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

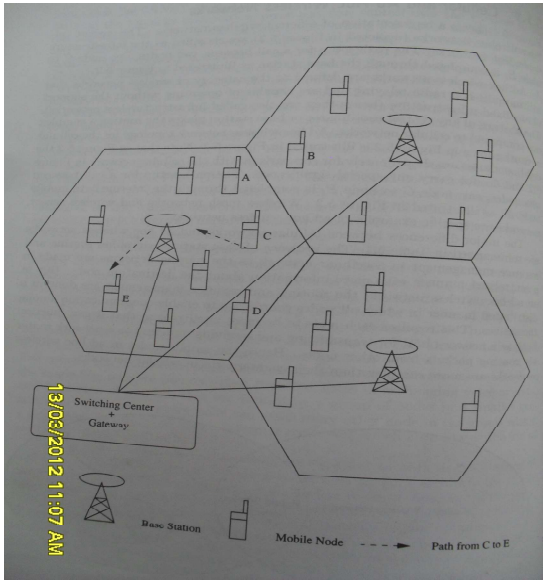
Mobile Adhoc Network (MANET)

- (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

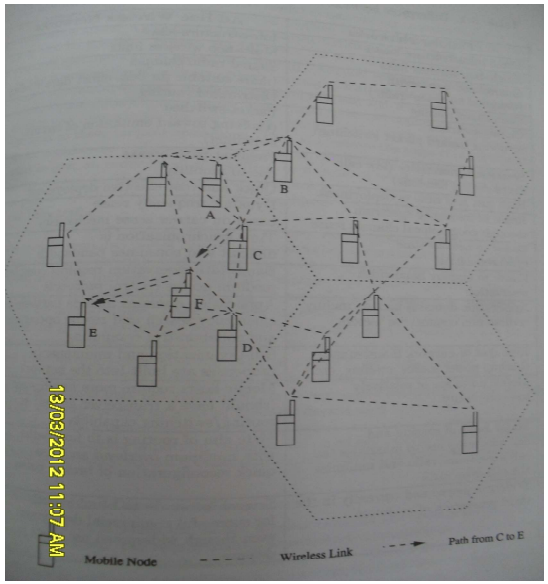
- cellular network having fixed infrastructure
- hybrid network cellular and adhoc
- adhoc networks in presence of infrastructure
- multi-hop cellular networks (MCNs)
- self organizing packet radio and adhoc networks with overlay (SOPRANO)
- QoS, energy efficient, pricing, load balancing cooperative 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

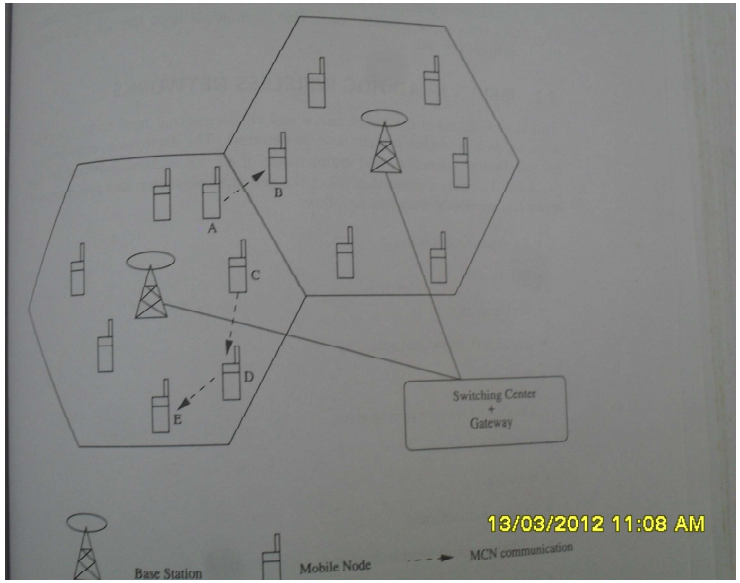
Wireless Sensor Network

- 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

MAC protocols for adhoc wireless networks

- nodes share common broadcast radio channel
- radio spectrum is limited, bandwidth is limited
- shared medium should be controlled in such a manner that all nodes receive a fair share
- node mobility, limited bandwidth, availability, error-prone broadcast channel,
- hidden and exposed terminal problem, power constraints issues compared to wired network
- needs different set of protocols for medium access

Issues: Designing MAC protocols

- bandwidth efficiency
- scarce bandwidth is utilized in an efficient manner
- control overhead involved must be kept as minimal as possible
- bandwidth efficiency defined as ratio of the bandwidth used for actual size data transmission to the total available bandwidth
- MAC protocol maximize the bandwidth efficiency

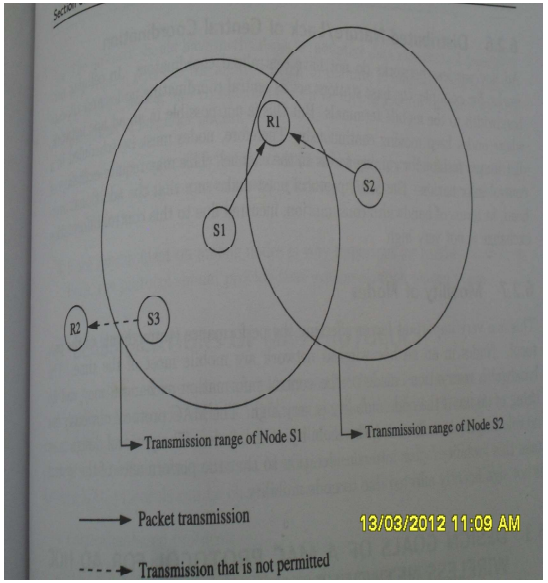
Issues: Designing MAC protocols

- QoS support
- mobility of nodes, bandwidth reservation made at one point of time may become invalid once the node moves out of the region where the reservation was made
- time critical traffic session - military application resource reservation
- synchronization between the node and network, for bandwidth reservation by nodes (time slots),
- exchange of control packets required for achieving time synchronization among nodes
- control packets must not consume too much of network bandwidth

Issues: Designing MAC protocols

- hidden and exposed terminal problems
- unique to wireless networks
- hidden terminal problem refers to the collision of packets at a receiving node due to
- the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver
  - collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other
  - transmit nodes S1 and S2 and receiver node R1

Hidden and Exposed terminal problems



src: textbook

Issues: Designing MAC protocols

- exposed terminal problem refers to the inability of a node which is blocked due to transmission by a nearby transmitting node, to transmit to another node
  - transmission from node S1 to another node R1 is in progress,
  - node S3 can not transmit to node R2 as it concludes that its neighbor node S1 is in transmitting mode and hence it should not interfere with the on-going transmission
- both reduces throughput of a network when the traffic load is high
- MAC protocol should be free from these problems

Issues: Designing MAC protocols

- Error-prone shared broadcast channel
- broadcast nature of the radio channel, i.e.,
  transmission made by a node are received by all nodes within its direct transmission range
- when a node is receiving data, no other in its neighborhood, apart from the sender, should transmit
- node should get access to the shared medium only when its transmissions do not affect any on going session
- multiple nodes may contend for the channel simultaneously, the possibility of packet collision is quite high
- MAC protocol should grant channel access to nodes in such a manner that collisions are minimized
- all nodes are treated fairly with respect to bandwidth allocation

Issues: Designing MAC protocols

- distributed nature/lack of central coordination
- cellular network base station acts as central coordinating nodes and allocate bandwidth to mobile terminals
- nodes must be scheduled in a distributed fashion for gaining access to the channel
- require exchange of control information and it should not be high avoiding bandwidth consumption
- mobility of nodes
  - affecting the performance (throughput) of the protocol
  - the bandwidth reservation or control information exchanged may be of no use if the node mobility is very high
- MAC protocol should consider mobility factor

Design goals of MAC protocol

- operation of protocol should be distributed
- provide QoS for real-time traffic
- access delay for any packet to get transmitted should be low
- efficient utilization of available bandwidth
- fair allocation of bandwidth to nodes
- minimum control overhead
- minimize the effects of hidden and exposed terminal problems
- scalable to large networks

Design goals of MAC protocol

- power control mechanisms to manage energy consumption of the nodes
- adaptive data rate control -
  - ability to control the rate of outgoing traffic considering load in the network and status of neighbor nodes
- try to use directional antenna, reduces interferences, increased spectrum reuse and reduced power consumption
- synchronization among nodes for bandwidth reservation, should provide time synchronization

Classifications of MAC protocols

- several categories based on various criteria such as initiation approach, time synchronization, and reservation approaches
- three basic types
- contention based protocols
- contention based with reservation mechanisms
- contention based with scheduling mechanisms
- and other MAC protocols

Contention based MAC protocols

- contention based channel access policy
- node does not make any resource reservation a priori
- whenever it receives a packet to be transmitted, it contends with its neighbor nodes for access to the shared channel
- these protocols can not provide QoS guarantees to sessions since nodes are not guaranteed regular access to the channel
- random access protocols divided into two types
  - sender initiated protocols - packet transmissions are initiated by the sender node
  - receiver initiated protocols - receiver node initiates the contention resolution protocol

