R N S INSTITUTE OF TECHNOLOGY

CHANNASANDRA, BANGALORE - 98

AD HOC NETWORKS

NOTES FOR 8TH SEMESTER INFORMATION SCIENCE

SUBJECT CODE: 06IS841

PREPARED BY

DIVYA K
1RN09IS016
8th Semester
Information Science
divya.1rn09is016@gmail.com

NAVYASHREE T S
1RN10IS402
8th Semester
Information Science
navyashree.1rn10is402@gmail.com

SPECIAL THANKS TO

SWATHI, PRIYANKA & SHARVANI

For your valuable support during the preparation of this notes

TEXT BOOK

AD HOC WIRELESS NETWORKS – C Siva Ram Murthy & B S Manoj, 2nd Edition, Pearson Education, 2005

CONTENTS

UNIT 1, UNIT 2, UNIT 4, UNIT 5, UNIT 6, UNIT 7

UNIT 1
INTRODUCTION

CELLULAR AND AD HOC WIRELESS NETWORKS

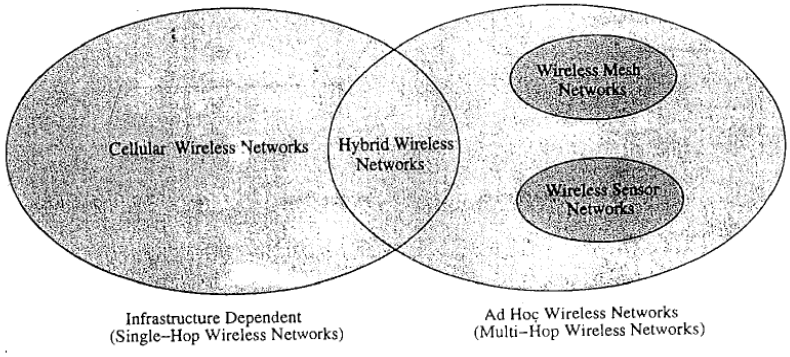


Figure : Cellular and ad hoc wireless networks.

The current cellular wireless networks are classified as the infrastructure dependent network. The path setup for a call between two nodes, say, node C to E, is completed through base station as illustrated in figure below.

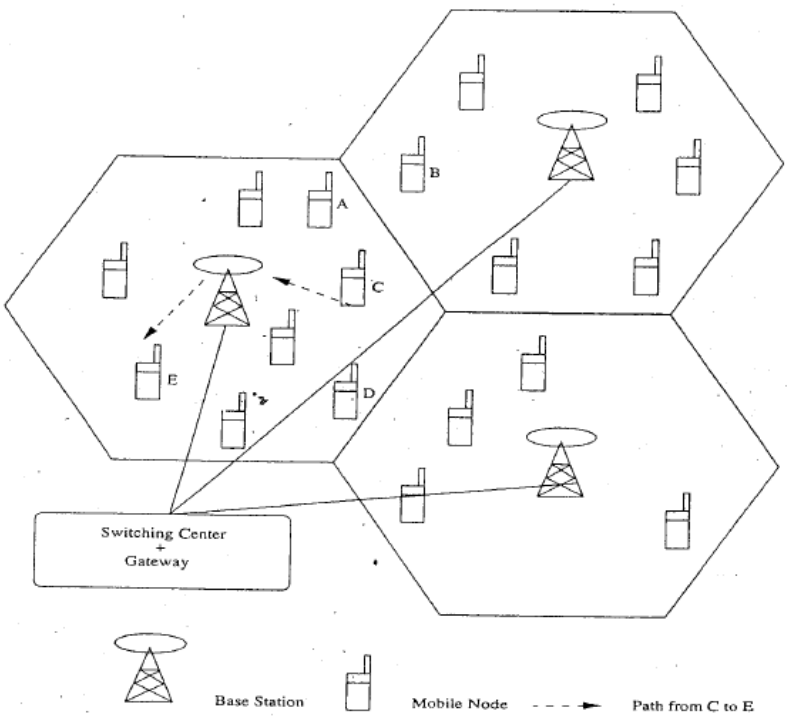


Figure 5.2 A cellular network

- Adhoc wireless networks are defined as a category of wireless network that utilize multi-hop radio replaying and are capable of operating without the support of any fixed infrastructure.
- Absence of any central co-ordinator or base station makes the routing complex.
- Adhoc wireless network topology for the cellular network shown in above figure is illustrated below.
- The path setup for a call between 2 nodes, say, node C to E , is completed through the intermediate mobile node F.
- Wireless mesh network and Wireless sensor networks are specific examples of adhoc wireless networks.

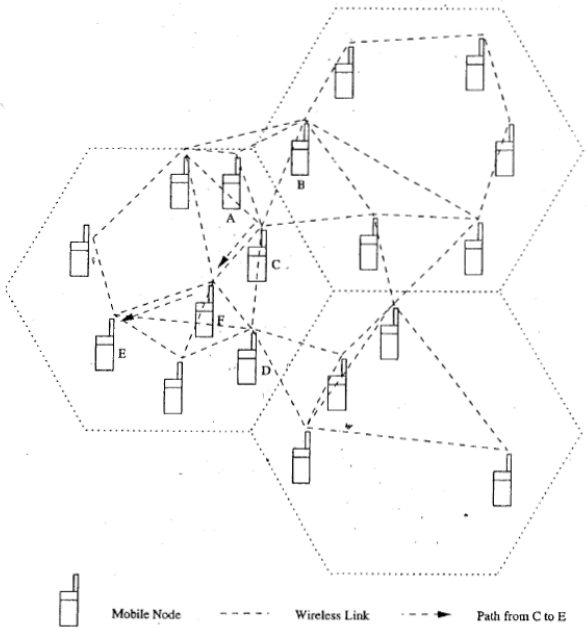


Figure 5.3: An ad hoc wireless network

- The presence of base station simplifies routing and resource management in a cellular network.
- But in adhoc networks, routing and resource management are done in a distributed manner in which all nodes co-ordinate to enable communication among them.

The following table shows the difference between cellular networks and adhoc wireless networks.

Cellular Networks	Ad Hoc Wireless Networks
Fixed infrastructure-based	Infrastructure-less
Single-hop wireless links	Multi-hop wireless links
Guaranteed bandwidth (designed for voice traffic)	Shared radio channel (more suitable for best-effort data traffic)
Centralized routing	Distributed routing
Circuit-switched (evolving toward packet switching)	Packet-switched (evolving toward emulation of circuit switching)
Seamless connectivity (low call drops during handoffs)	Frequent path breaks due to mobility
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
Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
Application domains include mainly civilian and commercial sectors	Application domains include battlefields, emergency search and rescue operations, and collaborative computing
High cost of network maintenance (backup power source, staffing, etc.)	Self-organization and maintenance properties are built into the network
Mobile hosts are of relatively low complexity	Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capability)
Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	Main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
Widely deployed and currently in the third generation of evolution	Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

APPLICATIONS OF AD HOC WIRELESS NETWORKS

Military Application

- Adhoc wireless networks can be very useful in establishing communication among a group of soldiers for tactical operations.
- Setting up of a fixed infrastructure for communication among group of soldiers in enemy territories or in inhospitable terrains may not be possible.
- In such a case, adhoc wireless networks provide required communication mechanism quickly.
- The primary nature of the communication required in a military environment enforces certain important requirements on adhoc wireless networks namely, Reliability, Efficiency, Secure communication & Support for multicast routing.

Collaborative & Distributed computing

- Adhoc wireless network helps in collaborative computing, by establishing temporary communication infrastructure for quick communication with minimal configuration among a group of people in a conference.
- In distributed file sharing application reliability is of high importance which would be provided by adhoc network.
- Other applications such as streaming of multimedia objects among participating nodes in ad hoc wireless networks require support for soft real-time communication
- Devices used for such applications could typically be laptops with add-on wireless interface cards, enhanced personal digital assistants (PDAs) or mobile devices with high processing power

Emergency Operations

- Ad hoc wireless networks are very useful in emergency operations such as search and rescue, crowd control and commando operations
- The major factors that favour ad hoc wireless networks for such tasks are → self-configuration of the system with minimal overhead, independent of fixed or centralised infrastructure, the freedom and flexibility of mobility, and unavailability of conventional communication infrastructure.
- In environments, where the conventional infrastructure based communication facilities are destroyed due to a war or due to natural calamities, immediate deployment of adhoc wireless networks would be a good solution for co-ordinating rescue activities.
- They require minimum initial network configuration with very little or no delay

Wireless Mesh Network

- Wireless mesh networks are adhoc wireless network that are formed to provide an alternate communication infrastructure for mobile or fixed nodes/users, without the spectrum reuse constraint & requirement of network planning of cellular network.
- It provides many alternate paths for a data transfer session between a source & destination, resulting in quick reconfiguration of the path when the existing path fails due to node failure.
- Since the infrastructure built is in the form of small radio relaying devices, the investment required in wireless mesh networks is much less than what is required for the cellular network counterpart.
- The possible deployment scenarios of wireless mesh networks include: residential zones, highways, business zones, important civilian regions and university campuses
- Wireless mesh networks should be capable of self-organization and maintenance.
- It operates at license-free ISM band around 2.4 GHz & 5 GHz.
- It is scaled well to provide support to large number of points.
- Major advantage is the support for a high data rate, quick & low cost of deployment, enhanced services, high scalability, easy extendability, high availability & low cost per bit.

Wireless Sensor Networks:

- Sensor networks are special category of Adhoc wireless network that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.

- Sensor nodes are tiny devices that have capability of sensing physical parameters processing the data gathered, & communication to the monitoring system.
- The issue that make sensor network a distinct category of adhoc wireless network are the following:

Mobility of nodes :

- ✓ Mobility of nodes is not a mandatory requirement in sensor networks.
- ✓ For example, the nodes used for periodic monitoring of soil properties are not required to be mobile & the nodes that are fitted on the bodies of patients in a post-surgery ward of a hospital are designed to support limited or partial mobility.
- ✓ In general, sensor networks need not in all cases be designed to support mobility of sensor nodes.

Size of the network :

- ✓ The number of nodes in sensor network can be much larger than that in a typical ad hoc wireless network.

Density of deployment :

- ✓ The density of nodes in a sensor network varies with the domain of application.
- ✓ For example, Military applications require high availability of the network, making redundancy a high priority.

Power constraints :

- ✓ The power constraints in sensor networks are much more stringent than those in ad hoc wireless networks. This is mainly because the sensor nodes are expected to operate in harsh environmental or geographical conditions, with minimum or no human supervision and maintenance.
- ✓ In certain case, the recharging of the energy source is impossible.
- ✓ Running such a network, with nodes powered by a battery source with limited energy, demands very efficient protocol at network, data link, and physical layer.
- ✓ The power sources used in sensor networks can be classified into the following 3 categories:
  - *Replenishable Power source*: The power source can be replaced when the existing source is fully drained.
  - *Non-replenishable Power source*: The power source cannot be replenished once the network has been deployed. The replacement of sensor node is the only solution.
  - *Regenerative Power source:* Here, Power source employed in sensor network have the capability of regenerating power from the physical parameter under measurement.

Data / Information fusion :

- ✓ Data fusion refers to the aggregation of multiple packets into one before relaying it.
- ✓ Data fusion mainly aims at reducing the bandwidth consumed by redundant headers of the packets and reducing the media access delay involved in transmitting multiple packets.
- ✓ Information fusion aims at processing the sensed data at the intermediate nodes and relaying the outcome to the monitor node.

Traffic Distribution :

- ✓ The communication traffic pattern varies with the domain of application in sensor networks.
- ✓ For example, the environmental sensing application generates short periodic packets indicating the status of the environmental parameter under observation to a central monitoring station.
- ✓ This kind of traffic requires low bandwidth.
- ✓ Ad hoc wireless networks generally carry user traffic such as digitized & packetized voice stream or data traffic, which demands higher bandwidth.

Hybrid Wireless Networks

- One of the major application area of ad hoc wireless network is in the hybrid wireless architecture such as Multi-hop Cellular Network [MCN] & Integrated Cellular Adhoc Relay [iCAR].
- The primary concept behind cellular networks is geographical channel reuse.

- Several techniques like cell sectoring, cell resizing and multi tier cells increase the capacity of cellular networks.
- MCNs combine the reliability & support of fixed base station of cellular network with flexibility & multi-hop relaying adhoc wireless networks.
- Major advantages are as follows:
  - Higher capacity than cellular networks due to the better channel reuse.
  - Increased flexibility & reliability in routing.
  - Better coverage & connectivity in holes of a cell can be provided by means of multiple hops through intermediate nodes in a cell.

ISSUES IN AD HOC WIRELESS NETWORKS

The major issues that affect the design, deployment, & performance of an ad hoc wireless network system are :

- ♥ Medium Access Scheme.
- ♥ Transport Layer Protocol.
- ♥ Routing.
- ♥ Multicasting.
- ♥ Energy Management.
- ♥ Self-Organisation.
- ♥ Security.
- ♥ Addressing & Service discovery.
- ♥ Deployment considerations.
- ♥ Scalability.
- ♥ Pricing Scheme.
- ♥ Quality of Service Provisioning

Medium Access Scheme

The primary responsibility of a Medium Access Control (MAC) protocol in adhoc wireless networks is the distributed arbitration for the shared channel for transmission of packets. The major issues to be considered in designing a MAC protocol for adhoc wireless networks are as follows:

1. ***Distributed Operation:***
   - The ad hoc wireless networks need to operate in environments where no centralized coordination is possible.
   - The MAC protocol design should be fully distributed involving minimum control overhead.
2. ***Synchronization:***
   - The MAC protocol design should take into account the requirement of time synchronization.
   - Synchronization is mandatory for TDMA-based systems for management of transmission and reception slots.
3. ***Hidden Terminals:***
   - Hidden terminals are nodes that are hidden(or not reachable) from the sender of a data transmission session, but are reachable to the receiver of the session.
4. ***Exposed terminals:***
   - Exposed terminals, the nodes that are in the transmission range of the sender of an on-going session, are prevented from making a transmission.
5. ***Throughput:***
   - The MAC protocol employed in adhoc wireless networks should attempt to maximize the throughput of the system.
   - The important considerations for throughput enhancement are
     - Minimizing the occurrence of collisions.
     - Maximizing channel utilization and
     - Minimizing control overhead.
6. ***Access delay:***
   - The average delay that any packet experiences to get transmitted.

- The MAC protocol should attempt to minimize the delay.

7. ***Fairness****:*
   - Fairness refers to the ability of the MAC protocol to provide an equal share or weighted share of the bandwidth to all competing nodes.
   - Fairness can be either *node-based* or *flow-based.*
8. ***Real-time Traffic support*:**
   - In a contention-based channel access environment, without any central coordination, with limited bandwidth, and with location-dependent contention, supporting time- sensitive traffic such as voice, video, and real-time data requires explicit support from the MAC protocol.
9. ***Resource reservation*:**
   - The provisioning of QoS defined by parameters such as bandwidth, delay, and jitter requires reservation of resources such as *bandwidth, buffer space*, and *processing power*.
10. ***Ability to measure resource availability:***
    - In order to handle the resources such as bandwidth efficiently and perform call admission control based on their availability, the MAC protocol should be able to provide an estimation of resource availability at every node.
    - This can also be used for making *cogestion control decisions*.
11. ***Capability for power control:***
    - The transmission power control reduces the energy consumption at the nodes, causes a decrease in interference at neighboring nodes, and increases frequency reuse.
12. ***Adaptive rate control:***
    - This refers to the variation in the data bit rate achieved over a channel.
    - A MAC protocol that has adaptive rate control can make use of a high data rate when the sender and receiver are nearby & adaptively reduce the data rate as they move away from each other.
13. ***Use of directional antennas:***
    - This has many advantages that include
      - Increased spectrum reuse.
      - Reduction in interference and
      - Reduced power consumption.

Routing

The responsibilities of a routing protocol include exchanging the route information; finding a feasible path to a destination. The major challenges that a routing protocol faces are as follows:

1. ***Mobility :***
   - The Mobility of nodes results in frequent path breaks, packet collisions, transient loops, stale routing information, and difficulty in resource reservation.
2. ***Bandwidth constraint :***
   - Since the channel is shared by all nodes in the broadcast region, the bandwidth available per wireless link depends on the number of nodes & traffic they handle.
3. ***Error-prone and shared channel :***
   - The Bit Error Rate (BER) in a wireless channel is very high [10^{-5} to 10^{-3}] compared to that in its wired counterparts [10^{-12} to 10^{-9}].
   - Consideration of the state of the wireless link, signal-to-noise ratio, and path loss for routing in ad hoc wireless networks can improve the efficiency of the routing protocol.
4. ***Location-dependent contention :***
   - The load on the wireless channel varies with the number of nodes present in a given geographical region.
   - This makes the contention for the channel high when the number of nodes increases.
   - The high contention for the channel results in a high number of collisions & a subsequent wastage of bandwidth.
5. ***Other resource constraints :***
   - The constraints on resources such as computing power, battery power, and buffer storage also limit the capability of a routing protocol.

The major requirements of a routing protocol in adhoc wireless networks are the following.

1. ***Minimum route acquisition delay :***
   - The route acquisition delay for a node that does not have a route to a particular destination node should be as minimal as possible.
   - The delay may vary with the size of the network and the network load.
2. ***Quick route reconfiguration :***
   - The unpredictable changes in the topology of the network require that the routing protocol be able to quickly perform route reconfiguration in order to handle path breaks and subsequent packet losses.
3. ***Loop-free routing*** *:*
   - This is a fundamental requirement to avoid unnecessary wastage of network bandwidth.
   - In adhoc wireless networks, due to the random movement of nodes, transient loops may form in the route thus established.
   - A routing protocol should detect such transient routing loops & take corrective actions.
4. ***Distributed routing approach :***
   - An adhoc wireless network is a fully distributed wireless network & the use of centralized routing approaches in such a network may consume a large amount of bandwidth.
5. ***Minimum control overhead :***
   - The control packets exchanged for finding a new route, and maintaining existing routes should be kept as minimal as possible.
6. ***Scalability :***
   - Scalability is the ability of the routing protocol to scale well in a network with a large number of nodes.
   - This requires minimization of control overhead & adaptation of the routing protocol to the network size.
7. ***Provisioning of QoS:***
   - The routing protocol should be able to provide a certain level of QoS as demanded by the nodes or the category of calls.
   - The QoS parameters can be bandwidth, delay, jitter, packet delivery ratio, & throughput.
8. ***Support for time-sensitive traffic :***
   - Tactical communications & similar applications require support for time-sensitive traffic.
   - The routing protocol should be able to support both hard real-time & soft real-time traffic.
9. ***Security and privacy :***
   - The routing protocol in adhoc wireless networks must be resilient to threats and vulnerabilities.
   - It must have inbuilt capability to avoid resource consumption, denial-of-service, impersonation, and similar attacks possible against an ad hoc wireless network.

Multicasting

It plays important role in emergency search & rescue operations & in military communication. Use of single-link connectivity among the nodes in a multicast group results in a tree-shaped multicast routing topology. Such a tree-shaped topology provides high multicast efficiency, with low packet delivery ratio due to the frequency tree breaks. The major issues in designing multicast routing protocols are as follows:

1.***Robustness :***
- The multicast routing protocol must be able to recover & reconfigure quickly from potential mobility-induced link breaks thus making it suitable for use in high dynamic environments.

2***. Efficiency :***
- A multicast protocol should make a minimum number of transmissions to deliver a data packet to all the group members.

3***. Control overhead :***
- The scarce bandwidth availability in ad hoc wireless networks demands minimal control overhead for the multicast session.

4***. Quality of Service :***

- QoS support is essential in multicast routing because, in most cases, the data transferred in a multicast session is time-sensitive.

5. ***Efficient group management :***

- Group management refers to the process of accepting multicast session members and maintaining the connectivity among them untill the session expires.

6 . ***Scalability :***

- The multicast routing protocol should be able to scale for a network with a large number of node

7. ***Security :***

- Authentication of session members and prevention of non-members from gaining unauthorized information play a major role in military communications.

Transport Layer Protocol

- The main objectives of the transport layer protocols include :
  - ✓ Setting up & maintaining end-to-end connections,
  - ✓ Reliable end-to-end delivery of packets,
  - ✓ Flow control &
  - ✓ Congestion control.

Examples of some transport layers protocols are,

a. UDP (User Datagram Protocol) :

- It is an unreliable connectionless transport layer protocol.
- It neither performs flow control & congestion control.
- It do not take into account the current network status such as congestion at the intermediate links, the rate of collision, or other similar factors affecting the network throughput.

b. TCP (Transmission Control Protocol):

- It is a reliable connection-oriented transport layer protocol.
- It performs flow control & congestion control.
- Here performance degradation arises due to frequent path breaks, presence of stale routing information, high channel error rate, and frequent network partitions.

Pricing Scheme

- Assume that an optimal route from node A to node B passes through node C, & node C is not powered on.
- Then node A will have to set up a costlier & non-optimal route to B.
- The non-optimal path consumes more resources & affects the throughput of the system.
- As the intermediate nodes in a path that relay the data packets expend their resources such as battery charge & computing power, they should be properly compensated.
- Hence, pricing schemes that incorporate service compensation or service reimbursement are required.

Quality of Service Provisioning (QoS)

- QoS is the performance level of services offered by a service provider or a network to the user.
- QoS provisioning often requires ,
  - ✓ Negotiation between host & the network.
  - ✓ Resource reservation schemes.
  - ✓ Priority scheduling &
  - ✓ Call admission control.
- ***QoS parameters :***

Applications	Corresponding QoS parameter
1.Multimedia application	1. Bandwidth & Delay.
2.Military application	2.Security & Reliability.
3.Defense application	3.Finding trustworthy intermediate hosts & routing.

4.Emergency search and rescue operations	4.Availability.
5.Hybrid wireless network	5.Maximum available link life, delay, bandwidth & channel utilization.
6.communication among the nodes in a sensor network	6.Minimum energy consumption, battery life & energy conservation

- ***QoS-aware routing :***
  i. Finding the path is the first step toward a QoS-aware routing protocol.
  ii. The parameters that can be considered for routing decisions are,
    - Network throughput.
    - Packet delivery ratio.
    - Reliability.
    - Delay.
    - Delay jitter.
    - Packet loss rate.
    - Bit error rate.
    - Path loss.

- ***QoS framework :***
  I. A framework for QoS is a complete system that attempts to provide the promised services to each user or application.
  II. The key component of QoS framework is a QoS service model which defines the way user requirements are served.

Self-Organization

- One very important property that an ad hoc wireless network should exhibit is organizing & maintaining the network by itself.
- The major activities that an ad hoc wireless network is required to perform for self-organization are,
  - ✓ Neighbour discovery.
  - ✓ Topology organization &
  - ✓ Topology reorganization (updating topology information)

Security

1) Security is an important issue in ad hoc wireless network as the information can be hacked.
2) Attacks against network are of 2 types :
   I. *Passive attack* → Made by malicious node to obtain information transacted in the network without disrupting the operation.
   II. *Active attack* → They disrupt the operation of network.
   Further active attacks are of 2 types :
   - *External attack*: The active attacks that are executed by nodes outside the network.
   - *Internal attack:* The active attacks that are performed by nodes belonging to the same network.

3) The major security threats that exist in ad hoc wireless networks are as follows :
   ★ ***Denial of service*** – The attack affected by making the network resource unavailable for service to other nodes, either by consuming the bandwidth or by overloading the system.
   ★ ***Resource consumption*** – The scarce availability of resources in ad hoc wireless network makes it an easy target for internal attacks, particularly aiming at consuming resources available in the network.
   The major types of resource consumption attacks are,
   - ✓ Energy depletion :
     - Highly constrained by the energy source
     - Aimed at depleting the battery power of critical nodes.

- ✓ Buffer overflow :
  - Carried out either by filling the routing table with unwanted routing entries or by consuming the data packet buffer space with unwanted data.
  - Lead to a large number of data packets being dropped, leading to the loss of critical information.

★ ***Host impersonation*** – A 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*** – A compromised node can act as an informer by deliberate disclosure of confidential information to unauthorized nodes.

★ ***Interference*** – A common attack in defense applications to jam the wireless communication by creating a wide spectrum noise.

Addressing and service discovery

- Addressing & service discovery assume significance in ad hoc wireless network due to the absence of any centralised coordinator.
- An address that is globally unique in the connected part of the ad hoc wireless network is required for a node in order to participate in communication.
- Auto-configuration of addresses is required to allocate non-duplicate addresses to the nodes.

Energy Management

- Energy management is defined as the process of managing the sources & consumers of energy in a node or in the network for enhancing the lifetime of a network.
- Features of energy management are :
  →Shaping the energy discharge pattern of a node's battery to enhance battery life.
  →Finding routes that consumes minimum energy.
  →Using distributed scheduling schemes to improve battery life.
  →Handling the processor & interface devices to minimize power consumption.
- Energy management can be classified into the following categories :

a. ***Transmission power management*** **:**
- The power consumed by the Radio Frequency (RF) module of a mobile node is determined by several factors such as
  * The state of operation.
  *The transmission power and
  *The technology used for the RF circuitry.
- The state of operation refers to transmit,receive, and sleep modes of the operation.
- The transmission power is determined by
  * Reachability requirement of the network.
  * Routing protocol and
  * MAC protocol employed.

b. Battery energy management :
- The battery management is aimed at extending the battery life of a node by taking advantage of its chemical properties,discharge patterns, and by the selection of a battery from a set of batteries that is available for redundancy.

c. ***Processor power management :***
- The clock speed and the number of instructions executed per unit time are some of the processor parameters that affect power consumption.
- The CPU can be put into different power saving modes during low processing load conditions.
- The CPU power can be completely turned off if the machines is idle for a long time.In such a cases, interrupts can be used to turn on the CPU upon detection of user interaction or other events.

d. Devices power management :
- Intelligent device management can reduce power consumption of a mobile node significantly.

- This can be done by the operating system(OS) by selectively powering down interface devices that are not used or by putting devices into different power saving modes, depending on their usage.

Scalability

- Scalability is the ability of the routing protocol to scale well in a network with a large number of nodes.
- It requires minimization of control overhead & adaptation of the routing protocol to the network size.

Deployment Considerations

The deployment of a commercial ad hoc wireless network has the following benefits when compared to wired networks

a) *Low cost of deployment :*
- The use of multi-hop wireless relaying eliminatesthe requirement of cables & maintenance in deployment of communication infrastructure.
- The cost involved is much lower than that of wired networks.

b) Incremental deployment :
- Deployment can be performed incrementally over geographical regions of the city.
- The deployed part of the network starts functioning immediately after the minimum configuration is done.

c) *Short deployment time :*
- Compared to wired networks, the deployment time is considerably less due to the absence of any wired links.

d) *Reconfigurability :*
- The cost involved in reconfiguring a wired network covering a Metropolitan Area Network(MAN) is very high compared to that of an ad hoc wireless network covering the same service area.

