LECTURE NOTES ON

MOBILE COMPUTING
(15A05802)

IV B.TECH II SEMESTER

(JNTUA-R15)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MOTHER THERESA INSTITUTE OF ENGINEERING & TECHNOLOGY

Melumoi,PALAMANER-517408

(Approved by AICTE, New Delhi Affiliated to JNTUA Ananthapuramu. ISO 9001:2015 Certified Institute)

UNIT-1

Introduction

A wireless local area network (WLAN) is a local area network (LAN) that doesn't rely on wired Ethernet connections. A WLAN can be either an extension to a current wired network or an alternative to it.

WLANs have data transfer speeds ranging from 1 to 54Mbps, with some manufacturers offering proprietary 108Mbps solutions. The 802.11n standard can reach 300 to 600Mbps.

Because the wireless signal is broadcast so everybody nearby can share it, several security precautions are necessary to ensure only authorized users can access your WLAN.

WLAN types

Private home or small business WLAN

Commonly, a home or business WLAN employs one or two access points to broadcast a signal around a 100- to 200-foot radius. You can find equipment for installing a home WLAN in many retail stores. With few exceptions, hardware in this category subscribes to the 802.11a, b, or g standards (also known as Wi-Fi); some home and office WLANs now adhere to the new 802.11n standard. Also, because of security concerns, many home and office WLANs adhere to the Wi-Fi Protected Access 2 (WPA2) standard.

Enterprise class WLAN

An enterprise class WLAN employs a large number of individual access points to broadcast the signal to a wide area. The access points have more features than home or small office WLAN equipment, such as better security, authentication, remote management, and tools to help integrate with existing networks. These access points have a larger coverage area than home or small office equipment, and are designed to work together to cover a much larger area. This equipment can adhere to the 802.11a, b, g, or n standard, or to security-refining standards, such as 802.1x and WPA2.

Wireless Network Types

Wireless networks use different technologies depending on the distance to achieve, the number of devices to connect, and the amount of information to transmit. The technologies include,

- Wireless personal-area networks (WPAN): Have a short range (up to 20–30 feet/7–10 meters), commonly use the 802.15 family of specifications to connect two or a few devices with low power consumption. Bluetooth is an example of WPAN protocol.
- Wireless local-area networks (WLAN): Consume more power but extend the connection to about 300 feet (100 meters). WLANs are the main topic of this book.
- Wireless metropolitan-area network (WMAN): Extend the range to a larger geographic area, such as a city or suburb. Applications vary from point-to-point or point-to-multipoint links to multiuser coverage. WMANs typically use licensed frequencies (a fee has to be paid for permission to use the frequency), although implementations in the ISM bands can also be found. WiMAX is an example of WMAN protocol (most WiMAX implementations use licensed bands).
- Wireless wide-area network (WWAN): Provide connectivity over a wide geographical area. Usually, WWANs are networks used for mobile phone and data service and are operated by carriers. WWANs typically use licensed frequencies.

FUNDAMENTALS OF WLANS

The terms "node," "station," and" terminal" are used interchangeably. While both portable terminals and mobile terminals can move from one place to another, portable terminals are accessed only when they are stationary. Mobile terminals (MTs), on the other hand, are more powerful, and can be accessed when they are in motion. WLANs aim to support truly mobile work stations.

Differences between Wireless and Wired Transmission

• **Address is not equivalent to physical location:** In a wireless network, address refers to a particular station and this station need not be stationary. Therefore, address may not always refer to a particular geographical location.

• **Dynamic topology and restricted connectivity:** The mobile nodes may often go out of reach of each other. This means that network connectivity is partial at times.

• **Medium boundaries are not well-defined:** The exact reach of wireless signals cannot be determined accurately. It depends on various factors such as signal strength and noise levels. This means that the precise boundaries of the medium cannot be determined easily.

• **Error-prone medium:** Transmissions by a node in the wireless channel are affected by simultaneous transmissions by neighboring nodes that are located within the direct transmission range of the transmitting node. This means that the error rates are significantly higher in the wireless medium. We need to build a reliable network on top of an inherently unreliable channel. This is realized in practice by having reliable protocols at the MAC layer, which hide the unreliability that is present in the physical layer.

WLAN standards

Several standards for WLAN hardware exist:

WLAN standard	Pros	Cons
802.11a	• Faster data transfer rates (up to 54Mbps) • Supports more simultaneous connections • Less susceptible to interference	• Short range (60-100 feet) • Less able to penetrate physical barriers
802.11b	• Better at penetrating physical barriers • Longest range (70-150 feet) • Hardware is usually less expensive	• Slower data transfer rates (up to 11Mbps) • Doesn't support as many simultaneous connections • More susceptible to interference
802.11g	• Faster data transfer rates (up to 54Mbps) • Better range than 802.11b (65-120 feet)	• More susceptible to interference
802.11n	The 802.11n standard was recently ratified by the Institute of Electrical and Electronics Engineers (IEEE), as compared to the previous three standards. Though specifications may change, it is expected to allow data transfer rates up to 600Mbps, and may offer larger ranges.	

Security standards

The 802.11x standards provide some basic security, but are becoming less adequate as use of wireless networking spreads. Following are security standards that extend or replace the basic standard:

WEP (Wired Equivalent Privacy)

WEP encrypts data traffic between the wireless access point and the client computer, but doesn't actually secure either end of the transmission. WEP's encryption level is relatively weak (only 40 to 128 bits). Many analysts consider WEP security to be weak and easy to crack.

WPA (Wi-Fi Protected Access)

WPA implements higher security and addresses the flaws in WEP, but is intended to be only an intermediate measure until further 802.11i security measures are developed.

HIPERLAN

The European counterparts to the IEEE 802.11 standards are the high performance radio LAN (HIPERLAN) standards defined by the European Telecommunications Standards Institute (ETSI). It is to be noted that while the IEEE 802.11 standards can use either radio access or infrared access, the HIPERLAN standards are based on radio access only. The standards have been defined as part of the ETSI broadband radio access networks (BRAN) project.

Four standards have been defined for wireless networks by the ETSI.

• **HIPERLAN/1** is a wireless radio LAN (RLAN) without a wired infrastructure, based on one-to-one and one-to-many broadcasts. It can be used as an extension to a wired infrastructure, thus making it suited to both ad hoc and infrastructure based networks. It employs the 5.15 GHz and the 17.1 GHz frequency bands and provides a maximum data rate of 23.5 Mbps.

• The **HIPERLAN/2** standard intends to provide short-range (up to 200 m)wireless access to Internet protocol (IP), asynchronous transfer mode (ATM1), and other infrastructure-based networks and, more importantly, to integrate WLANs into cellular systems. It employs the 5

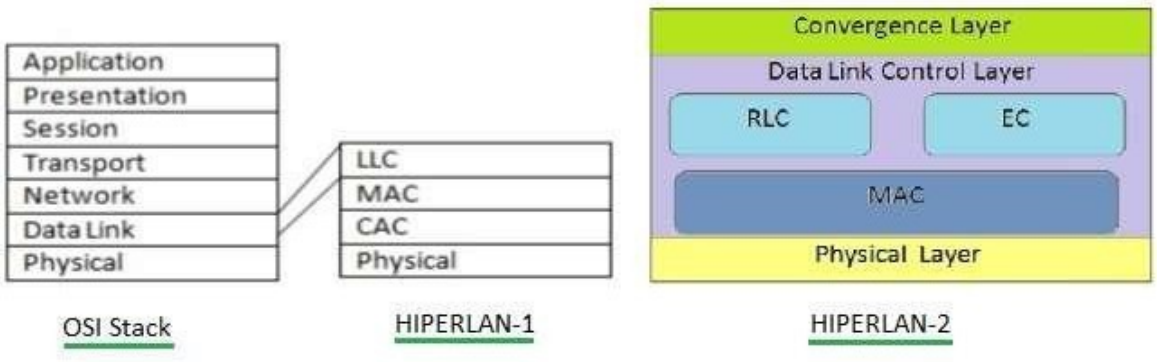
GHz frequency band and offers a wide range of data rates from 6 Mbps to 54 Mbps. HIPERLAN/2 has been designed to meet the requirements of future wireless multimedia services.