Contention based MAC protocols

- sender initiated protocols divided into two types
  - single channel sender initiated protocols
    - total available bandwidth is used as it is, without being divided;
    - a node that wins the contention to the channel can make use of the entire bandwidth
  - multichannel sender initiated protocols
    - available bandwidth is divided into multiple channels,
    - enables several nodes to simultaneously transmit data, each using separate channel
- some protocols dedicate a frequency channel exclusively for transmitting control information

Contention based MAC protocols with reservation mechanisms

- for supporting real-time traffic; requires QoS guarantees
- nodes are not guaranteed periodic access to the channel, they cannot support real time traffic
- for support real time traffic, need reserving bandwidth a priori, can provide QoS support to time sensitive traffic sessions
- can be classified into two types
- synchronous protocols
  - require time synchronization among all nodes in the network, so that reservations made by a node are known to other nodes in its neighborhood
  - global time synchronization is difficult to achieve
- asynchronous protocols
  - do not require any global synchronization among nodes in the network
  - use relative time information for effecting reservations

Contention based MAC protocols with scheduling mechanisms

- focus on packet scheduling at nodes and scheduling nodes for access to the channel
- node scheduling done in a manner to that all nodes are treated fairly
- no node is starved of bandwidth
- scheduling based schemes are also used for enforcing priorities among flows whose packets are queued at node
- some scheduling schemes also take into consideration battery characteristics, such as
- remaining battery power, while scheduling nodes for access to the channel

Contention based MAC protocols: Example

- do not have any bandwidth reservation mechanisms
- all ready nodes contend for the channel simultaneously and winning node gains access to the channel
- nodes are not guaranteed bandwidth,
- these protocols can not be used for transmitting real-time traffic which requires QoS guarantees from the system
- MACAW - A Media Access Protocol for Wireless LANs based on multiple access collision avoidance protocol (MACA)

Contention based MAC protocols: MACA

- MACA was proposed due to shortcoming of CSMA (used in wired network)
- in CSMA the sender first senses the channel for the carrier signal
- if carrier is present or not, it retries after a random period of time otherwise it transmits the packet
- CSMA senses the state of the channel only at the transmitter
- this protocol does not overcome the hidden terminal problem
- in adhoc network the transmitter and receiver may not be near each other at all times
- the packets transmitted by a node are prone to collisions at the receiver due to simultaneous transmissions by the hidden terminals
- bandwidth utilization in CSMA protocols is less because of the exposed terminal problem

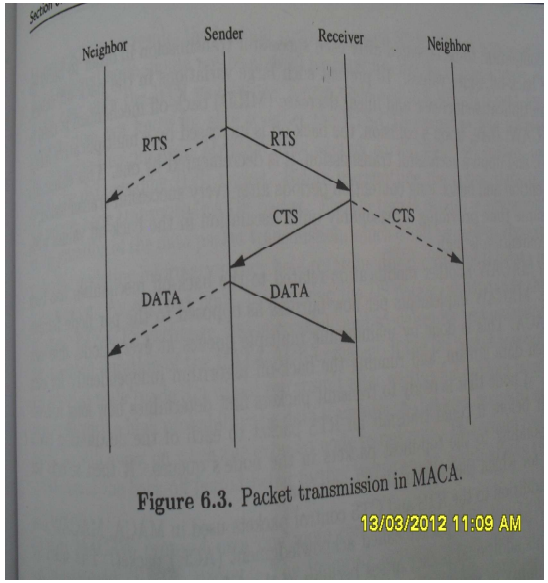
Contention based MAC protocols: MACA

- MACA does not make use of carrier sensing for channel access
- it uses two additional signaling packets: request to send RTS and clear to send CTS packet
- when a node wants to transmit a data packet, it first transmits an RTS packet
- the receiver node, on receiving RTS packet if it is ready to receive the data packet, transmit a CTS packet
- once sender receives the CTS packet without any error, it starts transmitting the data packet
- if a packet transmitted by a node is lost, the node uses the binary exponential backoff (BFB) algorithm to back off for a random interval of time before retrying

Contention based MAC protocols: MACA

- in the binary exponential backoff mechanism, each time a collision is detected, the node doubles its maximum backoff window
- neighbor nodes near the sender that hear the RTS packet do not transmit for a long enough period of time so that the sender could receiver the CTS packet
- both RTS and CTS packets carry the expected duration of data packet transmission
- a node near the receiver upon hearing the CTS packet, defers its transmission till the receiver receives the data packet, thus,
- MACA overcomes the hidden node problem

Contention based MAC protocols: MACA



src: textbook

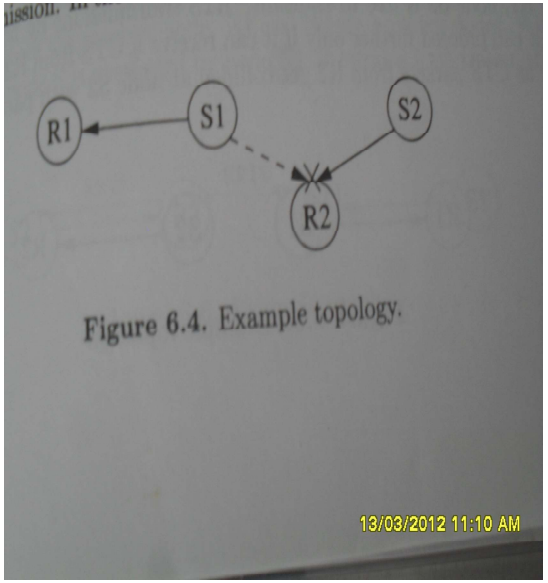
Contention based MAC protocols: MACA

- node receiving an RTS defers only for a short period of time till the sender could receive the CTS,
- if no CTS is heard by the node during its waiting period, it is free to transmit packets once the waiting interval is over
- thus, a node that hears only the RTS packet is free to transmit simultaneously when the sender of RTS is transmitting data packets, hence,
- the exposed terminal problem is also overcome in MACA
- MACA has certain problems and to overcome this MACAW was proposed
- the binary exponential back-off mechanism used in MACA at times starves flows

Contention based MAC protocols: MACAW

- for example, nodes S1 and S2 keep generating a high volume of traffic, the node that first captures the channel (say S1) starts transmitting packets
- the packets transmitted by the other node S2 get collided, and the node keeps incrementing its back-off window according to the BFB algorithm
- the probability of node S2 acquiring the channel keeps decreasing, and over a period of time it gets completely blocked
- to overcome this back-off algorithm has been modified in MACAW
- the packet header now has an additional field carrying the current back-off counter value of the transmitting node
- a node receiving the packet copies this value into its own back-off counter

Contention based MAC protocols: MACAW



src: textbook

Contention based MAC protocols: MACAW

- this mechanism allocates bandwidth in a fair manner
- another problem with BFB algorithm is that it adjusts the back-off counter value very rapidly, both when a node successfully transmits a packet and when a collision is detected by the node
- the back-off counter is reset to the minimum value after every successful transmission
- in the modified back-off process, this would require a period of contention to be repeated after each successful transmission in order to build up the back-off timer values
- to prevent such large variations in the back-off values a multiplicative increase and linear decrease (MILD) back-off mechanism is needed in MACAW

Contention based MAC protocols: MACAW

- upon a collision, the back-off is increased by a multiplication factor and upon a successful transmission it is decremented by one
- this eliminates contention and hence long contention periods after every successful transmission, at the same time providing a reasonably quick escalation in the back-off values when the contention is high
- another modification related to back-off mechanism
- implements per flow fairness as opposed to the per node fairness in MACA
- done by maintaining multiple queues at every node, one each for each data stream and running the back-off algorithm independently for each queue
- a node that is ready to transmit packets first determines how long it needs to wait before it could transmit an RTS packet to each of the destination nodes corresponding to the top-most packets in the node's queue

Contention based MAC protocols: MACAW

- it then selects the packet for which the waiting time is minimal
- in addition to RTS and CTS control packets in MACA, MACAW uses ACK packet also
- in MACA the responsibility of recovering from transmission errors lies with the transport layer,
- minimum timeout period of about 0.5 sec, significant delay is involved while recovering from errors
- in MACAW, the error recovery responsibility is given to the data link layer (DLL)
- in DLL, the recovery process can be made quicker as the timeout provides can be modified in order to suit the physical media being employed.