The following are the major issues to be considered in deploying an ad hoc wireless network :

a) *Scenario of deployment* :
- The scenario of deployment has significance because the capability required for a mobile node varies with the environment in which it is used.
- The following are some of the different scenarios in which the deployment issues vary widely :
  - *military deployment :*
    It can be either,
    - ✓ Data-centric network : Handle a different pattern of data traffic & can be partially comprised of static nodes.
      Eg : a wireless sensor network.
    - ✓ User-centric network: Consists of highly mobile nodes with or without any support from any infrastructure.
      Eg :soldiers or armored vehicles carrying soldiers equipped with wireless communication devices.
  - *Emergency operations deployment* :
    - Demands a quick deployment of rescue personnel equipped with hand-held communication equipment.
    - The network should provide support for time-sensitive traffic such as voice & video.
    - Short data messaging can be used in case the resource constraints do not permit voice communication.
  - *Commercial wide-area deployment :*
    - Eg : wireless mesh networks.
    - The aim of the deployment is to provide an alternate communication infrastructure for wireless communication in urban areas & areas where a traditional cellular base station cannot handle the traffic volume.
  - *Home network deployment :*

- Deployment needs to consider the limited range of the devices that are to be connected by the network.
- Eg : short transmission range avoid network patitions.

b) ***Required longevity of network :***

- If the network is required for a short while, battery-powered mobile nodes can be used.
- If the connectivity is required for a longer duration of time, fixed radio relaying equipment with regenerative power sources can be deployed.

c) ***Area of coverage :***

- Determined by the nature of application for which the network is set up.
- Eg : the home area network is limited to the surroundings of a home.
- The mobile nodes' capabilities such as the transmission range & associated hardware, software, & power source should match the area of coverage required.

d)***Service availability :***

- Defined as the ability of an ad hoc wireless network to provide service even with the failure of certain nodes.
- Has significance in a Fully mobile ad hoc wireless network used for tactical communication & in partially fixed ad hoc wireless network used in commercial communication infrastructure such as wireless mesh networks.

e)***Operational integration with other infrastructure :***

- Considered for improving the performance or gathering additional information, or for providing better QoS.
- In military environment, integration of ad hoc wireless networks with satellite networks or unmanned aerial vehicles(UAVs) improves the capability of the ad hoc wireless networks.

f)***Choice of protocol :***

- The choice of protocols at different layers of the protocol stack is to be done taking into consideration the deployment scenario.
- A TDMA-based & insecure MAC protocol may not be the best suited compared to a CDMA-based MAC protocol for a military application.

AD HOC WIRELESS INTERNET

- Ad hoc wireless internet extends the services of the internet to the end users over an ad hoc wireless network.
- Some of the applications of ad hoc wireless internet are :
  - ✓ Wireless mesh network.
  - ✓ Provisioning of temporary internet services to major conference venues.
  - ✓ Sports venues.
  - ✓ Temporary military settlements.
  - ✓ Battlefields &
  - ✓ Broadband internet services in rural regions.
- The major issues to be considered for a successful ad hoc wireless internet are the following :
  - ❖ **Gateway :**
    - They are the entry points to the wired internet.
    - Generally owned & operated by a service provider.
    - They perform following tasks ,
      - Keeping track of end users.
      - Bandwidth management.
      - Load balancing.
      - Traffic shaping.
      - Packet filtering.
      - Width fairness &
      - Address, service & location discovery.

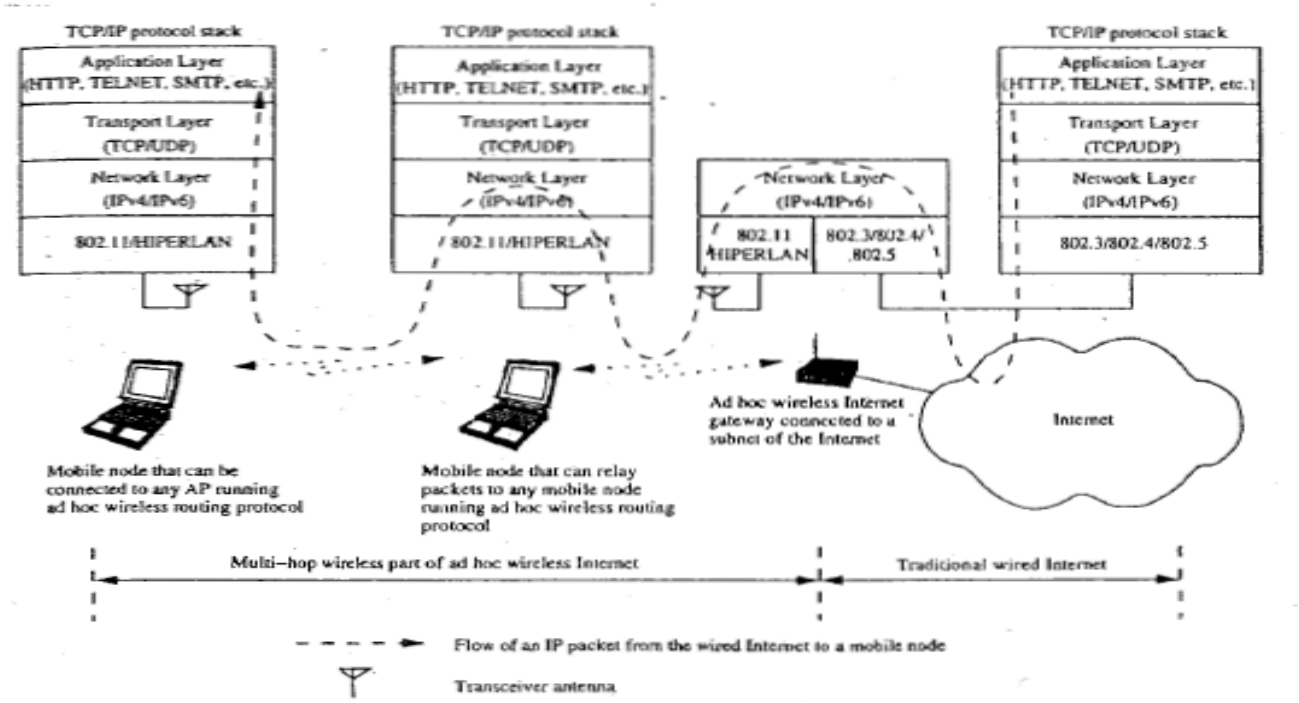


Figure 5.7 Schematic diagram of ad hoc wireless internet

- **Address mobility :**
  - This problem is worse here as the nodes operate over multiple wireless hops.
  - Solution such as Mobile IP can provide temporary alternative.
- **Routing :**
  - It is a major problem in ad hoc wireless internet, due to dynamic topological changes, the presence of gateways, multi-hop relaying, & the hybrid character of the network.
  - Possible solution is to use separate routing protocol for the wireless part of ad hoc wireless internet.
- **Transport layer protocol :**
  - Several factors are to be considered here, the major one being the state maintenance overhead at the gateway nodes.
- **Load balancing :**
  - They are essential to distribute the load so as to avoid the situation where the gateway nodes become bottleneck nodes.
- **Pricing / Billing :**
  - Since internet bandwidth is expensive, it becomes very important to introduce pricing/billing strategies for the ad hoc wireless internet.
- **Provisioning of security :**
  - Security is a prime concern since the end users can utilize the ad hoc wireless internet infrastructure to make e-commerce transaction.
- **QoS support :**
  - With the widespread use of voice over IP(VOIP) & growing multimedia applications over the internet, provisioning of QoS support in the ad hoc wireless internet becomes a very important issue.
- **Service, address & location discovery :**
  - Service discovery refers to the activity of discovering or identifying the party which provides service or resource.
  - Address discovery refers to the services such as those provided by Address Resolution Protocol (ARP) or Domain Name Service (DNS) operating within the wireless domain.
  - Location discovery refers to different activities such as detecting the location of a particular mobile node in the network or detecting the geographical location of nodes.

UNIT 2
MAC – 1

ISSUES IN DESIGNING MAC PROTOCOL FOR AD HOC WIRELESS NETWORK

The main issues in designing MAC protocol for ad hoc wireless network are:

Bandwidth efficiency

- Bandwidth must be utilized in efficient manner
- Minimal Control overhead
- BW = ratio of BW used for actual data transmission to the total available BW

Quality of service support

- ★ Essential for supporting time-critical traffic sessions
- ★ They have resource reservation mechanism that takes into considerations the nature of wireless channel and the mobility of nodes

Synchronisation

- ★ MAC protocol must consider synchronisation between nodes in the network
- ★ Synchronisation is very important for BW (time slot) reservation by nodes
- ★ Exchange of control packets may be required for achieving time synchronisation among nodes

Hidden and exposed terminal problems

- ★ The 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.

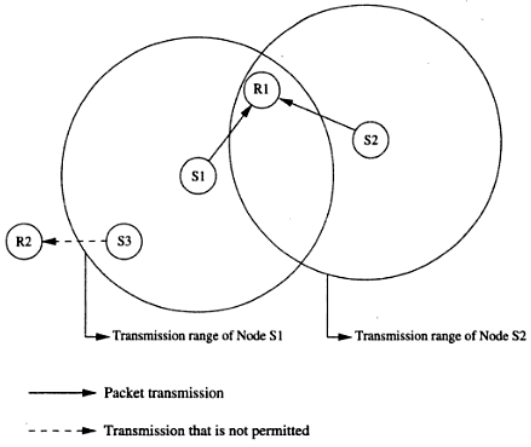


Figure 6.1. Hidden and exposed terminal problems.

- ★ S1 and S2 are hidden from each other & they transmit simultaneously to R1 which leads to collision
- ★ The 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
- ★ If S1 is already transmitting to R1, then S3 cannot interfere with on-going transmission & it cannot transmit to R2.
- ★ The hidden & exposed terminal problems reduce the throughput of a network when traffic load is high

Error-prone shared broadcast channel

- ★ When a node is receiving data, no other node in its neighbourhood should transmit
- ★ A node should get access to the shared medium only when its transmission do not affect any ongoing session
- ★ MAC protocol should grant channel access to nodes in such a manner that collisions are minimized
- ★ Protocol should ensure fair BW allocation

Distributed nature/lack of central coordination

- ★ Do not have centralised coordinators
- ★ Nodes must be scheduled in a distributed fashion for gaining access to the channel
- ★ MAC protocol must make sure that additional overhead, in terms of BW consumption, incurred due to this control information is not very high

Mobility of nodes

- ★ Nodes are mobile most of the time
- ★ The protocol design must take this mobility factor into consideration so that the performance of the system is not affected due to node mobility

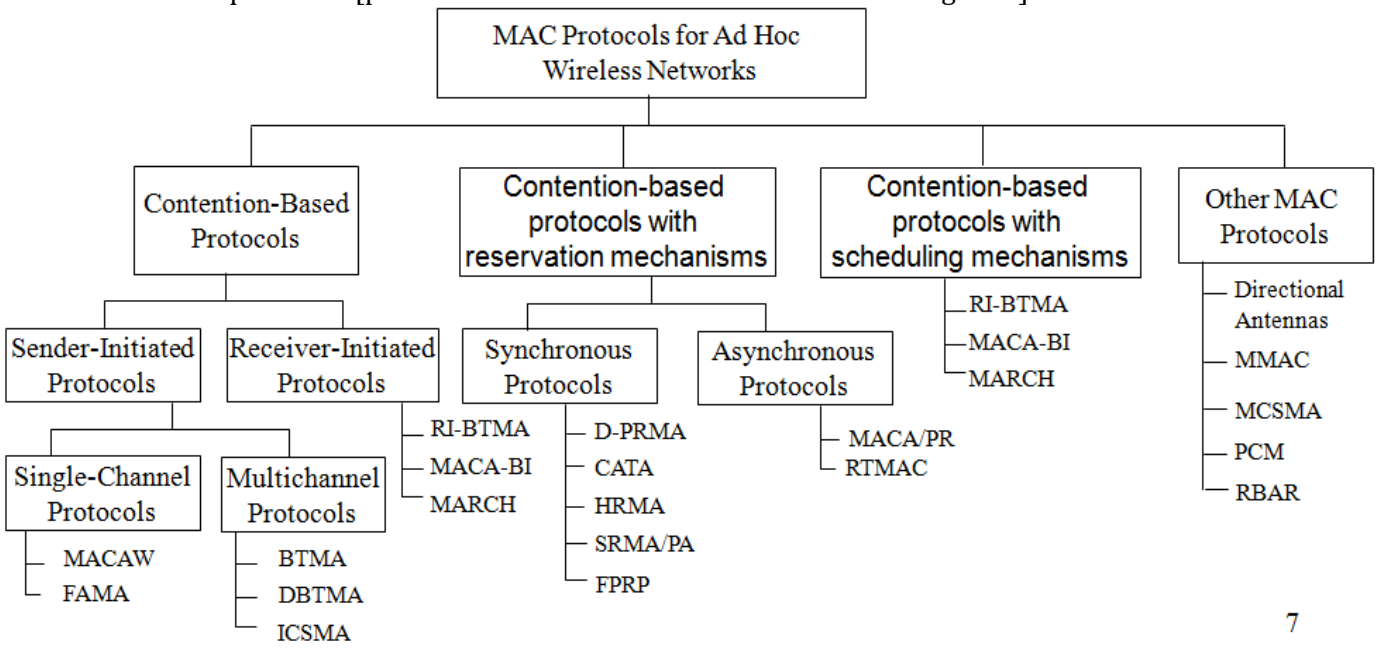
DESIGN GOALS OF A MAC PROTOCOL FOR AD HOC WIRELESS NETWORKS

- ♥ The operation of a protocol should be distributed
- ♥ The protocol should provide QoS support for real-time traffic
- ♥ The access delay, which refers to the average delay experienced by any packet to get transmitted, must be kept low
- ♥ The available bandwidth must be utilised efficiently
- ♥ The protocol should ensure fair allocation of bandwidth to nodes
- ♥ Control overhead must be kept as low as possible
- ♥ The protocol should minimise the effects of hidden and exposed terminal problems
- ♥ The protocol must be scalable to large networks
- ♥ It should have power control mechanisms in order to efficiently manage energy consumption of the nodes
- ♥ The protocol should have mechanisms for adaptive data rate control
- ♥ It should try to use directional antennas which can provide advantages such as reduced interference, increased spectrum reuse, and reduced power consumption
- ♥ The protocol should provide time synchronisation among nodes

CLASSIFICATION OF MAC PROTOCOLS

Ad hoc network MAC protocols can be classified into three basic types:

i. Contention-based protocols
ii. Contention-based protocols with reservation mechanisms
iii. Contention-based protocols with scheduling mechanisms
iv. Other MAC protocols [protocols which do not fall under above 3 categories]



7

- **Contention-based protocols**
  - ***Sender-initiated protocols***: Packet transmissions are initiated by the sender node.
    - *Single-channel sender-initiated protocols*: A node that wins the contention to the channel can make use of the entire bandwidth.
    - *Multichannel sender-initiated protocols:* The available bandwidth is divided into multiple channels.
  - ***Receiver-initiated protocols*:** The receiver node initiates the contention resolution protocol.
- **Contention-based protocols with reservation mechanisms**
  - ***Synchronous protocols***: All nodes need to be synchronized. Global time synchronization is difficult to achieve.
  - ***Asynchronous protocols:*** These protocols use relative time information for effecting reservations.
- **Contention-based protocols with scheduling mechanisms**
  - Node scheduling is done in a manner so that all nodes are treated fairly and no node is starved of bandwidth.
  - Scheduling-based schemes are also used for enforcing priorities among flows whose packets are queued at nodes.
  - Some scheduling schemes also consider battery characteristics.
- **Other protocols** are those MAC protocols that do not strictly fall under the above categories.

CONTENTION BASED PROTOCOLS

[OUT OF SYLLABUS] but some questions have been asked from this section. I have answered them just for your reference.

Explain in detail MACA for wireless LAN (MACAW) and floor acquisition multiple access protocol (FAMA)

MACAW (MACA for Wireless) is a revision of MACA.

- The sender senses the carrier to see and transmits a **RTS** (**Request To Send)** frame if no nearby station transmits a RTS.
- The receiver replies with a **CTS** (**Clear To Send**) frame.
- The MACAW protocol uses one more control packet called the **request-for-request-to-send (RRTS)**

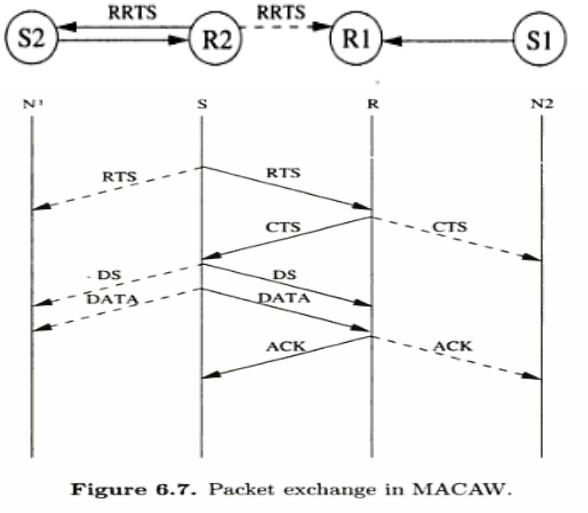


Figure 6.7. Packet exchange in MACAW.

- Neighbors
  - see CTS, then keep quiet.
  - see RTS but not CTS, then keep quiet until the CTS is back to the sender.
- The receiver sends an ACK when receiving an frame.
  - Neighbors keep silent until see ACK.
- Collisions
  - There is no collision detection.

- The senders know collision when they don't receive CTS.
- They each wait for the exponential back-off time.

Floor acquisition Multiple Access Protocols (FAMA)

- Based on a channel access discipline which consists of a carrier-sensing operation and a collision-avoidance dialog between the sender and the intended receiver of a packet.
- Floor acquisition refers to the process of gaining control of the channel.
- At any time only one node is assigned to use the channel.
- Carrier-sensing by the sender, followed by the RTS-CTS control packet exchange, enables the protocol to perform as efficiently as MACA.
- Two variations of FAMA
  - RTS-CTS exchange with no carrier-sensing uses the ALOHA protocol for transmitting RTS packets.
  - RTS-CTS exchange with non-persistent carrier-sensing uses non-persistent CSMA for the same purpose.

Explain MACA by invitation protocol and media access with reduced handshake protocol.

MACA-By Invitation Protocol

- It is a receiver-initiated protocol
- It reduces the number of control packets used in the MACA protocol
- It eliminated the need for the RTS packet
- In MACA-BI, the receiver node initiates data transmission by transmitting a ready-to-receive (RTR) control packet to the sender as shown in the figure

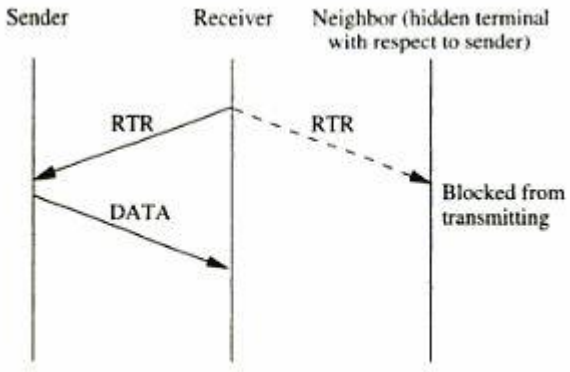


Figure 6.11. Packet transmission in MACA-BI.

- If it is ready to transmit, the sender node respond by sending a DATA packet
- Thus data transmission in MACA-BI occurs through a two-way handshake mechanism
- The efficiency of the MACA-BI scheme is mainly dependent on the ability of the receiver node to predict accurately the arrival rates of traffic at the sender nodes

Media Access with Reduced Handshake Protocol

- It is a receiver-initiated protocol.
- Doesn't require any traffic prediction mechanism.
- Exploits the broadcast nature of traffic from omni-directional antennas to reduce the number of handshakes involved in the data transmission
- A node obtains information about the data packet arrivals at its neighbouring nodes by overheading the CTS packets transmitted by them.
- It then sends a CTS packet to the concerned neighbour node for relaying data from that node
- This mechanism is as shown below

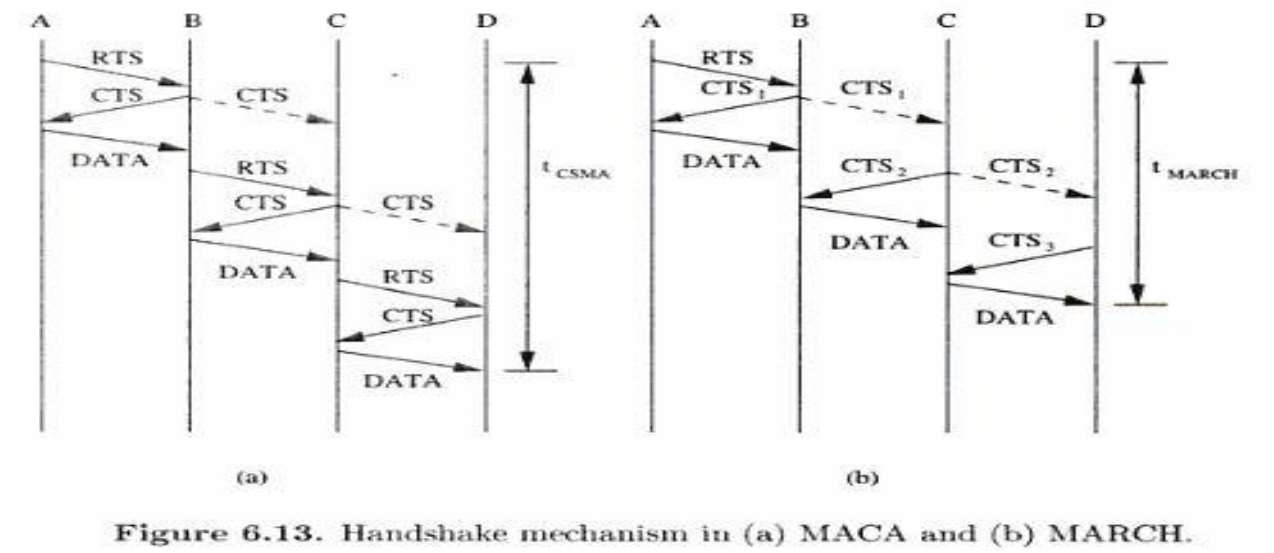


Figure 6.13. Handshake mechanism in (a) MACA and (b) MARCH.

- The throughput of MARCH is significantly high compared to MACA
- Control overhead is much less
- Less BW is consumed for control traffic

MACA protocol and Busy Tone Multiple Access Protocol also comes under Contention Based Protocol → Since they are out of syllabus, it is left to you whether to study it or not.

CONTENTION BASED PROTOCOLS WITH RESERVATION MECHANISMS

Distributed Packet Reservation Multiple Access Protocol (D-PRMA)

- It extends the centralized packet reservation multiple access (PRMA) scheme into a distributed scheme that can be used in ad hoc wireless networks.
- PRMA was designed in a wireless LAN with a base station.
- D-PRMA extends PRMA protocol in a wireless LAN.
- D-PRMA is a TDMA-based scheme.
- The channel is divided into fixed- and equal-sized frames along the time axis.

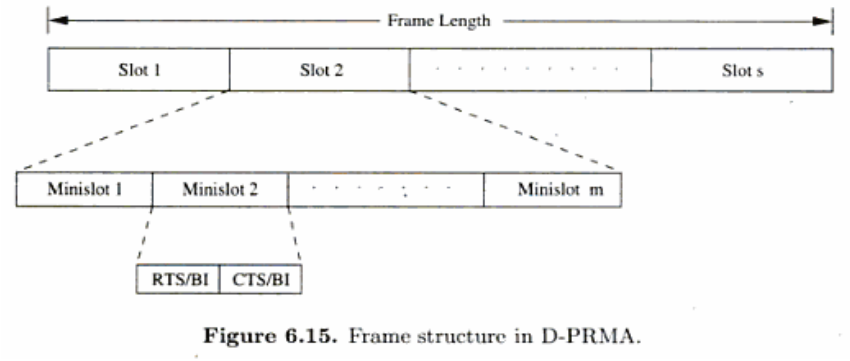


Figure 6.15. Frame structure in D-PRMA.

- Each frame is composed of s slots and each slot consists of m minislots
- Each minislot is further divided into two control fields, RTS/BI and CTS/BI
- These control fields are used for slot reservation and for overcoming the hidden terminal problem
- All nodes having packets ready for transmission contend for the first minislot of each slot
- The remaining (m-1) minislots are granted to the node that wins the contention.
- Also, the same slot in each subsequent frame can be reserved for this winning terminal until it completes its packet transmission session
- Within a reserved slot, communication between the source and receiver nodes takes by means of either time division duplexing (TDD) or frequency division duplexing (FDD)

- Any node that wants to transmit packets has to first reserve slots
- A certain period at the beginning of each minislot is reserved for carrier sensing
- In order to prioritize nodes transmitting voice traffic over nodes transmitting normal data traffic, two rules are followed in D-PRMA
    - 1st rule → voice nodes are allowed to start contending from minislot 1 with probability p=1. Others with p<1
    - 2nd rule → only if the node winning the minislot contention is a voice node, it is permitted to reserve the same slot in each subsequent frame until the end of the session
- In order to avoid the hidden terminal problem, all nodes hearing the CTS sent by the receiver are not allowed to transmit during the remaining period of that same slot
- In order to avoid the exposed terminal problem, a node hearing the RTS but not the CTS is still allowed to transmit
- Requirement 1 → when a node wins the contention in minislot 1, other terminals must be prevented from using any of the remaining (m-1) minislots in the same slot for contention
- Requirement 2 → when a slot is reserved in subsequent frames, other nodes should be prevented from contending for those reserved slots
- D-PRMA is more suited for voice traffic than for data traffic applications

Collision Avoidance Time Allocation Protocol (CATA)

- It is based on dynamic topology-dependent transmission scheduling
- Nodes contend for and reserve time slots by means of a distributed reservation and handshake mechanism.
- Support broadcast, unicast, and multicast transmissions.
- The operation is based on two basic principles:
    - The receiver(s) of a flow must inform the potential source nodes about the reserved slot on which it is currently receiving packets. The source node must inform the potential destination node(s) about interferences in the slot.
    - Usage of negative acknowledgements for reservation requests, and control packet transmissions at the beginning of each slot, for distributing slot reservation information to senders of broadcast or multicast sessions.
- Time is divided into equal-sized frames, and each frame consists of S slots.
- Each slot is further divided into five minislots.
- The first 4 minislots are used for transmitting control packets and are called control minislots (CMS)
- The last minislot is called data minislot (DMS)

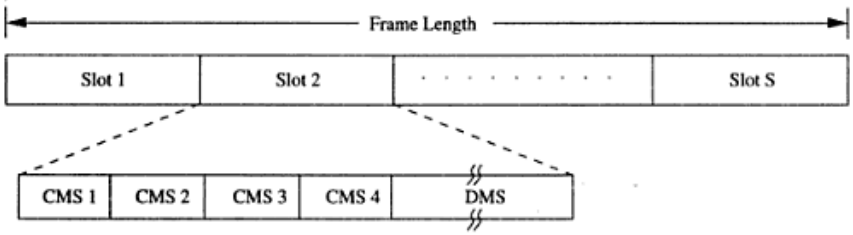


Figure 6.16. Frame format in CATA.

- Each node that receives data during the DMS of the current slot transmits a slot reservation (SR) packet during the CMS1 of the slot
- This serves to inform other neighbouring potential sender nodes about the currently active reservations
- The SR packet is either received without error at the neighbouring nodes or causes noise at those nodes, preventing them from attempting to reserve the current slot
- Every node that transmits data during the DMS of the current slot transmits a request-to-send packet
- The receiver node of a unicast session transmits a clear-to-send packet
- On receiving this packet, the source node clearly understands that the reservation was successful and transmits data during the DMS of that slot until unicast flow gets terminated

- Once the reservation has been made successfully in a slot, from the next slot onward, both the sender and receiver do not transmit anything during CMS3 and during CMS4 the sender node alone transmits a not-to-send (NTS) packet
- The not-to-send (NTS) packet serves as a negative acknowledgement
- A potential multicast or broadcast source node that receives the NTS packet or that detects noise, understands that its reservation request has failed & does not transmit during DMS of current slot
- The length of the frame is very important in CATA
- The worst case value of the frame-length = $Min(d^2+1, N)$, where d is the maximum degree of a node in the network and N is the total number of nodes in the network
- CATA works well with simple single-channel half-duplex radios
- It is simple and provides support for collision-free broadcast and multicast traffic

Hop Reservation Multiple Access Protocol

- A multichannel MAC protocol which is based on half-duplex, very slow frequency-hopping spread spectrum (FHSS) radios
- Uses a reservation and handshake mechanism to enable a pair of communicating nodes to reserve a frequency hop, thereby guaranteeing collision-free data transmission.