HIPERACCESS (originally called HIPERLAN/3) covers "the last mile" to the customer; it enables establishment of outdoor high-speed radio access networks, providing fixed radio connections to customer premises. HIPERACCESS provides a data rate of 25 Mbps. It can be used to connect HIPERLAN/2 deployments that are located far apart (up to 5 Km away). It offers point-to multipoint communication.

The **HIPERLINK** (originally called HIPERLAN/4) standard provides high speed radio links for point-to-point static interconnections. This is used to connect different HIPERLAN access points or HIPERACCESS networks with high-speed links over short distances of up to 150 m.

HIPERLAN/1 protocol stack

The HIPERLAN/1 protocol stack is restricted to the two lower-most layers in the OSI reference model: the data link layer (DLL) and the physical layer. TheDLL is further divided into the medium access control (MAC) sublayer and the channel access control (CAC) sub layer. The sections that follow describe the standard.



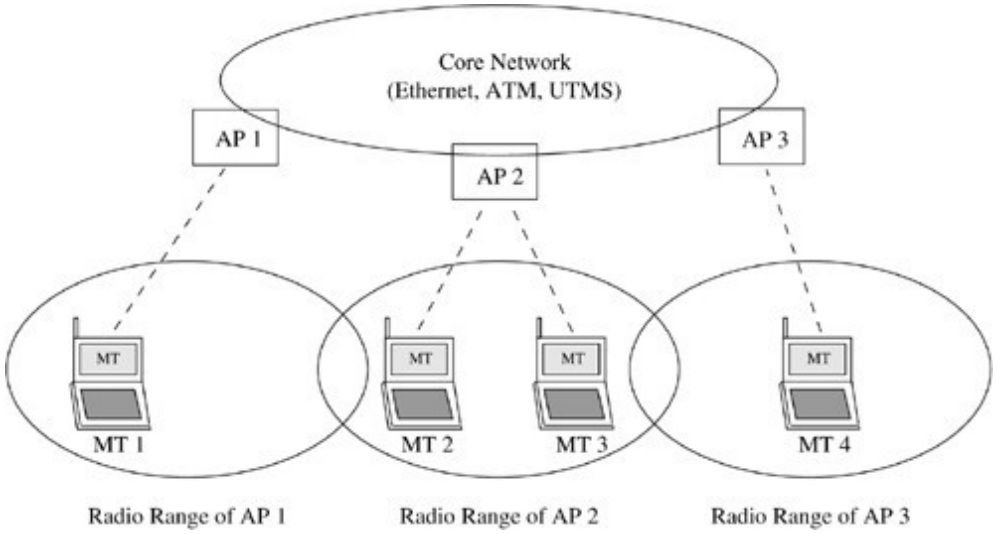
Protocol stack of HIPERLAN1 &HIPERLAN 2

The tasks of the physical layer are modulation and demodulation of a radio carrier with a bit stream, forward error-correction mechanisms, signal strength measurement. The HIPERLAN/ 1 MAC (HM) sublayer is responsible for processing the packets from the higher

layers and scheduling the packets according to the QoS requests from the higher layers specified by the HMQoS parameters.The CAC sublayer offers a connectionless data service to the MAC sublayer.

HIPERLAN/2

The HIPERLAN/2 network has a typical topology as shown in Figure . The igure shows MTs being centrally controlled by the APs which are in turn connected to the core network (infrastructure-based network).



There are two modes of communication in a HIPERLAN/2 network, which are described by the following two environments:

• **Business environment:** The ad hoc architecture of HIPERLAN/1 has been extended to support a centralized mode of communication using APs. This topology corresponds to business environments. Accordingly, each AP serves a number of MTs.

• **Home environment:** The home environment enables a direct mode of communication between the MTs. This corresponds to an ad hoc architecture that can be operated in a plug-and-play manner. The direct mode of communication is, however, managed by a central control entity elected from among the nodes called the central controller (CC).

The HIPERLAN/2 protocol stack consists of the physical layer, convergence layer (CL), and the data link control (DLC) layer. The physical layer is responsible for the conversion of the PDU train from the DLC layer to physical bursts that are suitable for radio transmission.

The functions of the CL layer are to adapt the requirements of the different higher layers of the core network with the services provided by the lower layers of HIPERLAN/2.
The DLC layer constitutes the logical link between the AP and the MTs.

BLUETOOTH

WLAN technology enables device connectivity to infrastructure-based services through a wireless carrier provider. However, the need for personal devices to communicate wirelessly with one another, without an established infrastructure, has led to the emergence of personal area networks (PANs).

In May 1998, several companies such as Intel, IBM, Nokia, and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop a *de facto* standard for PANs. Recently, IEEE has approved a Bluetooth-based standard (IEEE 802.15.1) for wireless personal area networks (WPANs).

Bluetooth Specifications

The Bluetooth specification consists of two parts: core and profiles. The core provides a common data link and physical layer to application protocols, and maximizes reusability of existing higher layer protocols. The profiles specifications classify Bluetooth applications into thirteen types.

The **protocol stack** of Bluetooth performs the functions of locating devices, connecting other devices, and exchanging data. It is logically partitioned into three layers, namely, the **transport protocol group, the middleware protocol group, and the application group.**

Figure 2.7. Bluetooth protocol stack.

Transport Protocol Group

This group is composed of the protocols designed to allow Bluetooth devices to locate each other and to create, configure, and manage the wireless links.

Radio (Physical) Layer

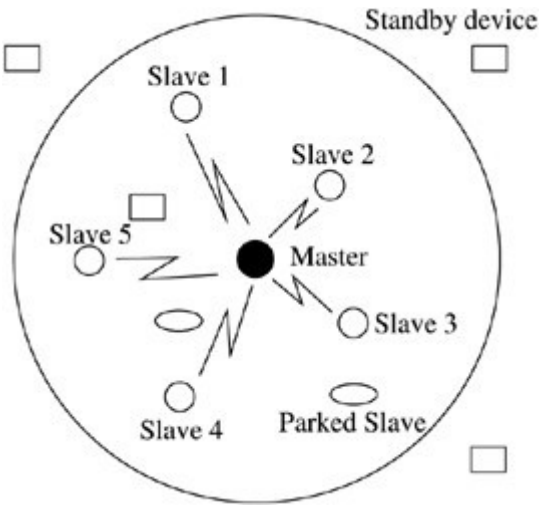
The radio part of the specification deals with the characteristics of the transceivers and design specifications such as frequency accuracy, channel interference, and modulation characteristics.

Baseband Layer

The key functions of this layer are frequency hop selection, connection creation, and medium access control. Bluetooth communication takes place by ad hoc creation of a network called a *piconet.*

Piconet

The initiator for the formation of the network assumes the role of the *master* (of the piconet). All the other members are termed as *slaves* of the piconet. A piconet can have up to seven active slaves at any instant. For the purpose of identification, each active slave of the piconet is assigned a locally unique active member address AM_ADDR.