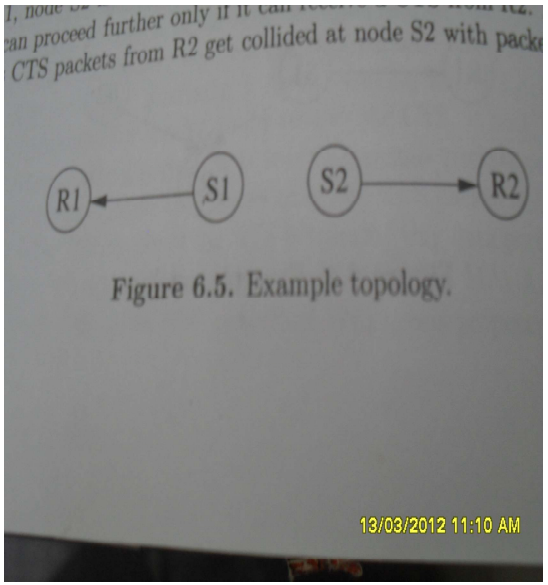
Contention based MAC protocols: MACAW

- in MACAW, after successful reception of each data packet, the receiver node transmits an ACK packet
- if the sender does not receive the ACK packet, it reschedules the same data packet for transmission
- the back-off counter is incremented if the ACK packet is not received by the sender
- if the ACK packet got lost in transmission, the sender would retry by transmitting an RTS for the same packet
- now the receiver, instead of sending back a CTS, sends an ACK for the packet received, and the sender moves onto transmit the next data packet

Contention based MAC protocols: MACAW

- In MACA, an exposed node (which received only RTS and not CTS packet) is free to transmit simultaneously when the source node is transmitting packets
- when a transmission is going on between nodes S1 and R1, node S2 is free to transmit
- RTS transmissions by node S2 are of no use, as it can proceed further only if it can receive a CTS from R2
- but this is not possible as CTS packets from R2 get collided at node S2 with packet transmitted by node S1
- as a result back-off counter at node S2 builds up unnecessarily
- so an exposed node (S2) should not be allowed to transmit

Contention based MAC protocols: MACAW



src: textbook

Contention based MAC protocols: MACAW

- an exposed node since it can hear only the RTS sent by the source node and not the CTS sent by the receiver (R1), does not know for sure whether the RTS-CTS exchange was successful
- to overcome the problem, MACAW uses another small (30 bytes) control packet called the data sending (DS) packet,
- before transmitting the actual data packet the source node transmits this DS packet,
- the DS packet carries information such as the duration of the data packet transmission, which could be used by the exposed nodes for updating information they hold regarding the duration of the data packet transmission

Contention based MAC protocols: MACAW

- as exposed node, overhearing DS packet, understands that the previous RTS-CTS exchange was successful, and so defers its transmissions until the expected duration of DATA-ACK exchange
- if DS packet was not used, the exposed node (S2) would retransmit after waiting for random intervals of time, and with a high probability the data transmission (between S1 and R1) would be still going on when the exposed node retransmits, this would result in a collision and the back-off period being further incremented which affects the node even more

Contention based MAC protocols: MACAW

- MACAW uses another control packet request for request to send (RRTS) packet
- transmission going on between S1 and R1; node S2 wants to transmit to node R2
- but R2 is a neighbor of R1, it receives CTS packets from node R1 and therefore it defers its own transmissions
- node S2 has no way to learn about the contention periods during which it can contend for the channel and so it keeps on trying, incrementing its back-off counter after each failed attempt, hence,
- the main reason for this problem is the lack of synchronization information at source S2
- MACAW overcomes this problem by using the RRTS packet

Contention based MAC protocols: MACAW

- receiver node R2 contends for the channel on behalf of source S2, if R2 had received an RTS previously for which it was not able to respond immediately because of the on-going transmission between nodes S1 and R1 then node R2 waits for the next contention period and transmits RRTS packet
- neighbor node that hear RRTS packet including R1 are made to wait for two successive slots (for RTS-CTS exchange to take place)
- S2 on receiving the RRTS from node R2, transmits the regular RTS packet to node R2, and the normal packet exchange (RTS-CTS-Data-ACK) continues from here

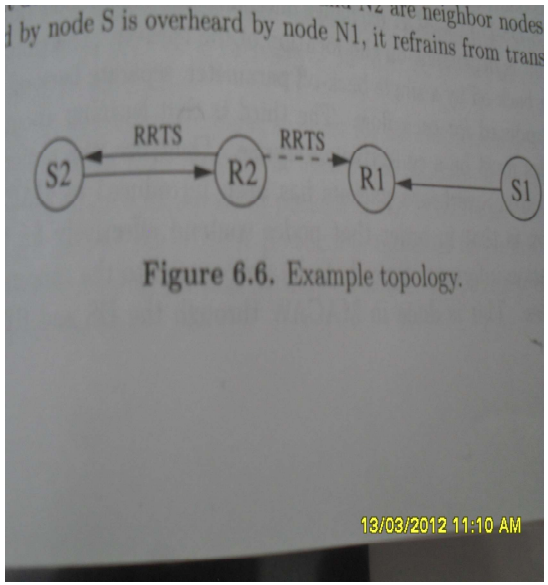
Contention based MAC protocols: MACAW

- S and R source and receiver N1 and N2 neighbor nodes
- RTS transmitted by S is over-headed by N1 and it refrains from transmitting S receives CTS
- when CTS transmitted by R is heard by neighbor node N2, it defers its transmissions until the data packet is received by receiver R
- on receiving this CTS, S immediately transmits the DS message carrying the expected duration of the data packet transmission
- on hearing this packet, node N1 back off until the data packet is transmitted
- finally, after receiving the data packet R sends ACK to S

Contention based MAC protocols: Summary of MACAW

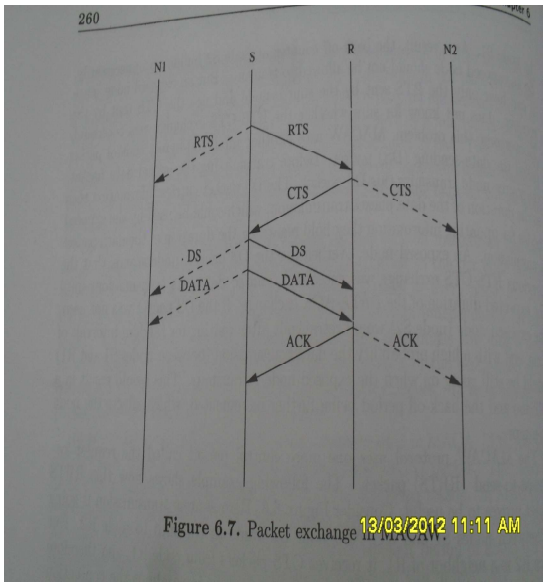
- congestion occurs at receiver node and not at the sender
- CSMA unsuitable for adhoc networks
- improved by RTS-CTS-DS-DATA-ACK
- congestion is dependent on the location of receiver
- instead of single back-off, separate back-off parameters for each flow
- learning about congestion at various nodes must be collective enterprise
- the notion of copying back-off values from overheard packets has been introduced in MACA
- nodes contend for the channel, synchronization information needs to be propagated to concerned nodes at appropriate time
- this is done by DS and RRTS

Contention based MAC protocols: MACAW



src: textbook

Contention based MAC protocols: MACAW



src: textbook

Routing Protocols for Adhoc Wireless Network

- mobile nodes, network topology changing
- routing protocol of wired network can not be directly applied in adhoc network
- highly dynamic topology, absence of established infrastructure for centralized administration,
- bandwidth constrained wireless links and resource (energy) constrained nodes

Issues in designing of Routing protocols

- mobility of nodes, resource constraints, error-prone channel state and
- hidden, exposed terminal problems
- mobility
- highly dynamic due to node mobility, on-going suffers frequent path breaks
- disruption due to movement of intermediate nodes or end node movement
- wired network all nodes are stationary, find alternate routes during path breaks, convergence is very slow
- therefore wired network routing protocols can not be used in adhoc network, mobility of nodes results in frequently changing network topologies
- need efficient and effective mobility management

Issues in designing of Routing protocols

- bandwidth constraint
- abundant bandwidth in wired network, exploitation of wavelength division multiplexing (WDM)
- wireless network radio band is limited, data rate offered very less
- routing protocols use the bandwidth optimally
- limited bandwidth availability imposes a constraint on routing protocols in maintaining topological information,
- more control overhead more bandwidth wastage

Issues in designing of Routing protocols

- error-prone shared broadcast radio channel
- time varying characteristics in terms of link capacity and link error probability
- routing protocol interacts with MAC layer to find alternate routes through better quality links
- transmission - collision of data and control packets, hidden terminal problem
- routing protocol should find paths with less congestion

Issues in designing of Routing protocols

- Hidden and exposed terminal problems
- MACA requires that transmitting node first explicitly notifies all potentials hidden nodes about the forthcoming transmission by means of
- a two-way handshake control protocol called RTS-CTS protocol exchange - it reduces the probability of collisions
- to increase efficiency, improved version of MACA known as MACAW
- MACAW requires that the receiver acknowledges each successful reception of a data packet
- transmission is four-way exchange RTS-CTS-DATA-ACK