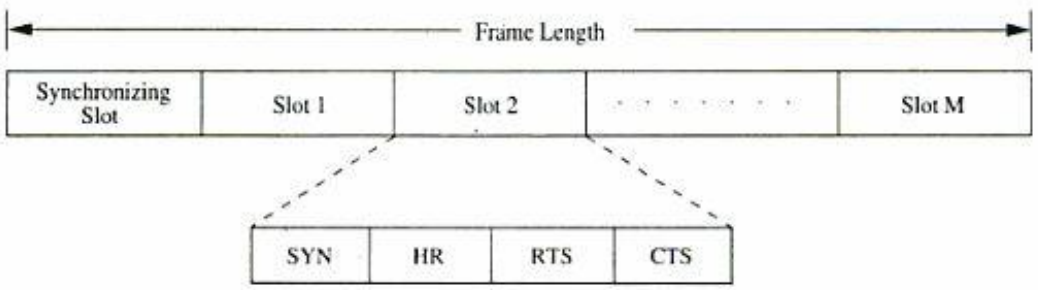


Figure 6.17. Frame format in HRMA.

- There are L frequency channels available
- HRMA uses one frequency channel, denoted by f_0 as a dedicated synchronising channel
- The nodes exchange synchronisation information on f_0
- The remaining L-1 frequencies are divided into M=(L-1)/2 frequency pairs
- f_i is used for transmitting and receiving hop-reservation packets, RTS, CTS and data packets
- f_i^* is used for sending and receiving acknowledgement (ACK) packets
- The data packets transmitted can be of any size.
- Data transmission can take place through a single packet or a train of packets.
- In HRMA, time is slotted and each slot is assigned a separate frequency hop
- Each time slot is divided into four periods, namely, synchronising period, HR period, RTS period, and CTS period
- Each period meant for transmitting or receiving the synchronising packet, FR packet, RTS packet, and CTS packet respectively.
- During the synchronising period of each slot, all idle nodes hop to the synchronising frequency f_0 and exchange synchronisation information

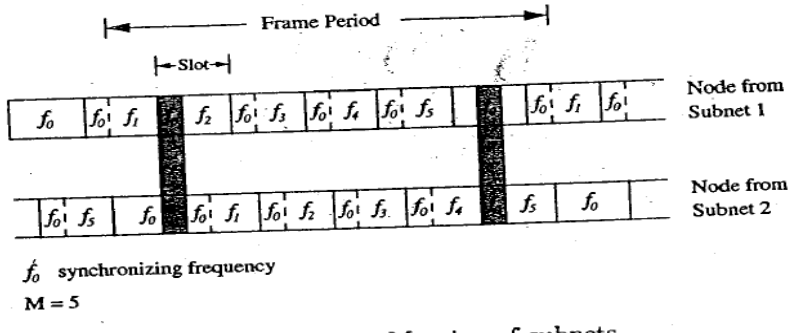


Figure Merging of subnets.

- When a new node enters the network, it remains on the synchronising frequency f_0 for a long enough period of time so as to gather synchronisation information such as the hopping pattern and the timing of the system
- If it receives no information, it assumes that it is the only node in the network, broadcasts its own synchronisation information and forms a one-node system
- Figure above depicts the worst-case frequency overlap scenario
- When a node receives data to be transmitted, it first listens to the HR period of the immediately following slot
- If it finds the channel to be free during the SR period, it transmits an RTS packet to the destination during the RTS period of the slot and waits for the CTS packet
- On receiving the RTS, the destination node transmits the CTS packet during the CTS period of the same slot and waits for the data packet
- If the source node receives the CTS packet correctly, it implies that the source and receiver nodes have successfully reserved the current hop
- After transmitting each data packet, the source node hops onto this acknowledgement frequency.
- The receiver sends an ACK packet back to the source.

Soft Reservation Multiple Access with Priority Assignment

- Developed with the main objective of supporting integrated services of real-time and non-real-time application in ad hoc networks, at the same time maximizing the statistical multiplexing gain.
- Nodes use a collision-avoidance handshake mechanism and a soft reservation mechanism
- Unique frame structure
- Soft reservation capability for distributed ad dynamic slot scheduling
- Dynamic and distributed access priority assignment and update policies
- Time constrained back-off algorithm
- Time is divided into frames, with each frame consisting of a fixed number of slots
- Each slot is further divided into 6 different fields (figure) namely SYNC, soft reservation (SR), reservation request (RR), reservation confirm (RC), data sending (DS) and acknowledgement (ACK)

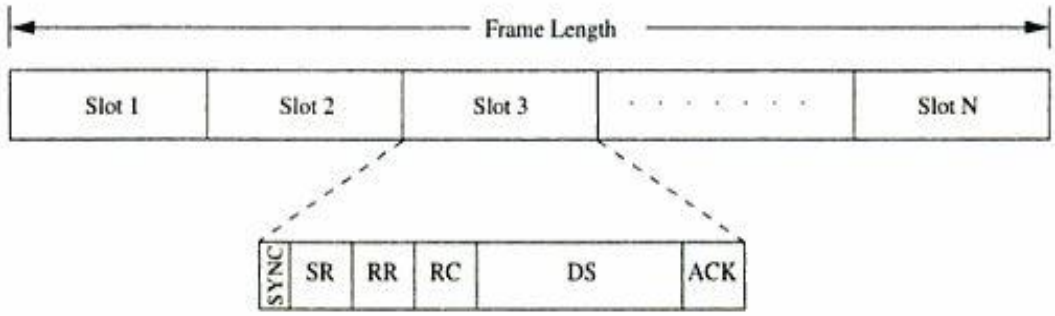


Figure 6.19. Frame structure in SRMA/PA.

- The SYNC field is used for synchronisation purposes
- The SR, RR, RC, and ACK fields are used for transmitting and receiving the corresponding control packets
- The DS field is used for data transmission
- The SR packet serves as a busy tone
- It informs the nodes about the reservation of the slot
- SR packet also carries the access priority value assigned to the node that has reserved the slot
- When an idle node receives a data packet for transmission, the node waits for a free slot and transmits the RR packet in the RR field of that slot
- A node determines whether or not a slot is free through the SR field of that slot
- In case of a voice terminal node, the node tries to take control of the slot already reserved by a data terminal if it finds it priority level to be higher than that of the data terminal

- This process is called *soft reservation.*
- Priority levels are initially assigned to nodes based on the service classes in a static manner
- It is required that priority of voice terminal $p_v^{(R)}$ > priority of data terminal $p_d^{(R)}$ such that delay-sensitive voice applications get preference over normal data applications
- A node that is currently transmitting is said to be in active state
- A node that is said to be in the idle state if it does not have any packet to be transmitted
- In the active state itself, nodes can be in one of the two states: access state and reserved state
- Access state is one in which the node is backlogged and is trying to reserve a slot for transmission
- The access priorities are assigned to nodes and updated in a distributed and dynamic manner
- This allows dynamic sharing of the shared channel
- In order to avoid collisions, a binary exponential back-off algorithm is used for non-real time connections and a modified binary exponential back-off algorithm is used for real time connections

Five-Phase Reservation Protocol

- A single-channel time division multiple access (TDMA)-based broadcast scheduling protocol.
- Nodes use a contention mechanism in order to acquire time slots.
- The protocol is fully distributed, that is, multiple reservations can be simultaneously made throughout the network.
- No ordering among nodes is followed
- Nodes need not wait for making time slot reservations

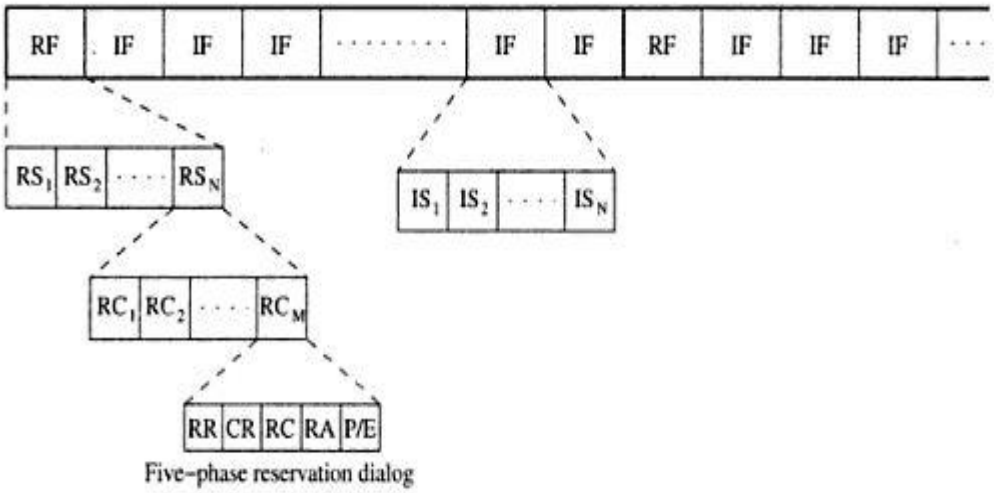


Figure 6.21. Frame structure in FPRP.

- Time is divided into frames
- There are two types of frames namely reservation frame and information frame
- Each RF is followed by a sequence of Ifs
- Each RF has N reservation slots (RS)
- Each IF has N information slots (IS)
- In order to reserve an IS, a node needs to contend during the corresponding RS
- Based on these contentions, a TDMA schedule is generated in the RF and is used in the subsequent Ifs until the next RF.
- Each RS is composed of M reservation cycles
- During the corresponding IS, a node would be in one of the three states: transmit(T), receive(R) or blocked(B)
- The protocol assumes the availability of global time at all nodes.
- The reservation takes five phases: reservation, collision report, reservation confirmation, reservation acknowledgement, and packing and elimination phase.

1. Reservation request phase: Nodes that need to transmit packets send reservation request (RR) packets to their destination nodes.

2. Collision report phase: If a collision is detected by any node during the reservation request phase, then that node broadcasts a collision report (CR) packet. The corresponding source nodes, upon receiving the CR packet, take necessary action.

3. Reservation confirmation phase: A source node is said to have won the contention for a slot if it does not receive any CR messages in the previous phase. In order to confirm the reservation request made in the reservation request phase, it sends a reservation confirmation (RC) message to the destination node in this phase.

4. Reservation acknowledgment phase: In this phase, the destination node acknowledges reception of the RC by sending back a reservation acknowledgment (RA) message to the source. The hidden nodes that receive this message defer their transmissions during the reserved slot.

5. Packing and elimination (P/E) phase: Two types of packets are transmitted during this phase: packing packet and elimination packet.

In this phase, a packing packet (PP) is sent by each node that is located within two hops from a TN, and that had made a reservation since the previous P/E phase. A node receiving a PP understands that there has been a recent success in slot reservation three hops away from it, and because of this some of its neighbors would have been blocked during this slot. The node can take advantage of this and adjust its contention probability p, so that convergence is faster.

MACA with Piggy-Backed Reservation

- Provide real-time traffic support in multi-hop wireless networks
- Based on the MACAW protocol with non-persistent CSMA
- The main components of MACA/PR are:
  - ✓ A MAC protocol
  - ✓ A reservation protocol
  - ✓ A QoS routing protocol
- Differentiates real-time packets from the best-effort packets
- Provide guaranteed BW support for real-time packets
- Provides reliable transmission of best efforts packets

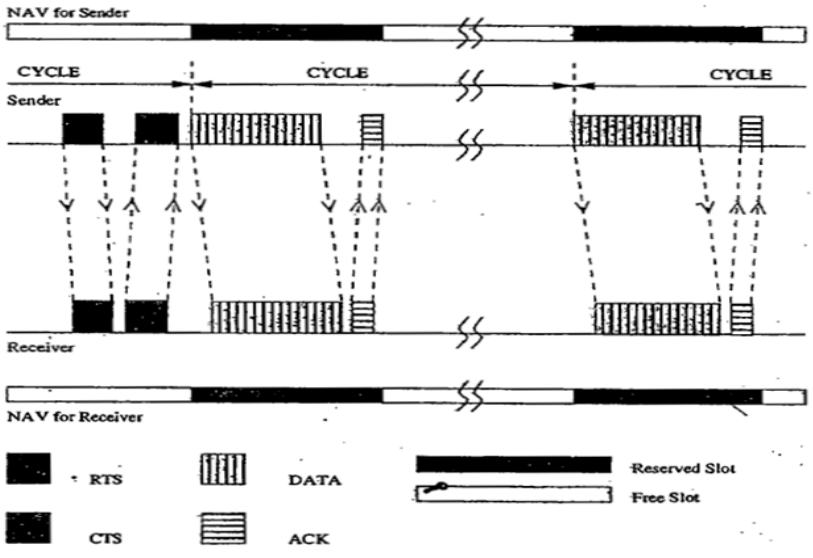


Figure 6.23. Packet transmission in MACA/PR.

- Time is divided into slots

- Slots are defined by the reservations made at nodes
- They are asynchronous in nature with varying lengths
- Each node in the network maintains a reservation table (RT) that records all the reserved transmit and receive slots/windows of all nodes within its transmission range
- The sender is assumed to transmit real-time packets at certain regular intervals, say, every CYCLE time period
- The first data packet of the session is transmitted in the usual manner
- The source node first sends an RTS packet, for which the receiver responds with a CTS packet
- Now the source node sends the first DATA packet of the real-time session
- Reservation information for the next DATA packet to be transmitted is piggy-backed on this current DATA packet.
- On receiving this DATA packet, the receiver node updates its reservation table with the piggy-backed reservation information
- It then sends ACK packet back to the source
- Receiver node piggy-backs the reservation confirmation information on the ACK packet
- Slot reservation information maintained in the reservation tables is refreshed every cycle
- Thus, MACA/PR is an efficient bandwidth reservation protocol that can support real-time traffic sessions
- Advantage → it does not require global synchronisation among nodes
- Drawback → a free slot can be reserved only if it can fit the entire RTS-CTS-DATA-ACK exchange

Real-Time Medium Access Control Protocol

- Provides a bandwidth reservation mechanism for supporting real-time traffic in ad hoc wireless networks
- RTMAC has two components
  - A MAC layer protocol is a real-time extension of the IEEE 802.11 DCF.
    - A medium-access protocol for best-effort traffic
    - A reservation protocol for real-time traffic
  - A QoS routing protocol is responsible for end-to-end reservation and release of bandwidth resources.

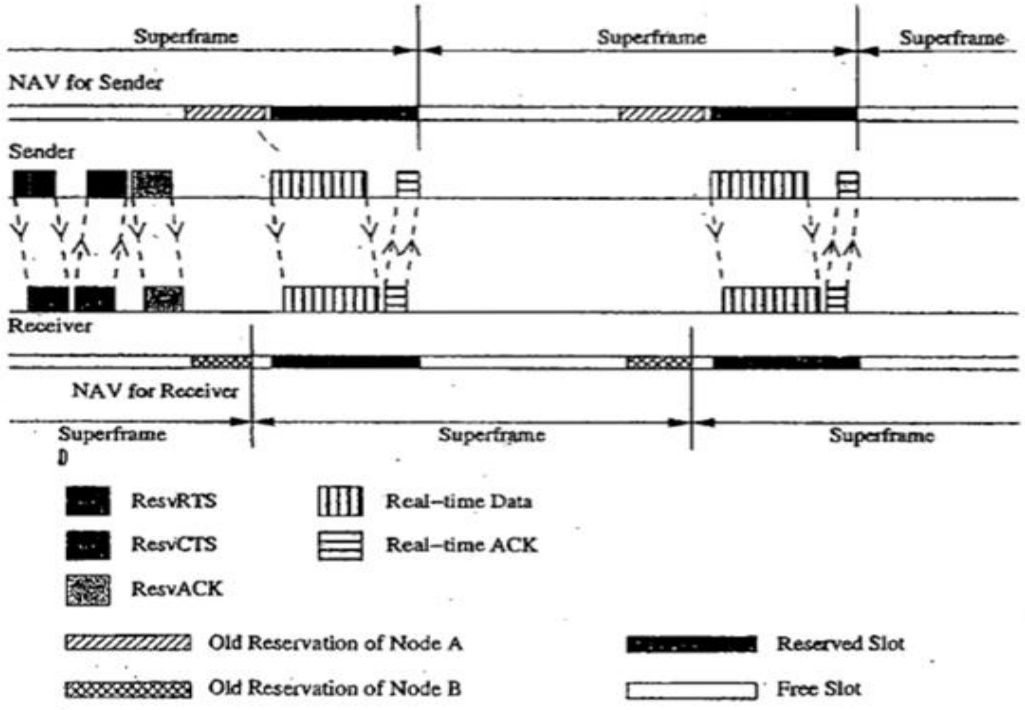


Figure 6.24. Reservation mechanism in RTMAC.

- A separate set of control packets, consisting of ResvRTS, ResvCTS, and ResvACK, is used for effecting BW reservation for real-time packets
- RTS, CTS and ACK control packets are used for transmitting best effort packets
- Time is divided into superframes. (figure)
- Bandwidth reservations can be made by a node by reserving variable-length time slots on superframes
- The core concept of RTMAC is the flexibility of slot placement in the superframe
- Each superframe consists of a number of reservation-slots
- The time duration of each resv-slot is twice the maximum propagation delay
- Data transmission normally requires a block of resv-slots
- A node that needs to transmit real-time packets first reserves a set of resv-slots
- The set of resv-slots reserved by a node for a connection on a superframe is called a connection-slot
- Each node maintains a reservation table containing information such as the sender id, receiver id, and starting and ending times of reservations that are currently active
- In RTMAC, no time synchronisation is assumed
- The protocol uses relative time for all reservation purpose
- A three way handshake protocol is used for effecting the reservation
- In the figure, NAV indicates the network allocation vector maintained at each node
- Main advantage is Bandwidth efficiency
- Another advantage is asynchronous mode of operation where nodes do not require any global time synchronisation

UNIT 4
ROUTING - 1

INTRODUCTION

Since the ad hoc wireless network consists of a set of mobile nodes (hosts) that are connected by wireless links, the network topology in such a network may keep changing randomly. Hence a variety of routing protocols for ad hoc wireless networks has been proposed.

ISSUES IN DESIGNING A ROUTING PROTOCOL FOR AD HOC WIRELESS NETWORKS

The major challenges that a routing protocol designed for ad hoc wireless networks faces are:

Mobility

- Network topology is highly dynamic due to movement of nodes. hence, an ongoing session suffers frequent path breaks.
- Disruption occurs due to the movement of either intermediate nodes in the path or end nodes .
- Wired network routing protocols cannot be used in adhoc wireless networks because the nodes are here are not stationary and the convergence is very slow in wired networks.
- Mobility of nodes results in frequently changing network topologies
- Routing protocols for ad hoc wireless networks must be able to perform efficient and effective mobility management.

Bandwidth Constraint

- Abundant bandwidth is available in wired networks due to the advent of fiber optics and due to the exploitation of wavelength division multiplexing (WDM) technologies.
- In a wireless network, the radio band is limited, and hence the data rates it can offer are much less than what a wired network can offer.
- This requires that the routing protocols use the bandwidth optimally by keeping the overhead as low as possible.
- The limited bandwidth availability also imposes a constraint on routng protocols in maintaining the topological information.

Error-prone shared broadcast radio channel

- The broadcast nature of the radio channel poses a unique challenge in ad hoc wireless networks.
- The wireless links have time-varying characteristics in terms of link capacity and link-error probability.
- This requires that the adhoc wireless network routing protocol interact with the MAC layer to find alternate routes through better-quality links.
- Transmissions in ad hoc wireless networks result in collisions of data and control packets.
- Therefore, it is required that ad hoc wireless network routing protocols find paths with less congestion.

Hidden and exposed terminal problems

- The 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 receiver, 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.
- Ex: consider figure 7.1. Here, if both node A and node C transmit to node B at the same time, their packets collide at node B. This is due to the fact that both node A and C are hidden from each other, as

they are not within the direct transmission range of each other and hence do not know about the presence of each other.

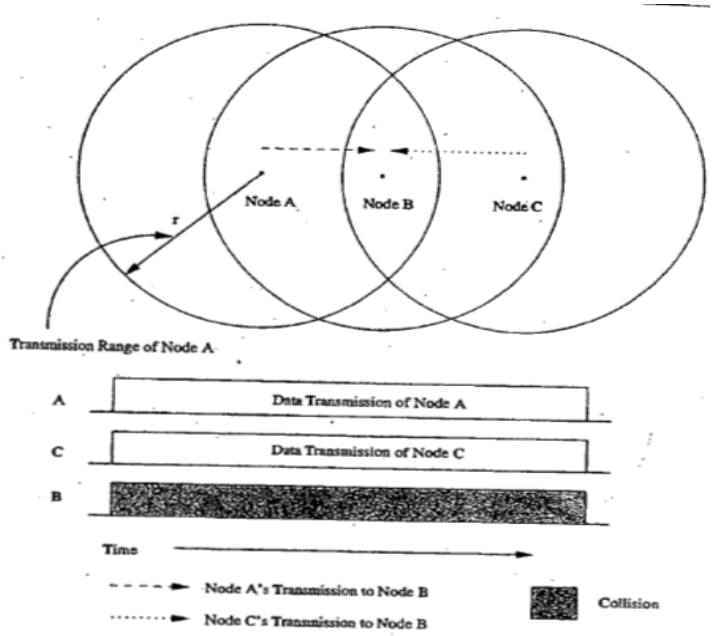


Figure 7.1. Hidden terminal problem.

- Solution for this problem include medium access collision avoidance (MACA):
  - Transmitting node first explicitly notifies all potential hidden nodes about the forthcoming transmission by means of a two-way handshake control protocol called RTS-CTS protocol exchange.
  - This may not solve the problem completely but it reduces the probability of collisions.
- Medium access collision avoidance for wireless (MACAW):
  - An improved version of MACA protocol.
  - Introduced to increase the efficiency.
  - Requires that a receiver acknowledges each successful reception of data packet.

- Successful transmission is a four-way exchange mechanism, RTS-CTS-Data-ACK, as illustrated in figure 7.2.

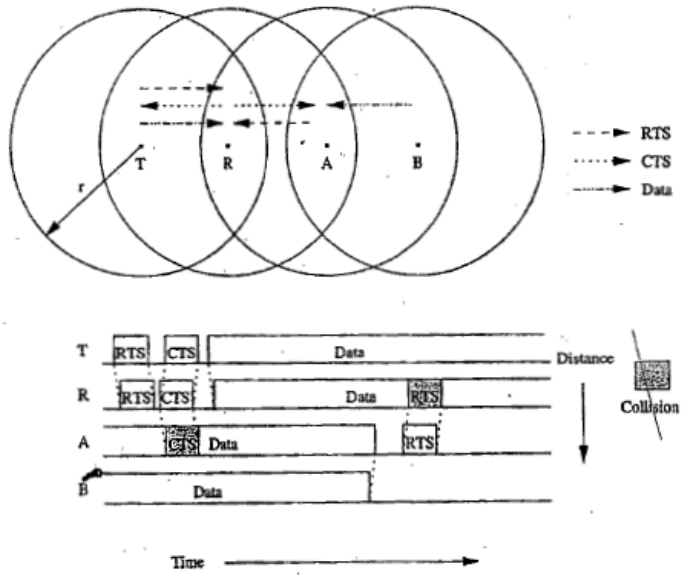


Figure 7.2. Hidden terminal problem with RTS-CTS-Data-ACK scheme.

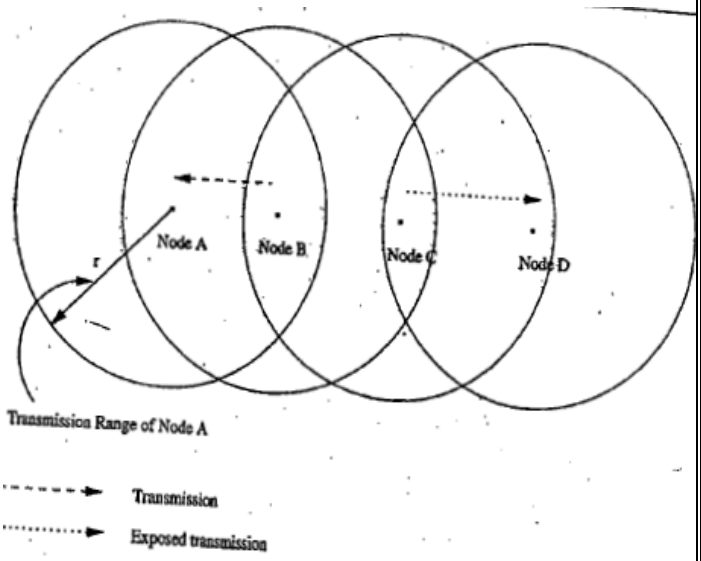


Figure 7.3. Exposed terminal problem.

- Other solutions include floor acquisition multiple access (FAMA) and Dual busy tone multiple access (DBTMA).
- The 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.
- Ex: consider the figure 7.3. Here, if a transmission from node B to another node A is already in progress, node C cannot transmit to node D, as it concludes that its neighbor node B, is in transmitting mode and hence should not interfere with the on-going transmission. Thus, reusability of the radio spectrum is affected.

Resource Constraints

- Two essential and limited resources are battery life and processing power.
- Devices used in adhoc wireless networks require portability, and hence they also have size and weight constraints along with the restrictions on the power source.
- Increasing the battery power and processing ability makes the nodes bulky and less portable.

Characteristics of an Ideal Routing Protocol for ad hoc wireless networks

A routing protocol for ad hoc wireless networks should have the following characteristics:

- It must be fully distributed as centralized routing involves high control overhead and hence is not scalable.
- It must be adaptive to frequent topology changes caused by the mobility of nodes.
- Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired.
- It must be localized, as global state maintenance involves a huge state propagation control overhead.
- It must be loop-free and free from state routes.
- The number of packet collisions must be kept to a minimum by limiting the number of broadcasts made by each node. The transmissions should be reliable to reduce message loss and to prevent the occurrence of state routes.
- It must converge to optimal routes once the network topology becomes stable. The convergence must be quick.
- It must optimally use scarce resources such as bandwidth, computing power, memory, and battery power.
- Every node in the network should try to store information regarding the stable local topology only. Changes in remote parts of the network must not cause updates in the topology information maintained by the node.
- It should be able to provide a certain level of quality of service (QoS) as demanded by the applications, and should also offer support for time-sensitive traffic.