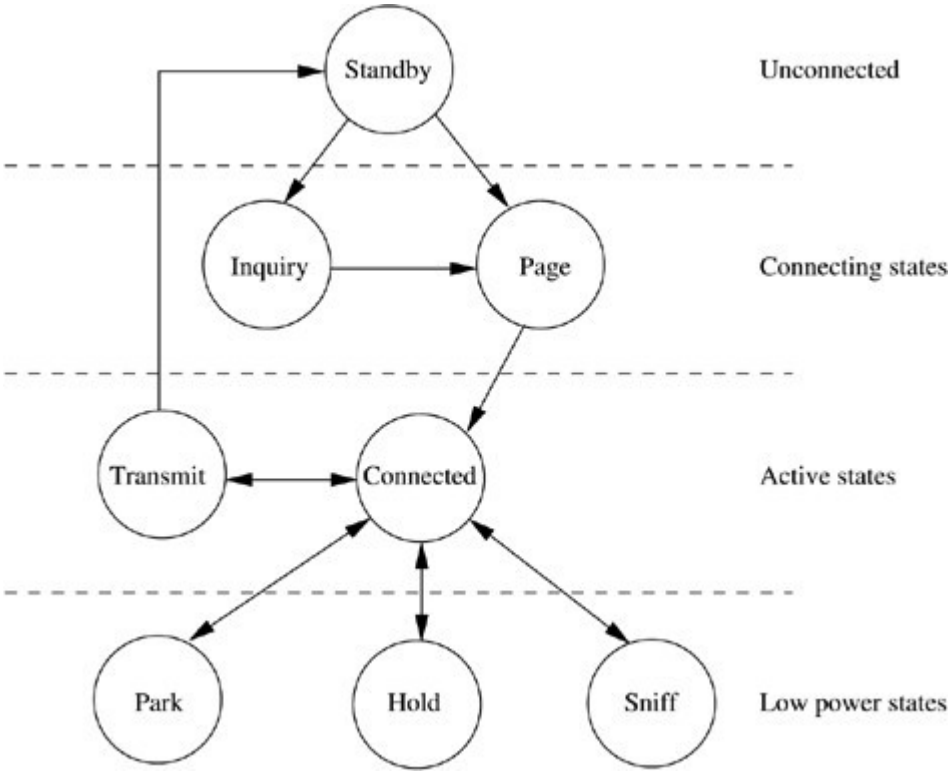
Operational states

Inquiry State

As shown in above Figure, a device which is initially in the standby state enters the inquiry state. As its name suggests, the sole purpose of this state is to collect information about other Bluetooth devices in its vicinity.

Page State

A device enters this state to invite other devices to join its piconet.



Active mode: In this mode, the Bluetooth unit actively participates in the piconet.

Sniff mode: This is a low-power mode in which the listening activity of the slave is reduced.

Hold mode: In this mode, the slave temporarily does not support ACL packets on the channel

Park mode: This is a very low-power mode. The slave gives up its active member address and is given an eight-bit parked member address.

HOMERF

- HomeRF is the technique that aimed at offering voice, data and video image at home or small scale office with a low cost by radio frequency instead of wiring.
- The HomeRF standard was developed by HomeRF Working Group that is composed of major companies such as Compaq, Intel, Motorola, National Semiconductor, Proxim and Siemens.
- The HomeRF standard diverged from the original 802.11 FHSS standard and incorporated the Digital Enhanced Cordless Telephone (DECT) technology used for cordless telephones in Europe.
- HomeRF follows shared wireless access protocol (SWAP).
- SWAP is used to set up a network that provides access to a public network telephone, the Internet (data), entertainment networks (cable television, digital audio, and video), transfer and sharing of data resources (disks, printer), home control, and automation.

Standard

- Data rate
  - 0.8, 1.6, 5, 10 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
- Frequency
  - 2.4 GHz ISM
- Security
  - Strong encryption, no open access
- Availability
  - Several products from different vendors
- Connection set-up time

- 10 ms bounded latency

- Quality of Service
  - Up to 8 streams A/V, up to 8 voice streams, priorities, best-effort
- Manageability
  - Like DECT & 802-LANs
- Special Advantages/Disadvantages
  - Advantage: extended QoS support, host/client and peer/peer, power saving, security
  - Disadvantage: future uncertain due to DECT-only devices plus 802.11a/b for data.

IEEE 802.11 STANDARDS

802.11 Physical Layers

- ***The basic 802.11 standard supports three different physical layers.***
- for sensing the wireless channel and determining whether or not it is idle.
- **Infrared** – 1 Mbps and 2 Mbps
  - Infra-red light, typical 10 m range, encoded using PPM
- **FHSS** (Frequency Hopping Spread Spectrum) uses 79 channels, each 1 MHz wide.
- **DSSS** (Direct Sequence Spread Spectrum) delivers 1 or 2 Mbps in the 2.4 GHz band.

WLAN: IEEE 802.11a

- **Dat a rate**
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on Router.
- **Transmission range**
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 **m**
- **Frequency**
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-ba**nd**
- **Security**
  - WEP, SSID
- Cost: Check market
  - adapter (a/b/g combo) $70, base station $160

- **Connection set-up time**
  - Connectionless/always on
- **Quality of Service**
  - Average,Typ. best effort, no guarantees (same as all 802.11 products)
- **Special Advantages/Disadvantages**
  - Advantage: fits into any 802.x standards.
  - Disadvantage: stronger shading due to higher frequency

WLAN: IEEE 802.11b

- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on Router
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10mbps indoor
- Frequency
  - Free 2.4 GHz ISM-band
- Security
  - WEP insecure, SSID
- Cost: Check market
  - Adapter $30, base station $40
- Availability
  - Many products, many vendors

- Connection set-up time
  - Connectionless/always on
- Special Advantages/Disadvantages
  - Advantage: many installed systems, available worldwide, integrated in laptops, simple system.
  - Disadvantage:
  - a. Transmission speed is slow
  - b. Uses the 2.4 gigahertz (GHz) of frequency the same as some house hold items like cordless, micro waves ovens etc.
  - c. Provides access to few users simultaneously.

WLAN: IEEE 802.11g

- Data rate
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s

  Transmission range
  - 300m outdoor, 30m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m
- Frequency
  - Free 2.4 – 2.497 GHz ISM-band
- Security
  - WEP , SSID
- Cost: Check market
  - Adapter $50, base station $50
- Availability
  - more products, more vendors
- Connection set-up time
  - Connectionless/always on
- Special Advantages/Disadvantages
  - Allows for more simultaneous users
  - Has the best signal range
  - Is compatible with 802.11b network adapters, routers, and access points.

  Disadvantage:

  Costs more than 802.11b

  Uses the 2.4 GHz frequency so it has the same interference problems as 802.11b

WIRELESS INTERNET

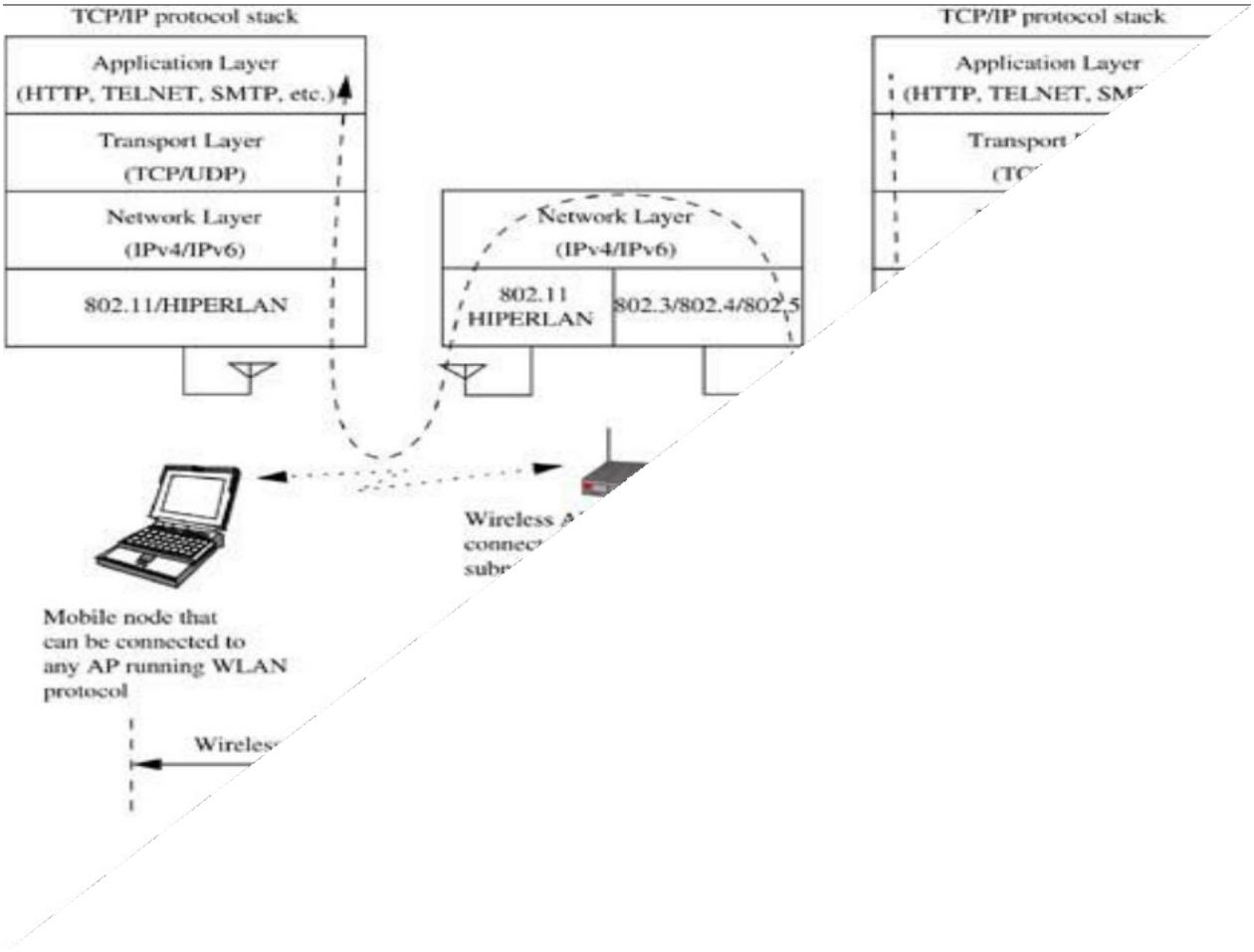
Wireless Internet refers to the extension of the services offered by the Internet to mobile users, enabling them to access information and data irrespective of their location.

