Mobile Adhoc Networks

Adhoc Wireless Networks

- Historical importance multihop relaying
  - 500 B.C. Darius I (522-486 B.C.) the king of Persia
  - shouting men on tall structures or heights
  - tribal societies with string of repeaters of drums, trumpets or horns
- ALOHAnet
  - Norman Abramson University of Hawaii and Universities of Hawaiian islands
  - single hop wireless communication
- PRNET by DARPA
  - PRNET combination of ALOHA and CSMA
  - radio interface direct sequence spread spectrum
  - designed to self organize, self-configure and
  - detect radio connectivity for dynamic operation of a routing protocol without any support from fixed infrastructure

PRNET Issues

- obtaining, maintaining and utilizing the topology information
- error and flow control over wireless links
- reconfiguration of paths to handle path breaks arising due to the mobility of nodes and routers
- processing and storage capabilities of nodes
- distributed channel sharing
- infrastructure less networks
- DARPA extended work multi-hop wireless network
  - survivable radio networks (SURAN) project
  - adhoc networking with small, low cost, low power devices, scalability and survivability

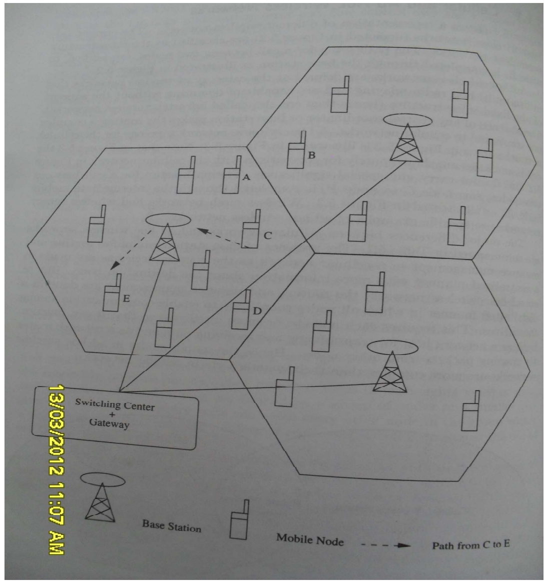
Mobile Adhoc Network (MANET)

- (1980) IETF for mobile adhoc network (MANET)
- 1994 Ericsson proposed Bluetooth for ubiquitous connectivity
- short range, low power, low complexity, inexpensive radio interface
- special interest group (SIG) for Bluetooth
- 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia and Toshiba
- Bluetooth single hop point to point wireless link
  - formation of piconets formed by group of nodes where
  - every node can reach every other node in the group within a single hop
  - multiple piconets forms a scatternet using multi-hop routing protocols

Types of Wireless Network

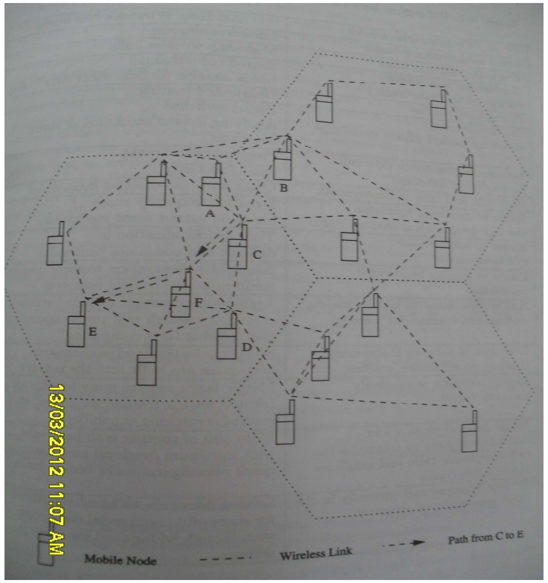
- cellular network having fixed infrastructure
- hybrid network cellular and adhoc
- adhoc networks in presence of infrastructure
- multi-hop cellular networks (MCNs)
- self organizing packet radio and adhoc networks with overlay (SOPRANO)
- QoS, energy efficient, pricing, load balancing cooperative functioning
- comparison with cellular and adhoc wireless network
- multi-hop radio relaying, absence of any central coordinator or base station makes routing complex
- adhoc wireless network: wireless mesh network and sensor network, hybrid architectures