CLASSIFICATIONS OF ROUTING PROTOCOLS

A classification tree is shown below:

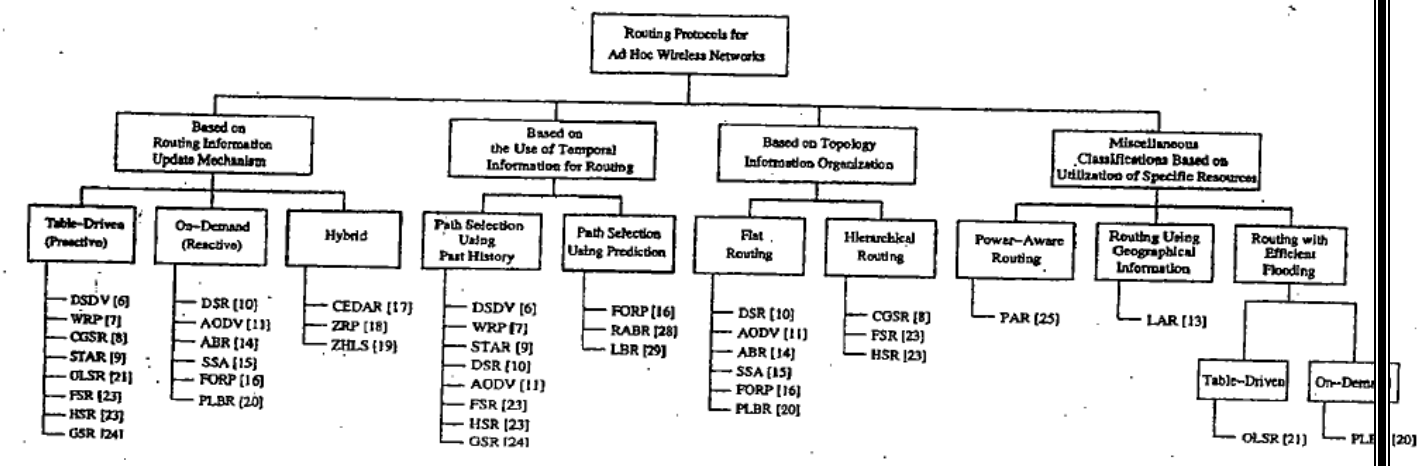


Figure 7.4. Classifications of routing protocols.

The routing protocol for adhoc wireless networks can be broadly classified into 4 categories based on

- Routing information update mechanism.
- Use of temporal information for routing
- Routing topology
- Utilization of specific resources.

Based on the routing information update mechanism

Ad hoc wireless network routing protocols can be classified into 3 major categories based on the routing information update mechanism. They are:

- *Proactive or table-driven routing protocols* :
  - Every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.
  - Routing information is generally 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.
- *Reactive or on-demand routing protocols*:
  - Do not maintain the network topology information.
  - Obtain the necessary path when it is required, by using a connection establishment process.
- *Hybrid routing protocols:*
  - Combine the 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.
  - For nodes that are located beyond this zone, an on-demand approach is used.

Based on the use of temporal information for routing

The protocols that fall under this category can be 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.
- *Routing protocols that use future temporal information:*
  - Use information about the about the expected future status of the wireless links to make approximate routing decisions.
  - Apart from the lifetime of wireless links, the future status information also includes information regarding the lifetime of the node, prediction of location, and prediction of link availability.

Based on the routing topology

Ad hoc wireless networks, due to their relatively smaller number of nodes, can make use of either a flat topology or a hierarchical topology for routing.

- *Flat topology routing protocols:*
  - Make use of a flat addressing scheme similar to the one used in IEEE 802.3 LANs.
  - It assumes the presence of a globally unique addressing mechanism for nodes in an ad hoc wireless network.
- *Hierarchical topology routing protocols:*
  - Make use of a logical hierarchy in the network and an associated addressing scheme.
  - The hierarchy could be based on geographical information or it could be based on hop distance.

Based on the utilization of specific resources

- *Power-aware routing:*
  - Aims at minimizing the consumption of a very important resource in the ad hoc wireless networks: the battery power.
  - The routing decisions are based on minimizing the power consumption either logically or globally in the network.
- *Geographical information assisted routing :*
  - Improves the performance of routing and reduces the control overhead by effectively utilizing the geographical information available.

TABLE-DRIVEN ROUTING PROTOCOLS

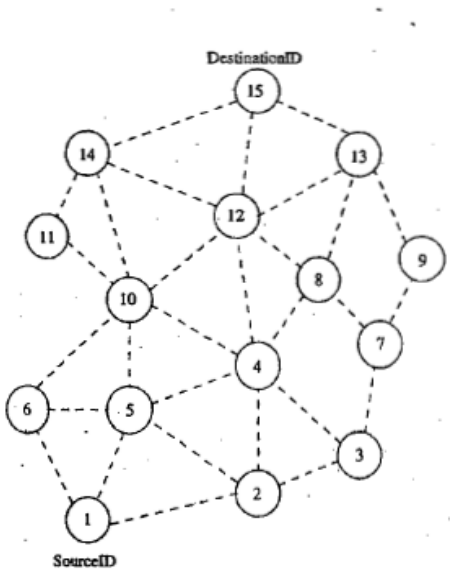
- These protocols are extensions of the wired network routing protocols

- They maintain the 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
- Ex: Destination sequenced distance vector routing protocol (DSDV), wireless routing protocol (WRP), source-tree adaptive routing protocol (STAR) and cluster-head gateway switch routing protocol (CGSR).

Destination sequenced distance-vector routing protocol

- It is an enhanced version of the 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.
- As it is a table-driven routing protocol, routes to all destinations are readily available at every node at all times.
- The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology.
- The table updates are of two types:
  - ***Incremental updates:*** Takes a single network data packet unit (NDPU). These are used when a node does not observe significant changes in the local topology.
  - ***Full dumps:*** Takes multiple NDPUs. It is done either when the local topology changes significantly or when an incremental update requires more than a single NDPU.
- Table updates are initiated by a destination with a new sequence number which is always greater than the previous one.

- Consider the example as shown in figure (a). Here node 1 is the source node and node 15 is the destination. As all the nodes maintain global topology information, the route is already available as shown in figure (b).
- Here the routing table node 1 indicates that the shortest route to the destination node is available through node 5 and the distance to it is 4 hops, as depicted in figure (b)
- The 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 node always assign an odd number to the link break update to differentiate it from the even sequence number generated by the destination.
- Figure 7.6 shows the case when node 11 moves from its current position.

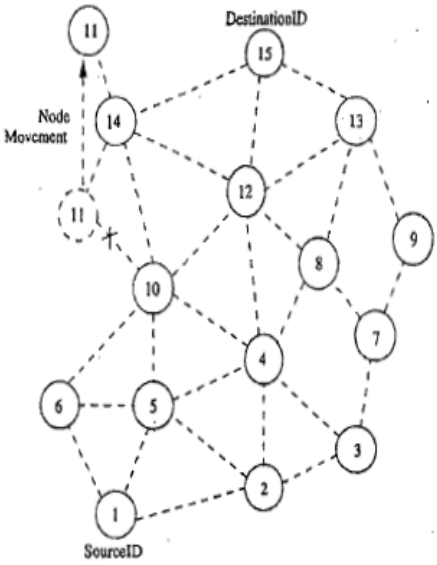


(a) Topology graph of the network

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b) Routing table for Node 1

Figure 7.5. Route establishment in DSDV.



Routing Table for Node 1

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

Figure 7.6. Route maintenance in DSDV.

Advantages

- Less delay involved in the route setup process.
- Mechanism of incremental update with sequence number tags makes the existing wired network protocols adaptable to ad hoc wireless networks.
- The updates are propagated throughout the network in order to maintain an up-to-date view of the network topology at all nodes.

Disadvantages

- The updates due to broken links lead to a heavy control overhead during high mobility.
- Even a small network with high mobility or a large network with low mobility can completely choke the available bandwidth.
- Suffers from excessive control overhead.
- 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 state routing information at nodes.

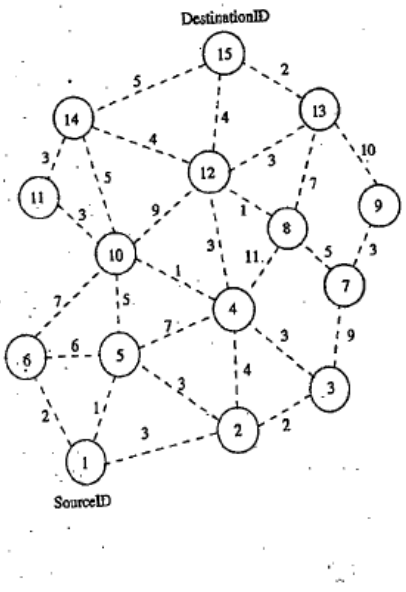
Wireless Routing Protocol (WRP)

- WRP is similar to DSDV; it inherits the properties of the distributed bellman-ford algorithm.
- To counter the count-to-infinity problem and to enable faster convergence, it employs a unique method of maintaining information regarding the shortest distance to every destination node in the network and penultimate hop node on the path to every destination node.
- Maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network.
- It differs from DSDV in table maintenance and in the update procedures.
- While DSDV maintains only one topology table, WRP uses a set of tables to maintain more accurate information.
- The table that are maintained by a node are :
    - Distance table (DT): contains the network view of the neighbors of a node. It contains a matrix where each element contains the distance and the penultimate node reported by the neighbor for a particular destination.
    - Routing table (RT): contains the up-to-date view of the network for all known destinations. It keeps the shortest distance, the predecessor/penultimate node, the successor node, and a flag indicating the status of the path. The path status may be a simplest (correct) path or a loop (error), or destination node not marked (null).

- Link cost table (LCT): contains the cost of relaying messages through each link. The cost of broken link is ∞.it also contains the number of update periods passed since the last successful update was received from that link.
- Message retransmission list (MRL): contains an entry for every update message that is to be retransmitted and maintains a counter for each entry.

- After receiving the update message, a node not only updates the distance for transmitted neighbors but also checks the other neighbors' distance, hence convergence is much faster than DSDV.

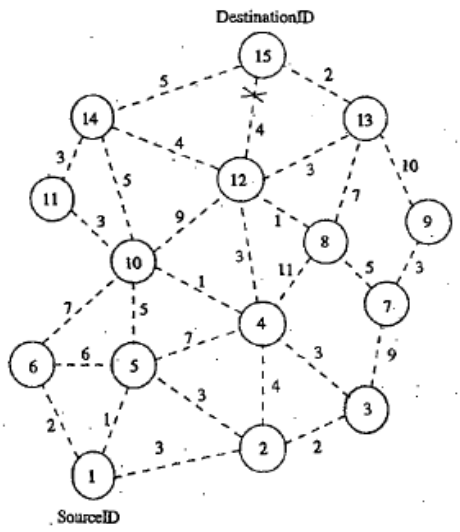
- Consider the example shown in figure below, where the source of the route is node 1 and destination is node 15. As WRP proactively maintains the route to all destinations, the route to any destination node is readily available at the source node.
- From the routing table shown, the route from node 1 to node 15 has the next node as node 2. The predecessor node of 15 corresponding to this route is route 12. The predecessor information helps WRP to converge quickly during link breaks.



Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	12	4
11	14	14	8
10	4	12	8
9	13	13	12
8	12	12	5
7	8	12	10
6	10	12	15
5	10	12	13
4	12	12	10
3	4	12	7
2	4	12	11
1	2	12	14

Figure 7.7. Route establishment in WRP.



Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	13	5
11	14	14	8
10	4	13	9
9	13	13	12
8	12	13	6
7	8	13	11
6	10	13	16
5	10	13	14
4	12	13	8
3	4	13	11
2	4	13	12
1	2	13	15

Figure 7.8. Route maintenance in WRP.

- When a node detects a link break, it sends an update message to its neighbors with the link cost of the broken link set to ∞. After receiving the update message; all affected nodes update their minimum distances to the corresponding nodes. The node that initiated the update message then finds an alternative route, if available from its DT. Figure 7.8 shows route maintenance in WRP.

Advantages

- WRP has the same advantages as that of DSDV.
- It has faster convergence and involves fewer table updates.

Disadvantages

- The complexity of maintenance of multiple tables demands a larger memory and greater processing power from nodes in the adhoc wireless network.
- It is not suitable for highly dynamic and also for very large ad hoc wireless networks.

Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Uses a hierarchical network topology.
- CGSR organizes nodes into clusters, with coordination among the members of each cluster entrusted to a special node named *cluster-head.*
- This cluster-head is elected dynamically by employing a least cluster change (LCC) algorithm.

- According to this algorithm, a node ceases to be a cluster-head only if it comes under the range of another cluster-head, where the tie is broken either using the lowest ID or highest connectivity algorithm.
- Clustering provides a mechanism to allocate bandwidth, which is a limited resource, among different clusters, thereby improving reuse.
- A token-based scheduling is used within a cluster for sharing the bandwidth among the members of the cluster.
- CGRS assumes that all communication passes through the cluster-head. Communication between 2 clusters takes place through the common member nodes that are members of both the cluster are called *gateways.*
- A gateway is expected to be able to listen to multiple spreading codes that are currently in operation in the clusters in which the node exist as a member.
- A gateway conflict is said to occur when a cluster-head issues a token to a gateway over spreading code while the gateway is tuned to another code.
- Gateways that are capable of simultaneously communicating over two interfaces can avoid gateway conflicts.
- The performance of routing is influenced by token scheduling and code scheduling that is handled at cluster-heads and gateways, respectively.
- Every member node maintains a routing table containing the destination cluster-head for every node in the network.
- In addition to the cluster member table, each node maintains a routing table which keeps the list of next-hop nodes for reaching every destination cluster.
- The cluster routing protocol is used here.
- Figure below shows the cluster head, cluster gateways, and normal cluster member nodes in an ad hoc wireless network.

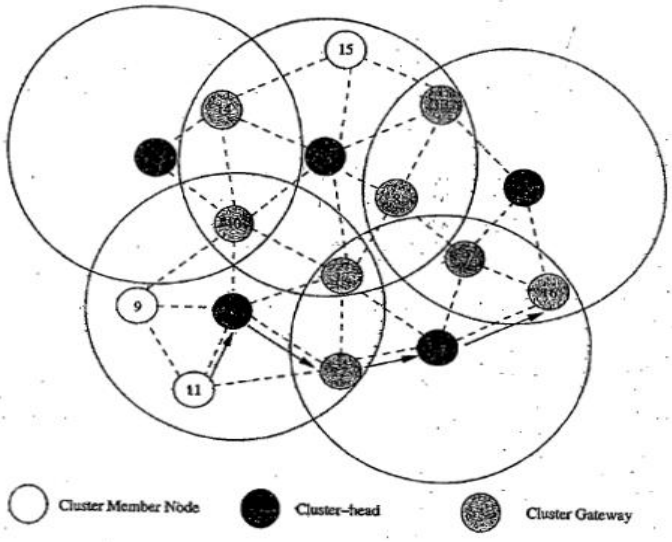


Figure 7.9. Route establishment in CGSR.

Advantages

- CGSR is a hierarchical routing scheme which enables partial coordination between nodes by electing cluster-heads.
- Better bandwidth utilization is possible.
- Easy to implement priority scheduling schemes with token scheduling and gateway code scheduling.

Disadvantages

- Increase in path length and instability in the system at high mobility when the rate of change of cluster-head is high.
- In order to avoid gateway conflicts, more resources are required.
- The power consumption at the cluster-head node is also a matter of concern.
- Lead to Frequent changes in the cluster-head, which may result in multiple path breaks.

Source-Tree Adaptive Routing Protocol (STAR)

- Key concept → least overhead routing approach (LORA)
- This protocol attempts to provide feasible paths that are not guaranteed to be optimal
- Involves much less control overhead
- In STAR protocol, every node broadcasts its source tree information
- The source tree of a node consists of the wireless links used by the node
- Every node builds a partial graph of the topology
- During initialization, a node sends an update message to its neighbors
- Each node will have a path to every destination node

- The path would be sub-optimal
- The data packet contains information about the path to be traversed in order to prevent the possibility of routing loop formation
- In the presence of a reliable broadcast mechanism, STAR assumes implicit route maintenance
- In addition to path breaks, the intermediate nodes are responsible for handling the routing loops
- The RouteRepair packet contains the complete source tree of node k and the traversed path of the packet
- When an intermediate node receives a RouteRepair update message, it removes itself from the top of the route repair path and reliably sends it to the head of the route repair path

Advantages

- Very low communication overhead
- Reduces the average control overhead

ON-DEMAND ROUTING PROTOCOLS

They 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 Protocol (DSR)

- Designed to restrict the bandwidth consumed by control packets in adhoc wireless networks by eliminating the periodic table update messages
- It is beacon-less and does not require periodic hello packet transmissions
- Basic approach → to establish a route by flooding RouteRequest packets in the network
- Destination node responds by sending a RouteReply packet back to the source
- Each RouteRequest carries a sequence number generated by the source node and the path it has traversed
- A node 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
- Thus, all nodes except the destination forward a RouteRequest packet during the route construction phase
- In figure 7.10, source node 1 initiates a RouteRequest packet to obtain a path for destination node 15
- This protocol uses a route cache that stores all possible information extracted from the source route contained in a data packet
- During network partitions, the affected nodes initiate RouteRequest packets
- DSR also allows piggy-backing of a data packet on the RouteRequest
- As a part of optimizations, if the intermediate nodes are also allowed to originate RouteReply packets, then a source node may receive multiple replies from intermediate nodes
- In fig 7.11, if the intermediate node 10 has a route to the destination via node 14, it also sends the RouteReply to the source node
- The source node selects the latest and best route and uses that for sending data packets
- Each data packet carries the complete path to its destination
- If a link breaks, source node again initiates the route discovery process

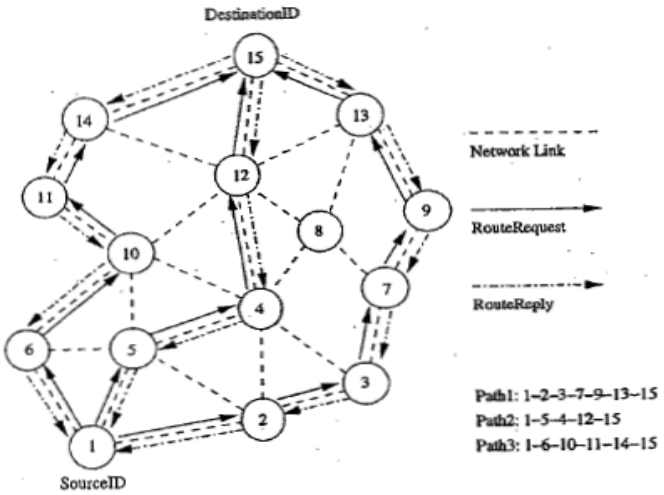


Figure 7.10. Route establishment in DSR.

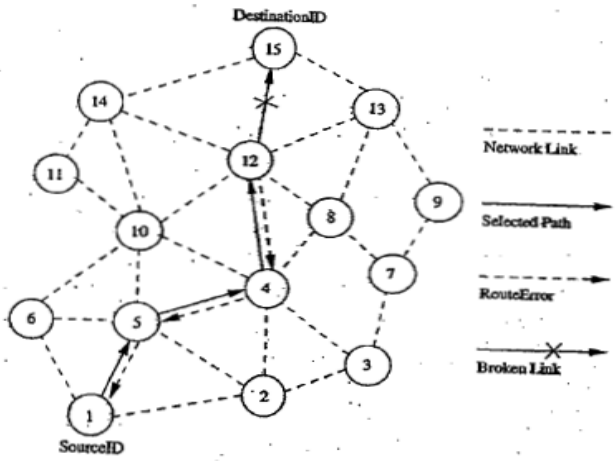


Figure 7.11. Route maintenance in DSR.

Advantages

- Uses a reactive approach which eliminates the need to periodically flood the network with table update messages
- Route is established only when required
- Reduce control overhead

Disadvantages

- Route maintenance mechanism does not locally repair a broken link
- Stale route cache information could result in inconsistencies during route construction phase
- Connection set up delay is higher
- Performance degrades rapidly with increasing mobility
- Routing overhead is more & directly proportional to path length

Ad Hoc On-Demand Distance Vector Routing Protocol

- Route is established only when it is required by a source node for transmitting data packets
- It employs destination sequence numbers to identify the most recent path
- Source node and intermediate nodes store the next hop information corresponding to each flow for data packet transmission
- Uses DestSeqNum to determine an up-to-date path to the destination
- A RouteRequest carries the source identifier, the destination identifier, the source sequence number, the destination sequence number, the broadcast identifier and the time to live 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 a RouteReply if it has a valid route to the destination
- The validity of the intermediate node is determined by comparing the sequence numbers
- If a RouteRequest is received multiple times, then duplicate copies are discarded
- Every intermediate node enters the previous node address and its BcastID
- A timer is used to delete this entry in case a RouteReply packet is not received
- AODV does not repair a broken path locally
- When a link breaks, the end nodes are notified
- Source node re-establishes the route to the destination if required

Advantage

- Routes are established on demand and DestSeqNum are used to find latest route to the destination
- Connection setup delay is less

Disadvantages

- Intermediate nodes can lead to inconsistent routes if the source sequence number is very old

- Multiple RouteReply packets to single RouteRequest packet can lead to heavy control overhead
- Periodic beaconing leads to unnecessary bandwidth consumption

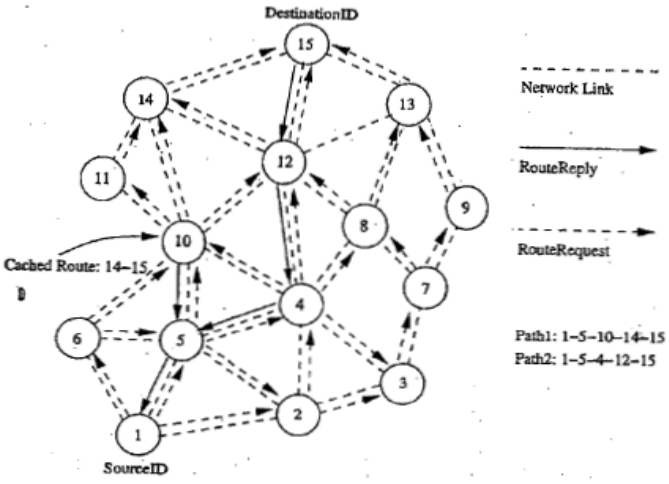


Figure 7.12. Route establishment in AODV.

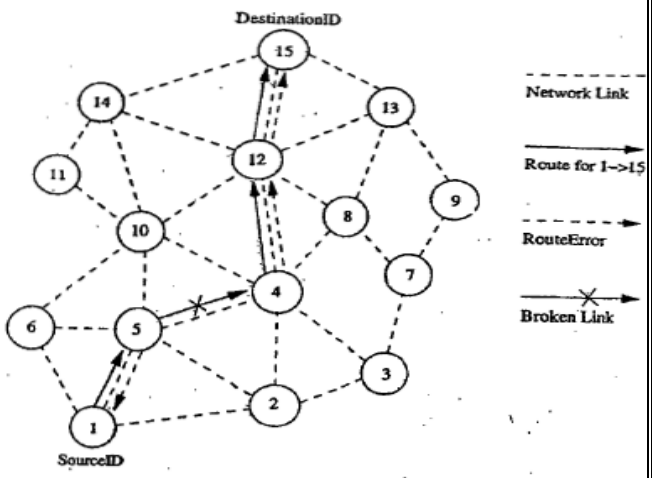


Figure 7.13. Route maintenance in AODV.

Temporally Ordered Routing Algorithm (TORA)

- Source-initiated on-demand routing protocol
- Uses a link reversal algorithm
- Provides loop free multi path routes to the destination
- Each node maintains its one-loop local topology information
- Has capability to detect partitions
- Unique property → limiting the control packets to a small region during the reconfiguration process initiated by a path break

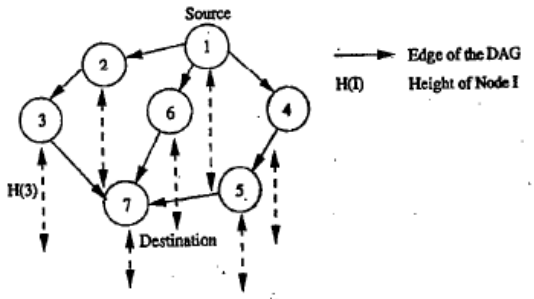


Figure 7.14. Illustration of temporal ordering in TORA.

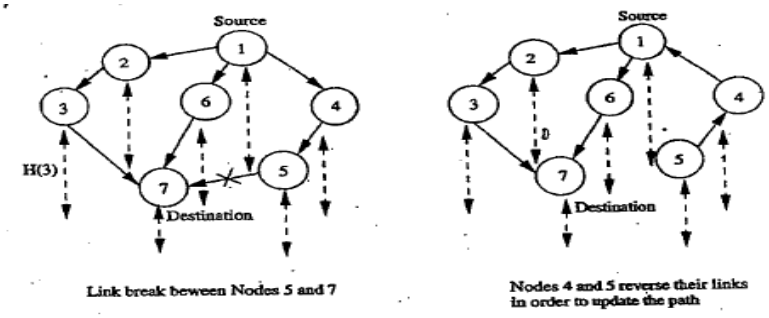


Figure 7.15. Illustration of route maintenance in TORA.

- TORA has 3 main functions: establishing, maintaining and erasing routes
- The route establishment function is performed only when a node requires a path to a destination but does not have any directed link
- This process establishes a destination-oriented directed acyclic graph using a query/update mechanism
- Once the path to the destination is obtained, it is considered to exist as long as the path is available, irrespective of the path length changes due to the re-configurations that may take place during the course of data transfer session
- If the node detects a partition, it originated a clear message, which erases the existing path information in that partition related to the destination

Advantages

- Incur less control overhead
- Concurrent detection of partitions
- Subsequent deletion of routes

Disadvantages

- Temporary oscillations and transient loops

- Local reconfiguration of paths result in non-optimal routes

Location-Aided Routing (LAR)

- It utilizes the location information for improving the efficiency of routing by reducing the control overhead
- LAR assumes the availability of the global positioning system (GPS) for obtaining the geographical position information necessary for routing
- LAR designates two geographical regions for selective forwarding of control packets, namely, ExpectedZone and RequestZone
- The ExpectedZone is the region in which the destination node is expected to be present, given information regarding its location in the past and its mobility information
- The RequestZone is a geographical region within which the path-finding control packets are permitted to be propagated
- This area is determined by the sender of a data transfer session.
- The control packets used for path-finding are forwarded by nodes which are present in the RequestZone and are discarded by nodes outside the zone
- LAR uses flooding, but here flooding is restricted to a small geographical region
- The nodes decide to forward or discard the control packets based on two algorithms, namely, LAR1 & LAR2

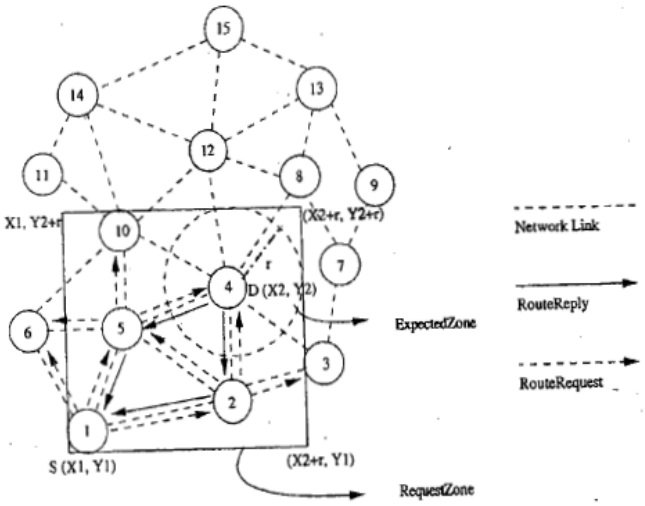


Figure 7.16. *RequestZone* and *ExpectedZone* in LAR1.