The major issues that are to be considered for wireless Internet are the following.

• Address mobility

• Inefficiency of transport layer protocols

• Inefficiency of application layer protocols



An illustration of wireless Internet.

Address Mobility

The network layer protocol used in the Internet is Internet protocol (IP) which was designed for wired networks with fixed nodes. IP employs a hierarchical addressing with a globally unique 32-bit address1 which has two parts, network identifier and host identifier, as shown in Figure 4.2 (a).

The mobile hosts may move from one subnet to another, but the packets addressed to the mobile host may be delivered to the old subnet to which the node was originally attached, as illustrated in Figures 4.2 (b) and 4.2 (c).

Figure 4.2 shows the mobility of a node (with IP address 10.6.6.1) attached to subnet A (subnet address 10.6.6.x) moving over to another subnet B with address 10.6.15.x. In this case, the packets addressed to the node will be routed to the subnet A instead of the subnet B, as the network part in the mobile node's address is 10.6.6.x (seeFigure 4.2 (c)).

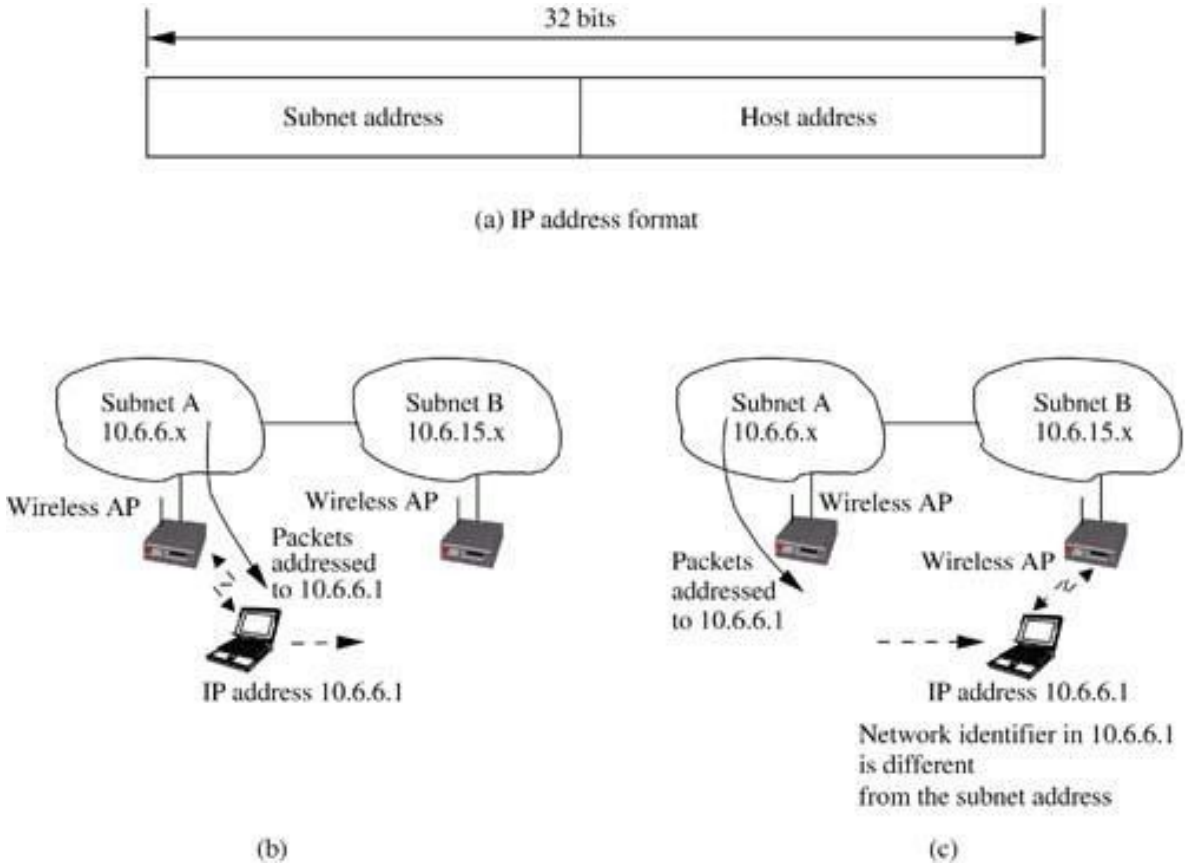


Figure 4.2. The address mobility problem.

Inefficiency of Transport Layer Protocols

Wireless Internet requires efficient operation of the transport layer protocols as the wireless medium is inherently unreliable due to its time-varying and environment-dependent characteristics. Traditional TCP invokes a congestion control algorithm in order to handle congestion in the networks. If a data packet or an ACK packet is lost, then TCP assumes that the loss is due to congestion and reduces the size of the congestion window by half. With every successive packet loss the congestion window is reduced, and hence TCP provides a degraded performance in wireless links. Even in situations where the packet loss is caused by link error or collision, the TCP invokes the congestion control algorithm leading to very low throughput. The identification of the real cause that led to the packet loss is important in improving the performance of the TCP over wireless links. Some of the

solutions for the transport layer issues include indirect-TCP (ITCP), snoop TCP, and mobile TCP.

Inefficiency of Application Layer Protocols

Traditional application layer protocols used in the Internet such as HTTP, TELNET, simple mail transfer protocol (SMTP), and several markup languages such as HTML were designed and optimized for wired networks.

Many of these protocols are not very efficient when used with wireless links. The major issues that prevent HTTP from being used in wireless Internet are its stateless operation, high overhead due to character encoding, redundant information carried in the HTTP requests, and opening of a new TCP connection with every transaction. Wireless bandwidth is limited and much more expensive compared to wired networks. Also, the capabilities of the handheld devices are limited, making it difficult to handle computationally and bandwidth-wise expensive application protocols. Wireless application protocol (WAP) and optimizations over traditional HTTP are some of the solutions for the application layer issues.

OPTIMIZING WEB OVER WIRELESS

The limitations of wireless networks that provide the motivation for such optimizations are low bandwidth, low reliability, high latency, and high cost per byte transferred. Integrating Web access over wireless devices would have to take into account the drawbacks of the wireless medium and the capabilities of the devices.

Four main categories of optimizations that can improve the performance of Web access systems over wireless channels can be identified.

