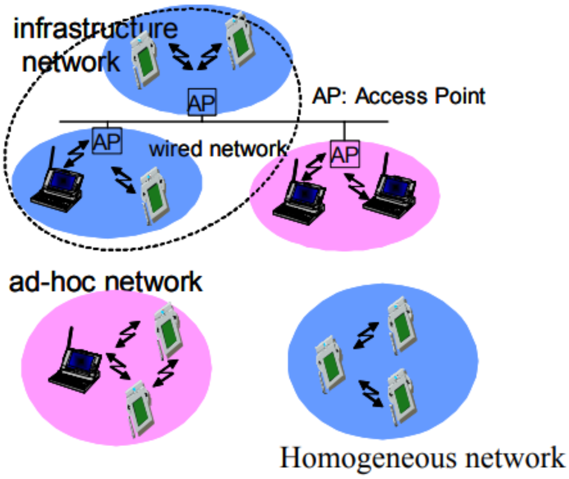
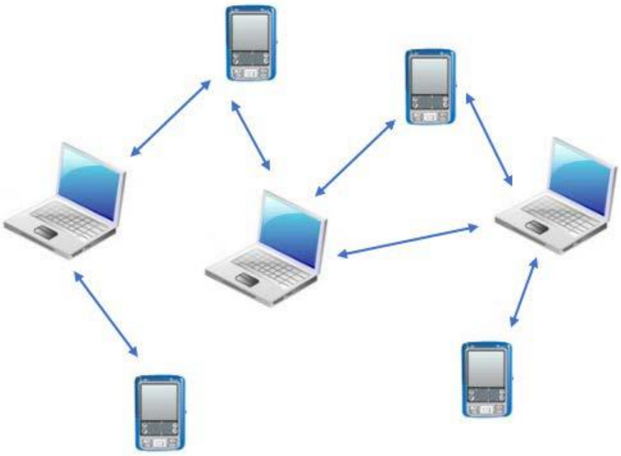
Mobile Ad-Hoc Networks

Ad hoc networks are created between two or more wireless PCs together, without the use of a wireless router or an access point. The computers communicate directly with each other. **Ad hoc networks** can be very helpful during meetings or in any location where a **network** doesn't exist and where people need to share files.

- **Ad hoc network** is often local area **network** or other small area **network** formed by wireless devices. It is a network without any base stations "infrastructure-less" or multi-hop. It is a collection of two or more devices equipped with wireless communications and networking capability. Supports anytime and anywhere computing.
- Two topologies:
  - ❍ Heterogeneous (left) • Differences in capabilities.
  - ❍ Homogeneous or fully symmetric (Right) • all nodes have identical capabilities and responsibilities.





A **Mobile Ad Hoc Network** (MANET) is an interconnected system of **wireless** nodes which communicate over bandwidth- constrained **wireless** links. Each **wireless** node can function as a sender, a receiver or a router. When the node is a sender, it can send messages to any specified destination node through some route.

- (Mobile Ad-Hoc NETwork) a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of centralized infrastructure (access points, bridges, etc.)

A **mobile ad hoc network (MANET)** is a continuously self-configuring, self-organizing, infrastructure-less **network** of **mobile** devices connected without wires. It is sometimes known as "on-the-fly" **networks** or "spontaneous **networks**".

Ad hoc is a word that originally comes from Latin and means "for this" or "for this situation." In current American English it is used to describe something that has been formed or used for a special and immediate purpose, without previous planning.

- **Autonomous terminal:** A node may function as both host and a router.
- **Distributed Operations:** since there is no fixed network the control and management operations are distributed among the terminals.
- **Multi-hop routing:** packets should be delivered via one or more nodes.
- **Dynamic network topology**: As the network change rapidly, the mobile nodes dynamically establish routing among themselves i.e. they form their own network
- **Fluctuating link capacity**: One end-to-end path can be shared by several sessions.
- **Light-weight terminal**: The MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage.

Definition

- "A collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services."
- Ad-hoc network topology is dynamic—nodes enter and leave the network continuously
- No centralized control or fixed infrastructure to support network configuration or reconfiguration

Example scenarios for MANETs

- Meetings
- Emergency or disaster relief situations
- Military communications
- Wearable computers
- Sensor networks

Types of Wireless Ad Hoc Networks

- Mobile ad hoc network (MANET): An ad hoc network of mobile devices.
- Vehicular ad hoc network (VANET): Used for communication between vehicles. ...
- Smartphone ad hoc network (SPAN): **Wireless** ad hoc network created on smartphones via existing technologies like Wi-Fi and Bluetooth.