Issues in designing of Routing protocols

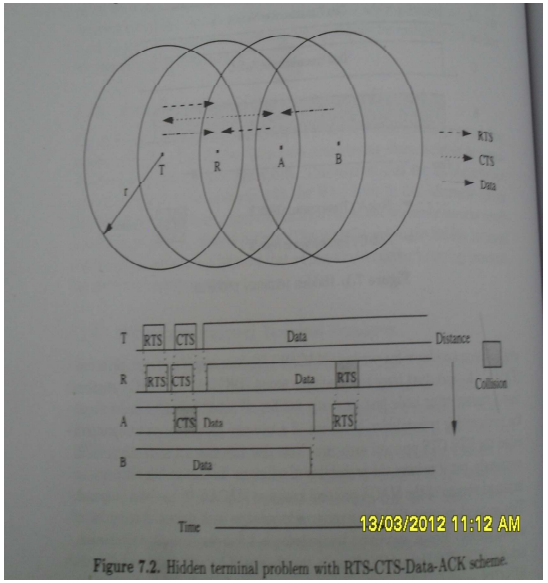


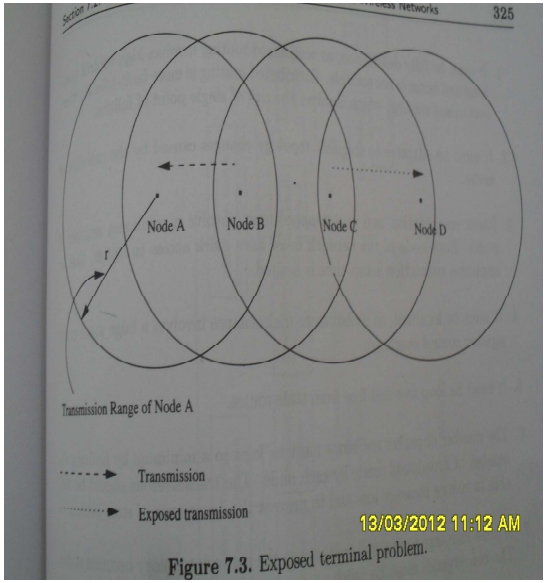
Figure 7.2. Hidden terminal problem with RTS-CTS-Data-ACK scheme.

src: textbook

Issues in designing of Routing protocols

- in absence of bit errors and mobility, RTS-CTS control packet exchange cannot ensure collision free data transmission that has no interference from hidden terminals
- important assumption that every node in the capture area of receiver (transmitter) receives the CTS (RTS) cleanly
- nodes that do not hear either of these clearly can disrupt the successful transmission of DATA or ACK
- one situation occurs when node A hidden from transmitter T and within the capture area of the receiver R,

Issues in designing of Routing protocols



src: textbook

Issues in designing of Routing protocols

- does not hear the CTS properly because it is within the capture area of node B that is transmitting and the hidden from both R and T,
- in this case node A did not successfully receive the CTS originated by node R and hence assumes that there is no on-going transmission in the neighborhood
- since node A is hidden from node T any attempt to originate its own RTS would result in collision of on-going transmission between nodes T and R
- exposed terminal problem (discussed earlier)
- resource constraints: battery life and processing power
- increasing both makes node bulky and less portable
- optimally manage resources

Characteristics of Ideal Routing protocol

- must be fully distributed; centralized routing involves high control overhead and hence not scalable
- distributed routing more fault tolerant
- centralized routing risk of single point of failure
- adaptive to frequent topology changes due to mobility of nodes
- route computation and maintenance must involve minimum number of nodes
- each node must have quick access to routes, i.e., minimum connection setup time is desired
- must be localized, as global state maintenance a huge state propagation control overhead
- must be loop free and free and from stale routes

Characteristics of Ideal Routing protocol

- number of packets collisions must be kept to minimum by limiting the number of broadcasts made by each node
- transmission should be reliable to reduce message loss and to prevent the occurrence of state routes
- must converge to optimal routes once the network topology becomes stable, convergence must be quick
- must optimally use scarce resources such as bandwidth, computing power, memory and batter power
- must provide QoS, support for time sensitive traffic
- every node should try to store information regarding the stable local topology only;
- changes in remote parts of network must not cause updates in the topology information maintained by the node

Classification of Routing protocols

- broadly classified into four categories based on
  - routing information update mechanism
  - use of temporal information for routing
  - routing topology
  - utilization of specific resources
- based on routing information update mechanism three major categories
- proactive or table-driven routing protocols
- network topology information maintained in routing tables, exchange periodically
- information flooded in the whole network
- whenever a node requires a path to a destination, it runs an appropriate path finding algorithm on the topology information it maintains

Classification of Routing protocols

- reactive or on-demand routing protocols
- do not maintain the network topology information
- they obtain the necessary path when it is required, by using a connection establishment process
- do not exchange routing information periodically
- hybrid routing protocols
- best features of the above two categories
- nodes within a certain distance from the node concerned, or within a particular geographical region,
- are said to be within the routing zone of the given node
- for routing within this zone, a table-driven approach is used
- nodes that are located beyond this zone, an on-demand approach is used

Classification of Routing protocols

- based on the use of temporal information for routing
- highly dynamic network, path breaks are frequent,
- the use of temporal information regarding the lifetime of the wireless links and lifetime of the paths selected assumes significance
- further classified into two types
- routing protocols using past temporal information
- use information about the past status of the links or the status of links at the time of routing to make routing decisions
- for example, the routing metric based on the availability of wireless links along with a shortest path-finding algorithm.
- topological changes may break the path, making the path undergo a resource wise expensive path reconfiguration process

Classification of Routing protocols

- routing protocols that use future temporal information
- use expected future status of wireless link to make approximate routing decisions
- future status like lifetime of the node, (remaining battery charge and discharge rate of non-replenishable resource),
- prediction of location, prediction of link availability
- based on routing topology
- Internet - hierarchical manner in order to reduce the state information maintained at the core routers
- adhoc network small number of nodes - either use flat topology or hierarchical topology for routing

Classification of Routing protocols

- flat topology based routing protocol
- use of flat addressing scheme similar to the one used in IEEE 802.3 LANs
- it assumes the presence of a globally unique addressing for nodes in an adhoc network
- hierarchical topology based routing protocol
- use of logical hierarchy in the network and associated addressing scheme
- hierarchy could be based on geographical information or on hop distance

Classification of Routing protocols

- Based on utilization of specific resources
- power aware routing
- aims at minimizing the consumption of important resource, battery power, may be locally or globally
- geographical information assisted routing
- improve the performance of routing and reduce the control overhead by utilizing the geographical information

Table driven Routing protocols

- extensions of the wired network routing protocols
- maintain global topology information in the form of tables at every node
- tables are updated frequently in order to maintain consistent and accurate network state information
- destination sequenced distance-vector routing protocol (DSDV)
- wireless routing protocol (WRP)
- source tree adaptive routing protocol (STAR)
- cluster head gateway switch routing protocol (CGSR)

Destination Sequenced Distance Vector Routing protocol (DSDV)

- one of the first protocol for adhoc network
- it is an enhanced version of distributed Bellman-Ford algorithm where
- each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network
- it incorporates table updates with increasing sequence number tags to prevent loops, to counter the count-to-infinity problem and for faster convergence
- it is table driven routing protocol, routes to all destinations are available at every node at all times

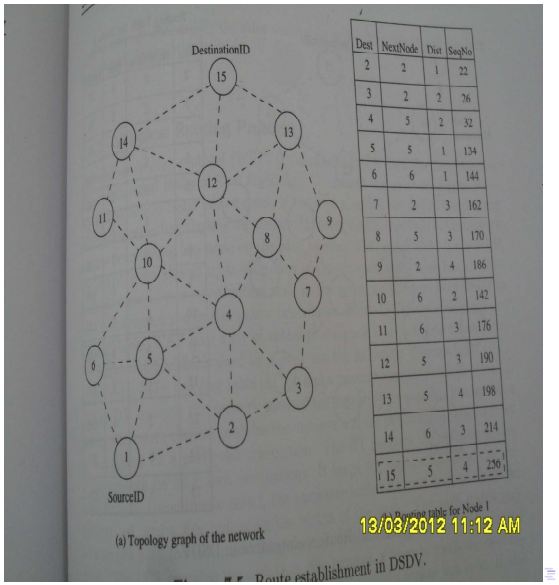
Destination Sequenced Distance Vector Routing protocol (DSDV)

- tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology
- tables are forwarded if a node observes a significant change in local topology
- table updates are of two types: incremental updates and full dumps
- incremental update takes a single network data packet unit (NDPU) while a full dump may take multiple NDPUs
- incremental updates are used when a node does not observe significant changes in the local topology
- full dump is done either when the local topology changes significantly or when an incremental update requires more than a single NDPU

Destination Sequenced Distance Vector Routing protocol (DSDV)

- tables updates are initiated by a destination with a new sequence number which is always greater than the previous one
- upon receiving an updated table, a node either updates its tables based on the received information or
- holds it for some time to select the best metric (lowest number of hops) received from multiple versions of the same update table from different neighboring nodes
- based on the sequence number of the table update, it may forward or reject the table
- node 1 is source node and node 15 is destination shortest route through node 5 and distance to it is 4