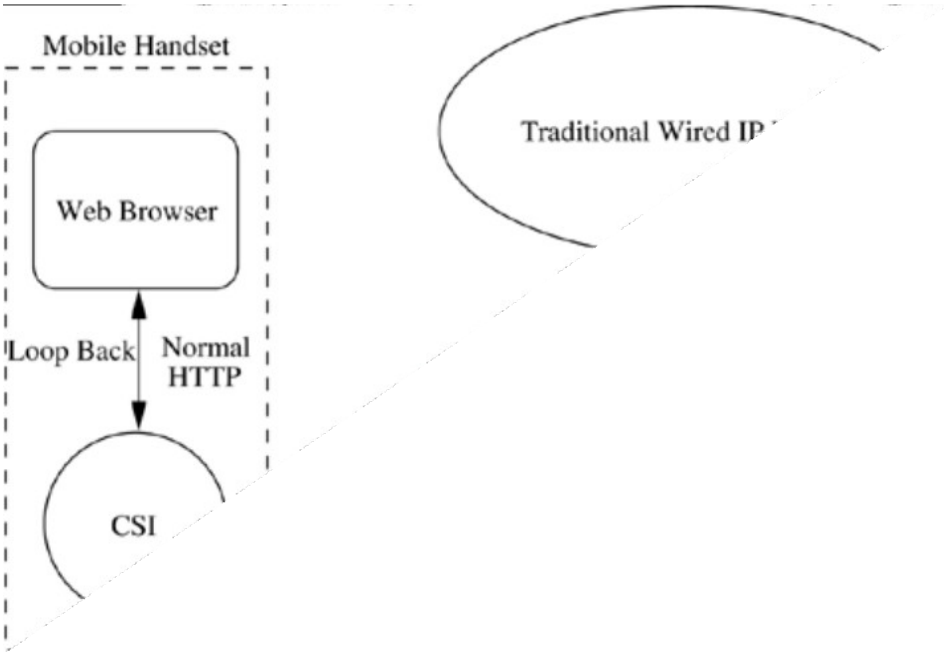
These are:

• **Caching:** Cache objects are either purged at the end of the session or may persist across sessions. But it is advantageous to have cached data persist across browser sessions, as this increases cache hit ratios. Appropriate cache coherency methods are added to detect and change old information.

• **Differencing:** For transaction processing caching techniques do not help as different replies to the same application server are often different. Still, the fact that these replies tend to be similar can be exploited to reduce the network traffic over the wireless interface. A base object carries fundamental features that do not change across transactions and is created and maintained by both the client and server interfaces. Whenever a new transaction takes place, the server computes the difference stream and only the difference stream is transmitted.

• **Protocol reduction:** This approach aims at reducing the overhead of repeated setup and tear-down of TCP/IP connections for each Web-object to be transmitted. This can be eliminated by establishing a single TCP/IP connection between the CSI and the SSI that will persist for the entire session. The connection setup/tear-down overhead is on the local and wired connections only.

Header reduction: HTTP requests are prefixed with headers that indicate to the origin server the rendering capabilities of the browser and also the various content formats handled by it. The alternative to this is that the CSI sends this information in the first request and SSI records this information.


Mobile Handset
Traditional Wired IP
Web Browser
Loop Back
Normal
HTTP
CSI

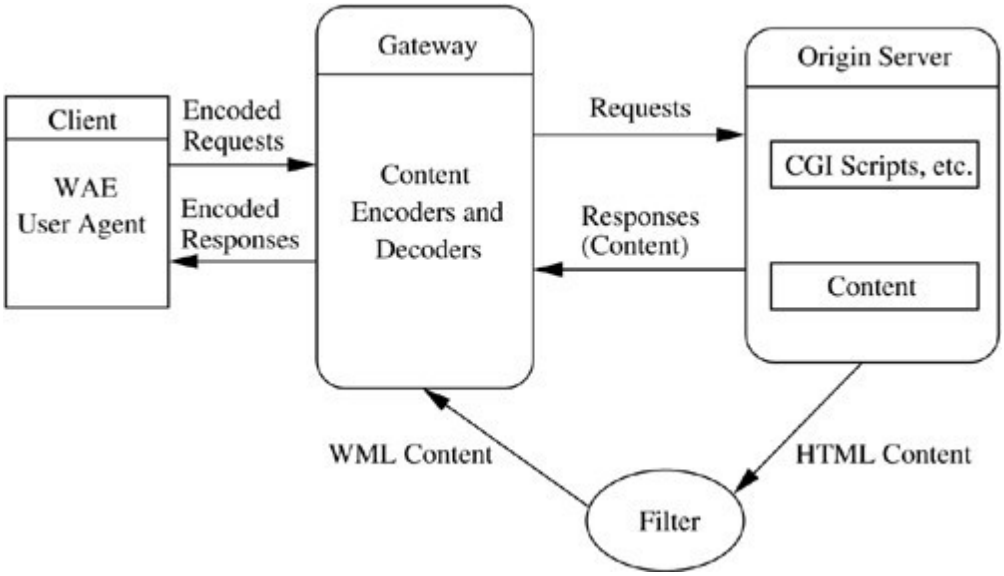
WIRELESS APPLICATION PROTOCOL (WAP)

WAP stands for wireless application protocol. This name is a misnomer, because WAP represents a suite of protocols rather than a single protocol. WAP has today become the *de facto* standard for providing data and voice services to wireless handheld devices.

The WAP Model

WAP adopts a client-server approach. It specifies a proxy server that acts as an interface between the wireless domain and core wired network. This proxy server, also known as a WAP gateway, is responsible for a wide variety of functions such as protocol translation and optimizing data transfer over the wireless medium.

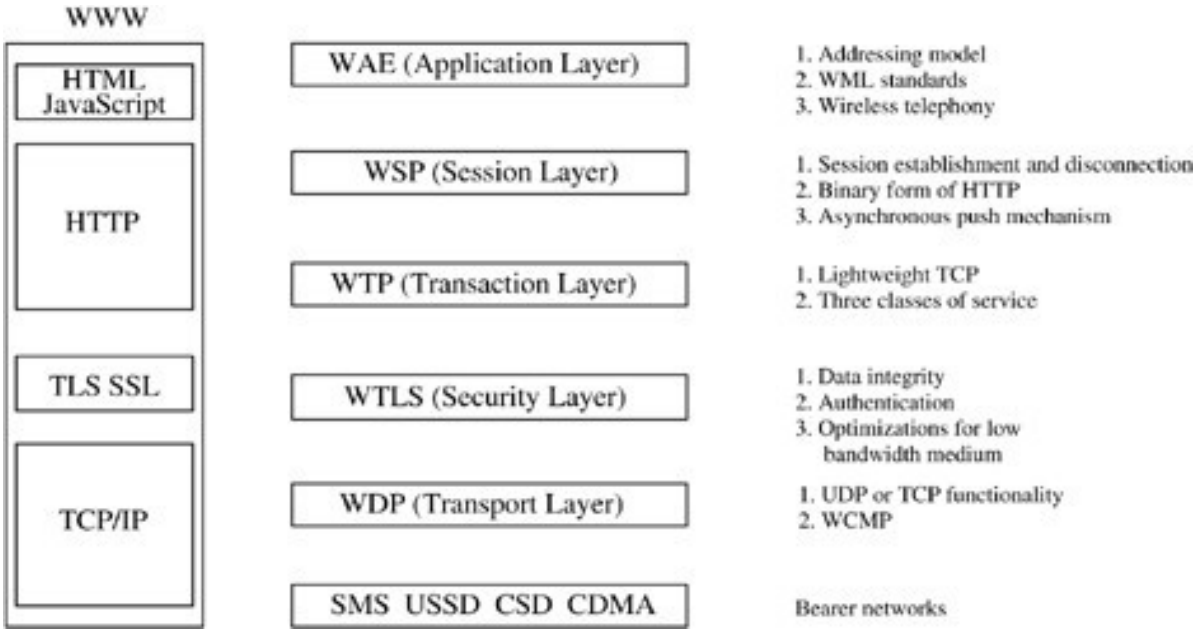
Below Figure illustrates the client-server model that WAP employs. The WAP-enabled handset communicates with a Web content server or an origin via a WAP gateway. It is at the WAP gateway that the convergence of the wireless and wired domains actually occurs. The gateway receives WAP requests from the handset, and these have to be converted into suitable HTTP requests to be sent to the origin server. If the origin server cannot provide the required information in wireless markup language (WML) form, then there must be an additional filter between the server and the gateway to convert the HTML content into WAP compatible WML content. The gateway may additionally perform functions such as caching and user agent profiling as part of some optimization measures. This is also known as *capability and preference information.* By means of user agent profiling, the MN specifies its characteristics such as hardware characteristics, software capabilities, and user preferences, to the server so that the content can be formatted appropriately to be displayed correctly.