Self-Configuring and Self-Healing Processes

Figure bellow shows how ad hoc networks determine their configuration. In Fig. 1a each node identifies the nodes that are available for communications, based on signal strength, which is mainly related to distance, but is also affected by obstructions or interference. Some nodes may be beyond range; others may be detectable but have insufficient signal strength for reliable communications.

Once the available nodes are identified, this information is communicated to other nodes, along with information about the desired destination (Fig. 1b). Using the lists of available connections, the network configuration algorithm selects a particular routing for each user to its destination. This process requires system operating software to have good decision-making algorithms, based on practical criteria for signal strength, path reliability over time, and network configuration patterns.

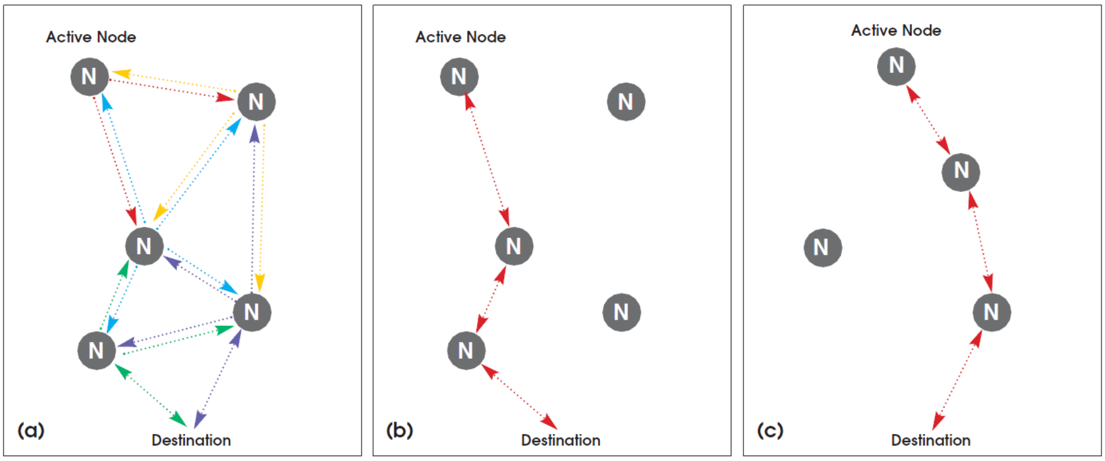


Figure 1 · Creation and adaptation of an ad hoc network: (a) Determination of available nodes, (b) Selection of the optimal routing, and (c) Reconfiguration when the network makeup changes.

Over time, or even near-continuously, the network will change. Users may come and go, nodes may be in motion, or changes in the electromagnetic environment may alter the propagation between nodes. As these changes take place, the network will update its configuration and identify new paths from users to destinations, as illustrated in Fig. 1c. This type of reconfiguration will be repeated over and over as the network changes. Note that this is the same process used in the Internet, where system loading and hardware issues require redirection of a user's data through different routers.

Advantages of Ad Hoc Networks

The principal advantages of an ad hoc network include the following:

- Independence from central network administration (Decreased dependence on infrastructure).
- Self-configuring, nodes are also routers.
- Self-healing through continuous re-configuration.
- Scalable—accommodates the addition of more nodes (Ease of deployment).
- Flexible—similar to being able to access the Internet from many different locations thereby incorporating many different devices and making possible for other users to use available services.
- Speed of deployment.

Limitations of Ad Hoc Networks

there are some limitations:

- Each node must have full performance.
- Throughput is affected by system loading.
- Reliability requires a sufficient number of available nodes. Sparse networks can have problems.
- Large networks can have excessive latency (time delay), which affects some applications.

PROBLEMS IN MANET:

- Routing
- Security and Reliability
- Quality of Service
- Internetworking
- Power Consumption

Routing in Mobile Ad Hoc Networks

Routing is the process of finding the best path for traffic in a network, or across multiple networks. The role of **routing** is similar to the road map for a hotel. In both cases, we need to deliver messages at proper location and in an appropriate way.

An **ad hoc routing** protocol is a standard, that controls how nodes decide which way to route packets between computing devices in a mobile **ad hoc network**. In **ad hoc networks**, nodes are not familiar with the topology of their **networks**.