Cellular Network



src: textbook

Adhoc Network



src: textbook

Cellular vs. Adhoc

Cellular Network	Adhoc Network
fixed infrastructure	infrastructure less
single hop link	multi hop link
guaranteed bandwidth	shared radio channel
centralized routing	distributed routing
circuit switched	packet switching
seamless connectivity	frequent path breaks
high cost and time of deployment	quick and cost effective deployment
reuse of frequency spectrum through geographical channel reuse	dynamic frequency reuse based on carrier sense mechanism

Cellular vs. Adhoc

Cellular Network	Adhoc Network
easier to achieve time synchronization	time synchronization is difficult and consumes bandwidth
easier to employ bandwidth reservation	bandwidth reservation requires complex MAC protocols
civilian and commercial applications	battlefields, emergency search and rescue operation, collaborative/distributed computing
high cost of network maintenance	self organization and maintenance properties built into network
mobile hosts - low complexity	mobile host - intelligence, routing/switching capability

Cellular vs. Adhoc

Cellular Network	Adhoc Network
major goals of routing maximize call acceptance and minimize call dropping	main aim of routing to find path with minimum overhead and quick reconfiguration of broken paths
base station simplifies routing and resource management centralized manner	routing and resource management distributed manner and all nodes coordinate

Adhoc Network Examples

- military applications tactical operations
  - in enemy territories, inhospitable terrains
  - coordination of military objects moving at high speeds, real time traffic
  - quick and reliable communication, secure communication
  - adhoc network set up by military tanks may not suffer from power constraint
  - set of wearable devices used by foot soldiers
- multimedia multicasting
  - group of soldiers or set of selected one
- vehicle mounted nodes
  - require high power transceivers, long life batteries - not economical one
  - use of GPS for location tracking or satellite based services

Adhoc Network Examples

- collaborative and distributed computing
  - group of persons to share data on the fly
  - distributed file sharing, streaming of multimedia objects for soft real time communications
  - heterogeneity, interoperability
- emergency operations
  - search and rescue operations, crowd control and commando operations,
  - self configuration, terrain, mobility
  - war, natural calamities - earthquakes,
  - immediate deployment of adhoc networks
  - coordination of functioning, voice communication mainly, fault tolerant communication

Wireless Mesh Networks

- alternate communication infrastructure for mobile or fixed nodes
- provides alternate paths for a data transfer session between a source and destination
- quick reconfiguration, self organization and maintenance
- small radio relaying devices mounted on rooftops of homes or lamp posts
- economical deployment compared cellular network
  - possible deployment residential zones for broadband Internet connectivity,
  - highways communication facility for moving automobiles,
  - business zones for alternate communication system to cellular network
  - university campus

Wireless Mesh Networks

- overcome single or multiple node failures useful in strategic applications
- high data rate, quick and low cost of deployment high scalability and availability
- operate at license free ISM bands around 2.4 GHz and 5 GHz
- data rate 2 Mbps to 60 Mbps depending on technology used for physical layer and MAC layer
- IEEE 802.11a provides maximum data rate 54 Mbps
- smart environment application
  - truck driver for location discovery services
  - support large number of nodes, power control and better throughput
  - high availability against single point failure in cellular network

Wireless Sensor Network

- special category of adhoc network
- tiny devices, sensing physical parameters, data collection, communicating to monitoring station
- temperature, humidity, nuclear radiation, border intrusion, stress on critical structure
- military, health care, home security, environmental monitoring
- issues: mobility of nodes - behavior monitoring of wild animals
- size of network - large number of nodes
- density of deployment - require high availability and making redundancy
- power constraints - harsh environment or geographical conditions, recharging may be impossible
- needs efficient protocols, data link and physical layer