Destination Sequenced Distance Vector Routing protocol (DSDV)



Destination Sequenced Distance Vector Routing protocol (DSDV)

- reconfiguration of a path used by an on-going data transfer session is handled by the protocol in the following way:
- the end node of the broken link initiates a table update message with the broken link's weight assigned to infinity (∞) and
- with a sequence number greater than the stored sequence number for that destination
- each node upon receiving an update with weight ∞, quickly disseminates it to its neighbors in order to propagate the broken link information to the whole network
- a single link break leads to the propagation of table update information to the whole network
- a node always assigns an odd sequence number to the link break update to differentiate it from the even sequence number generated by the destination

Destination Sequenced Distance Vector Routing protocol (DSDV)

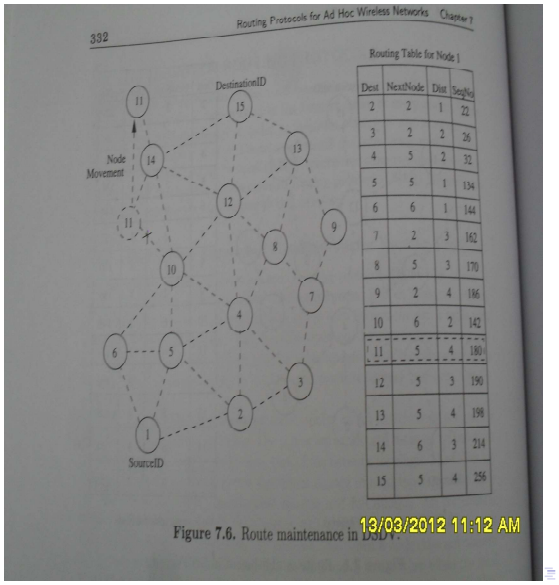


Figure 7.6. Route maintenance in

Destination Sequenced Distance Vector Routing protocol (DSDV)

- consider the case when node 11 moves from the current position,
- a neighbor node perceives the link break, it sets all the paths passing through the broken link with distance ∞
- for example, node 10 knows about the link break, it sets the path to node 11 as ∞ and broadcasts its routing table to its neighbors
- those neighbors detecting significant changes in their routing tables rebroadcast it to their neighbors
- in this way the broken link information propagates throughout the network

Destination Sequenced Distance Vector Routing protocol (DSDV)

- node 1 sets the distance to node 11 as ∞ when node 14 receives a table update message from node 11,
- it informs the neighbors about the shortest distance to node 11
- this information is also propagated throughout the network
- all nodes receiving the new update message with the higher sequence number set the new distance to node 11 in their corresponding tables
- the updated table at node 1 (shown in figure) the current distance from node 1 to node 11 has increased from three to four hops

Destination Sequenced Distance Vector Routing protocol (DSDV)

- advantages
- the availability of routes to all destinations at all times implies that much less delay is involved in the route setup process
- the mechanism of incremental updates with sequence number tags makes the existing wired network protocols adaptable to adhoc networks
- the updates are propagated throughout the network in order to maintain an up-to-date view of the network topology at all the nodes

Destination Sequenced Distance Vector Routing protocol (DSDV)

- disadvantages
- the updates due to broken links lead to a heavy control overhead during high mobility
- small network with high mobility or a large network with low mobility can choke the available bandwidth
- the protocol suffers from the excessive control overhead that is proportional to the number of nodes in the network and therefore
- is not scalable in adhoc network having limited bandwidth and whose topologies are highly dynamic
- another disadvantage is that in order to obtain information about a particular destination node, a node has to wait for a table update message initiated by the same destination node,
- this delay could result in stale routing information at nodes

On Demand Routing protocols

- unlike table-driven routing protocol, on-demand routing protocols execute the path finding process and
- exchange routing information only when a path is required by a node to communicate with a destination
- Dynamic Source Routing (DSR) protocol
- on demand protocol designed to restrict the bandwidth consumed by control packets in adhoc network by
- eliminating the periodic table update messages required in the table-driven approach
- major difference between DSR and other on demand routing protocols is that
- it is beacon less and hence does not require periodic hello packet transmissions, which are used by a node to inform its neighbors of its presence

Dynamic Source Routing (DSR) protocol

- the basic approach of on demand routing protocol during the route construction phase is to establish a route by flooding RouteRequest packets in the network
- the destination node, on receiving a RouteRequest packet responds by sending a RouteReply packet back to the source, which
- carries the route traversed by the Route Request packet received
- consider a source node that does not have a route to the destination
- when it has data packets to be sent to that destination, it initiates a RouteRequest packet
- this RouteRequest is flooded throughout the network
- each node, upon receiving a RouteRequest packet, rebroadcast the packet to its neighbors if it has not forwarded already or
- if the node is not the destination node, provided the packet's time to live (TTL) counter has not exceeded

Dynamic Source Routing (DSR) protocol

- each RouteRequest carries a sequence number generated by the source node and the path it has traversed
- a node upon receiving a RouteRequest packet, checks the sequence number on the packet before forwarding it
- the packet is forwarded only if it is not a duplicate RouteRequest
- the sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same RouteRequest by an intermediate node that receives it through multiple paths
- thus all node except the destination forward a Route Request during the route construction phase
- a destination node after receiving the first RouteRequest packet, replies to the source node through the reverse path the RouteRequest packet had traversed.

Dynamic Source Routing (DSR) protocol

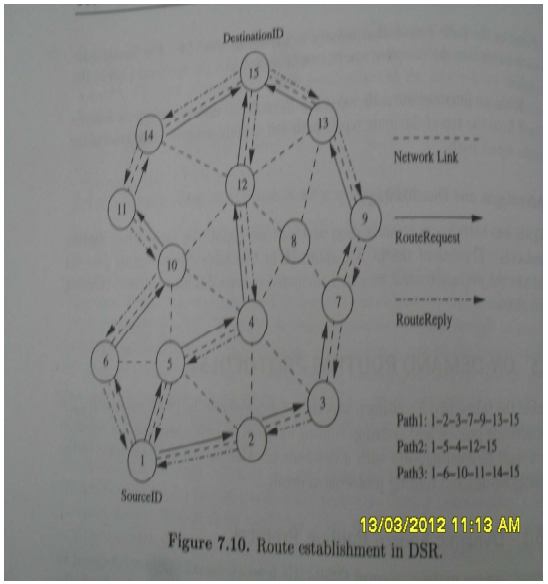


Figure 7.10. Route establishment in DSR.

src: textbook

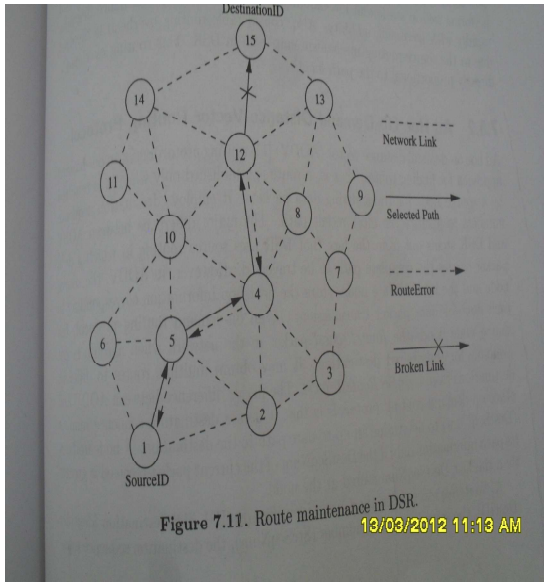
Dynamic Source Routing (DSR) protocol

- node 1 initiates RouteRequest to obtain a path for destination node 15
- the protocol uses a route cache that stores all information extracted from the source route contained in a data packet
- nodes can learn about the neighboring routes traversed by data packets if operated in the promiscuous mode (the mode in which node can receive the packets that are neither broadcast nor addressed to itself)
- if an intermediate node receiving a RouteRequest has a route to the destination node in its route cache then
- it replies to the source node by sending a RouteReply with the entire route information from the source code to destination node

Dynamic Source Routing (DSR) protocol

- optimization techniques used with DSR to improve performance of the protocol
- DSR uses route cache at intermediate nodes, route cache is populated with routes
- cache also used to reply to the source by intermediate node
- using promiscuous mode, possible to update route cache and active routes maintained
- during network partitions, the affected nodes initiate RouteRequest packets
- exponential backoff algorithm is used to avoid frequent RouteRequest flooding in the network when the destination is in another disjoint set
- DSR allows piggy backing of a data packet on RouteRequest

Dynamic Source Routing (DSR) protocol



src: textbook (Route maintenance in DSR)

Dynamic Source Routing (DSR) protocol

- if optimization is not allowed in the DSR then route construction phase is simple
- all intermediate nodes flood the RouteRequest packet if it is not redundant
- RouteRequest packet received from node 1 by its neighbor nodes 2,5,6, they forward it
- node 4 receives the RouteRequest from both nodes 2 and 5 and discards the other redundant or duplicate RouteRequest packets
- RouteRequest is propagated till it reaches the destination which initiates RouteReply
- as part of optimization if the intermediate nodes are also allowed to originate RouteReply packets then a source node may receive multiple replies from intermediate nodes