- Nodes must route packets for other nodes to keep the network fully connected.
- In MANETs, routing must be addressed.

Mobile ad-hoc network comprises of **wireless** nodes that communicate each other by exchanging the information. The path chosen for transferring the information from one node to another node is called **routing** and the **protocols** used is called **routing protocols**.

Route-finding:

- Want to determine an “optimal “way to find “optimal “routes.

Dynamic links

- Broken links must be updated when a node moves out of communication range with another node.
- New links must be formed when a node moves into communication range with another node.
- Based on this new information, routes must be modified.
- Frequency of route changes a function of node mobility.

Route discovery

- Initial discovery of valid route from source to destination.
- Source node can send a query for a destination node.
- Only destination node responds to query.

- If destination located in source’s transmission range, destination responds and link established.
    - No periodic routing updates needed.
    - Approach must be extended to case where destination node not in source node’s transmission range.
- One approach is to perform controlled flooding of the query.
    - Nodes receiving query will append their address to the route being recorded in the packet header and broadcast updated packet to all neighbors.
        - When a node receives a query, it checks to see if its address is already in the header (indicating this packet was already flooded by this node).
        - If address present, node drops packet.

    - Each query labeled with unique “request ID”.
        - Each node keeps a cache with request ID’s of packets it has already forwarded.
        - Discards packets with request ID listed in node’s cache.
        - Avoids duplicate queries sent throughout the network.
    - Node only propagates first copy of each route request packet it sees.

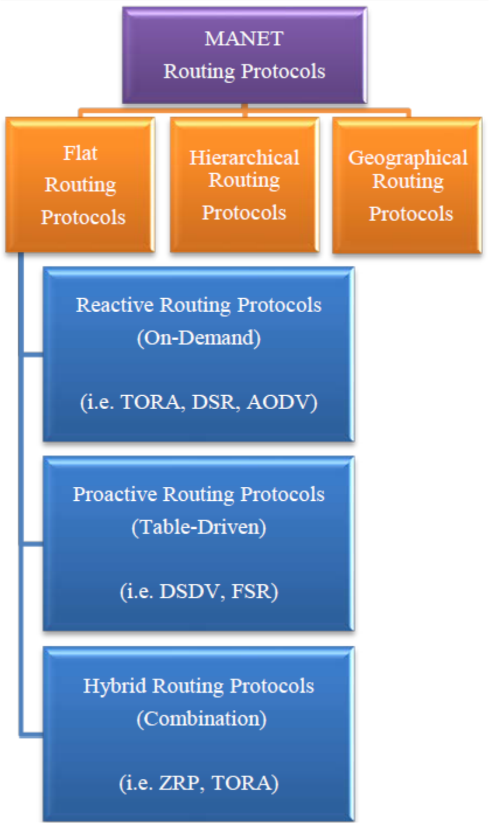
- Typically source and destination will not be far away in an ad-hoc network
    - Can add a TTL (time to live) to route request.
    - Each node reduces the TTL by one when it propagates the request.
    - If the TTL hits zero, the route request packet is dropped.
- When query reaches destination.
    - Destination sends response back using route in packet header if available.
    - Destination sends response back to node from which it received route request.
- Route discovery information can be piggybacked onto data such as TCP connection packets.
    - Reduces latency (e.g., start-up time for TCP connection).
    - Increases overhead, since packets flooded throughout network.
- Intermediate nodes can cache routes discovered.
    - Can use these routes if want to send a packet to a node listed in route.
    - Reduces overhead in terms of number of route request packets required.
- Nodes can operate in “promiscuous” mode
    - Listen to all packets exchanged on network.
    - Cache routes listed in packets.

Route Maintenance

- Nodes can determine broken links through ACK/NACK included with most protocols.
- If link broken

- Node that detects broken link reports this information back to sending node.
- Or node can try to fix the broken link by sending out its own route request to the destination.

- If no ACK/NACK present in the link-layer protocol, nodes can listen to channel to determine if next hop transmits packet or not.
  - If do not hear forwarding of packet, assume link lost.
- Explicit routing acknowledgements can also be used to determine the state of links.


