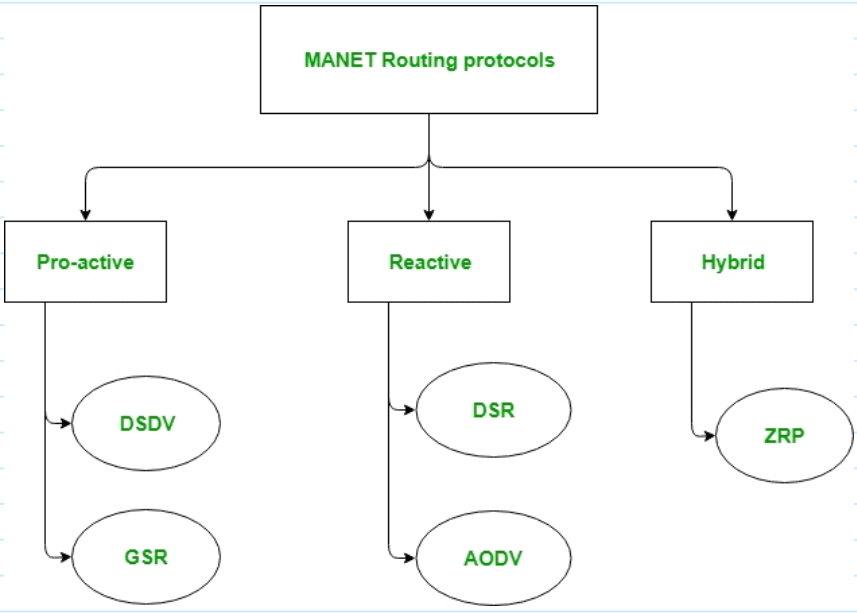
Bandwidth: Since MANETs rely on wireless communication, bandwidth can be limited. This can lead to congestion and delays, particularly when multiple nodes are competing for the same channel.

Routing: Routing in MANETs can be complex, particularly when dealing with dynamic network topologies. This can result in inefficient routing and longer delays in data transmission.

Power Consumption: Since MANETs rely on battery-powered devices, power consumption can be a significant issue. Nodes may need to conserve power to extend the life of the battery, which can limit the amount of data that can be transmitted.

MANET Routing Protocols

In Mobile Ad hoc Network (MANET), nodes do not know the topology of their network, instead they have to discover it by their own as the topology in the ad-hoc network is dynamic topology. The basic rules is that a new node whenever enters into an ad-hoc network, must announce its arrival and presence and should also listen to similar announcement broadcasts made by other mobile nodes.



1. Pro-active routing protocols: These are also known as table-driven routing protocols.

- Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes.
- Since the topology in the mobile ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes.
- It has a limitation that it doesn't work well for the large networks as the entries in the routing table becomes too large since they need to maintain the route information to all possible nodes.

a. **Destination Sequenced Distance Vector Routing Protocol (DSDV):**
   - Pro-active/table driven routing protocol.
   - Extends the distance vector routing protocol of wired networks.
   - Based on the Bellman-Ford routing algorithm.
   - Developed to address the count-to-infinity problem in mobile ad-hoc networks.
   - Each routing entry in the routing table includes a destination sequence number.
   - Updates are included in the routing table only if they have a higher sequence number.
   - Ensures a loop-free and consistent view of the network.

b. **Global State Routing (GSR):**
   - Pro-active/table driven routing protocol.

- Extends the link state routing of wired networks.
- Based on Dijkstra's routing algorithm.
- Developed to address the global flooding issue in mobile ad-hoc networks.
- Each node maintains an adjacency list, topology table, next hop table, and distance table.
- Does not flood link state routing packets globally into the network.
- Provides a more efficient and controlled dissemination of routing information.

2. Reactive routing protocols: These are also known as on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network. It consists of two major phases namely, route discovery and route maintenance.

1. **Dynamic Source Routing protocol (DSR):**

- It is a reactive/on-demand routing protocol.
- In this type of routing, the route is discovered only when it is required/needed
- The process of route discovery occurs by flooding the route request packets throughout the mobile network.

  It consists of two phases:
  - **Route Discovery:** This phase determines the most optimal path for the transmission of data packets between the source and the destination mobile nodes.
  - **Route Maintenance:** This phase performs the maintenance work of the route as the topology in the mobile ad-hoc network is dynamic in nature and hence, there are many cases of link breakage resulting in the network failure between the mobile nodes.