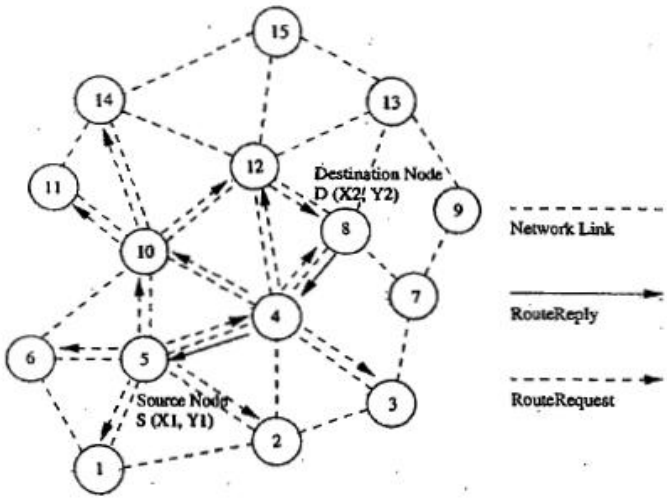


Figure 7.17. Route establishment in LAR2.

- In the LAR1 algorithm (fig 7.16), the source node explicitly specifies the RequestZone in the RouteRequest packet which is broadcast to its neighbors
- These nodes verify their own geographical locations to check whether they belong to the ExpectedZone
- Finally, when the RouteRequest reaches the destination node, it originates a RouteReply that contains the current location and current time of the node
- In LAR2 algorithm (fig 7.17), the source node includes the distance between itself and the destination node
- When the intermediate node receives this RouteRequest packet, it computes the distance to the node D
- A RouteRequest packet is forwarded only once and the distance between the forwarding node and D is updated in the RouteRequest packet for further relaying
- In order to compensate for the location error, a larger RequestZone that can accommodate the amount of error that occurred is considered

Advantage

- LAR reduces the control overhead by limiting the search area for finding a path
- Efficient use of geographical position information
- Reduced control overhead
- Increased utilization of bandwidth

Disadvantage

- Depends heavily on the availability of GPS infrastructure.
- Hence, cannot be used in situations where there is no access to such information

Associativity-Based Routing (ABR)

- It is a distributed routing protocol that selects routes based on the stability of the wireless links
- It is a beacon-based on-demand routing protocol
- A link is classified as stable or unstable based on its temporal stability
- The temporal stability is determined by counting the periodic beacons that a node receives from its neighbors
- Each node maintains the count of its neighbor's beacons and classifies each link as stable or unstable
- The link corresponding to a stable neighbor is termed as a stable link, while a link to an unstable neighbor is called an unstable link
- A source node floods RouteRequest packets throughout the network if a route is not available in its route cache
- All intermediate nodes forward the RouteRequest packet
- A RouteRequest packet carries the path it has traversed and the beacon count for the corresponding nodes in the path
- When the first RouteRequest reaches the destination, the destination waits for a time period T to receive multiple RouteRequests through different paths
- If two paths have the same proportion of stable links, the shorter of them is selected
- If more than one path is available, then a random path among them is selected as the path between source and destination

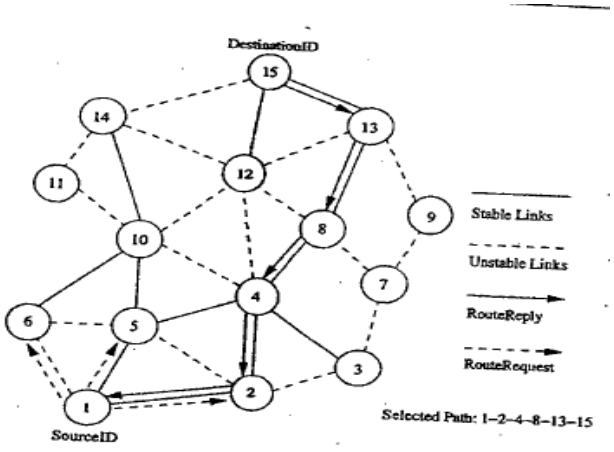


Figure 7.18. Route establishment in ABR.

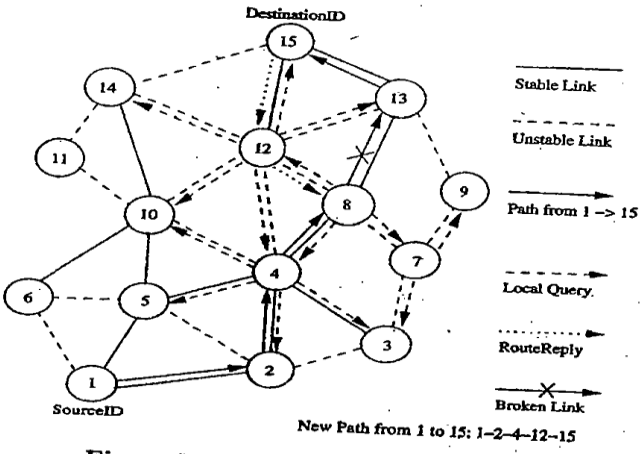


Figure 7.19. Route maintenance in ABR.

- In figure 7.18, source node initiates the RouteRequest to the flooded for finding a route to the destination node
- Solid lines represent stable links
- Dotted lines represent unstable links
- ABR uses stability information only during the route selection process at the destination node
- If a link break occurs at an intermediate node, the node closer to the source, which detects the break, initiates a local route repair process
- In this process, the node locally broadcasts a route repair packet, termed the local query (LQ) broadcast, with a limited time to live (TTL), as shown in figure 7.19
- This way a broken link is bypassed locally without flooding a new RouteRequest packet in the whole network.

Advantage

- Stable routes have a higher preference compared to shorter routes
- They result in fewer path breaks which, in turn, reduces the extent of flooding due to reconfiguration of paths in the network

Disadvantage

- Chosen path may be longer than the shortest path between the source and destination because of the preference given to stable paths
- Repetitive LQ broadcasts may result in high delays during route repairs

Signal Stability-Based Adaptive Routing Protocol (SSA)

- Uses signal stability as the prime factor for finding stable routes
- This protocol is beacon-based, in which signal strength of the beacon is measured for determining link stability
- The signal strength is used to classify a link as stable or unstable
- This protocol consists of two parts: forwarding protocol (FP) and dynamic routing protocol (DRP)
- These protocols use an extended radio interface that measures the signal strength from beacons
- DRP maintains the routing table by interacting with the DRP processes on other hosts
- FP performs the actual routing to forward a packet on its way to the destination
- Every node maintains a table that contains the beacon count and the signal strength of each of its neighbors
- If a node receives strong beacons, then link is classified as strong/stable link
- The link is otherwise classified as weak/unstable link
- Each node maintains a table called the signal stability table (SST) which is based on the signal strengths of its neighbors' beacons
- This table is used by the nodes in the path to the destination to forward the incoming RouteRequest over strong links for finding the most stable end-to-end path
- A source node which does not have a route to the destination floods the network with RouteRequest packets
- SSA protocol process a RouteRequest only if it is received over a strong link
- A RouteRequest received through a weak link is dropped without being processed
- The destination selects the first RouteRequest packet received over strong links
- The destination initiates a RouteReply packet to notify the selected route to the source
- In figure 7.20, source node broadcasts a RouteRequest for finding the route to the destination node
- Solid lines represent the stable links
- Dotted lines represent the weak links
- SSA restricts intermediate nodes from forwarding a RouteRequest packet if the packet has been received over a weak link
- When a link breaks, the end nodes of the broken link notify the corresponding end nodes of the path
- A source node, after receiving a route break notification packet, rebroadcasts the RouteRequest to find another stable path to the destination
- Stale entries are removed only if data packets that use the stale route information fail to reach the next node
- If no strong path is available when a link gets broken, then the new route is established by considering weak links also
- This is done when multiple RouteRequest attempts fail to obtain a path to the destination using only the stable links

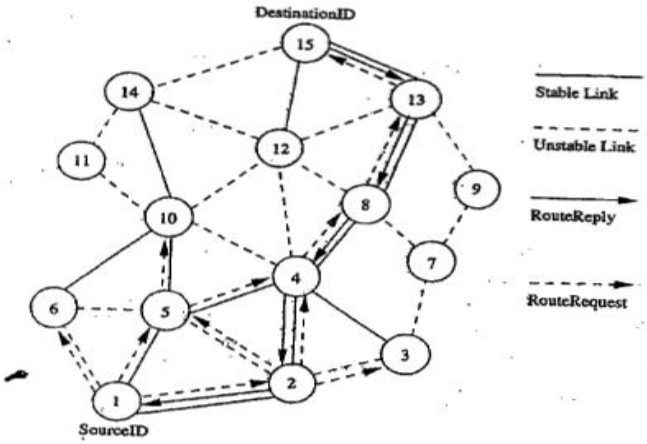


Figure 7.20. Route establishment in SSA.

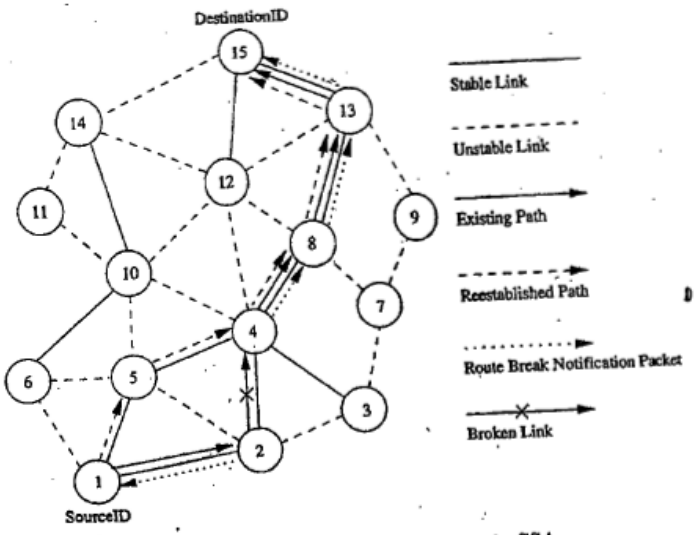


Figure 7.21. Route maintenance in SSA.

Advantage

- Finds more stable routes when compared to the shortest path route selection protocols
- Accommodates temporal stability by using beacon counts to classify a link as stable or weak

Disadvantage

- It puts a strong RouteRequest forwarding condition which results in RouteRequest failures
- Multiple flooding of RouteRequest packets consumes significant amount of bandwidth
- Increases the path setup time
- Strong link criterion increases the path length

Flow-Oriented Routing Protocol (FORP)

- Employs a prediction-based multi-hop-handoff mechanism for supporting time-sensitive traffic in adhoc wireless networks
- Proposed for IPv6-based ad hoc wireless networks where QoS needs to be provided
- The multi-hop-handoff is aimed at alleviating the effects of path breaks on the real time packet flows
- A sender or an intermediate node initiates the route maintenance process only after detecting a link break
- It may result in high packet loss leading to a low QoS provided to the user
- FORP utilizes the mobility and location information of nodes to estimate the link expiration time (LET)
- LET is the approximate lifetime of a given wireless link
- The minimum of the LET values of all wireless links on a path is termed as the route expiry time (RET)
- Every node is assumed to be able to predict the LET of each of its links with its neighbors
- The LET between two nodes can be estimated using information such as current position of the nodes, their direction of movement, and their transmission ranges
- FORP requires the availability of GPS information in order to identify the location of nodes
- When a sender node needs to setup a real time flow to a particular destination, it checks its routing table for the availability of a route to that destination
- If a route is available, then that is used to send packets to the destination
- Otherwise sender broadcasts a flow-REQ packet carrying information regarding the source and destination nodes
- The Flow-REQ packet also carries a flow identification number/sequence number which is unique for every session
- A neighbor node, on receiving this packet, first checks if the sequence number of the received Flow-REQ is higher than the sequence number corresponding to previous packet
- If the sequence number on the packet is less than that of the previous packet, then the packet is discarded
- This is done to avoid looping of flow-REQ packets

- The Flow-REQ packet, when received at the destination node, contains the list of nodes on the path it had traversed, along with the LET values of every wireless link on that path
- FORP assumes all the nodes in the network to be synchronized to a common time by means of GPS information

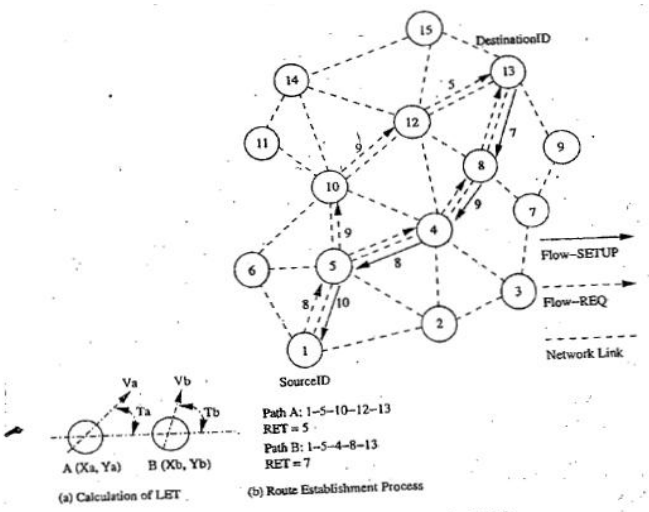


Figure 7.22. Route establishment in FORP:

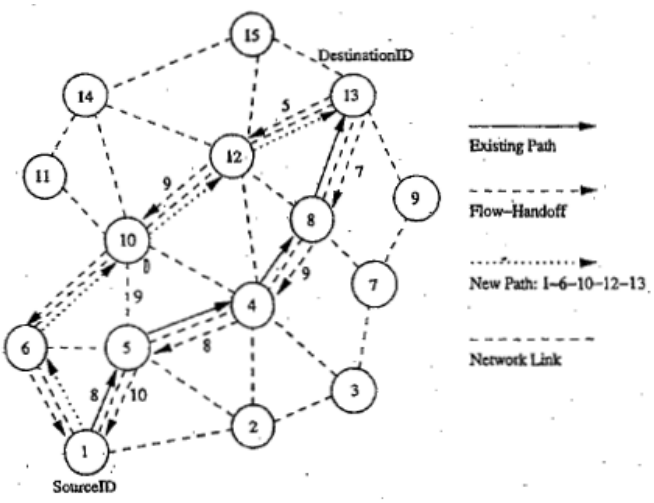


Figure 7.23. Route maintenance in FORP.

Advantage

- Use of LET and RET estimates reduces path breaks
- Reduces the reduction in packet delivery
- Reduces number of out-of-order packets
- Reduces non-optimal paths

Disadvantage

- Works well when topology is highly dynamic
- Requirements of time synchronization increases the control overhead
- Dependency on GPS infrastructure affects the operability of this protocol wherever it is not available

UNIT 5
ROUTING – 2

HYBRID ROUTING PROTOCOLS

Here, each node maintains the network topology information up to m nodes.

Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR)

- CEDAR integrates routing and support for QoS.
- It is based on extracting core nodes (also called as Dominator nodes) in the network.
- Core nodes together approximate the minimum Dominating Set (DS).
- A DS of a graph is defined as a set of nodes such that every node in the graph is either present in the DS or is a neighbor of some node present in the DS.
- There exists at least one core node within every three hops.
- The nodes that choose a core node as their dominating node are called core member nodes of the core node concerned.
- The path between two core nodes is termed as virtual link.
- CEDAR employs a distributed Algorithm to select core nodes.
- The selection of core nodes represents the core extraction phase.
- CEDAR uses the core broadcast mechanism to transmit any packet throughout the network in the unicast mode, involving as minimum number of nodes as possible.
- Route Establishment in CEDAR: It is carried out in two phase.
- The first phase finds a core path from source to destination. The core path is defined as the path from dominator of the source node (source core) to the dominator of the destination node (destination core).
- In the second phase, a QoS feasible path is found over the core path.
- A node initiates a RouteRequest if the destination is not in the local topology table of its core node; otherwise the path is immediately established.
- For establishing a route, the source core initiates a core broadcast in which the RouteRequest is sent to all neighboring core nodes which inturn forwards it.
- A core node which has the destination node as its core member replies to the source core.
- Once the core path is established, a path with the requested QoS support is then chosen.

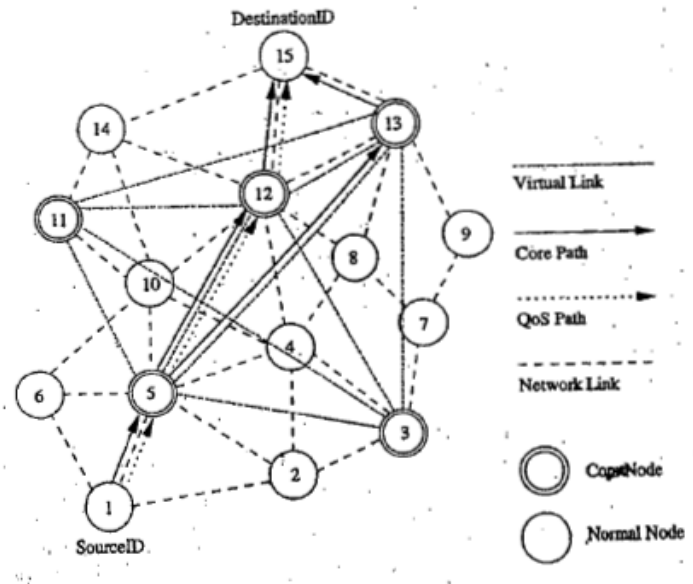


Figure 7.24. Route establishment in CEDAR.

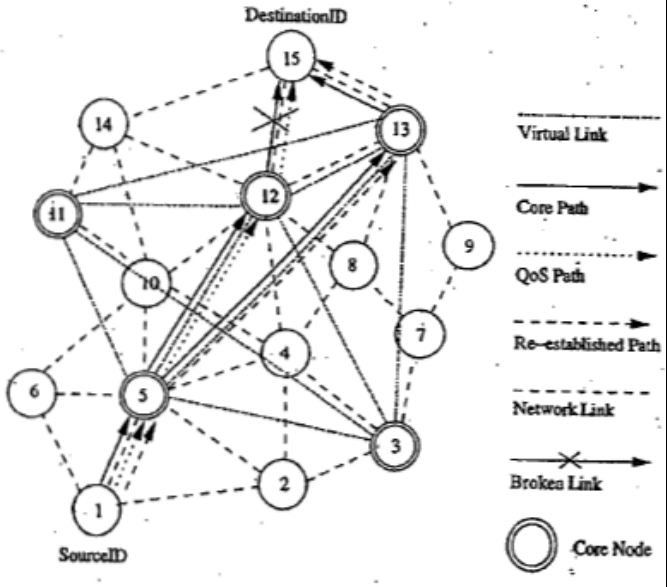


Figure 7.25. Route maintenance in CEDAR.

- Route Maintenance in CEDAR: attempts to repair a broken route locally when a path break occurs.

- A node after which the break occurred:
  - Sends a notification of failure.
  - Begins to find a new path from it to the destination.
  - Rejects every received packet till the moment it finds the new path to the destination.
- Meanwhile, as the source receives the notification message:
  - It stops to transmit.
  - Tries to find a new route to the destination.
  - If the new route is found by either of these two nodes, a new path from the source to the destination is established.

Advantages

- Performs both routing and QoS path computation very efficiently with the help of core nodes.
- Utilization of core nodes reduces traffic overhead.
- Core broadcasts provide a reliable mechanism for establishing paths with QoS support.

Disadvantages

- Since route establishment is carried out at core nodes, the movement of core nodes adversely affects the performance of the protocol.
- Core node update information causes control overhead.

Zone Routing Protocol (ZRP)

- Effectively combines the best features of both Proactive and Reactive routing protocols.
- It use a Proactive routing scheme within a limited zone in the r-hop neighborhood of every node.
- Use a Reactive routing scheme for nodes beyond this.
- An Intra-Zone Routing Protocol (IARP) is used in the zone where a particular node employs proactive routing.
- The Reactive routing protocol used beyond this zone is referred to as Inter-Zone Routing Protocol (IERP).
- The routing zone of a given node is a subset of the network, within which all nodes are reachable within less than or equal to.

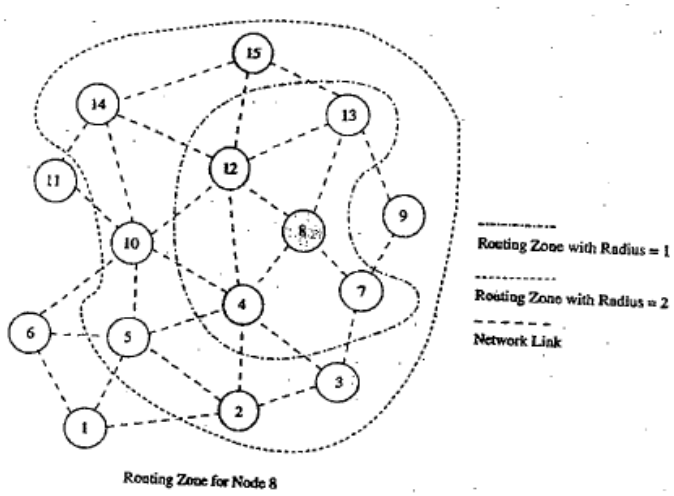


Figure 7.26. Routing zone for node 8 in ZRP.

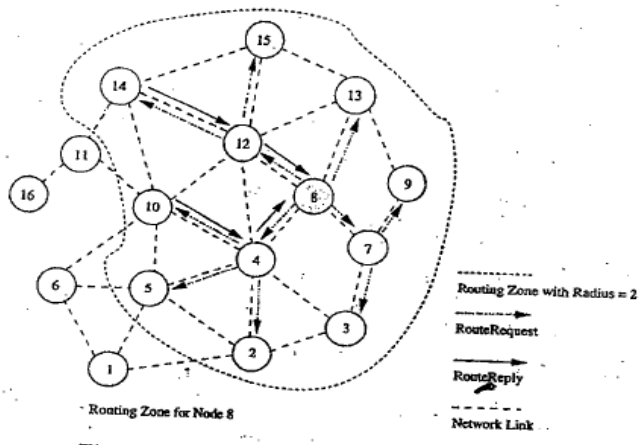


Figure 7.27. Path finding between node 8 and node 16.

- Route Establishment: When a node s (node 8 in the fig 7.27) has packets to be sent to a destination node d (node 15 in fig), it checks whether node d is within its zone.
- If the destination belongs to its own zone, then it delivers the packets directly.
- Otherwise, node s broadcasts the RouteRequest to its peripheral nodes (in fig, node 8 broadcasts RouteRequest to node 2, 3, 5, 7, 9, 10, 13, 14 and 15).
- If any peripheral node finds node d to be located within its routing zone, it sends a RouteReply back to node 8 indicating the path; otherwise, the node rebordercasts the RouteRequest packet to the peripheral nodes.

- This process continues until node d is located.
- During RouteRequest propagation, every node that forwards the RouteRequest appends its address to it.
- This information is used for delivering the RouteReply packet back to the source.
- The criteria for selecting the best path may be the shortest path, least delay path etc.
- When an intermediate node in an active path detects a broken link in the path, it performs a local path reconfiguration in which the broken link is bypassed by means of a short alternate path connecting the ends of the broken link
- A path update message is then sent to the sender node
- This results in sub-optimal path between two end points.

Advantage
Reduce the control overhead by combining the best features of Proactive and Reactive protocols.

Disadvantage
Control overhead may increase due to the large overlapping of nodes routing zones.

Zone Based Hierarchical Link State Routing Protocol (ZHLS)

- ZHLS uses the geographical location info of the nodes to form non-overlapping zones. A Hierarchical Addressing that consists of a zone ID and a node ID is employed.
- Similar to ZRP, ZHLS also employs a Proactive approach inside the geographical zone and a Reactive approach behind the zone.
- Every node requires GPS support for obtaining its own geographical location that is used to map itself into corresponding zone.
- The assignment of zone addresses to geographical areas is important and is done during a phase called the network design phase or network deployment phase.
- Each node maintains two link state packets: (LSP)
- Node level LSP: list of connected neighbors.
- Zone LSP: list of connected zones.
- Route Establishment → If a source node src wants to communicate with a destination node dest, src checks whether dest resides in its own zone.
- If dest belongs to same zone, then packets are delivered to the dest as per the Intra-Zone routing table.
- If dest does not belong to the same zone, then the src originates a location request packet containing the sender's and destination's information. This location info is forwarded to every other zone.
- The gateway node of a zone at which the location request packet is received verifies its routing table for the destination node.
- The gateway node that finds the destination node required by a location request packet originates a location response packet containing the zone information to the sender.

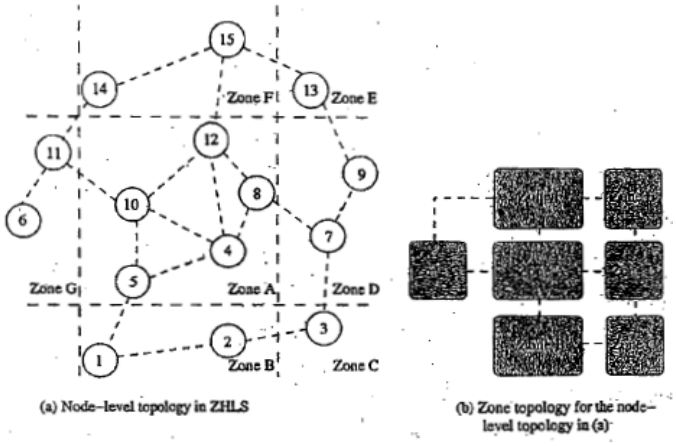


Figure 7.28. Zone-based hierarchical link state routing protocol.

Table 7.1: Zone link state packets

Source Zone	Zone Link State Packet
A	B, D, F, and G
B	C and A
C	B and D
D	A, C, and E
E	A, D, and F
F	A, E, and G
G	A and F

- Route Maintenance → If a given gateway node away causing a zone level connection failure,

routing can still take place with the help of the other gateway nodes.
- This is due to the hierarchical addressing that makes use of zone ID and node ID.

Advantages
- Reduce storage requirements and common overhead.
- Robust and resilient to path breaks.
- Non overlapping zones.

Disadvantages
- Additional overhead incurred in creation of zone level topology.
- Path to Destination is suboptimal.
- Geographical info may not be available in all environments.

ROUTING PROTOCOLS WITH EFFICIENT FLOODING MECHANISMS
- Many protocols flood the network with RouteRequest packets in order to obtain a path to the destination.
- Flooding of control packets results in:
  - Wastage of bandwidth.
  - Increase in number of collisions.
- Protocols with efficient flooding mechanisms:
  - Preferred link-based routing (PLBR) protocol.
  - Optimized link state routing (OLSR) protocol.

Preferred Link Based Routing (PLBR) Protocols
- Use the preferred link approach in an implicit manner by processing a RouteRequest packet only if it is received through a strong link.
- Here a node selects a subset of nodes from its Neighbors List (NL). This subset is referred to as the Preferred List (PL) selection of this subset may be based on link or node characteristics.
- All neighbors receive RouteRequest packets because of the broadcast radio channel, but only neighbors present in the PL forward them further.
- Each node maintains information about its neighbors and their neighbors in a table called Neighbor's Neighbor Table (NNT). It periodically transmits a beacon containing the changed neighbor's information.

Route Establishment
- If dest is in src's NNT, the route is established directly. Otherwise, src transmits a RouteRequest packet containing
  - Source node's address (SrcID)
  - Destination node's address (DestID)
  - Unique sequence number (SeqNum)
  - Traversed path (TP)
  - PL
  - TTL flag
  - NoDelay flag
- A node is eligible for forwarding a RouteRequest only if it satisfies the following criteria:
- The node ID must be present in the received RouteRequest packet's PL
- RouteRequest packet must not have been already forwarded by the node, and the TTL on the packet must be greater than zero.
- If the dest is in the eligible node's NNT, the RouteRequest is forwarded as a unicast packet to the neighbor

- If the computed PLT is empty, the RouteRequest packet is discarded and marked as sent.
- If the RouteRequest reaches the destination, the route is selected by the route selection procedure given below.