The WAP client-server model.

The WAP Protocol Stack

The WAP protocol stack is designed in a layered fashion that allows the architecture to provide an environment that is both extensible and scalable for application development. The WAP architecture allows other services to access the WAP stack at well-defined interfaces.


WWW
HTML
JavaScript
HTTP
TLS SSL
TCP/IP
WAE (Application Layer)
1. Addressing model
2. WML standards
3. Wireless telephony
WSP (Session Layer)
1. Session establishment and disconnection
2. Binary form of HTTP
3. Asynchronous push mechanism
WTP (Transaction Layer)
1. Lightweight TCP
2. Three classes of service
WTLS (Security Layer)
1. Data integrity
2. Authentication
3. Optimizations for low bandwidth medium
WDP (Transport Layer)
1. UDP or TCP functionality
2. WCMP
SMS USSD CSD CDMA
Bearer networks

UNIT-2

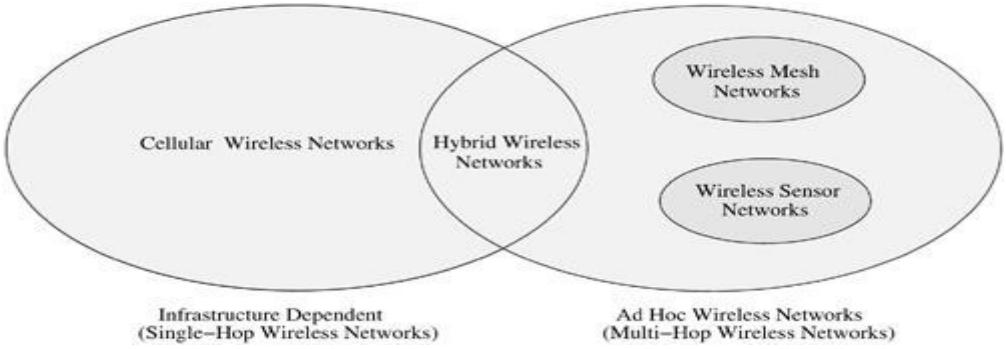
AD HOC WIRELESS NETWORKS

Introduction:

Cellular and Ad Hoc Wireless Networks

Figure: 1 shows a representation of different wireless networks. The current cellular wireless networks (depicted in Figure: 2) are classified as the infrastructure dependent networks. The path setup for a call between two nodes, say, node *C* to node *E,* is completed through the base station as illustrated in Figure 2.

Figure 1. Cellular and ad hoc wireless networks.



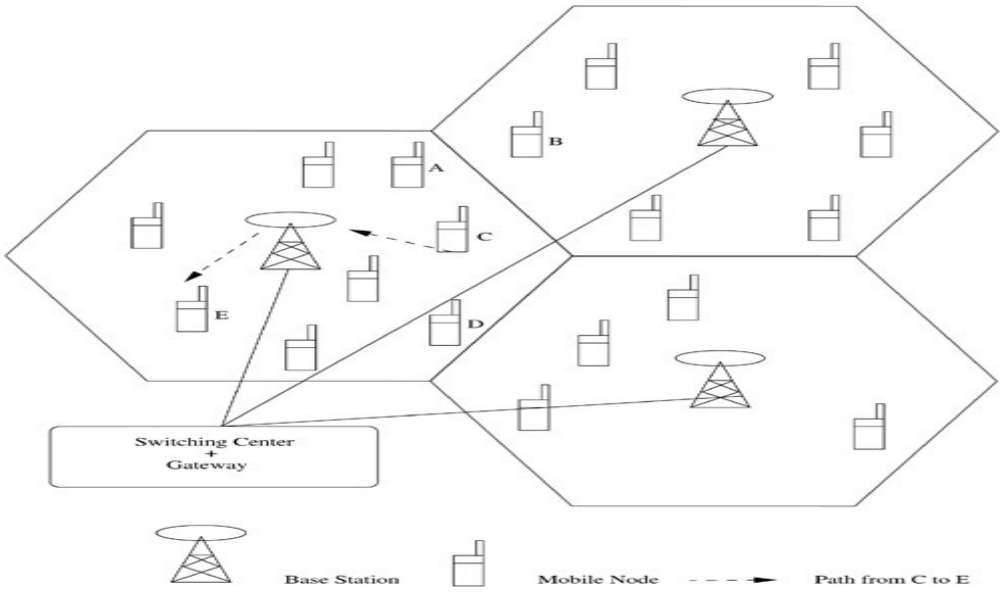


Figure 2. A cellular network

Ad hoc wireless network topology for the cellular network shown in Figure 2 is illustrated in Figure 3. Note that in Figure 3, the cell boundaries are shown purely for comparison with the cellular network in Figure 2 and do not carry any special significance. The path setup for a call between two nodes, say, node *C* to node *E,* is completed through the intermediate mobile node *F*, as illustrated in Figure 3. Wireless mesh networks and wireless sensor networks are specific examples of adhoc wireless networks.

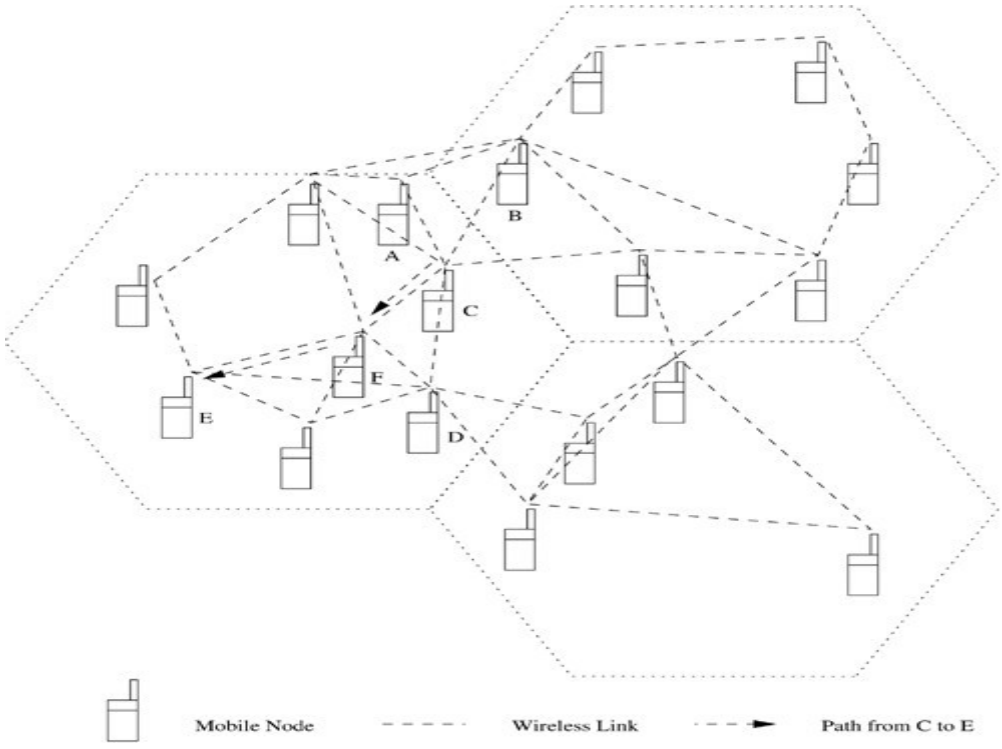


Figure 3. An ad hoc wireless network

Differences between cellular networks and ad hoc 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 Applications

Ad hoc wireless networks can be very useful in establishing communication among a group of soldiers for tactical operations. Setting up a fixed infrastructure for communication among a group of soldiers in enemy territories or in inhospitable terrains may not be possible. In such environments, ad hoc wireless networks provide the required communication mechanism quickly.