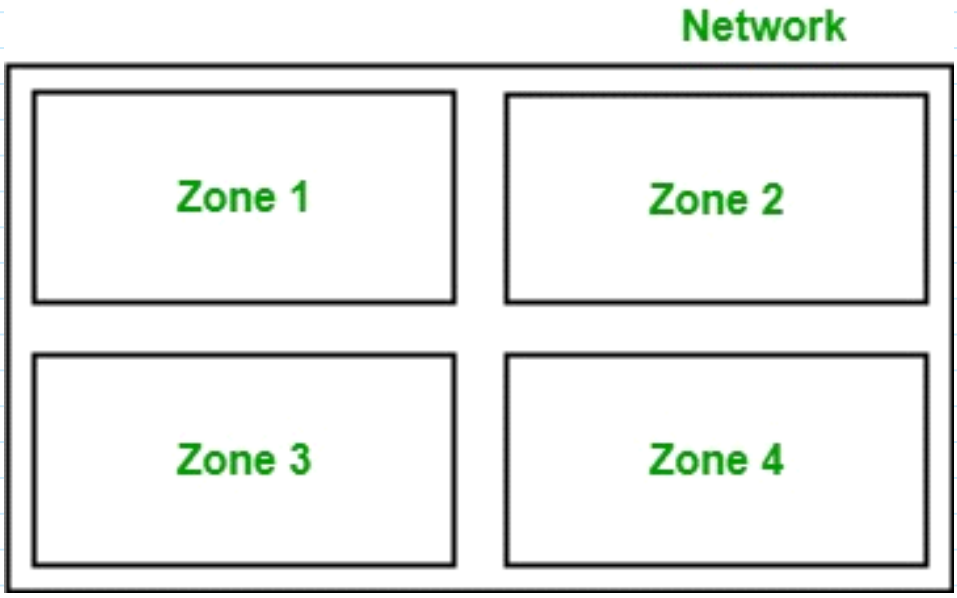
2. **Ad-Hoc On Demand Vector Routing protocol (AODV):**

   - Reactive/on-demand routing protocol.
   - Extends the Dynamic Source Routing (DSR) protocol and addresses its disadvantages.
   - In DSR, the complete path is included in the data packet's header, resulting in increased header size and network congestion as the network size grows.
   - AODV stores the path in the routing table instead of the data packet's header.
   - Reduces the overhead of data packet headers and improves network performance.
   - Operates in two modes: route discovery and route maintenance.
   - Route discovery is initiated when a source node needs to send data to a destination node for which it has no route.
   - Route maintenance involves monitoring the stability of established routes and making necessary updates or repairs as needed.

3. Hybrid Routing protocol: It basically combines the advantages of both,

reactive and pro-active routing protocols. These protocols are adaptive in nature and adapts according to the zone and position of the source and destination mobile nodes. One of the most popular hybrid routing protocol is **Zone Routing Protocol (ZRP)**.

The whole network is divided into different zones and then the position of source and destination mobile node is observed. If the source and destination mobile nodes are present in the same zone, then proactive routing is used for the transmission of the data packets between them. And if the source and destination mobile nodes are present in different zones, then reactive routing is used for the transmission of the data packets between them.



Characteristics of MANET Routing Protocol:

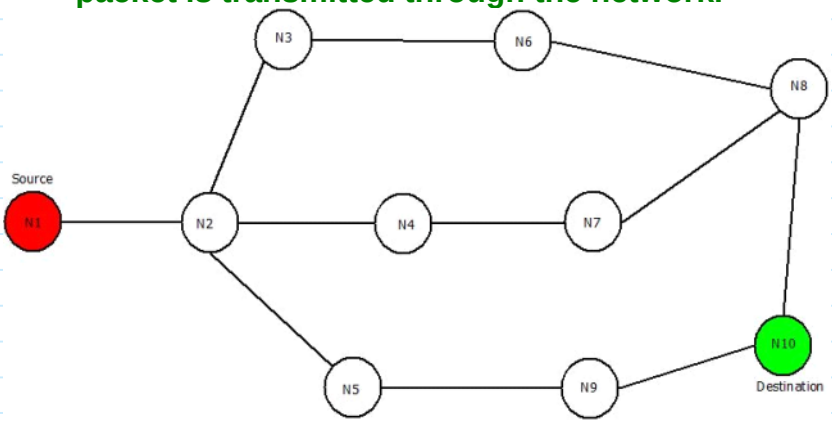
To avoid the problems with routing in MANET, routing protocols should have following characteristics:

- It should be widely distributed.
- It must be localized.
- Because of nodes mobility, it should be adjustable to frequent change in topology.
- It must be free of impermeable routes.
- The convergence of routes must be fast.
- Each node in the network should be required to store information about the network's stable local topology.
- It should be able to provide high-quality service