Route selection:

- When multiple Route Request packets reach dest,the route selection procedure selects the best route among them.
- The criterion for selecting the best route can be the shortest path, or the least delay path, or the most stable path.
- Dest starts a timer after receiving the first route request packet. The timer expires after a certain RouteSelectWait period, after which no more RouteRequest packets would be accepted.
- From the received Route Request packets, a route is selected as follows:
- For every RouteRequest i that reached Dest during the RouteSelectWait period, Max(Wmin) is selected, where is the min. Weight of the link in the path followed by i if two or more paths have the same value for the shortest path is selected.
- After selecting a route, all subsequent RouteRequest packets from the same src with a seqnum less than or equal to the seqnum of the selected RouteRequest are discarded.
- If the node delay flag is set, the route selection procedure is omitted and TP of the first RouteRequest reaching the Dest is selected as the route.

Algorithms for preferred links computation

Neighbor-Degree-Based preferred link algorithm(NDPL)
Weight Based preferred link algorithm(WBPL)

NDPL

Let d → node that calculates the preferred list table PLT.
TP Traversed path.
OLD_{PL} → preferred list of the received RouteRequest packet.
NNT_d → NNT of the node d.
N(i) → neighbors of node I and itself.
INL→ include list, a set containing all reachable neighbors by transmitting the RouteRequest packet.
EXL → Exclude list, a set containing all neighbors that are unreachable by transmitting the RouteRequest packet after execution of the algorithm.

Step 1: Node d marks the nodes that are not eligible for further forwarding the RouteRequest packet.

a) If a node i of TP is a neighbor of node d mark all neighbors of i as reachable i.e add N(i) to INL.
b) If a node i of OLD_{PL} is a neighbor of node d and i < d, then include N(i) in INL.
c) If neighbor i of node d has a neighbor n present in TP, add N(i) to INL.
d) If neighbor i of node d has a neighbor n present in OLD_{PL} and n < d, add N(i) to INL.

Step 2: If neighbor i of node d is not in INL, put i in PLT and mark all neighbor of i as reachable. If i is present in INL, mark the neighbors of i as unreachable by adding them to EXL.
Step 3: If neighbor i of d has a neighbor n present in EXL, put i in PLT and mark all neighbors of i as reachable. Delete all neighbors of i from EXL.
Step 4: Reduction steps are applied here in order to remove overlapping neighbors from PLT without compromising on reachability.

a) Remove each neighbor i from PLT if N (i) is covered by remaining neighbors of PLT. Here the minimum degree neighbor is selected every time
b) Remove neighbor i from PLT whose N (i) is covered by node d itself.

WBPL

1. Let $BCnt_i$ be the count of *beacons* received from a neighbor i and TH_{bcon} is the number of beacons generated during a time period equal to that required to cover twice the transmission range ($TH_{bcon} = \frac{2 \times transmission\ range}{maximum\ velocity \times period\ of\ beacon}$). Weight given to i based on time stability (WT^i_{time}) is

$$WT_{time} = \begin{cases} 1 & \text{if } BCnt_i > TH_{bcon} \\ BCnt_i/TH_{bcon} & \text{otherwise.} \end{cases}$$

2. Estimate the distance (D^i_{Est}) to i from the received power of the last few packets using appropriate propagation models. The weight based on spatial stability is $WT^i_{spatial} = \frac{R - D_{Est}}{R}$.
3. The weight assigned to the link i is the combined weight given to time stability and spatial stability. $W_i = WT^i_{time} + WT^i_{spatial}$.
4. Arrange the neighbors in a non-increasing order of their weights. The nodes are put into the PLT in this order.
5. If a link is overloaded, delete the associated neighbor from PLT. Execute *Step* 1 of NDPL and delete $\forall i,\ i \in PLT \cap i \in INL$. Also, delete those neighbors from PLT that satisfy *Step* 4 of NDPL.

Advantages

- Minimizes broadcast storm problem. Hence, highly scalable.
- Reduction in control overhead results in decrease in the number of collisions and improvement in efficiency of the protocol.

Disadvantage

- Computationally more complex.

Optimized Link State Routing (OLSR)

- It is a proactive routing protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying (MPR).
- This protocol optimizes the pure link state routing protocol.
- Optimizations are done in two ways:
  - By reducing the size of control packets.
  - By reducing the no. of links that are used for forwarding the link state packets.
- The subset of links or neighbors that are designated for link state updates and are assigned the responsibility of packet forwarding are called multipoint relays.
- The set consisting of nodes that are multipoint relays is referred to as MPRset.
- Each node(say, P) in the n/w selects an MPRset that processes and forwards every link state packet that node P originates.
- The neighbor nodes that do not belong to the MPRset process the link state packets originated by node P but do not forward them.
- Similarly, each node maintains a subset of neighbors called MPR selectors, which is nothing but the set of neighbors that have selected the node as a multipoint relay.
- In order to decide on the membership of the nodes in the MPRset, a node periodically sends Hello messages that contain
  - List of neighbors with which the node has bidirectional links
  - List of neighbors whose transmission was received in the recent past but with whom bidirectional links have not yet been confirmed.
- The nodes that receive this Hello packet update their own two-hop topology tables.
- The selection of multipoint relays is also indicated in the Hello packet.
- The Data structure called neighbor table is used to store the list of neighbors, the two-hop neighbors, and the status of neighbor nodes.
- The neighbor nodes can be in one of the three possible link status states, i.e
  - Unidirectional
  - Bidirectional

- Multipoint relay

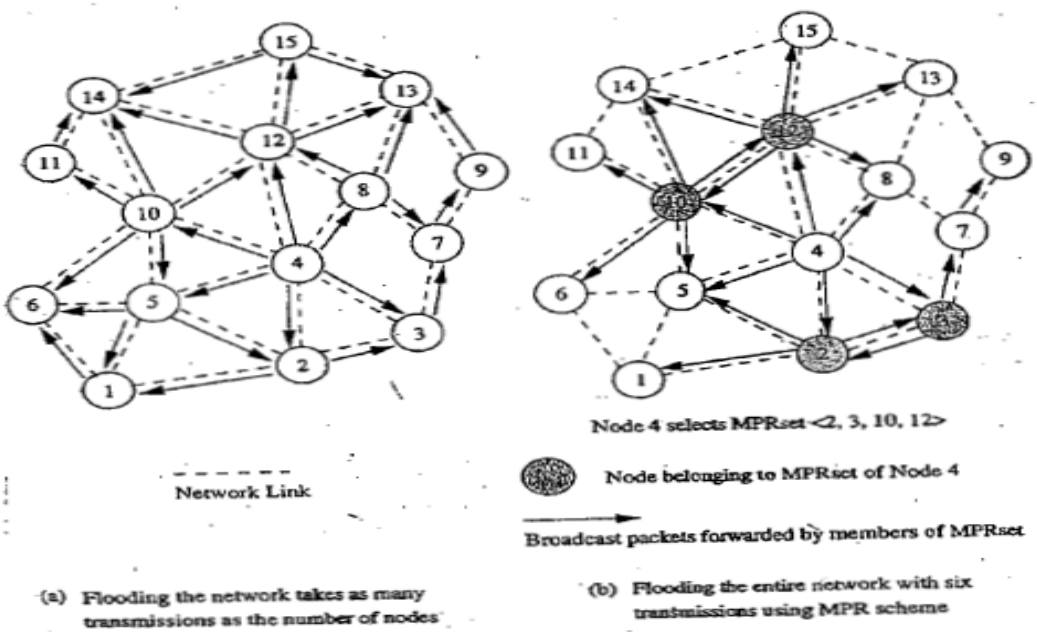


Figure 7.30. An example selection of MPRset in OLSR.

Selection of multipoint relay nodes (refer fig b)
Ni(x) → ith hop neighbor set of node x
MPR(x) → MPRset of node x.
Step1: MPR(x) ← Ø /* initializing empty MPRset */
Step2: MPR(x) ← {those nodes that belong to N1(x) and which are the only neighbors of nodes in N2(x)}
Step3: while there exists some node in N2(x) which is not covered by MPR(x)

a) For each node in N1(x),which is not in MPR(x),compute the maximum number of nodes that it covers among the uncovered nodes in the set N2(x).
b) Add to MPR(x) the node belonging to N1(x) for which this number is maximum.

Advantages:

- Reduces the routing overhead.
- Reduces the no. of broadcasts done.
- Hence low connection setup time and reduced control overhead.

HIERARCHICAL ROUTING PROTOCOLS

The use of routing hierarchy has several advantages → Reduction in size of routing tables and better scalability.

Hierarchical State Routing (HSR) protocol

- It is a distributed multi-level hierarchical routing protocol that employs clustering at different levels with efficient membership management at every level of clustering.
- Each cluster has its leader.
- Clustering is organized in levels:
  - **Physical**: between nodes that have physical wireless one-hop links between them.
  - **Logical**: based on certain relations.
- Fig 7.31 shows an ex for multilevel clustering

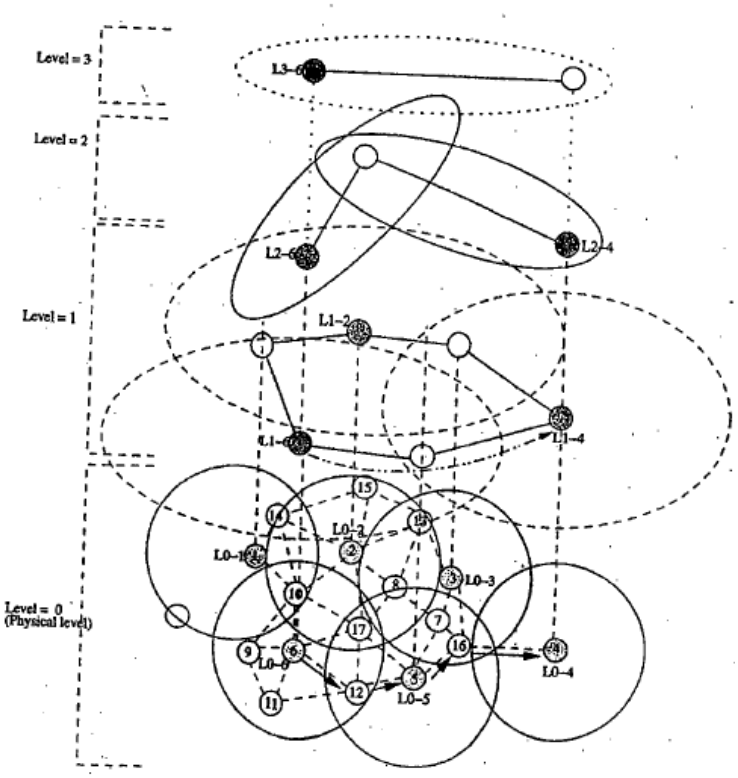


Figure 7.31. Example of HSR multi-level clustering.

- Node 8 is described as L0-8
- Its node ID=8
- It leads a cluster at level zero.
- Node 3 is described as L1-3
- Its node ID=3
- It leads a cluster at first level.
- The path between two cluster leaders is called virtual link
- The path between L1-3 L1-2 is: (3-2-8-13-12)
- HSR address is <HID-node ID>
- HSR address of node 10 is: <12,12-10>
- Every node maintains information about its peer's topology and the status of links to them. This information is broadcast to all the members of the cluster periodically.
- Cluster leaders exchange similar info with their peers.
- Each cluster leader broadcasts the info to the lower level informing all the nodes about the hierarchical topology of the n/w.

Route establishment

- Go to highest node in the hierarchy.
- Establish connections on virtual links.
- Send data through channel.

Advantages

- Reduces routing table size storage required is O (n x m).
- For flat topology, it is O (nm)
  - n→ no. of nodes
  - m→ no. of levels

Disadvantage

- Process of exchanging information concerned all the levels of the hierarchy as well as the process of leader election in every cluster makes it quite problematic for adhoc networks.

Fish-Eye State Routing Protocol (FSR)

- It is a generalization of the GSR protocol.
- It uses Fisheye technique to reduce the routing overhead.
- Principle: Property of a fish's eye that can capture pixel information with greater accuracy near its eye's focal point.
- This accuracy decreases with an increase in the distance from the center of the focal point
- This property is translated to routing in adhoc wireless networks by a node
- Each node maintains accurate information about near nodes.
- Nodes exchange topology information only with their neighbors.
- A sequence numbering scheme is used to identify the recent topology changes
- This constitutes a link-level information exchange of distance vector protocols and complete topology information exchange of link state protocols.
- FSR defines routing scope, which is the set of nodes that are reachable in a specific no. of hops.
- The scope of a node at two hops is the set of nodes that can be reached in two hops fig 7.32 shows scope of node 5 with one hop and two hops.
- The routing overhead is significantly reduced

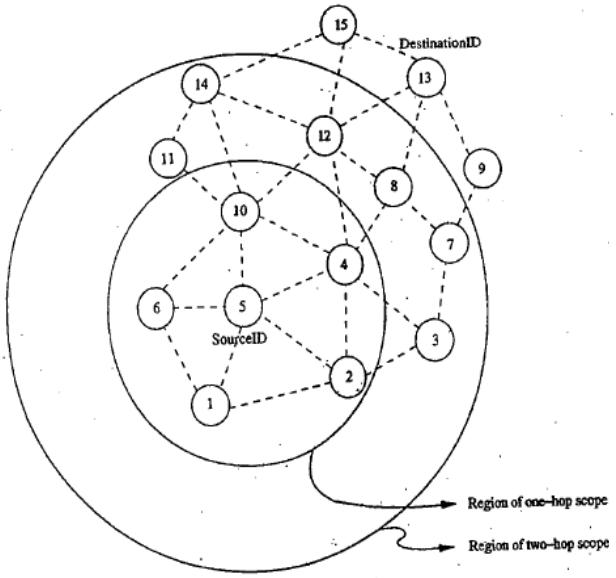


Figure 7.32. Fisheye state routing.

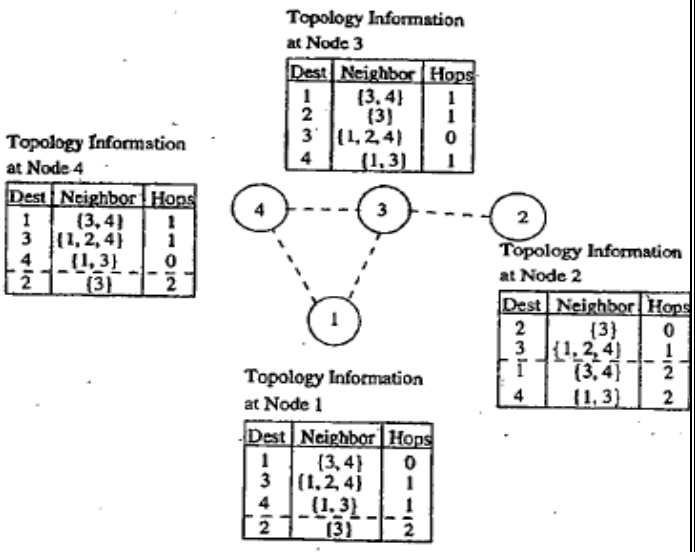


Figure 7.33. An illustration of routing tables in FSR.

- The link state info for the nodes belonging to the smallest scope is exchanged at the highest frequency. Frequency of exchanges decreases with an increase in scope.
- Fig 7.33 illustrates an example depicting the n/w topology information maintained at nodes in a n/w.
- Message size for a typical topology information update packet is significantly reduced
- The routing information for the nodes that are one hop away from a node are exchanged more frequently than the routing information about nodes that are more than one hop away
- Information regarding nodes that are more than one hop away from the current node are listed below the dotted line in the topology table.

Advantages

- Reduce bandwidth consumption by link state update packets.
- Suitable for large and highly mobile adhoc wireless network.

Disadvantages

- Very poor performance in small adhoc networks

POWER-AWARE ROUTING PROTOCOLS

Power-Aware Routing Metrics

The limitation on the availability of power for operation is a significant bottleneck.
Hence, the use of routing metrics contributes to the efficient utilization of energy and increases the lifetime of the network

- ***Minimal energy consumption per packet***
  - This metric aims at minimizing the power consumed by a packet in traversing from source node to the destination node.
  - The energy consumed by a packet when traversing through a path is the sum of the energies required at every intermediate hop in that path.
  - This metric doesn't balance the load
  - Disadvantages
    - Selection of path with large hop length
    - Inability to measure the power consumption in advance
    - Inability to prevent the fast discharging of batteries at some nodes
- ***Maximize network connectivity***
  - This metric attempt to balance the routing load among the cut set (the subset of the nodes in the network, the removal of which results in network partitions).

- It is difficult to achieve a uniform battery draining rate for the cut set.

- ***Maximum variance in Node power levels***
  - This metric proposes to distribute the load among all nodes in the network so that the power consumption pattern remains uniform across them.
  - This problem is very complex when the rate and size of the data packets vary
- ***Minimum cost per packet***
  - In order to maximize the life of every node in the network, this routing metric is made as a function of the state of the node's battery.
  - A node's cost decreases with an increase in its battery change and vice versa.
  - Cost of node can be easily computed
  - Advantage → congestion handling & cost calculation
- ***Minimize maximum node cost***
  - This metric minimizes the maximum cost per node for a packet after routing a number of packets or after a specific period.
  - This delays the failure of a node, occurring due to higher discharge because of packet forwarding

UNIT 6
TRANSPORT LAYER

INTRODUCTION

The objectives of transport layer protocol include the setting up of an end-to-end connection, end-to-end delivery of data packets, flow control, congestion control.

ISSUES IN DESIGNING A TRANSPORT LAYER PROTOCOL FOR AD HOC WIRELESS NETWORKS

1. **Induced Traffic:**
   - In a path having multiple link, the traffic at any given link (or path) due to the traffic through neighbouring links (or paths) is referred to as induced traffic.
   - This is due to the broadcast nature of the channel and the location-dependent contention on the channel
   - Induced Traffic affects the throughput achieved by the transport layer protocol.
2. **Induced throughput unfairness:**
   - This refers to the throughput unfairness at the transport layer due to the throughput/delay unfairness existing at the lower layer such as the n/w and MAC layers.
   - A transport layer should consider these in order to provide a fair share of throughput across contending flows
3. **Separation of congestion control, reliability and flow control:**
   - A transport layer protocol can provide better performance if end-to-end reliability, flow control and congestion control are handled separately.
   - Reliability and flow control are end-to-end activities, whereas congestion can at times be a local activity
   - Objective → minimisation of the additional control overhead generated by them
4. **Power and Band width constraints:**
   - Nodes in ad hoc wireless networks face resource constraints including the two most important resources: (i) power source and (ii) bandwidth
   - The performance of a Transport layer protocol is significantly affected by these resource constraints
5. **Interpretation of congestion:**
   - Interpretation of network congestion as used in traditional networks is not appropriate in ad hoc networks.
   - This is because the high error rates of wireless channel, location-dependent contention, hidden terminal problem, packet collisions in the network, path breaks due to mobility of nodes, and node failure due to drained battery can also lead to packet loss in ad hoc wireless networks
6. **Completely decoupled transport layer:**
   - Another challenge faced by Transport layer protocol is the interaction with the lower layers.
   - Cross-layer interaction between the transport layer and lower layers is important to adapt to the changing network environment
7. **Dynamic topology:**
   - Experience rapidly changing network topology due to mobility of nodes
   - Leads to frequent path breaks, partitioning and remerging of networks & high delay in re-establishment of paths
   - Performance is affected by rapid changes in network topology.

DESIGN GOALS OF A TRANSPORT LAYER PROTOCOL FOR AD HOC WIRELESS NETWORKS

- ✓ The protocol should maximize the throughput per connection.
- ✓ It should provide throughput fairness across contending flows.
- ✓ It should incur minimum connection set up and connection maintenance overheads.
- ✓ It should have mechanisms for congestion control and flow control in the network.
- ✓ It should be able to provide both reliable and unreliable connections as per the requirements of the application layer.
- ✓ It should be able to adapt to the dynamics of the network such as rapid changes in topology.
- ✓ Bandwidth must be used efficiently.
- ✓ It should be aware of resource constraints such as battery power and buffer sizes and make efficient use of them.
- ✓ It should make use of information from the lower layers for improving network thruput.
- ✓ It should have a well-defined cross-layer interaction framework.
- ✓ It should maintain End-to-End Semantics.

CLASSIFICATION OF TRANSPORT LAYER SOLUTIONS

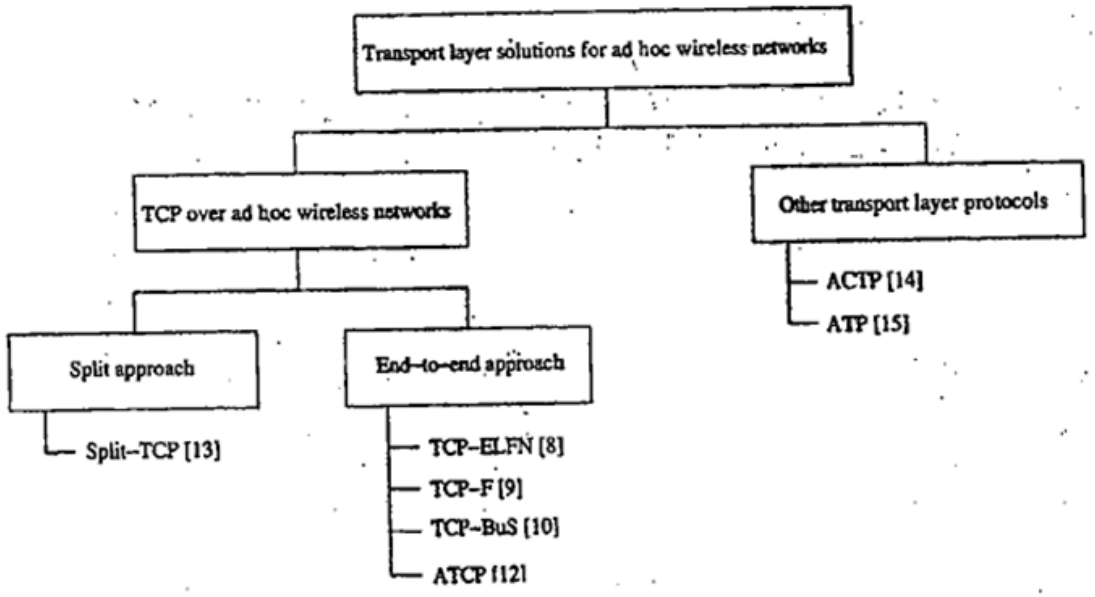


Figure 9.1. Classification of transport layer solutions.

TCP OVER AD HOC WIRELESS NETWORKS:

- **TCP** is reliable, end-to-end, connection-oriented TL protocol that provides a byte stream based service.
- Major responsibilities of TCP include
  - ✓ Congestion control.
  - ✓ Flow control.
  - ✓ In-order delivery of packets.
  - ✓ Reliable transportation of packets.

Discuss briefly the reasons why TCP does not perform well in Adhoc wireless network

The major reasons behind throughput degradation that TCP faces when used in ad hoc wireless networks are the following.

1. Misinterpretation of packet loss:

- In traditional TCP design, the packet loss is mainly attributed to network congestion.
- Ad hoc wireless network experience a much higher packets loss due to
  - ✓ High bit rate
  - ✓ Increased Collections etc.

2. Frequent path breaks:

- If the route re-establishment time is greater than the RTO period of TCP sender, then the TCP sender assumes congestion in the n/w ,retransmits lost packets and initiates congestion control algorithm. This leads to wastage of bandwidth and battery power.

3. Effect of path length:

As path length increases, the throughput decreases.

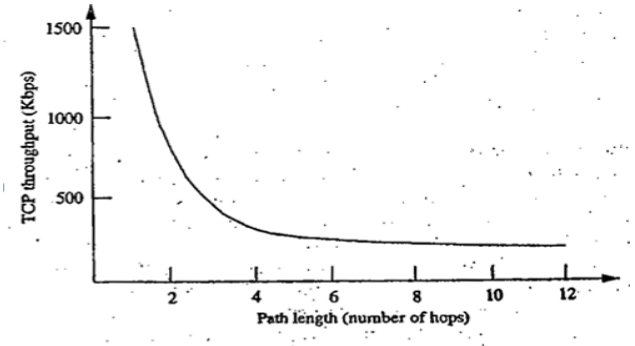


Figure 9.3. Variation of TCP throughput with path length.

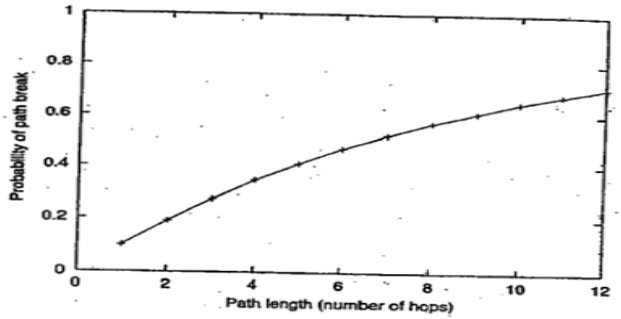


Figure 9.4. Variation of p_b with path length ($p_t = 0.1$).

4. Misinterpretation of congestion window:

- When there are frequent path breaks, the congestion window may not reflect the maximum transmission rate acceptable to the network and the receiver.

5. Asymmetric link behavior:

- Radio channel used in ad hoc wireless network has different properties such as location dependent contention, directional properties etc leading to asymmetric links.
- This can lead to TCP invoking the congestion control algorithm and several retransmissions.

6. Uni directional path:

- TCP relies on end-to-end ACK for ensuring reliability. Path break on an entirely different reverse path can affect the performance of the network as much as a path breaks in the forward path.

7. Multipath Routing:

- For TCP, multipath routing leads to significant amount of out of order packets, when intern generates a set of duplicate acknowledgement (DUPACKs),which cause additional power consumption and invocation of congestion control.

8. Network partitioning and remerging:

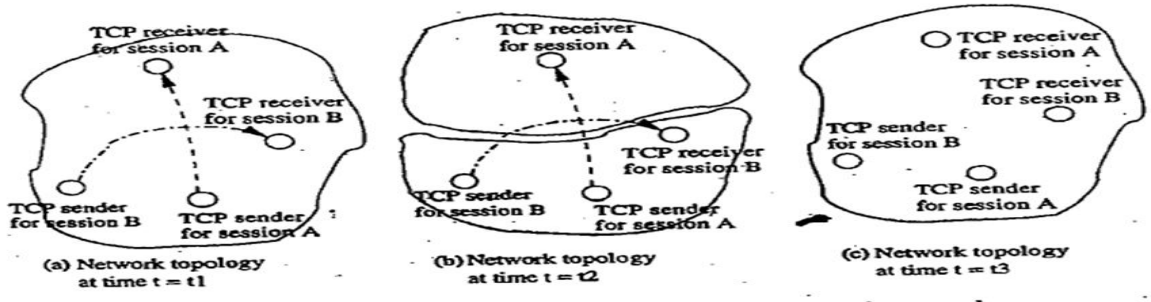


Figure 9.5. Effect of partitioning and merging of network.

- Fig below illustrates the effect of network partitions in ad hoc wireless networks.
- A network with two TCP sessions A & B is shown in (a) at time t1.

- At time t2, the network gets partitioned into two as shown in (b) due to dynamic topological changes.
- Now TCP session A's sender & receiver belong to two different partitions & TCP session B experiences path break.