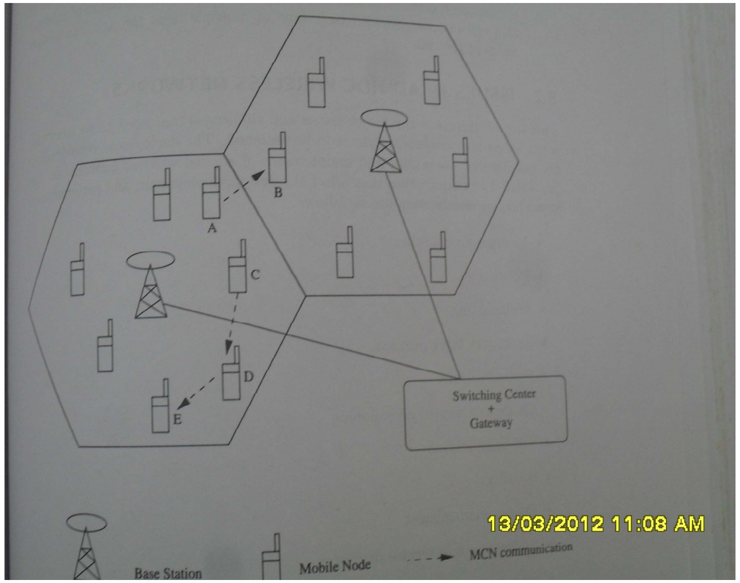
Wireless Sensor Network

- replenishable power source - power source can be replaced when existing source is drained
- non-replenishable power source - only replacement of the node is the only solution
- regenerative power source - using transducers
- data/information fusion - aggregation of information
- data fusion refers to the aggregation of multiple packets into one before relaying it
- traffic distribution - low bandwidth monitoring environmental parameter, military application border intrusions, time constraints for delivery
- in contrast adhoc networks - streaming needs higher bandwidth

Hybrid Wireless Network

- multi hop cellular networks (MCN), integrated cellular adhoc relay networks
- cellular network shrunk cell size, pico cell, channel reuse, cell sectoring, cell resizing, multi tier cells to increase the capacity of cellular networks - increasing equipment cost
- capacity (maximum throughput) of cellular network can be increased if the network incorporates the properties of multi hop relaying along with support of fixed infrastructure
- MCN combines the reliability and support of fixed base stations of cellular networks with flexibility and multi hop relaying of adhoc networks

MCN Architecture



src: textbook

MCN Architecture

- two nodes in the same cell and want to communicate with each other,
- connection is routed through multiple wireless hops over the intermediate nodes
- the base station may or may not be involved in this multi hop path
- for example A node in one cell and B node in another cell, but directly within A's transmission range - can transmit directly
- C node can communicate to E through D where C, D and E are in same cell through D as intermediate relay node
- MCN high capacity lowering cost of communication to less than in single hop cellular network

MCN Architecture: Advantages

- higher capacity than cellular network, better channel reuse, reduction of transmission power
- increased flexibility and reliability in routing
- flexibility in terms of selecting the best suitable nodes for routing, done through multiple mobile nodes or through base station or by a combination of both
- reliability in terms of resilience to failure of base station node can reach other node using multi hop paths
- better coverage and connectivity in holes of a cell can be provided by means of multiple hops through intermediate nodes in the cell

Issues in Adhoc Wireless Networks

- deployment, operation and maintenance, performance
- medium access scheme, routing, multicasting,
- transport layer protocol, pricing scheme
- QoS, self organization, security, energy management,
- addressing and service discovery, scalability
- Medium access scheme
- medium access control (MAC) distributed arbitration for the shared channel for transmission of packets