Collaborative and Distributed Computing

Another domain in which the ad hoc wireless networks find applications is collaborative computing. The requirement of a temporary communication infrastructure for quick communication with minimal configuration among a group of people in a conference or gathering necessitates the formation of an ad hoc wireless network.

Emergency Operations

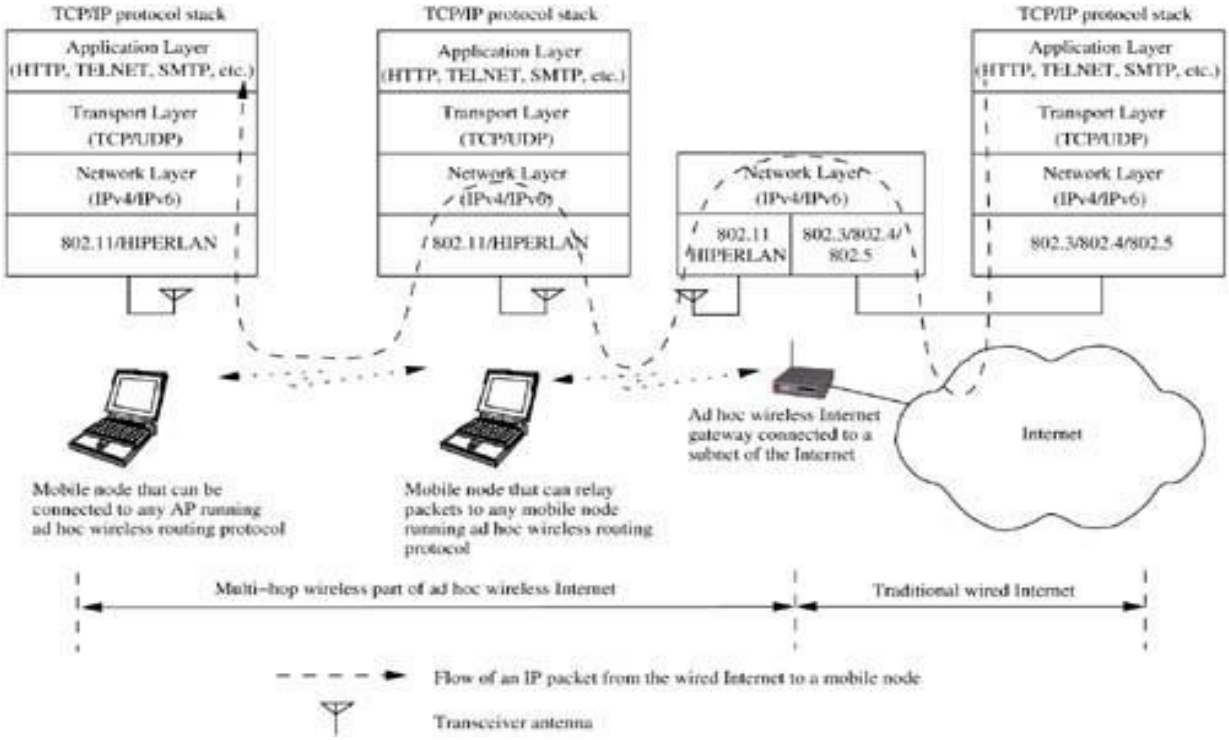
Ad hoc wireless networks are very useful in emergency operations such as search and rescue, crowd control, and commando operations. The major factors that favour ad hoc wireless networks for such tasks are self-configuration of the system with minimal overhead, independent of fixed or centralized infrastructure, the nature of the terrain of such applications, the freedom and flexibility of mobility, and the unavailability of conventional communication infrastructure.

ISSUES IN AD HOC WIRELESS NETWORKS

The major issues that affect the design, deployment, and performance of an ad hoc wireless system are as follows:

- Medium access scheme
- Routing
- Multicasting
- Transport layer protocol
- Pricing scheme
- Quality of service provisioning
- Self-organization
- Security
- Energy management
- Addressing and service discovery
- Scalability
- Deployment considerations

AD HOC WIRELESS INTERNET



A schematic diagram of the ad hoc wireless Internet.

The major issues to be considered for a successful ad hoc wireless Internet are the following:

Gateways: Gateway nodes in the ad hoc wireless Internet are the entry points to the wired internet.

Address mobility: The ad hoc wireless Internet also faces the challenge of address mobility. This problem is worse here as the nodes operate over multiple wireless hops. Solutions such as Mobile IP can provide temporary alternatives for this.

Routing: Routing is a major problem in the ad hoc wireless Internet, due to the dynamic topological changes, the presence of gateways, multi-hop relaying, and the hybrid character of the network. The possible solution for this is the use of a separate routing protocol.

Transport layer protocol: Even though several solutions for transport layer protocols exist for ad hoc wireless networks, unlike other layers, the choice lies in favor of TCP's extensions Proposed for ad hoc wireless networks.

Load balancing: It is likely that the ad hoc wireless Internet gateways experience heavy traffic. Hence the gateways can be saturated much earlier than other nodes in the network. Load balancing techniques 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. Gateway is the preferred choice for charging the traffic to and from the Internet.

QoS support: With the widespread use of voice over IP (VoIP) and growing multimedia applications over the Internet, provisioning of QoS support in the ad hoc wireless Internet becomes a very important issue.

ISSUES IN DESIGNING A MAC PROTOCOL FOR AD HOC WIRELESS NETWORKS

The following are the main issues that need to be addressed while designing a MAC protocol for ad hoc wireless networks.

Bandwidth Efficiency

As mentioned earlier, since the radio spectrum is limited, the bandwidth available for communication is also very limited. The MAC protocol must be designed in such a way that the scarce bandwidth is utilized in an efficient manner.

Quality of Service Support

QoS support is essential for supporting time-critical traffic sessions such as in military communications. The MACprotocol for ad hoc wireless networks that are to be used in such real-time applications must have some kind of a resource reservation mechanism that takes into consideration the nature of the wireless channel and the mobility of nodes.

Synchronization

The MAC protocol must take into consideration the synchronization between nodes in the network. Synchronization is very important for bandwidth (time slot) reservations by nodes.

Hidden and Exposed Terminal Problems

The hidden and exposed terminal problems are unique to wireless networks. 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.

Error-Prone Shared Broadcast Channel Mobility of Nodes

This is a very important factor affecting the performance (throughput) of the protocol. Nodes in an ad hoc wireless network are mobile most of the time. The bandwidth reservations made or the control information exchanged may end up being of no use if the node mobility is very high.