MANET Routing Protocols
Flat Routing Protocols
Hierarchical Routing Protocols
Geographical Routing Protocols
Reactive Routing Protocols (On-Demand) (i.e. TORA, DSR, AODV)
Proactive Routing Protocols (Table-Driven) (i.e. DSDV, FSR)
Hybrid Routing Protocols (Combination) (i.e. ZRP, TORA)

MANET Routing Protocols

Proactive vs. Reactive Routing

Proactive (table driven) routing protocol

- In proactive routing, each node has one or more tables that contain the latest information of the routes to any node in the network.
- nodes continuously evaluate and update routes
  - Periodic updates.
  - Triggered updates—when a link changes.
  - Efficient if routes used often.
  - Large amount of overhead.
  - Similar to conventional routing protocols.
- Proactive routing protocols
  - DSDV ((Destination-sequenced distance-vector)).
  - CGSR ((Cluster head Gateway Switch Routing)).

Reactive (on-demand) routing protocol

In reactive routing protocols, a node initiates a route discovery, only when it wants to send packet to its destination. Routes created only when needed. They do not maintain or constantly update their route tables with the latest route topology.

- Therefore, the communication overhead is reduced but the delay is increased due the on-demand route establishment process.
- nodes evaluate and update routes only when they are needed
  - When a node has a packet to send, it checks to see if it has a valid route.
  - If no valid route known, node must send out a route-request message to obtain a valid route (controlled flooding of the network).
  - Data sent using valid route.
  - Efficient if routes not used often.
- Each node maintains consistent, up-to-date routing information in the form of a table with the next-hop to reach every node in the network.
- Changes in link state transmitted throughout the network to update each node's routing table.
- Reactive routing protocols:
  - AODV ((Ad-hoc on-demand distance vector)).
  - DSR ((Dynamic Source Routing)).

Hybrid protocols

- Example: Zone Routing Protocol (intra-zone: proactive; inter-zone: on-demand)

Comparison of Protocols

- **Proactive approaches**
  - More efficient when routes used often
  - Assures routes ready when needed
  - Requires periodic route updates (overhead)
  - Node mobility affects entire network as routing update
- **Reactive approaches**
  - More efficient when routes used occasionally
  - Require node to first find route before data can be transmitted
  - Periodic route updates not required
  - Can have localized route discovery to deal with node mobility

Security in Mobile Ad Hoc Networks

- A major issue in Mobile ad-hoc network is "SECURITY".
- Two approaches in protecting mobile ad-hoc networks
  - **Reactive approach**: Seeks to detect security threats and react accordingly.
  - **Proactive approach**: Attempts to prevent an attacker from launching attacks through various cryptographic techniques.

ISSUES

- Secure Multicasting
- Secure routing
- Privacy-aware Routing
- Key management

- Intrusion detection System

Secure multicasting: Is a communication method where a single data packet can be transmitted from a sender and replicated to a set of receivers.

Secure routing: Most MANET routing protocols are vulnerable to attacks that can freeze the whole network. Need some solutions that work even if some nodes compromised.

Privacy-aware Routing: Building routing protocols that prevent intermediate nodes from performing traffic analysis.
Schemes for minimizing size of crypto-tags (digital signatures) are needed.

Key Management

- □ security goals in MANET are mainly achieved through trusted Certificate Authority (CA).
- □ compromised CA can easily damage the entire network.

Intrusion detection and response schemes: Anomaly detection is difficult in MANETs (ex: types of attacks and their source). collaborative IDS schemes are needed.

GOALS

- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Availability
- Detection and Isolation

Authentication: A node must know the identity of the peer node it is communicating with. Without authentication, an attacker could gain sensitive information and interfere with other nodes

Confidentiality: Ensures certain information is never disclosed to unauthorized entities.

Integrity: Message being transmitted is never corrupted.

Non-Repudiation: The sender cannot later deny sending the information and the receiver cannot deny the reception.

Availability: Nodes should be available for communication at all times. A node need continue to provide services despite attacks.
E.g.: Key management service.

Detection and Isolation: Require the protocol can identify misbehaving nodes and render them unable to interfere with routing.

IDS-MANET

- IDS: Intrusion detection System which is used to detect and report the malicious activity in ad hoc networks.
- Ex: Detecting critical nodes using IDS
- Intrusion Detection System (IDS) can collect and analyze audit data for the entire network.

- Critical node is a node whose failure or malicious behavior disconnects or significantly degrades the performance of the network.
- Packets may be dropped due to network congestion or because a malicious node is not faithfully executing a routing algorithm.
- Researchers have proposed a number of collaborative IDS systems.
- Some of the schemes are neighbor-monitoring, trust-building, and cluster-based voting schemes which are used to detect and report the malicious activity in ad hoc networks.