Issues in Adhoc Wireless Networks: MAC

- distributed operation
  - no centralized coordination,
  - fully distributed involving minimum control overhead,
  - polling based MAC, partial coordination is required
- synchronization
  - time synchronization for TDMA,
  - involves bandwidth and battery power usage,
  - control packets used for synchronization can also increase collisions in the network
- hidden terminals
  - nodes hidden from the sender but reachable to the receiver
  - it can collision at the receiver node reducing throughput of MAC
  - MAC protocol should be able to alleviate the effects of hidden terminals

Issues in Adhoc Wireless Networks: MAC

- exposed terminals
  - nodes are in the transmission range of the sender and
  - are prevented from making a transmission,
  - exposed terminals should be allowed to transmit in a controlled fashion without causing collision
- throughput
  - maximize it, minimizing collision,
  - maximizing channel utilization and minimizing control overhead
- access delay
  - average delay that any packet experiences to get transmitted
- real time traffic support
  - contention based channel access,
  - without any central coordination,
  - with limited bandwidth and with location dependent contention,
  - video, audio etc. needs explicit support from MAC

Issues in Adhoc Wireless Networks: MAC

- fairness
  - ability of MAC to provide an equal share or weighted share of the bandwidth to all competing nodes,
  - it can be node based or flow based;
  - former attempts equal bandwidth share for competing nodes whereas
  - latter provides equal share for competing data transfer
  - important in multi-hop network, unfair relaying load for a node results in draining resources
- resource reservation
  - QoS using parameters bandwidth, delay, jitter requires reservation of resources like bandwidth, buffer space, and processing power
  - difficult task for MAC
- ability to measure resource availability
  - efficient use of bandwidth,
  - estimation of resource availability,
  - making congestion control decision

Issues in Adhoc Wireless Networks: MAC

- capability for power control
  - transmission power control reduces the energy consumption,
  - causes decrease in interference at neighboring nodes and increases frequency reuse
- adaptive rate control
  - variation in data bit rate,
  - higher rate if sender and receiver are nearby and reduce rate if they mover away from each other
- use of directional antenna
  - increases spectrum reuse,
  - reduction in interference, and
  - reduced power consumption, most MACs use omnidirectional

Issues in Adhoc Wireless Networks: Routing

- feasible path to destination based on criteria such as
- hop length, minimum power control, lifetime of link,
- gathering path breaks, utilizing minimum bandwidth, minimum processing power
- Challenges in routing
- mobility
  - results in frequent path breaks, packet collision,
  - transient loops, stale routing information and
  - difficulty in resource reservation
- bandwidth constraint
  - channel shared by all nodes in broadcast region,
  - bandwidth available per link depends on number of nodes and traffic
  - error prone and shared channel - BER is very high - order or 10^{-5} to 10^{-3} compared to wired one - order of 10^{-12} to 10^{-9}
  - signal to noise ratio, path loss for routing

Issues in Adhoc Wireless Networks: Routing

- location dependent contention
  - load varies with the number of nodes present in a given geographical region,
  - makes contention for the channel high when the number of nodes increases
  - high contention results in high number of collisions, wastage of bandwidth
  - good routing protocol - built in mechanisms for distributing the network load uniformly across the network
- other resource constraints
  - computing power, battery power, buffer storage

Issues in Adhoc Wireless Networks: Routing

- major requirements of routing protocol
- minimum route acquisition delay
  - node that does not have a route to particular destination node,
  - should be minimal,
  - varies with size of network and network load
- quick route reconfiguration
  - unpredictable changes in the topology,
  - need to handle path breaks and subsequent packet losses
- loop free routing
  - avoid unnecessary wastage of network bandwidth,
  - due to random movement of nodes, transient loops may form in the route
  - protocol should detect and take corrective actions

Issues in Adhoc Wireless Networks: Routing

- distributing routing approach
  - centralized routing consumes a large amount of bandwidth, as network is fully distributed
- minimum control overhead
  - control packets exchanged for finding a new route and maintaining existing routes should be minimum,
  - consume precious bandwidth and cause collisions, reducing network throughput
- scalability
  - scale and perform efficiently with a large number of nodes,
  - minimize control overhead and adapt to network size