Dynamic Source Routing (DSR) protocol

- intermediate node 10 has a route to the destination via node 14; it also sends the RouteReply to the source node
- source node selects the latest and best route and uses that for sending data packets
- when intermediate node in the path moves away, link breaks, say,
- link between nodes 12 and 15 fails,
- RouteError message is generated from the node adjacent to the broken link to inform the source node
- source node reinitiates the route establishment procedure
- the cached entries at the intermediate nodes and the source node are removed when a RouteError packet is received
- if a link breaks dues to the movement of edge nodes (node 1 and node 15) the source node again initiates the route discovery process

Dynamic Source Routing (DSR) protocol

- advantages
- protocol uses a reactive approach which eliminates the need to periodically flood the network with table update message which are required in table driven approach
- on-demand (reactive) approach route is established only when it is required and hence
- the need to find routes to all other nodes in the network as required by table driven approach is eliminated
- intermediate nodes utilizes the route cache information efficiently to reduce the control overhead

Dynamic Source Routing (DSR) protocol

- disadvantages
- the route maintenance mechanism does not locally repair a broken link
- stale route cache information could result in inconsistencies during the reconstruction phase
- connection setup delay is higher than in table driven protocols
- DSR protocols perform well in static and low mobility environments, performance degrades with increasing mobility
- routing overhead is involved due to source routing and proportional to path length

Adhoc On Demand Distance Vector Routing Protocol (AODV)

- on demand, employs destination sequence numbers to identify the most recent path
- the major difference between AODV and DSR
- DSR uses source routing in which a data packet carries the complete path to be traversed
- AODV, source node and intermediate nodes store the next hop information corresponding to each flow for data packet transmission
- on-demand routing protocol, the source code floods the RouteRequest packet in the network when a route is not available for the desired destination
- it may obtain multiple routes to different destinations from a single RouteRequest

Adhoc On Demand Distance Vector Routing Protocol (AODV)

- AODV uses a destination sequence number DestSeqNum to determine an uptodate path to the destination
- a node updates its path information only if the DeptSeqNum of the current packet received is greater than the last DeptSeqNum stored at the node
- A RouteRequest carries source identifier (SrcID), the destination identifier (DestID), the source sequence number (SrcSeqNum), destination sequence number (DestSeqNum), the broadcast identifier (BcastID), time to live (TTL) field
- DestSeqNum indicates the freshness of the route that is accepted by the source
- when an intermediate node receives a RouteRequest, it either forwards it or prepares RouteReply if it has a valid route to the destination

Adhoc On Demand Distance Vector Routing Protocol (AODV)

- validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RouteRequest packet
- if RouteRequest is received multiple times, indicated by BcastID-SrcID pair, the duplicate copies are discarded
- all intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send RouteReply packets to the source
- every intermediate node, while forwarding RouteRequest, enters the previous node address and its BcastID

Adhoc On Demand Distance Vector Routing Protocol (AODV)

- a timer is used to delete this entry in case RouteReply is not received before the timer expires
- this helps in storing an active path at the intermediate node as AODV does not employ source routing of data packets
- when a node receives a RouteReply packet information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination

Adhoc On Demand Distance Vector Routing Protocol (AODV)

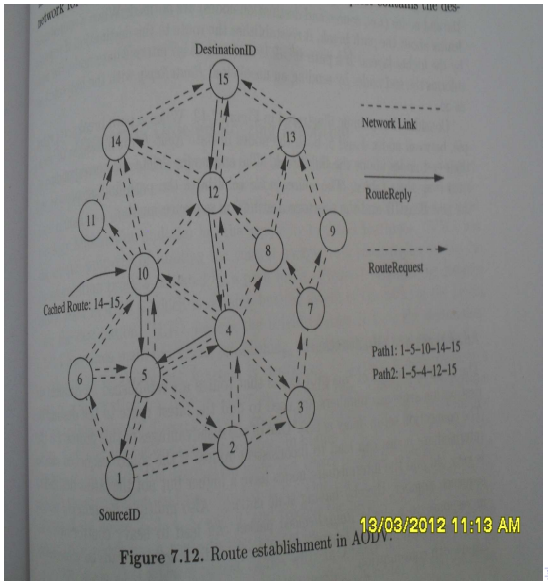


Figure 7.12. Route establishment in AODV.

Adhoc On Demand Distance Vector Routing Protocol (AODV)

- node 1 initiates path finding process by originating RouteRequest to be flooded in the network for destination node 15
- assume that the RouteRequest contains destination sequence number as 3 and the source sequence number 1,
- when nodes 2,5,6 receives the RouteRequest packet, they check their routes to the destination,
- in case route to destination is not available, they further forward it to their neighbors i.e. nodes 3,4,10 neighbors of 2,5,6

Adhoc On Demand Distance Vector Routing Protocol (AODV)

- assume that intermediate nodes 3, 10 have routes to the destination node, say 10-14-15 and 3-7-9-13-15 respectively,
- if the destination sequence number at intermediate node 10 is 4 and is 1 at intermediate node 3 then
- only node 10 is allowed to reply along the cached route to the source
- this is because node 3 has an older route to node 15 compared to the route available at the source node
- (the destination sequence number at node 3 is 1, but the destination sequence number is 3 at the source node) while
- node 10 has a more recent node (the destination sequence number is 4) to the destination

Adhoc On Demand Distance Vector Routing Protocol (AODV)

- if RouteRequest reaches the destination node 15 through path 4-12-15 or any other alternative route, the destination also sends RouteReply to the source
- in this case multiple RouteReply packets reach the source, all the intermediate nodes receiving a RouteReply update their route tables with the latest destination sequence number
- they also update the routing information if it leads to a shorter path between source and destination
- AODV does not repair a broken path locally, when a link breaks, determined by observing periodical beacons or through link-level acknowledgments, the end nodes are notified.

Adhoc On Demand Distance Vector Routing Protocol (AODV)

- when a source node learns about the path break, it reestablishes the route to the destination if required by the higher layers
- if a path break is detected at an intermediate node, the node informs the end nodes by sending an unsolicited RouteReply with the hop count set as ∞
- when a path breaks, say, between nodes 4 and 5 both nodes initiate RouteError message to inform their end nodes about the link break
- the end nodes delete the corresponding entries from their tables
- source node reinitiates the path finding process with the new BcastID and previous destination sequence number

Adhoc On Demand Distance Vector Routing Protocol (AODV)

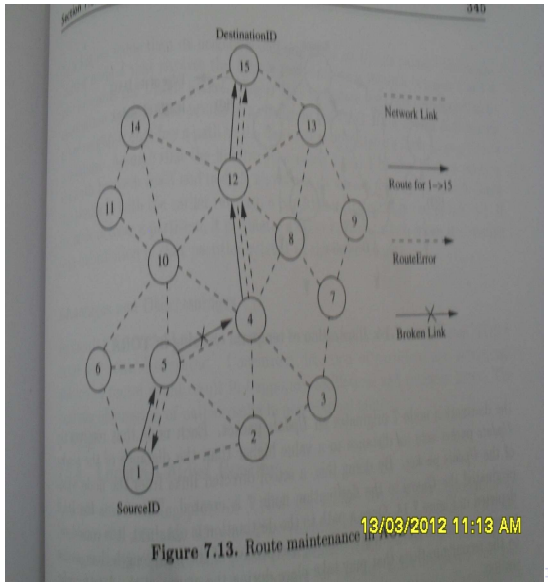


Figure 7.13. Route maintenance

Adhoc On Demand Distance Vector Routing Protocol (AODV)

- advantages
- routes are established on demand and destination sequence numbers are used to find the latest route to the destination
- connection setup delay is less
- disadvantages
- disadvantage is that intermediate nodes can lead to inconsistent routes if
- the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries
- heavy control overhead due to multiple RouteReply in response to single RouteRequest
- periodic beaconing leads to unnecessary bandwidth consumption

Multicast Routing in Adhoc Wireless Network

- applications in civilian operations
- collaborative and distributed computing
- emergency search and rescue
- law enforcement and warfare situations
- where setting up and maintaining a communication infrastructure may be difficult or costly
- communication and coordination among a given set of nodes are necessary in all these applications

Multicast Routing in Adhoc Wireless Network

- play an important role to provide communication
- advantageous to use multicast rather than multiple unicast where bandwidth comes at a premium
- conventional wired network IP multicast routing protocols such as
- DVMRP, MOSPF, CBT and PIM do not perform well in adhoc network because of dynamic nature of the network topology
- low bandwidth, less reliable wireless links, causes long convergence times and
- may give rise to formation of transient routing loops which consumes bandwidth