Dynamic Source Routing Protocol : Working

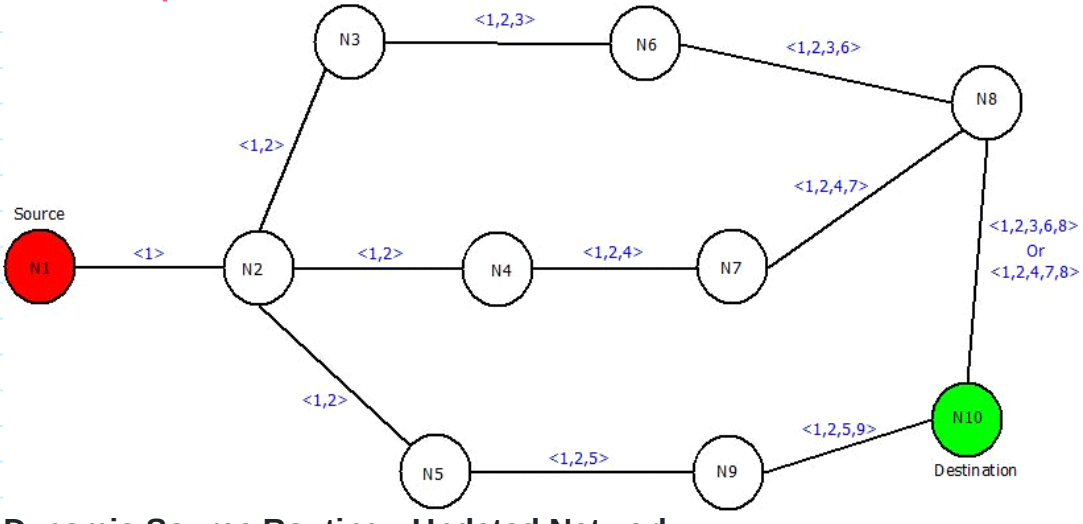
- **Dynamic Source Routing does broadcast the route to its neighbors but does not floods the information. It only trace the route by calculating the total distance or by calculating the number of nodes present in between source and destination nodes.**
- **Consider a network containing 10 nodes where node N1 being the source and node N10 being the destination nodes. Below mentioned**

steps will let you know how DSR protocol works and how Re-Request packet is transmitted through the network.



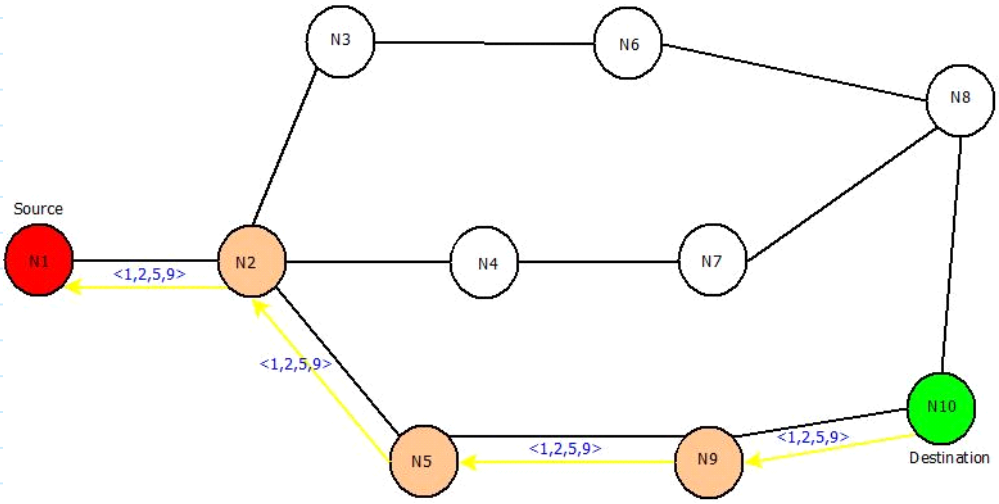
Dynamic Source Routing : Network

- **Step 1**: Start from source node N1 and broadcast the information about it to its neighbors i.e. in this case the route information is "**<1>**", because of its one-to-one link between node N1 and N2.
- **Step 2**: Broadcast previous route information to neighbors of node N2 i.e. to node N3, N4, N5. The new route will remain same "**<1,2>**" in all the cases.
- **Step 3**: Take node N3 and broadcast previous route(<1,2>) to next neighboring nodes i.e. node N6. New route till node N6 will be "**<1,2,3>**" and same process can be done for other nodes i.e. Node N4 and N5.
- **Step 4** : Further, broadcast the new routes i.e. **<1,2,3,6>** , **<1,2,4>** , **<1,2,5>** to nodes N8, N7 & N9 respectively.
- **Step 5**: Repeat the above steps until destination node is reached via all the routes.
- The updated routes will be as:



Dynamic Source Routing : Updated Network

- After this, "**Re-Request**" packet will be sent in backward direction i.e. from destination node "N10" to source node "N1". It will trace the shortest route by counting the number of nodes from route discovered in previous steps.
- The three possible routes are :
  - **Route 1**: **<1,2,3,6,8>**
  - **Route 2**: **<1,2,4,7,8>**
  - **Route 3**: **<1,2,5,9>**
- **Route 3** i.e. "**<1,2,5,9>**" will be chosen as it contains the least number of nodes and hence it will definitely be the shortest path and then data can be transferred accordingly.
- The Re-Request Packet route can be located as:



Dynamic Source Routing

Advantages : Dynamic Source Routing Protocol

- **A perfect route is discovered always.**
- **Highly efficient.**
- **Low bandwidth Consumption.**

Disadvantages : Dynamic Source Routing Protocol

- **If the route gets broke, data transmission cannot happen.**
- **Time taking algorithm-Slow.**
- **If network is large , then it is impossible for the data packets header to hold whole information of the routes.**

Route Maintenance in Mobile Ad-hoc Networks:

- Route maintenance is an important aspect of routing in mobile ad-hoc networks (MANETs).
- It involves monitoring the stability and availability of established routes between nodes.
- Route maintenance mechanisms ensure that the network adapts to changes such as node mobility, link failures, and network congestion.
- When a route becomes unstable or breaks due to node movement or link failure, route maintenance mechanisms are responsible for finding and establishing a new route.
- Route maintenance protocols aim to minimize disruptions in network connectivity and ensure efficient and reliable packet delivery.

Routing Errors in Mobile Ad-hoc Networks:

- Routing errors can occur in mobile ad-hoc networks due to various reasons.
- One common type of routing error is a broken route, where the path between a source and destination node is no longer valid or functional.
- Broken routes can result from node mobility, link failures, node failures, or network congestion.
- Another type of routing error is a routing loop, where packets are stuck circulating between a set of nodes without reaching the destination.
- Routing loops can occur due to incorrect routing table entries or inconsistencies in route updates.
- Routing errors can lead to packet loss, increased latency, and reduced network performance.
- To mitigate routing errors, MANETs employ various mechanisms such as route

discovery, route maintenance, and error detection and correction techniques.

Fisheye State Routing (FSR)

Fisheye Routing (FSR) is a distance-vector routing protocol designed for mobile ad-hoc networks (MANETs). It is named "fisheye" because it focuses on optimizing routing information in the immediate vicinity of a node, while gradually reducing the level of detail as the distance from the node increases. Here are some key points about Fisheye Routing:

- Fisheye Routing aims to reduce the overhead of routing updates and improve scalability in large and dynamic networks.
- It employs a technique called "fisheye" to selectively update and exchange routing information based on the proximity of nodes.
- FSR divides the network into multiple levels, where each level represents a different degree of network visibility from a node's perspective.
- Nodes maintain routing tables with different levels of granularity, depending on the distance from the node.
- Nodes exchange routing updates with their immediate neighbors more frequently and with more detailed information, while updates for more distant nodes are less frequent and less detailed.
- This hierarchical approach allows FSR to focus on the local neighborhood while reducing the overhead of maintaining and updating routing information for distant nodes.
- FSR uses a combination of sequence numbers and timers to manage the freshness of routing information and ensure consistency across the network.
- It is designed to adapt to changes in network topology, including node mobility, link failures, and network partitions.
- Fisheye Routing can provide efficient and scalable routing in large-scale MANETs, especially in scenarios where the network topology changes frequently.

Ad-hoc on Demand Distance Vector (ADDV).

Ad-hoc On-Demand Distance Vector (AODV) is a reactive/on-demand routing protocol designed for mobile ad-hoc networks (MANETs). It is based on the distance vector algorithm and is specifically designed to establish routes on-demand as needed. Here are some key points about AODV:

- AODV operates on the principle of route discovery and route maintenance.
- When a source node wants to send data to a destination node for which it has no route information, it initiates a route discovery process.
- During the route discovery process, the source node broadcasts a Route Request (RREQ) packet to its neighboring nodes, which further broadcast the RREQ until it reaches the destination or an intermediate node with a fresh route to the destination.
- Once the RREQ reaches the destination or an intermediate node with a route to the destination, a Route Reply (RREP) packet is sent back to the source node, establishing the route.
- The route is then maintained by periodic route updates and route maintenance mechanisms to adapt to changes in the network, such as node mobility and link failures.
- AODV utilizes sequence numbers to ensure loop-free and up-to-date routing information.

- It supports both unicast and multicast communication in MANETs.
- AODV is known for its low routing overhead and fast convergence time in dynamic and highly mobile networks.
- It is widely implemented and used in various MANET applications, including military, disaster management, and vehicular networks.