Issues in Adhoc Wireless Networks: Routing

- provisioning of QoS
  - certain level of QoS ad demanded by nodes or category of calls,
  - QoS parameters bandwidth, delay, jitter, packet delivery ratio and throughput, supporting differentiated classes of service
- support for time sensitive traffic
  - support hard real time and soft real time traffic
- security and privacy
  - resilient to threats and vulnerabilities,
  - avoid resource consumption, denial of service,
  - impersonation, and other attacks

Issues in Adhoc Wireless Networks: Multicasting

- important applications: emergency search and rescue operations, military communication
- nodes form a group to carry out certain tasks that require point to multipoint and multipoint to multipoint voice and data communication
- arbitrary movement of nodes changes the topology dynamically in an unpredictable manner
- constraints of power and bandwidth makes multicast routing challenging
- traditional wired multicast protocols e.g. core based trees,
- protocol independent multicast,

Issues in Adhoc Wireless Networks: Multicasting

- distance vector multicast routing protocol do not perform well in adhoc networks
- tree based multicast structure is highly unstable and needs readjustment to include broken links
- link state table results in high control overhead
- single link connectivity among the nodes in multicast group results in tree shaped topology,
- it provides high efficiency with low packet delivery ration due to tree breaks
- multiple links among the nodes in adhoc results in a mesh shaped structure, work well in a high mobility environment

Issues in Adhoc Wireless Networks: Multicasting

- robustness - able to recover and reconfigure from link breaks for use in highly dynamic environments
- efficiency - minimum number of transmissions to deliver a data packet to all the group members
- control overhead - minimal control overhead in scare bandwidth
- QoS - time sensitive for data transferred
- efficient group management - accepting members and maintaining connectivity until session expires, with minimal exchange of control messages
- scalability - able to scale for a network with large number of nodes
- security - authentication for a member, military communications

Issues in Adhoc Wireless Networks: Transport layer protocols

- setting up and maintaining end to end connections, reliable delivery, flow control and connection control
- UDP - connection less transport layer protocol - no flow control and congestion control or reliable data delivery
- congestion at the intermediate links, rate of collision affecting network throughput
- increases contention of links for example,
  - adhoc network employs contention based MAC protocol,
  - nodes in a high contention region experience several backoff states,
  - resulting in increased number of collisions and high latency
  - connection less transport layer unaware of this and increase the load in the network and degrading the performance

Issues in Adhoc Wireless Networks: Transport layer protocols

- degradation of performance due to
  - frequent path breaks,
  - presence of stale routing information,
  - high channel error rate and frequent network partitions
- due to mobility and limited transmission range, experiences frequent path breaks
- each path break results in
  - route reconfiguration, finding alternate path,
  - takes longer time than retransmission timeout,
  - resulting in retransmission of packets and
  - execution of the congestion control algorithm
- congestion control algorithm decreases the size of congestion window, resulting in low throughput and execution of congestion control algorithm on every path break affects throughput

Issues in Adhoc Wireless Networks: Transport layer protocols

- latency associated with reconfiguration of a broken path and the use of route cache result in stale route information - hence,
- the packets will be forwarded through multiple paths to a destination, causing an increase in the number of out-of-order packets
- multipath routing protocol eg. temporally ordered routing algorithm TORA
- split multipath routing SMR; employ multiple paths between source-destination
- out-of-order packet arrival force to generate duplicate acknowledgments on receiving duplicate ACKs the sender invokes the congestion control algorithm

Issues in Adhoc Wireless Networks: Transport layer protocols

- wireless channel - high errors, unreliable, interference, hidden terminals contributes the increased loss of TCP data packets or ACKs
- When the TCP ACK is delayed more than the round trip timeout the congestion control algorithm is invoked
- due to mobility, experiences isolation of nodes, occurrence of partitions
- TCP connection across multiple partitions sender and receiver are in two different partitions, all packets get dropped, resulting in multiple retransmissions of packets and increase number of retransmission timers
- this behavior causes inactivity