Multicast Routing in Adhoc Wireless Network

- in wired network multicasting consists of establishing a routing tree for a group of routing nodes that constitute the multicast session
- once the routing tree or spanning tree (an cyclic connected subgraph containing all the nodes in the tree) is established,
- a packet sent to all nodes in the tree traverses each node and each link in the tree only once
- such a multicast structure is not appropriate for adhoc network because the tree could easily break due to highly dynamic topology
- multicast tree structures are not stable and need to be reconstructed continuously as connectivity changes
- maintaining a routing tree for the purpose of multicasting packets, when underlying topology keeps changing frequently can incur substantial control traffic

Multicast Routing in Adhoc Wireless Network

- multicast trees used in conventional wired network multicast protocol require a global routing sub-structure such as
- a link state or a distance vector sub-structure
- frequent exchange of routing vectors or link state tables, triggered by changing topology, yields excessive control and processing overhead
- periods of routing table instability lead to instability of the multicast tree which in turn results in
- increased buffering time for packets, higher packet losses and increase in the number of retransmissions
- the problem of determining which nodes in the network should participate for targeting of multicast data packets, transmitted from a source, to a select set of receivers

Issues in designing a Multicast routing protocol

- limited bandwidth availability, error-prone shared broadcast channel,
- mobility of nodes with limited energy resources, hidden terminal problem and
- limited security make the design of multicast routing protocol a challenging one
- robustness - due to mobility of nodes, link failures are quite common
- data packets sent by source may be dropped, results in a low packet delivery ratio
- it should be robust enough to sustain the mobility of node and achieve a high packet delivery ratio
- efficiency - bandwidth is scarce,
- multicast efficiency is defined as the ratio of the total number of data packets received by the receivers to the total number of data and control packets transmitted in the network

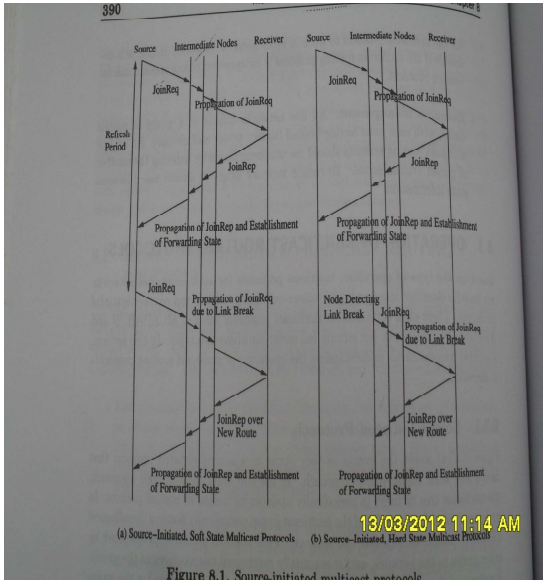
Issues in designing a Multicast routing protocol

- control overhead - to keep track of the members in multicast group the exchange of control packets is required
- consumes bandwidth, control overhead should be minimum
- Qos - military strategic applications, provisioning of QoS, parameters are throughput, delay, delay jitter and reliability
- dependency on the unicast routing protocol - if multicast routing protocol needs support of particular routing protocol, then it is difficult for the multicast protocol to work in heterogeneous network
- it is desirable if the multicast routing protocol is independent of any specific unicast routing protocol
- resource management - limited battery power, memory, mobile nodes,
- use minimum power by reducing the number of packet transmissions,
- to reduce memory usage it should use minimum state information

Classification of Multicast routing protocols

- Operation of multicast routing protocols
- based on the type of operation, classified into two types
- source initiated protocols and receiver initiated protocols
- other multicast protocols MCEDAR and AMRoute
- Source initiated protocols
- events that occur uses a soft state maintenance approach
- multicast tree or mesh is periodically updated by means of control packets
- source(s) of multicast group periodically floods JoinRequest (JoinReq) packet throughout the network
- it is propagated by other nodes in the network; eventually it reaches all the receivers of the group

Source initiated Multicast routing protocols



src: textbook

Classification of Multicast routing protocols

- receivers of multicast group express their wish to receive packets for the group by responding with a JoinReply (JoinRep) packet
- which is propagated along the reverse path of that followed by the Joinreq packet
- JoinRep packet establishes forwarding states in the intermediate nodes (either in tree or mesh) and finally reaches the source
- forwarding state refers to the information regarding the multicast group maintained at the nodes in the multicast tree or mesh
- which aids the nodes in forwarding multicast packets to the appropriate next hop neighbor nodes
- this is a two pass protocol for establishing the tree or mesh
- no explicit procedure for route repair
- soft state protocols, the source periodically initiates the above procedure (once every refresh period)

Classification of Multicast routing protocols

- hard state source initiated protocol
- similar to soft state source initiated protocol, except that there is a explicit route repair procedure
- that is initiated when a link break is detected
- route repair procedure - upstream node which detects that one of its downstream nodes has moved away,
- initiates a tree construction procedure.
- different protocols use different strategies for route repair
- some choose to have the downstream node search for its former parent by means of limited flooding
- while other impose this responsibility on the upstream node

Classification of Multicast routing protocols

- receiver initiated protocols
- receiver uses flooding to search for paths to the sources of multicast groups to which it belongs
- soft state procedure
- tree or mesh construction is three phase process
- first, receiver floods JoinReq packet, propagated by the other nodes
- the sources of multicast group and/or nodes which are already part of multicast tree or mesh allowed to respond to JoinReq packet with a JoinRep packet,
- indicating that they would be able to send data packets for that multicast group

Receiver initiated Multicast routing protocols

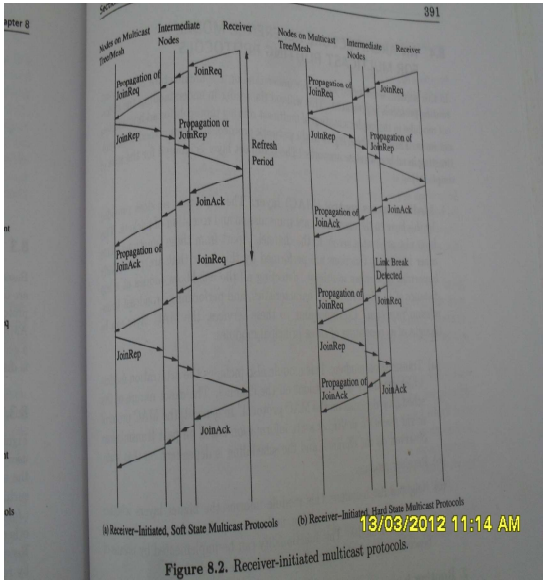


Figure 8.2. Receiver-initiated multicast protocols.

src: textbook

Classification of Multicast routing protocols

- receiver chooses the JoinRep with smallest hop count and
- sends JoinAcknowledgement (JoinAck) packet along the reverse path taken by JoinRep
- route maintenance is accomplished by the periodic initiation of this procedure by the receiver
- hard state procedure
- initial tree or mesh joining phase is the same as that in corresponding soft state protocol
- route repair mechanism comes into play when a link break is detected
- responsibility is to restore topology can be ascribed to either the downstream or to upstream node

Classification of Multicast routing protocols

- reference model for understanding the architecture of multicast routing protocols
- three layers concerned with multicasting
- MAC layer, Routing layer and Application layer
- MAC layer
  - service provided are transmission and reception of packets
  - arbitrates access to the channel
  - detecting all neighbors (nodes at a hop distance of 1)
  - observing link characteristics
  - performing broadcast transmission/reception

Reference Model for architecture of Multicast routing protocols

- MAC can be thought of three principal modules
- transmission module - includes arbitration modules which schedules transmissions on the channel,
- scheduling nature depends on MAC protocol
- MAC may maintain multicast state information based on past transmission observed on the channel and scheduling depends on the state
- receiver module
  - neighbor list handler - informs higher layers weather a particular node is a neighbor node or not
  - maintains a list of all neighbor nodes
  - can be implemented by beacons or by overhearing all packets on the channel

Reference Model for architecture of Multicast routing protocols

- Routing layer
- responsible for forming and maintaining the unicast session/multicast group
- uses set of tables, timers, and route caches
- provides services to application layer for join and leave a multicast group and to transmit and receiver multicast packets
- consists of following components or modules
- unicast route information handler - discovery by on-demand or table driven approach
- multicast information handler - maintains all pertinent information related to the state of the current node with respect to the multicast groups of which it is a part, in the form of a table

Reference Model for architecture of Multicast routing protocols

- this state includes a list of downstream nodes and the addresses of its upstream nodes, sequence number information etc.; maintained per group or per source per group
- forwarding module - uses information provided by multicast information handler to decide whether a receiver multicast packet should be broadcast or be forwarded to a neighbor node, or be sent to the application layer
- tree/mesh construction module - used to construct the multicast topology
- use information provided by the unicast routing information handler for this purpose
- module might initiate flooding on being requested to join a group by the application layer

Reference Model for architecture of Multicast routing protocols

- when application layer process sends session termination messages to this module,
- this module transmits the appropriate messages to the network for terminating the participation of the current node in multicast session
- session maintenance module - initiates route repair on being informed of a link break by lower layer,
- might use information from multicast and unicast routing tables to perform a search for the node in order to restore the multicast topology
- route cache maintenance module - purpose is to glean information from routing packets overhead on the channel for possible use later
- such information might be addresses of nodes which have requested for a route to a multicast group source etc.