9. The use of sliding window based transmission:

- TCP uses a sliding window for flow control.
- This can contribute to degraded performance in bandwidth constrained ad hoc wireless network.
- It can also lead to burstiness in traffic due to the subsequent transmission of TCP segments.

FEEDBACK BASED TCP (TCP – F)

- Improves performance of TCP.
- Uses a feedback based approach.
- The routing protocol is expected to repair the broken path within a reasonable time period

Operation:

- In TCP-F, an intermediate node, upon detection of a path break, originates route failure notification (RFN) packet. This intermediate node is called Failure point (FP).
- This RFN packet is routed toward the sender of the TCP session, Sender information that is obtained from TCP packets.
- If any intermediate nodes that receive RFN has an alternate route to the same destination, then it discards the RFN packet and uses the alternate path for forwarding further data packets, thus reducing control overhead involved in the route reconfiguration process.
- When TCP sender receives an RFN packet, it goes into a state called snooze. In this state, a sender,
  - Stops sending any more packets to the destination.
  - Cancels all timers.
  - Freezes its congestion window.
  - Freezes the retransmission timer.
  - Sets up a route failure timer.
- When route failure timer expires, the TCP sender changes from snooze state to connected state.
- When the route re-establishment has been done, then the failure point sends Route Re-establishment Notification (RRN) packet to the sender and the TCP state is updated back to the connected state.

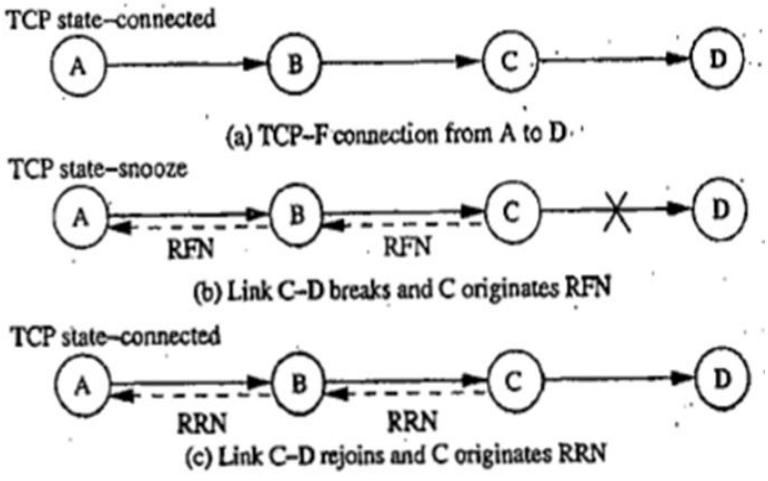


Figure 9.6. Operation of TCP-F.

Advantages :

- Simple feedback solution for problem arising from path breaks.
- Permits TCP congestion control mechanism to respond to congestion in the network.

Disadvantages:

- If a route to sender is not available at the FP, then additional control packets may need to be generated for routing RFN packets.
- TCP-F has an additional state compared to traditional TCP state mechanism.
- Congestion window used after a new route is obtained may not reflect the acheivable transmission rate acceptable to the network and the TCP-F receiver.

TCP WITH EXPLICIT LINK FAILURE NOTIFICATION: (TCP-ELFN)

- Improves TCP performance in adhoc wireless network.
- Similar to TCP-F.

Operation:

- ELFN is originated by the node detecting a path break upon detection of a link failure to the TCP sender.
- This can be implemented in two ways :
    1. By sending an ICMP Destination Unreachable (DUR) message to the sender.
       (or)
    2. By piggy-backing this information to the sender.
- Once the TCP sender receives the ELFN packet, it disables its retransmission timers and enters a standby state.
- In this state, it periodically originates probe packets to see if a new route is established.
- Upon reception of an ACK by the TCP receiver for the probe packets, it leaves the standby state, and continues to function as normal.

Advantages:

- Improves TCP performance by decoupling the path break information from the congestion information by the use of ELFN.
- Less dependent on routing protocol & requires only link failure notification about the path break.

Disadvantages:

- When the network is temporarily partitioned, the path failure may last longer & this can lead to the origination of periodic probe packets consuming bandwidth & power.
- Congestion window used after a new route is obtained may not reflect the achievable transmission rate acceptable to the network and the TCP receiver.

TCP-BUS (TCP WITH BUFFERING CAPABILITY AND SEQUENCE INFORMATION)

- It is similar to TCP-F and TCP-ELFN in its use of feedback information from an intermediate node on detection of a path break. But it is more dependent on the routing protocol.
- TCP-BuS was proposed, with Associativity-Based Routing (ABR) protocol as the routing scheme. Hence it makes use of some special messages such as LQ and REPLY for finding partial path.

Operation:

- Upon detection of a path break, an upstream intermediate node, called pivot node (PN),originates an explicit route disconnection notification (ERDN) message to the TCP-BuS sender.
- ERDN propagated in a reliable way.
- Upon receiving ERDN packet, the TCP-BuS sender stops transmission and freezes all timers and windows as in TCP-F.
- The packets in transmit at the intermediate nodes from the TCP-BuS sender to the PN are buffered until a new partial path from the PN to the TCP-BuS receiver is obtained by the PN.
- Upon detection of a path break, the downstream node originates a Route Notification (RN) packet to the TCP-BuS receiver, which is forwarded by all the downstream nodes in the path.
- PN attempts to find new partial path (route) to the TCP-BuS receiver , and the availability of such a partial path to destination is intimated to the TCP-BuS sender through an explicit route successful notification (ERSN) packet.TCP utilizes route reconfiguration mechanism of ABR to obtain partial path to the destination.
- Upon a successful LQ-REPLY process to obtain a new route to the TCP-BuS receiver, PN informs the TCP-BuS sender of the new partial path using ERSN Packet.(it is sent reliably)
- TCP-BuS sender also periodically originates probe packets to check the availability of a path to the destination.
- Below figure illustrates the operation of TCP-BuS.

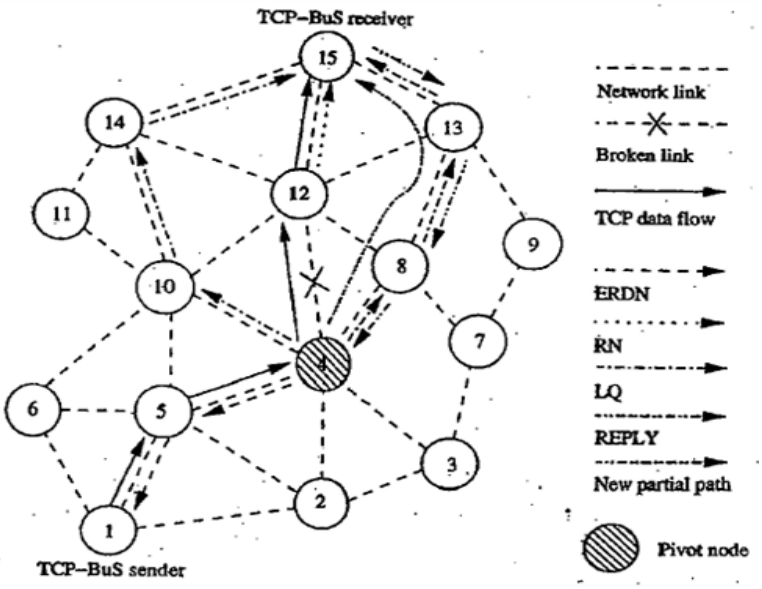


Figure 9.7. Operation of TCP-BuS.

Advantages:

- Performance improvement.
- Avoidance of fast retransmission due to the use of buffering, sequence numbering, and selective acknowledgement.
- Also takes advantage of the underlying routing protocols.

Disadvantages:

- Increased dependency on the routing protocol and the buffering at the intermediate nodes.
- The failure of intermediate nodes that buffer the packets may lead to loss of packets and performance degradation.
- The dependency on the routing protocol may degrade its performance with order routing protocols that do not have similar control messages as in ABR.

AD HOC TCP

- Based on feedback information received from the intermediate nodes, the TCP sender changes its state to the
  - *Persist state.*
  - *Congestion control state or*
  - *Retransmission state.*
- When an intermediate node finds that the network is partitioned, then the TCP sender state is changed to the persist state where it avoids unnecessary retransmissions.
- Figure shows the thin layer implementation of ATCP between the traditional TCP layer and the IP layer.
- This does not require changes in the existing TCP protocol.
- This layer is active only at the TCP sender.

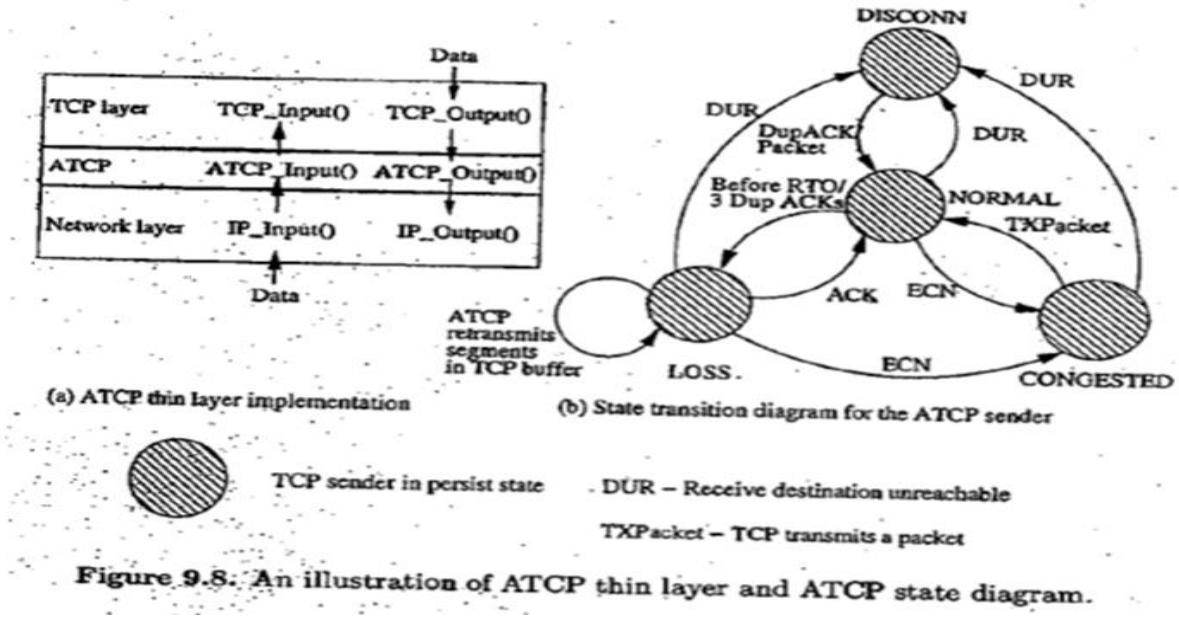


Figure 9.8. An illustration of ATCP thin layer and ATCP state diagram.

- Major function of the ATCP Layer is that it monitors the :
  - Packet sent and received by TCP sender,
  - The state of the TCP sender,
  - State of the network.
- Fig (b) shows the state transmission diagram for the ATCP at the TCP sender.

- The four states in the ATCP are:
  1. *NORMAL.*
  2. *CONGESTED*
  3. *LOSS*
  4. *DISCONN*
- When a TCP connection is established, the ATCP sender state is in NORMAL, here ATCP does not interfere with the operation of TCP and it remains invisible.

Table 9.1. The actions taken by ATCP

Event	Action
Packet loss due to high BER	Retransmits the lost packets without reducing congestion window
Route recomputation delay	Makes the TCP sender go to persist state and stop transmission until new route has been found
Transient partitions	Makes the TCP sender go to persist state and stop transmission until new route has been found
Out-of-order packet delivery due to multipath routing	Maintains TCP sender unaware of this and retransmits the packets from TCP buffer
Change in route	Recomputes the congestion window

Advantages:

- It maintains the end to end semantics of TCP.
- It is compatible with traditional TCP.
- Improves throughput of TCP in adhoc wireless network.

Disadvantages:

- Dependency on the network layer protocol to detect the route changes and partitions.
- Addition of thin ATCP layer to TCP/IP protocol stack requires changes in the interface functions currently being used

Split TCP

- Major issues that affect the performance of TCP over adhoc wireless network is the degradation of throughput with increasing path length.
- This can also lead to unfairness among TCP sessions where one session may obtain much higher throughput than other sessions.
- This unfairness problem is further worsened by the use of MAC protocols, which are found to give a higher throughput for certain link level sessions, leading to an effect known as channel capture.
- Split TCP provides a unique solution to this problem by splitting the transport layer objectives into:
- Congestion control.
- End to End reliability.
- In addition, split TCP splits a long TCP connection into a set of short concatenated TCP connections (called segments or zones) with a number of selected intermediate nodes (known as proxy nodes) as terminating points of these short connections.
- Figure illustrates the operation of split-TCP where a three segment split –TCP connection exists between source node1 and destination node 15.
- A proxy node receives the TCP packets, reads its contents, stores it in its local buffer, and sends an acknowledgement to the source (or the previous proxy)
- This acknowledgement is called Local acknowledgement (LACK) does not guarantee end to end delivery.
- The responsibility of further delivery of packets is assigned to the proxy node.
- In figure, node 1 initiates a TCP session to node 15, node 4 and node 13 are chosen as proxy nodes.

- The number of proxy nodes in a TCP session is determined by the length of the path between source & destination node.
- Based on a distributed algorithm, the intermediate nodes that receive TCP packets determine whether to act as a proxy node or just as a simple forwarding node.
- In figure, the path between nodes 1 & 4 is the first zone (segment), the path between nodes 4 to 13 is the second zone (segment), and the last zone is between node 13 and 15.
- The proxy node 4, upon receipt of each TCP packet from source node1,acknowledges it with a LACK packet, & buffers the received packets. This buffered packet is forwarded to the next proxy node at a transmission rate proportional to the arrival of LACKs from the next proxy node or destination.

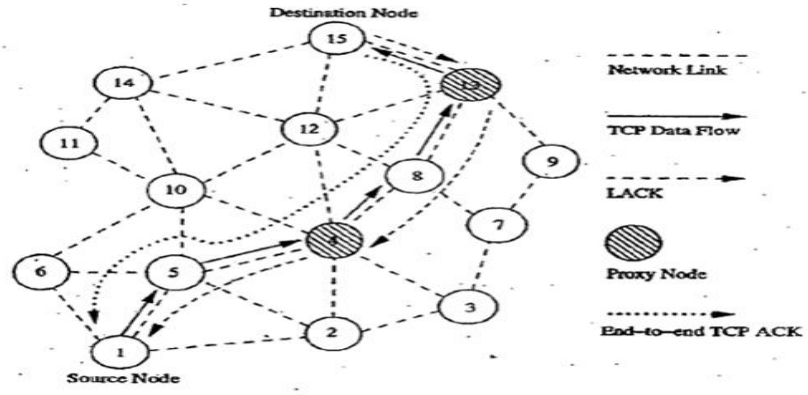


Figure 9.9. An illustration of Split-TCP.

Advantages:

- Improved throughput.
- Improved throughput fairness.
- Lessened impact of mobility.

Disadvantages:

- Requires modifications to TCP protocol.
- End to End connection handling of traditional TCP is violated.
- The failure of proxy nodes can lead to throughput degradation.

COMPARISION OF TCP SOLUTIONS FOR ADHOC WIRELESS NETWORKS

Issue	TCP-F	TCP-ELFN	TCP-BuS	ATCP	Split-TCP
Packet loss due to BER or collision	Same as TCP	Same as TCP	Same as TCP	Retransmits the lost packets without invoking congestion control	Same as TCP
Path breaks	RFN is sent to the TCP sender and state changes to snooze	ELFN is sent to the TCP sender and state changes to standby	ERDN is sent to the TCP sender, state changes to snooze, ICMP DUR is sent to the TCP sender, and ATCP puts TCP into persist state	Same as TCP	Same as TCP
Out-of-order packets	Same as TCP	Same as TCP	Out-of-order packets reached after a path recovery are handled	ATCP reorders packets and hence TCP avoids sending duplicates	Same as TCP
Congestion	Same as TCP	Same as TCP	Explicit messages such as ICMP source quench are used	ECN is used to notify TCP sender. Congestion control is same as TCP	Since connection is split, the congestion control is handled within a zone by proxy nodes
Congestion window after path reestablishment	Same as before the path break	Same as before the path break	Same as before the path break	Recomputed for new route	Proxy nodes maintain congestion window and handle congestion
Explicit path break notification	Yes	Yes	Yes	Yes	No
Explicit path reestablishment notification	Yes	No	Yes	No	No
Dependency on routing protocol	Yes	Yes	Yes	Yes	No
End-to-end semantics	Yes	Yes	Yes	Yes	No
Packets buffered at intermediate nodes	No	No	Yes	No	Yes

OTHER TRANSPORT LAYER PROTOCOLS FOR AD HOC WIRELESS NETWORKS

APPLICATION CONTROLLED TRANSPORT PROTOCOL

- It is a light-weight transport layer protocol
- Assigns the responsibility of ensuring reliability to the application layer
- ACTP stands in between TCP and UDP where TCP experiences low performance with high reliability and UDP provides better performance with high packet loss in Adhoc wireless networks
- The key design philosophy of ACTP is to leave the provisioning of reliability to the application layer and provide a simple feedback information about the delivery status of packets to the application layer
- Supports the priority of packets to be delivered
- Each API function call to send a packet contains the additional information required for ACTP such as the maximum delay, message number and priority of the packet
- Delivery status is maintained at the ACTP layer. This reflect
  - Successful delivery of the packet
  - A possible loss of the packet
  - Remaining time for the packet
  - No state information exists at the ACTP layer

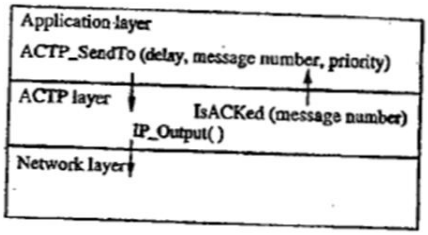


Figure 9.10. An illustration of the interface functions used in ACTP.

Advantages:

- Provides freedom of choosing the required reliability level to the application layer
- Scalable for large networks
- Throughput is not affected by path breaks

Disadvantage:

- Not compatible with TCP

AD HOC TRANSPORT PROTOCOL

- ATP is specifically designed for ad hoc wireless networks and is not a variant of TCP
- The major aspects by which ATP defers from TCP are
  - Coordination among multiple layers
  - Rate-based transmissions
  - Decoupling congestion control and reliability
  - Assisted congestion control
- ATP uses services from network and MAC layers for improving its performance
- ATP uses information from lower layers for
  - Estimation of the initial transmission rate
  - Detection, avoidance and control of congestion
  - Detection of path breaks
- ATP utilises timer-based transmission
- The network congestion information is obtained from the intermediate nodes
- Field in which delay information is included is referred as rate feedback field
- ATP has three phases namely: increase, decrease and maintain

Advantages:

- Improved performance
- Decoupling congestion control and reliability mechanisms
- avoidance of congestion window fluctuations

Disadvantage:

- lack of interoperability with TCP

UNIT 7
SECURITY

NETWORK SECURITY REQUIREMENTS

A security protocol for ad hoc wireless networks should satisfy the following requirements

1. ***Confidentiality:***
   a. The data sent by the sender must be comprehensible only to the intended receiver.
   b. Though an intruder might get hold of the data being sent, he / she must not be able to derive any useful information out of the data.
   c. One of the popular techniques used for ensuring confidentiality is *data encryption.*

2. ***Integrity:***
   a. The data sent by the source node should reach the destination node without being altered.
   b. It should not be possible for any malicious node in the network to tamper with the data during transmission

3. ***Availability:***
   a. The network should remain operational all the time.
   b. It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it.
   c. It should be able to provide guaranteed services whether an authorized user requires them

4. ***Non-Repudiation:***
   a. It is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
   b. *Digital signatures* are used for this purpose.

ISSUES AND CHALLENGES IN SECURITY PROVISIONING

1. *Shared broadcast radio channel :*
   a. The radio channel used for communication in adhoc wireless networks is broadcast in nature & is shared by all nodes within its direct transmission range.
   b. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network.
   c. This problem can be minimized to a certain extent by using *directional antennas.*

2. *Limited resource availability :*
   a. Resources such as bandwidth, battery power, & computational power are scarce in adhoc wireless networks.
   b. Hence it is difficult to implement complex cryptography-based security mechanisms in networks.

3. *Insecure operational environment :*
   a. The operating environments where adhoc wireless is used may not always be secure.
   b. One important application of such networks is in battlefields.

4. *Physical Vulnerability :*
   a. Nodes in these networks are usually compact & hand-held in nature.
   b. They could get damaged easily & are also vulnerable to theft.

5. *Lack of central authority :*

a. In wired networks & infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points & implement security mechanisms at such points.
b. Since adhoc –wireless networks do not have central points, these mechanisms cannot be applied in ad hoc wireless networks.

6. *Lack of associations:*
   a. Since these networks are dynamic in nature, a node can join or leave the network at any pont of time.
   b. If no proper authentication mechanism is used for associating nodes in a network, an intruder would be able to join into the network quite easily & carry out his/her attacks.

NETWORK SECURITY ATTACKS

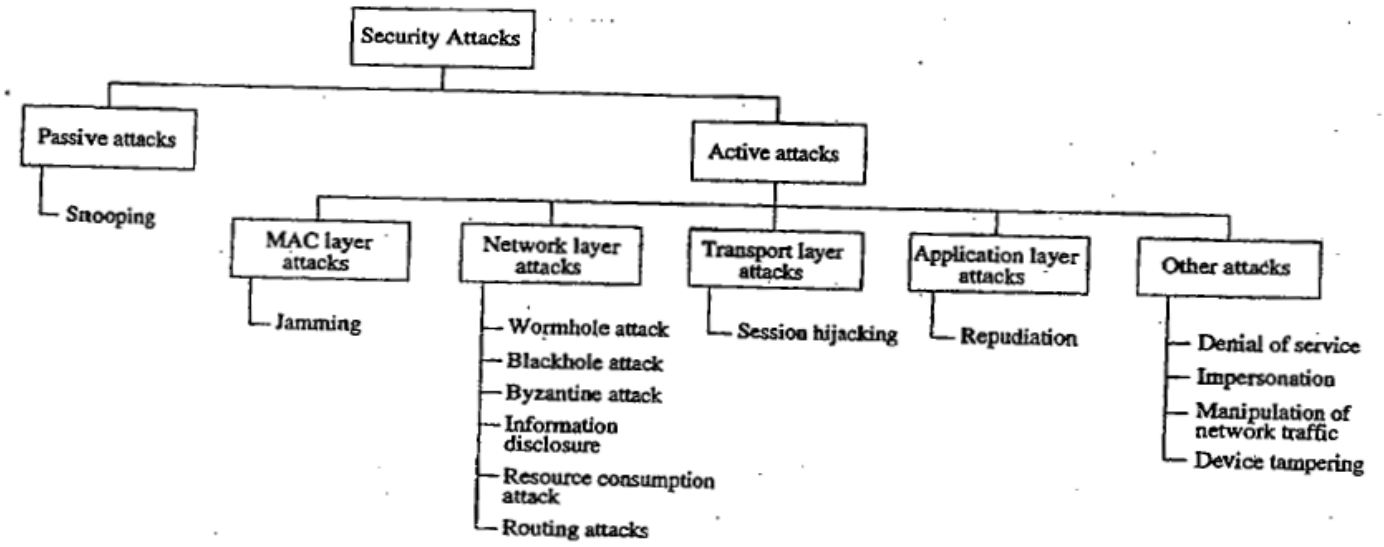


Figure 9.11. Classifications of attacks.

Attacks on adhoc wireless networks can be classified into 2 broad categories, namely:

1. *Passive attack*
   a. It does not disrupt the operation of the network; the adversary snoops the data exchanged in the network without altering it.
   b. One way to overcome such problems is to use powerful encryption mechanisms to encrypt the data being transmitted.

2. *Active attack*
   a. An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network.
   b. They can be further classified into 2 categories :
      i. External attacks, which are carried out by nodes that do not belong to the network. They can be prevented using standard encryption techniques and firewalls.
      ii. Internal attacks are from compromised nodes that are actually part of the network.

NETWORK LAYER ATTACKS

There are many types of attacks pertaining to the network layer in network protocol stack. Some of them are as follows:

1. ***wormhole attack:***

a. In this attack, an attacker receives packets at one location in the network & tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network. This tunnel between 2 colliding attackers is referred to as a wormhole.
b. If proper mechanisms are not employed to defend the network against wormhole attacks, existing routing protocols for adhoc wireless networks may fail to find valid routes.

2. ***Blackhole attack:***
   a. In this attack, a malicious node falsely advertises good paths to destination node during path-finding process or in route update messages.
   b. The intention of malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node.

3. ***Byzantine attack:***
   a. Here, a compromised intermediate note or a set of compromised intermediate nodes work in collusion & carries out attack such as creating routing loops, routing packets on non-optimal paths & selectively dropping packets.

4. ***Information disclosure:***
   a. A compromised node may leak confidential or important information to unauthorized nodes in the network.

5. ***Resource consumption attack:***
   a. In this attack, a malicious node tries to consume/waste resources of other nodes present in the network.
   b. The resources targeted are battery power, bandwidth & computational power, which are limitedly available in adhoc wireless networks.

6. ***Routing attacks:***
   a. There are several types of attacks mounted on routing protocol & they are as follows:
      i. *Routing table overflow:*
         - In this type of attack, an adversary node advertises routes to non-existent nodes, to the authorized nodes present in the network.
         - The main objective of this attack is to cause an overflow of routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes.
      ii. *Routing table poisoning*:
         - Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes.
         - This may result in sub-optimal routing, congestion in network or even make some parts of network inaccessible.
      iii. *Packet replication:*
         - In this attack, an adversary node would replicate state packets.
      iv. *Route cache poisoning:*
         - Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar activities.
      v. *Rushing attack:*
         - On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack.

TRANSPORT LAYER ATTACKS:

1. *Session Hijacking:*
   a. Here, an adversary takes control over a session between 2 nodes.

b. Since most authentication processes are carried out only at the start of session, once the session between 2 nodes get established, the adversary node masquerades as one of the end-nodes of the session & hijacks the sessions.

APPLICATION LAYER ATTACKS:

1. *Repudiation:*
   a. It refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication

OTHER ATTACKS:

This section discusses security attacks that cannot strictly be associated with any specific layer in the network protocol stack

MULTI-LAYER ATTACKS

Multi-layer attacks are those that could occur in any layer of the network protocol stack. Some of the multi-layer attacks in adhoc wireless networks are:

1. Denial of Service

- In this type of attack, an adversary attempts to prevent legitimate & authorized users of services offered by the network from accessing those services.
- This may lead to a failure in the delivery of guaranteed services to the end users.
- Some of the DoS attacks are as follows:
  - **Jamming** – in this form of attack, the adversary initially keeps monitoring the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender. Frequency hopping spread spectrum(FHSS) and direct sequence spread spectrum (DSSS) are two commonly used techniques that overcome jamming attacks
  - **SYN flooding** – here, an adversary sends a large number of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The victim node builds up a table/data structure for holding information regarding all pending connections. Since the maximum possible size of the table is limited, the increasing number of half-connections results in an overflow in the table.
  - **Distributed DoS attack** – here, several adversaries that are distributed throughout the network collide and prevent legitimate users from accessing the services offered by the network.

2. *Impersonation*

- In these attacks, an adversary assumes the identity & privileges of an authorized node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the network by injecting false routing information into the network.
- A *man-in-the-middle* attack is another type of impersonation attack.