Issues in Adhoc Wireless Networks: Pricing scheme

- functioning depends on relaying nodes and willingness to relay traffic of other nodes
- A to B optimal route passes through C, C is not powered on A has to setup costlier non optimal route to B
- affects throughput, consumption of more resources,
- relay node - computing power, battery charge, service compensation and reimbursement
- military mission, rescue operation, law enforcement - no need of pricing scheme
- commercial deployment needs it

Issues in Adhoc Wireless Networks: QoS provisioning

- performance level of QoS, negotiation between host and network
- resource reservation, priority scheduling, call admission control
- QoS per flow, per link, per node
- service provider (network) and host (user) - boundary is blurred
- lack of central coordination and limited resources
- QoS parameters - differs from application to application
  - multimedia applications - bandwidth and delay
  - military applications - security and reliability
  - defense applications - trustworthy intermediate nodes (hosts) and routing through them
  - emergency search and rescue - availability
  - multiple link disjoint paths requirement
  - sensor network - minimum energy consumption, battery life, energy conservation
  - channel utilization, link life, delay for hybrid networks

Issues in Adhoc Wireless Networks: QoS provisioning

- QoS aware routing - use QoS parameters for finding a path, network throughput, packet delivery ratio,
- may be application specific reliability, delay, delay jitter, packet loss rate, BER, and path loss
- bandwidth utilization, selection of path with necessary bandwidth
- Qos framework
- providing required service, serving per session basis or per class basis
- finding all feasible paths that satisfy user requirements
- QoS signaling, QoS MAC, connection admission control, scheduling schemes, resource management
- react to topology change, end to end of service delivered

Issues in Adhoc Wireless Networks: Self organization

- organizing and maintaining network by itself,
- neighbor discovery, topology organization and reorganization
- every node gather this information through periodic transmission of short packets named beacons
- or promiscuous snooping on the channel for detecting activities of neighbors
- certain MAC protocols permit varying transmission power to improve upon spectrum reusability

Issues in Adhoc Wireless Networks: Self organization

- topological organization phase node gathers information about entire network or part of network
- topology reorganization - due to mobility of nodes, failure of nodes, or complete depletion of power sources of the nodes
- exchange of topological information and adaptability
- partitioning or merging of networks requires topological reorganization should be able to do quickly and efficiently

Issues in Adhoc Wireless Networks: Security

- military applications
- lack of any central coordination and shared medium makes more vulnerable for attack
- passive and active attacks
- passive attack malicious nodes to perceive the nature of activities and obtain information
- active attacks disrupt the operation of the network
- external active attack and internal active attack
- nodes that performs internal attack are compromised nodes
- denial of service - makes network resource unavailable for service to other nodes either by consuming the bandwidth or by overloading the system
  - DoS interrupts the operation of network by keeping a target node busy by making it process unnecessary packets

Issues in Adhoc Wireless Networks: Security

- resource consumption - scarce availability of resources makes it an easy target for internal attacks by consuming resources like
- energy depletion - depleting the battery power of critical nodes by directing unnecessary traffic through them
- buffer overflow
  - filling the routing table with unwanted routing entries or
  - by consuming the data packet buffer space with unwanted data
  - can lead to dropping of large number of data packets leading to loss of critical information
- routing table attack
  - lead to preventing a node from updating route information for important destinations and
  - filling the routing table with routes for nonexistent destinations

Issues in Adhoc Wireless Networks: Security

- host impersonation - compromised internal node can act as another node and respond with appropriate control packets to create wrong route entries and can terminate the traffic meant for the intended destination node
- information disclosure - compromised node can act as an informer by deliberate disclosure of confidential information to unauthorized nodes
  - information like traffic between a selected pair of nodes and pattern of traffic changes, periodicity of exchange very valuable for military applications
- interference - jam wireless communication by creating a wide spectrum noise, can be done using a single wide band jammer, sweeping across the spectrum
- MAC and physical layer should be able to handle such external threats