Reference Model for architecture of Multicast routing protocols

- route cache is updated as newer information is obtained from more recent packets heard on the channel
- module is optional, increases efficiency by reducing control overhead
- application layer
- utilizes the services of the routing layer to satisfy multicast requirements of applications
- consists of two modules
- data packet transmit/receiver controller
- multicast session initiator/terminator

Reference Model for architecture of Multicast routing protocols

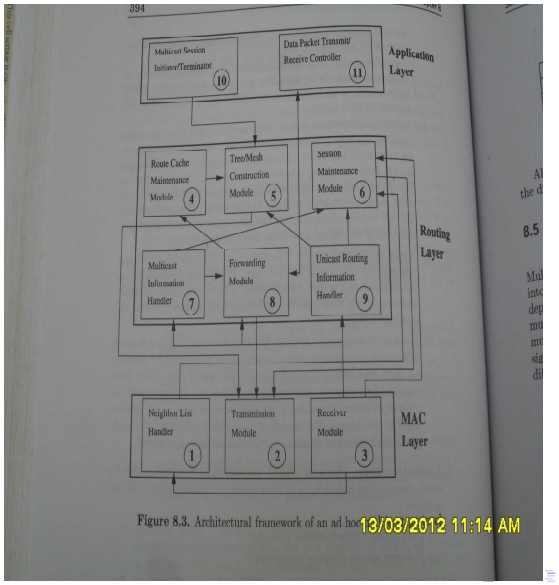


Figure 8.3. Architectural framework of an ad ho

13/03/2012 11:14 AM

Sequence of Steps in Multicasting

- joining a group - module (10) (multicast session initiator/terminator) exists in application layer makes
- a request to join a group to module (5) (tree/mesh construction module) in routing layer
- which can use cached information from module (4) (route cache maintenance) and
- the unicast route information from module (9) (unicast routing information handler)
- it then initiates flooding of JoinReq packets by using module (2) (transmission module) of MAC layer;
- these JoinReq packets are passed by module (3) (receive module) of other nodes to their forwarding module (8),
- which updates the multicast table and propagates this message

Sequence of Steps in Multicasting

- during the reply phase the forwarding states in the multicast tables of intermediate nodes are established
- data packet propagation - data packets are handled by module (11) (data packet transmit/receive controller) in application layer,
- which passes them on to module (8) (forwarding module)
- which makes the decision on whether to broadcast the packets after consulting module (7) (multicast information handler).
- similar process occurs in all nodes in multicast group until the data packets are sent by forwarding module of the receivers to application layer
- route repair - handled by module (6) (session maintenance module) on being informed by module (1) (neighborlist handler) of link breaks
- it uses unicast and multicast routing tables to graft the node back into multicast topology

Classifications of multicast routing protocols

- into two categories application-independent / generic multicast protocols and application-dependent multicast protocols
- application -independent multicast protocols are used for conventional multicasting
- application -dependent multicast protocols are used for specific application
- application-independent multicast protocols can be classified along three different dimensions
- based on topology - tree based and mesh based
- tree based a single path exists between a source-receiver pair,
- efficient mesh based there may be more than one path between a source-receiver pair, robust due to multipath availability

Classifications of multicast routing protocols

- tree based classified - source tree based and shared tree based
- in source tree based multicast protocols, the tree rooted at the source,
- shared tree based protocols a single tree is shared by all sources within multicast group and is rooted at a node referred to as core node
- source tree based protocols perform better than shared tree based protocols at heavy loads because of efficient traffic distribution
- shared tree based protocols are more scalable
- it heavily depends on the core node, a single point failure at the core node affects the performance of the multicast protocols

Classifications of multicast routing protocols

- based on initialization of multicast session
- multicast group formation can be initiated by the source as well as by the receivers
- if the group formation is initiated by the source node, then it is called source initiated multicast routing protocol,
- initiated by receivers called receiver initiated multicast routing protocol
- some protocols can not be distinguished between source and receiver for initialization - called as source or receiver initiated protocols

Classifications of multicast routing protocols

- based on topology maintenance mechanism
- maintenance of multicast topology can be done either by the soft state approach or by hard state approach
- in soft state approach, control packets are flooded periodically to refresh route
- which leads to high packet delivery ratio at the cost of more control overhead whereas in
- hard state approach, control packets are transmitted only when a link breaks results into lower control overhead at the cost of low packet delivery ratio

Classifications of multicast routing protocols

- tree based multicast routing protocols
- well established in wired multicast protocols to achieve high efficiency
- there is only one path between a source-receiver pair
- drawback is that they are not robust enough to operate in highly mobile environments
- classified into two types: source tree based and shared tree based
- source tree based protocol - a single multicast tree is maintained per source, whereas
- shared tree based protocol - a single tree is shared to all the sources in the multicast group
- shared tree based protocols are more scalable compared to source tree based protocols

Classifications of multicast routing protocols

- scalability means that the ability of the protocol to work well without any degradation in the performance when the number of sources in a multicast session or the number of multicast sessions is increased
- in source tree based multicast routing protocols, an increase in the number of sources gives rise to a proportional increase in the number of source trees
- this results in a significant increase in bandwidth consumption in already bandwidth constrained network
- shared tree based multicast protocol this increase in bandwidth usage is not as high as in source tree based protocols because
- even when the number of sources for multicast sessions increases, the number of trees remains the same

Classifications of multicast routing protocols

- another factor affects the scalability of source tree based protocols is the memory requirement
- when multicast group size is large with a large number of multicast sources,
- in a source tree based multicast protocol, the state information that is maintained per source per group consumes a large amount of memory at the nodes
- in shared tree based multicast protocol, since the state information is maintained per group, the additional memory required when the number of sources increases is not very high
- hence, shared tree based multicast protocols are more scalable compared to source tree based protocols

Classifications of multicast routing protocols

- mesh based multicast routing protocols
- links break due to mobility of the nodes
- multiple wireless hops between source and receiver - suffers from link breaks
- mesh based protocols provide multiple paths between a source receiver pair
- adds robustness at the cost of multicast efficiency
- On demand multicast routing protocol (ODMRP)
- a mesh is formed by a set of nodes called forwarding nodes which are responsible for forwarding data packets between a source receiver pair
- these forwarding nodes maintain the message-cache which is used to detect duplicate data packets and duplicate JoinReq Control packets

Mesh based Multicast routing protocols

- Mesh initialization phase
- multicast mesh is formed between the source and the receivers
- to create the mesh each source in the multicast group floods the JoinReq control packet periodically
- upon reception of the JoinReq control packet form a source, potential receivers can send JoinReply through the reverse shortest path
- route between a source and receiver is established after the source receives the JoinReply packet
- S1 and S2 sources flood JoinReq control packets the nodes that receives a JoinReq control packet store the upstream node identification number ID and broadcast the packet again
- R1, R2 and R3 receivers receive JoinReq control packet each node sends JoinReply control packet along the reverse path to the source

Mesh based Multicast routing protocols

- say, R2 receives JoinReq Control packets from S1 and S2 through paths S1-I2-I3-R2 and S2-I6-I4-I5-R2 respectively,
- JoinReply packet contains the source ID and corresponding next node ID (upstream node through which it received the JoinReq packet)
- when node I2 receives the JoinReply control packet from receiver R1 it sets a forwarding flag and becomes forwarding node for that particular multicast group
- after waiting for a specified time it composes a new JoinReply packet and forwards it
- subsequent forwarding of JoinReply packets by the intermediate nodes along the reverse path to source establishes the route
- format of JoinReply packet sent by receiver R2

source ID	Next Node ID
S1	I3
S2	I5

Mesh based Multicast routing protocols

- Mesh maintenance phase
- maintain the multicast mesh formed with sources, forwarding nodes and receivers
- mesh protects the session from being affected by mobility of nodes
- for example, due to movement of receiver R3 (from A to B)
- when the route S2-I9-I10-R3 breaks
- R3 can still receive data packets through route S2-I6-I4-I7-I8-R3 and this contributes to the high packet delivery ratio
- ODMRP uses a soft state approach to maintain the mesh - to refresh the routes between the source and the receiver

Mesh based Multicast routing protocols

- source periodically floods the JoinReq control packet
- when receiver R3 receives a new JoinReq packet from node I11 (sent by source S2)
- it sends a JoinReply on this new shortest path R3-I11-I10-I9-S2 thereby maintaining the mesh structure
- advantage and disadvantage
- ODMRP uses the soft state approach for maintaining mesh, it exhibits robustness at the cost of high control overhead
- the same data packet (from source S2 to receiver R3) propagates through more than one path to destination node resulting in an increased number of data packet transmission, reducing efficiency