DEVICE TAMPERING

- Unlike nodes in a wired network, nodes in adhoc wireless networks are usually compact, soft and hand-held in nature.
- They could get damaged or stolen easily.

KEY MANAGEMENT

Having seen the various kinds of attacks possible on adhoc wireless networks, we now look at various techniques employed to overcome the attacks.

- **CRYPTOGRAPHY** is one of the most common & reliable means to ensure security & can be applied to any communication network.
- In the parlance of cryptography, the original information to be sent from one person to another is called ***plaintext***.

- The plaintext is converted into ***ciphertext*** by the process of ***encryption.***
- An authentic receiver can decrypt / decode the ciphertext back into plaintext by the process of ***decryption.***
- The process of encryption and decryption are governed by keys, which are small amounts of information used by the cryptographic algorithms. When the keys is to be kept secret to ensure the security of the system, it is called a ***secret key.***
- The secure administration of cryptographic keys is called ***Key Management.***
- The 4 main goals of cryptography are confidentiality, integrity, authentication & non-repudiation.
- There are 2 major kinds of cryptographic algorithms:
    1. ***Symmetric*** *key algorithms*, which use the same key for encryption & decryption.
    2. ***Asymmetric*** *key algorithms,* which use two different keys for encryption & decryption.

The asymmetric key algorithms are based on some mathematical principles which make it feasible or impossible to obtain one key from another; therefore, one of the keys can be made public while the others is kept secret (private). This is called public key cryptography

SYMMETRIC KEY ALGORITHMS

- ♥ Symmetric key algorithms rely on the presence of shared key at both the sender & receiver, which has been exchanged by some previous arrangement.
- ♥ There are 2 kinds of symmetric key algorithms:
    - One involving block ciphers &
    - The stream ciphers.
- ♥ A block cipher is an encryption scheme in which plaintext is broken into fixed-length segments called blocks, & the blocks are encrypted one at a time.
- ♥ The simplest example includes substitution & transposition.
- ♥ In *substitution,* each alphabet of plaintext is substituted by another in the cipher text,& this table mapping of the original & the substituted alphabet is available at both the sender & receiver.
- ♥ A *Transposition cipher,* permutes the alphabet in plaintext to produce the cipher text.

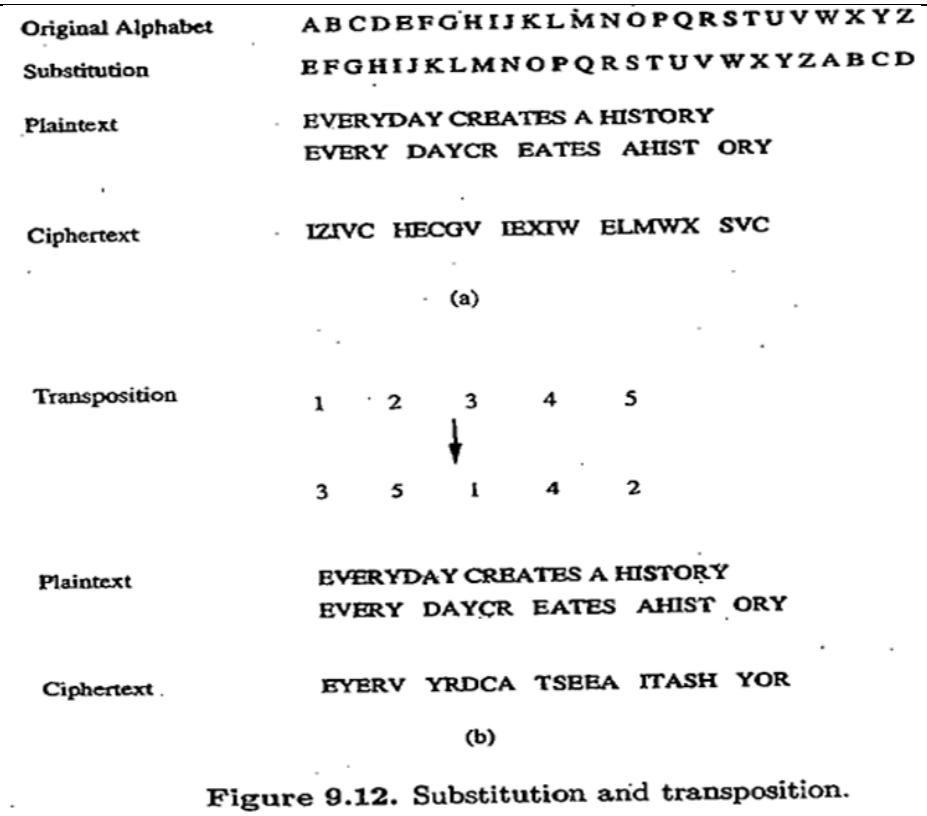


Figure 9.12. Substitution and transposition.

- ♥ Fig (a) shows encryption using substitution & fig (b) shows a transposition cipher.
- ♥ The block length used is 5.
- ♥ A stream cipher is, in effect, a block cipher of block length one.
- ♥ One of the simplest stream ciphers is *vernam cipher*, which uses a key of same length as plaintext for encryption.
- ♥ For example : If the plaintext is the binary string 10010100 & key is 01011001.then the encrypted string is given by the XOR of the plaintext & key, to be 11001101. The plaintext is again recovered by XOR-ing the cipher text with the same key.

ASYMMETRIC KEY ALGORITHMS

- Asymmetric key (or public key) algorithms use different keys at the sender end & receiver ends for encryption & decryption, respectively.
- Let the encryption process be represented by a function E, & decryption by D.
  Then plaintext 'm' is transformed into the ciphertext 'c' as
  $$C = E(m)$$
  The receiver then decodes c by applying D. Hence, D is such that
  $$m = D(c) = D(E(m))$$
- When this asymmetric key concept is used in public key algorithms, the key E is made public, while D is made private, known only to the intended receiver.
- RSA algorithm is the best example of public key cryptography.
- Digital signatures scheme are also based on public key encryption.
- These are called reversible public key systems
- In this case, the person who wishes to sign a document encrypts it using his/her private key D, which is known only to him/her.
- Anybody who has his/her public key E can decrypt it and obtain the original document
- A trusted third party is responsible for issuing these digital signatures and for resolving any disputes regarding the signatures
- This is usually a governmental or business organisation

KEY MANAGEMENT APPROACHES

- The primary goal of key management is to share a secret (some information) among a specified set of participants.
- The main approaches to key management are key predistribution, key transport, key arbitration and key agreement.

1. KEY PREDISTRIBUTION:

- Key predistribution, as the name suggests, involves distributing key to all interested parties before the start of communication.
- This method involves much less communication & computation, but all participants must be known *a priori*, during the initial configuration.
- Once deployed, there is no mechanism to include new members in the group or to change the key.
- As an improvement over predistribution scheme, sub-groups may be formed within a group, and some communication may be restricted to a subgroup.
- However, formation of subgroups is also an *a priori* decision.

2. KEY TRANSPORT:

- In key transport systems, one of the communicating entities generates keys & transports them to the other members.
- The simplest scheme assumes that a shared key already exists among the participating members. This shared key is used to encrypt a new key & is transmitted to all corresponding nodes.
- Only those nodes which have the prior shared key can decrypt it.
- This is called the *Key Encrypting Key (KEK) method.*
- An interesting method for key transport without prior shared keys is the shamir's three-pass protocol.

The scheme is based on a special-type of encryption called communicative Encryption schemes.

Consider 2 nodes X & Y which wish to communicate. Node X selects a key K which it wants to use in its communication with node Y.It then generates a random key K_x ,using which it encrypts K with f, & sends to node Y. Node Y encrypts this with a random key k_y using g,& sends this back to node X.

Now, node X decrypts this message with its key K_x, & after applying inverse function f^{-1},sends it to node y. finally, node Y decrypts the message using K_y & g^{-1} to obtain key K.

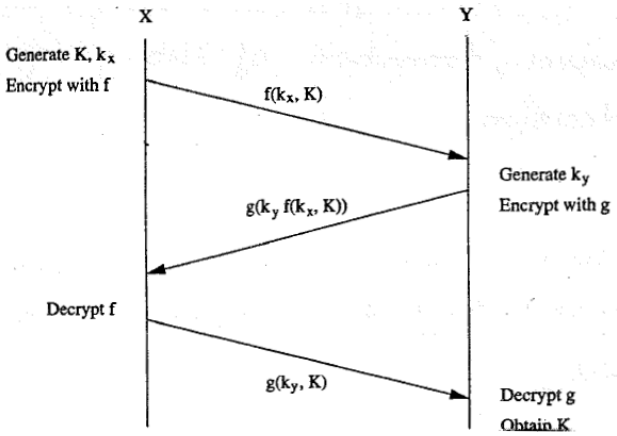


Figure: Shamir's three-pass protocol

3. KEY ARBITRATION:

- Key arbitration schemes use a central arbitrator to create & distribute keys among all participants.
- Hence, they are a class of key transport schemes.
- In ad hoc wireless networks, the problem with implementation of arbitrated protocols is that the arbitrator has to be powered on at all times to be accessible to all nodes
- This leads to a power drain on that particular node
- Alternative is to make the keying service distributed
- If any one of the replicated arbitrators is attacked, the security of the whole system breaks down

4. KEY AGREEMENT:

- Key agreement protocols are used to establish a secure context over which a session can be run, starting with many parties who wish to communicate & an insecure channel.
- In group key agreement schemes, each participant contributes a part to the secret key.
- Require least amount of preconfiguration
- Have high computational capability
- The most popular key agreement schemes use the Diffie-Hellman exchange, an asymmetric key algorithm based on discrete logarithms.

KEY MANAGEMENT IN ADHOC WIRELESS NETWORKS

- Adhoc wireless networks pose certain specific challenges in key management, due to the lack of infrastructure in such networks.
- 3 types of infrastructure have been identified, which are absent in adhoc wireless networks:
  - The first is the network infrastructure, such as dedicated routers & stable links, which ensure communication with all nodes.
  - The second missing infrastructure is services, such as name resolution, directory & TTP's.
  - The third missing infrastructure in adhoc wireless network is the administrative support of certifying authorities.

Password-Based Group Systems:

- A password-based system has been explored where, in the simplest case, a long string is given as the password for users for one session.
- However, human beings tend to favour natural language phrases as passwords, over randomly generated strings.
- Such passwords, if used as keys directly during a session, are very week & open to attack directly during a high redundancy, & the possibility of reuse over different sessions.
- Hence, protocols have been proposed to derive a strong key (not vulnerable to attacks).
- This password-based system could be two-party, with a separate exchange between any 2 participants, or it could be for the whole group, with a leader being elected to preside over the session.
- The protocol used is as follows :

- Each participant generates a random number, & sends it to all others.
- When every node has received the random number of every other node, a common pre-decided function is applied on all the numbers to calculate a reference value.
- The nodes are ordered based on the difference between their random number & the reference value.

Threshold Cryptography:

- Public Key Infrastructure (PKI) enables the easy distribution of keys & is a scalable method.
- Each node has a public/private key pair,& a certifying authority (CA) can bind the keys to a particular node. But CA has to be present at all times, which may not be feasible in Adhoc wireless networks.
- A scheme based on threshold cryptography has been proposed by which n servers exist in an adhoc wireless network, out of which any (t+1) servers can jointly perform arbitration or authorization successfully, but t servers cannot perform the same. This is called an (n, t+1) configuration, where n >= 3t +1.
- To sign a certificate, each server generates a partial signature using its private key & submits it to a combiner. The combiner can be any one of the servers.
  - In order to ensure that the key is combined correctly, t+1 combiners can be used to account for at most t malicious servers.
  - Using t+1 partial signatures, the combiner computes a signature & verifies its validity using a public key.
  - If verification fails, it means that at least one of the t+1 keys is not valid, so another subset of t+1 partial signature is tried. If combiner itself is malicious, it cannot get a valid key, because partial key itself is always invalid.

Self-Organised Public Key Management for Mobile Adhoc Networks:

- Self-organised public key system makes use of absolutely no infrastructure.
- The users in the adhoc wireless network issue certificates to each other based on personal acquaintance.
- A certificate is binding between a node & its public key. These certificates are stored & distributed by the users themselves. Certificates are issued only for specific period of time, before it expires; the certificate is updated by the user who had issued the certificate.
- Each certificate is initially stored twice, by the issuer & by the person for whom it is issued.
- If any of the certificates are conflicting (e.g: the same public key to different users, or the same user having different pubic keys), it is possible that a malicious node has issued a false certificate.
- A node then enables such certificates as conflicting & tries to resolve the conflict.
- If the certificates issued by some node are found to be wrong, then that node may be assumed to be malicious.
- A certificate graph is a graph whose vertices are public keys of some nodes and whose edges are public key certificates issued by users.

SECURE ROUTING IN AD HOC WIRELESS NETWORKS

Ensuring secure communication in adhoc wireless networks include the mobility of nodes, a promiscuous mode of operation, limited processing power & limited availability of resources such as battery power, bandwidth & memory.

REQUIREMENTS OF A SECURE ROUTING PROTOCOL FOR ADHOC WIRELESS NETWORKS

The fundamental requirements for a secure routing protocol for adhoc wireless networks are listed as below:

- Detection of malicious nodes:
  - A secure routing protocol should be able to detect the presence of any malicious node in the network & should avoid the participation of such nodes in the routing process.
- Guarantee of correct route discovery:
  - If a route between the source & destination node exist, the routing protocol should be able to find the route, & should also ensure the correctness of the selected route.

- Confidentiality of network topology:
  - Once the network topology is known, the attacker may try to study the traffic pattern in the network. If some of the nodes are found to be more active compared to others, the attacker may try to mount attacks.
  - This may ultimately affect the ongoing routing process. Hence, confidentiality of network topology is important.
- Stability against attacks:
  - The routing protocols must be self-stable in the sense that it must be able to revert to its normal operating state within a finite amount of time after passive or an active attack.
  - Some of the security-aware routing protocols proposed for adhoc wireless networks are discussed.

SECURITY AWARE ADHOC ROUTING PROTOCOL

- This routing protocol uses security as one of the key metrics in path finding.
- In adhoc wireless networks, communication between end nodes through possibly multiple intermediate nodes is based on the fact that the two end nodes trust the intermediate nodes.
- SAR defines level of trust as a metric for routing & as one of the attributes for security to be taken into consideration while routing.
- The routing protocol based on level of trust is explained in below figure.

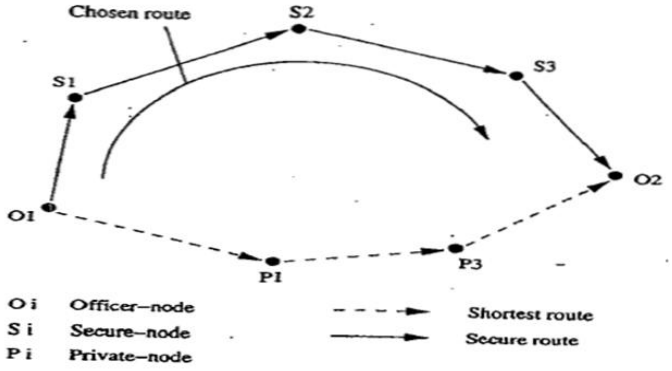


Figure 9.14. Illustration of the level of trust metric.

- Two paths exist between the two officers O1 and O2 who want to communicate with each other
- One of these paths is a shorter path which runs through private nodes whose trust levels are very low
- Hence, the protocol chooses a longer but secure path which passes through other secure nodes
- Nodes of equal levels of trust distribute a common key among themselves and with those nodes having higher levels of trust
- The SAR mechanism can be easily incorporated into the traditional routing protocols for ad hoc wireless networks
- It could be incorporated into both on-demand and table-driven routing protocols
- The SAR protocol allows the application to choose the level of security it requires
- But the protocol requires different keys for different levels of security
- This tends to increase the number of keys required when the number of security levels used increase

SECURE EFFICIENT AD HOC DISTANCE VECTOR ROUTING PROTOCOL

- SEAD routing protocol is a secure ad hoc routing protocol based on the destination-sequenced distance vector (DSDV) routing protocol
- This protocol is mainly designed to overcome security attacks such as DoS and resource consumption attacks
- The protocol uses a one-way hash function and does not involve any asymmetric cryptographic operation

DISTANCE VECTOR ROUTING

- Distance vector routing protocols belong to the category of table-driven routing protocols

- Each node maintains a routing table containing the list of all known routes to various destination nodes in the network
- The metric used for routing is the distance measured in terms of hop-count
- The routing table is updated periodically by exchanging routing information
- An alternative approach to this is triggered updates, in which each node broadcasts routing updates only if its routing table gets altered.

ONE-WAY HASH FUNCTION

- SEAD uses authentication to differentiate between updates that are received from non-malicious nodes and malicious nodes
- This minimizes resource consumption attacks caused by malicious nodes
- SEAD uses a one-way hash function for authenticating the updates
- A one-way hash function (H) generates a one-way hash chain (h_1, h_2,.....).
- The function H maps an input bit-string of any length to a fixed length bit-string
- To create a one-way hash chain, a node generated a random number with initial value x € $(0,1)^p$, where p is the length in bits of the output bit-string
- h_0 is the first number in the has chain is initialised to x
- The remaining values are computed using a general formula $h_i = H(h_i\text{-}1)$ for $0 \le i \le n$, for some *n.*
- SEAD avoids routing loops unless the loop contains more than one attacker
- The protocol is robust against multiple coordinated attacks
- SEAD protocol would not be able to overcome attacks where the attacker uses the same metric and sequence number which were used by the recent update message, and sends a new routing update

AUTHENTICATED ROUTING FOR AD HOC NETWORKS

- ARAN is a secure routing protocol which successfully defeats all identified attacks in the network layer
- It takes care of authentication, message integrity and non-repudiation
- During the route discovery process of ARAN, the source node broadcasts RouteRequest packets
- Destination packets responds by unicasting back a reply packet on the selected path
- The ARAN protocol uses a preliminary cryptographic certification process, followed by an end-to-end route authentication process, which ensures secure route establishment

ISSUE OF CERTIFICATES

- There exists an authenticated trusted server whose public key is known to all legal nodes in the network
- The ARAN protocol assumes that keys are generated a priori by the server and distributed to all nodes in the network
- On joining the network, each node receives a certificate from the trusted server
- The certificate received by a node A from the trusted server T looks like the following:

$$T \rightarrow A: \quad cert_A = [IP_A, K_{A+}, t, e]K_{T-} \qquad (9.12.1)$$

Here, IP_A, K_{A+}, t, e, and K_{T-} represent the IP address of node A, the public key of node A, the time of creation of the certificate, the time of expiry of the certificate, and the private key of the server, respectively.

END-TO-END ROUTE AUTHENTICATION

- The main goal of this end-to-end route authentication process is to ensure that the correct intended destination is reached by the packets sent from the source node
- The source node *S* broadcasts a *RouteRequest/RouteDiscovery* packet destined to destination node *D.*

$$S \rightarrow broadcasts := [RDP, IP_D, Cert_S, N_S, t]K_{S-}$$

$$A \rightarrow broadcasts := [[RDP, IP_D, Cert_S, N_S, t]K_{S-}]K_{A-}, Cert_A$$

$$D \rightarrow X := [REP, IP_S, Cert_D, N_S, t]K_{D-}$$

Where,

K_{A+}	Public key of node A.
K_{A-}	Private key of node A.
K_{AB}	Symmetric key shared by nodes A and B.
$\{d\}K_{A+}$	Encryption of data d with key K_{A+}.
$[d]K_{A-}$	Data d digitally signed by node A.
cert_A	Certificate belonging to node A.
e	Certificate expiration time.
N_A	Nonce issued by node A.
IP_A	IP address of node A.
RDP	Route Discovery Packet identifier.
REP	REPly packet identifier.
t	timestamp.

Table 9.3. Comparison of vulnerabilities of ARAN with DSR and AODV protocols

Attacks	Protocols		
	AODV	DSR	ARAN
Modifications required during remote redirection	Sequence number and hop-counts	Source routes	None
Tunneling during remote redirection	Yes	Yes	Yes
Spoofing	Yes	Yes	No
Cache poisoning	No	Yes	No

SECURITY AWARE AODV PROTOCOL

- AODV is an on-demand routing protocol where the route discovery process is initiated by sending RouteRequest packets only when data packets arrive at a node for transmission
- A malicious intermediate node could advertise that it has the shortest path to the destination, thereby redirecting all the packets through itself
- This is known as black hole attack

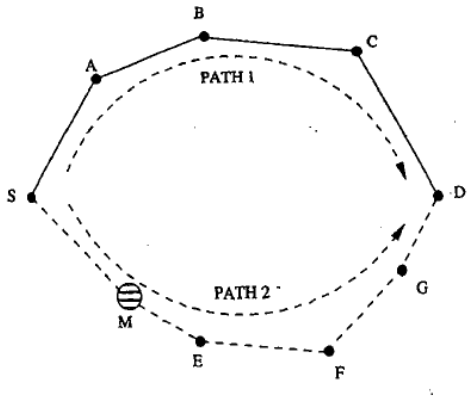


Figure 9.15. Illustration of blackhole problem.

- Let node M be the malicious node that enters the network
- It advertises that it has the shortest path to the destination node D when it receives the RouteRequest packet sent by node S
- The attacker may not be able to succeed if node A, which also receives the RouteRequest packet from node S, replies earlier than node M
- Advantage → malicious node does not have to search its routing table for a route to the destination
- Hence the malicious node would be able to reply faster than node A

SOLUTIONS FOR THE BLACK HOLE PROBLEM

- One of the solutions for the blackhole problem is to restrict the intermediate nodes from originating RouteReply packets
- Only the destination node would be permitted to initiate RouteReply packets
- Security is not completely assured

- The delay involved in the route discovery process increases as the size of the network increases

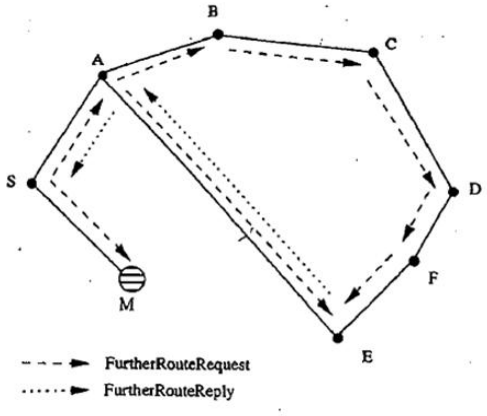


Figure 9.16. Propagation of *FurtherRouteRequest* and *FurtherRouteReply*.

- The source node S sends FurtherRouteRequest packets to this neighbour node E
- Node E responds by sending a FurtherRouteReply packet to source node S
- Since node M is a malicious node which is not present in the routing list of node E, the FurtherRouteReply packet sent by node E will not contain a route to the malicious node M.
- This protocol completely eliminates the blackhole attack caused by a single attacker
- Disadvantage → control overhead of the routing protocol increases considerably
- If the malicious nodes work in a group, this protocol fails miserably.

AD HOC NETWORKS UNIT WISE QUESTIONS
(PREVIOUS VTU QUESTION PAPERS)

UNIT 1

1. Give any 5 differences btw cellular wireless networks and ADHOC wireless n/w (5) or (10)
2. Explain any 6 issues of ADHOC wireless n/w (12)
3. Write a note on ADHOC wireless internet (3)
4. Explain the wireless sensor n/w with its issues compared to adhoc n/w (10)
5. Briefly explain the following with proper diagrams:
   i. Cellular wireless n/w
   ii. adhoc wireless n/w
   iii. Hybrid wireless n/w
   iv. Wireless sensor n/w (08)
6. Discuss the following major issues and challenges that need to be considered when an adhoc wireless system is to be designed
   i. Medium access scheme
   ii. Routing
   iii. Transport layer protocol
   iv. Self organization
   v. Address and service discovery
   vi. Scalability (12)

UNIT 2

1. Describe in detail the MACAW and MACA-BY-invitation protocols. (10)
2. Explain any 2 contention based with preservation mechanism MAC protocols (10)
3. Discuss the major issues to be considered for a successful adhoc wireless internet (10)
4. Explain the classification of MAC protocols (10)
5. Briefly discuss the following:
   i. Quality of service support
   ii. Hidden and exposed terminal problem
   iii. Mobility of nodes
   iv. Error prone shared broadcast channel (08)
6. Briefly discuss the following:
   i. Contention based protocols
   ii. Contention based protocols with reservation mechanisms
   iii. Contention based protocols with scheduling mechanisms (09)
7. What are the advantages of reservation based MAC protocols over contention based MAC protocols (03)
8. Define soft reservation. Explain SRMA/PA using frame structure (10)
9. Briefly explain the 5 phase reservation protocol with frame structure (10)

UNIT 4

1. What are the characteristics of routing protocols for adhoc wireless n/w? (08)
2. Give the classification of routing protocols for adhoc wireless n/w (06)
3. Explain any 1 table driven routing protocol for adhoc wireless n/w (06)
4. With an example, explain the process of route establishment in wireless routing protocol (10)
5. Explain the temporary ordered routing algorithm. Also, mention its advantages and disadvantages (10)
6. Discuss the differences in topology reorganization in DSDV and CGSR routing protocols (06)

7. Explain the salient features and topology maintenance/routing information maintenance in cluster head gateway switch routing protocol (10)
8. What are the key diff btw LAR! And LAR2 algorithms (04)
9. Explain route establishment in DSDV with an example (10)
10. List the characteristics of an ideal routing protocol for and adhoc wireless n/w (10)

UNIT 5

1. Explain core contention based distributed adhoc routing protocol (10)
2. Describe any two hierarchical routing protocols (10)
3. Explain flow oriented routing protocol (10)
4. Explain the various routing metrics (10)
5. Explain the "optimal link state routing" with diagram (10)
6. Explain the following proper aware routing metrics:
   i. Minimal energy consumption per packet
   ii. Maximize network connectivity
   iii. Minimum variance in node power level
   iv. Minimum cost per packet
   v. Minimize maximum node cost (10)
7. Explain any 1 hierarchical routing protocol (12)
8. Discuss the adv and disadvantage of zone routing protocol and zone based hierarchical link state routing protocol (08)

UNIT 6

1. Explain the issues and design goals of transport layer protocol for adhoc wireless n/w (10)
2. Explain adhoc and split TCP (10)
3. Explain multilayer attacks (10)
4. Briefly explain at least four major reasons behind throughput degradation that TCP faces when used in adhoc n/w (08)
5. What are the pros and cons of assigning the responsibility of end to end reliability to the application layer? (06)
6. Assume that when the current size of congestion window is 48kb. The TCP sender experiences a timeout. What will be the congestion window size if the next 3 transmission bursts are successful? Assume that MSS is 1kb. Consider (i)TCP Tahoe and (ii) TCP Reno (06)
7. Give 5 reasons stating why TCP doesn't work well in adhoc wireless n/w (10)
8. Briefly explain the state transition diagram for Adhoc TCP sender (ATCP) (10)

UNIT 7

1. Give the classification of security attacks in adhoc wireless n/w. (06)
2. Describe the symmetric key algorithm for security (06)
3. Explain the key management in adhoc wireless n/w (08)
4. Explain cluster TDMA (10)
5. Explain ticket based QOS routing protocol (10)
6. Explain with diagram "security aware adhoc routing protocol" (08)
7. Explain how security provisioning in adhoc wireless differ from that in infrastructure based networks (06)
8. List and explain how some of the inherent properties of the wireless adhoc n/w introduce difficulties while implementing security in routing protocols (06)
9. Briefly discuss network layer attacks (10)
10. Explain key management in adhoc wireless n/w (10)

*****ALL THE BEST*****