DESIGN GOALS OF A MAC PROTOCOL FOR AD HOC WIRELESS NETWORKS

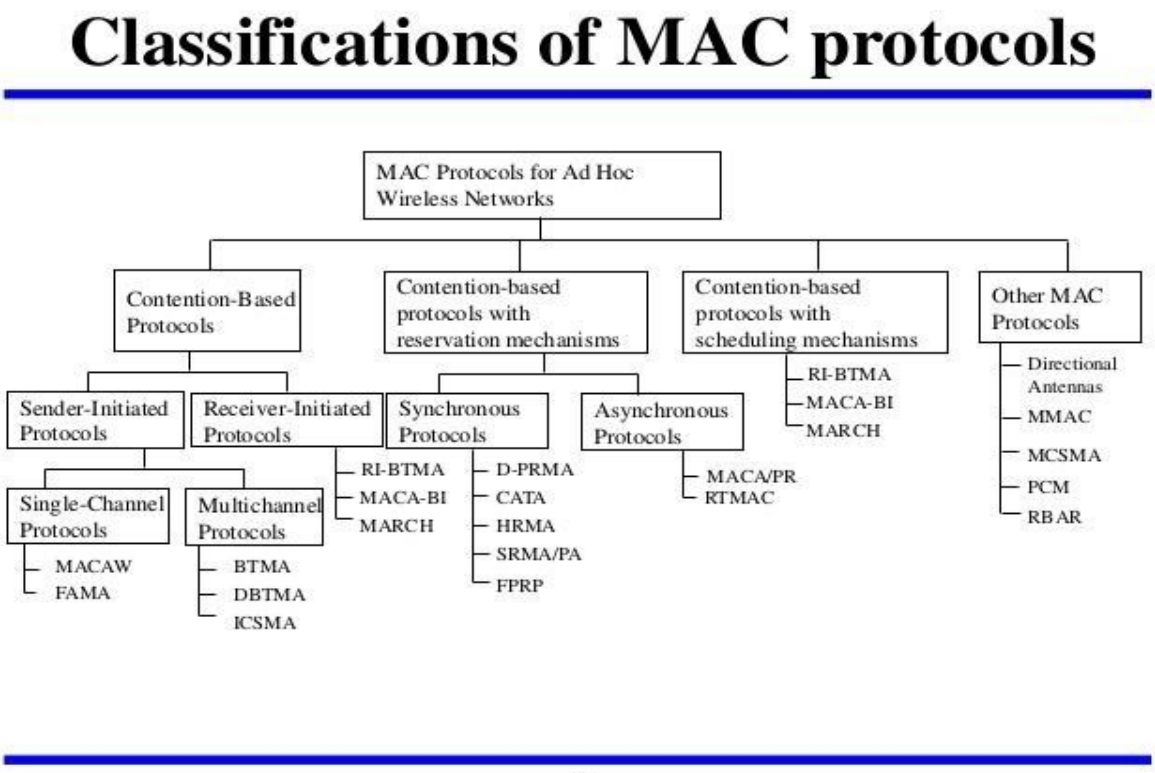
The following are the important goals to be met while designing a medium access control (MAC) protocol for ad hoc wireless networks:

- The operation of the 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 utilized efficiently.
- The protocol should ensure fair allocation (either equal allocation or weighted allocation) of bandwidth to nodes.
- Control overhead must be kept as low as possible.
- The protocol should minimize the effects of hidden and exposed terminal problems.
- The protocol must be scalable to large networks.

CLASSIFICATIONS OF MAC PROTOCOLS

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

- **Contention-based protocols**
- **Contention-based protocols with reservation mechanisms**
- **Contention-based protocols with scheduling mechanisms**



Contention-Based Protocols

- These protocols follow a contention-based channel access policy.
- A node does not make any resource reservation *a priori. Whenever it receives a packet to be transmitted, it contends with its* neighbour nodes for access to the shared channel.
- Sender-initiated protocols: Packet transmissions are initiated by the sender node.

- Receiver-initiated protocols: The receiver node initiates the contention resolution protocol.
- Single-channel sender-initiated protocols: In these protocols, the total available bandwidth is used as it is, without being divided.
- Multichannel sender-initiated protocols: In multichannel protocols, the available bandwidth is divided into multiple channels.

Contention-Based Protocols with Reservation Mechanism

- Ad hoc wireless networks sometimes may need to support real-time traffic, which requires QoS guarantees to be provided.
- In contention-based protocols, nodes are not guaranteed periodic access to the channel. Hence they cannot support real-time traffic. In order to support such traffic, certain protocols have mechanisms for **reserving bandwidth *a priori.***
- Synchronous protocols: Synchronous protocols require **time synchronization** among all nodes in the network, so that reservations made by a node are known to other nodes in its neighbourhood.
- Asynchronous protocols: They do not require any global synchronization among nodes in the network. These protocols usually use relative time information for effecting reservations.

Contention-Based Protocols with Scheduling Mechanisms

- These protocols focus on packet scheduling at nodes, and also scheduling nodes for access to the channel. 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 take into consideration battery characteristics, such as remaining battery power, while scheduling nodes for access to the channel.

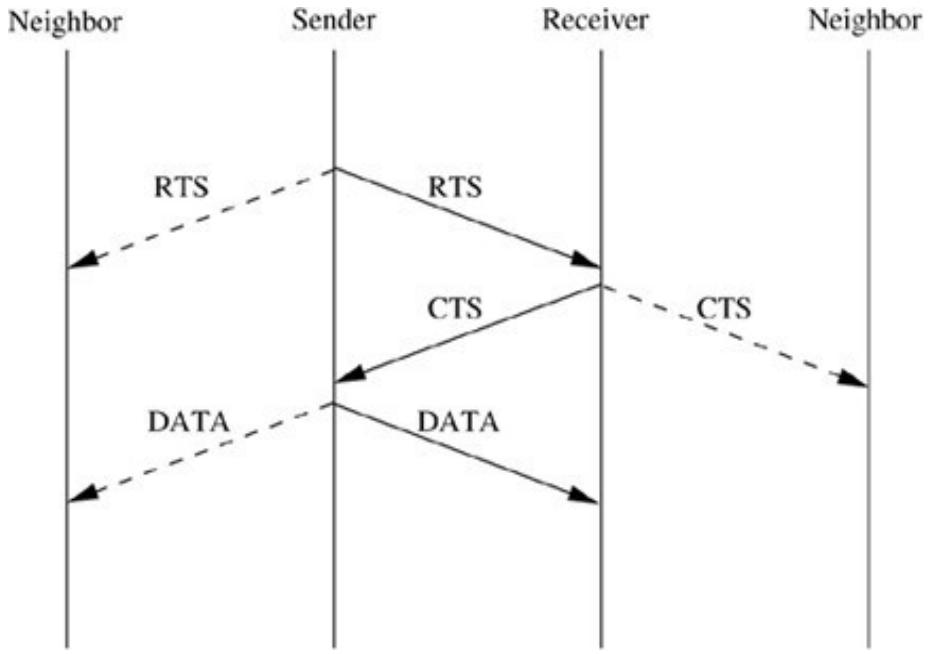
Contention-Based Protocols

This protocol is based on the multiple access collision avoidance protocol (MACA). MACA was proposed due to the shortcomings of CSMA protocols when used for wireless networks.

MACAW: Multiple Access Collision Avoidance for Wireless.

MACA:

- Multiple access collision avoidance protocol (MACA).
- It is an alternative to the traditional carrier sense multiple access (CSMA) protocols.
- In CSMA protocols, the sender first senses the channel for the carrier signal. If the carrier is present, it retries after a random period of time. Otherwise, it transmits the packet.
- MACA does not make use of carrier-sensing for channel access.
- It uses two additional signalling packets: the request-to-send (RTS) packet and the clear-to-send (CTS) packet.
- When a node wants to transmit a data packet, it first transmits an RTS packet. The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a CTS packet.
- Once the sender receives the CTS packet without any error, it starts transmitting the data packet.



- If a packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back off lost packets.
- In the BEB mechanism, each time a collision is detected, the node doubles its maximum back-off window.

Floor Acquisition Multiple Access Protocols

The floor acquisition multiple access (FAMA) protocols are 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 given point of time, the control of the channel is assigned to only one node, and this node is guaranteed to transmit one or more data packets to different destinations without suffering from packet collisions.

Two FAMA protocol variants:
RTS-CTS exchange with no carrier sensing, and
RTS-CTS exchange with non-persistent carrier-sensing.

Multiple access collision avoidance (MACA) , which was discussed earlier in this chapter, belongs to the category of FAMA protocols. In MACA, a ready node transmits an RTS packet. A neighbour node receiving the RTS defers its transmissions for the period specified in the RTS. On receiving the RTS, the receiver node responds by sending back a CTS packet, and waits for a long enough period of time in order to receive a data packet.

FAMA – Non-Persistent Transmit Request

This variant of FAMA, called FAMA – non-persistent transmit request (FAMA-NTR), combines non-persistent carrier-sensing along with the RTS-CTS control packet exchange mechanism. Before sending a packet, the sender node senses the channel. If the channel is found to be busy, then the node backs off for a random time period and retries later. If the channel is found to be free, it transmits the RTS packet. After transmitting the RTS, the sender listens to the channel for one round-trip time in addition to the time required by the receiver node to transmit a CTS. If it does not receive the CTS within this time period or if theCTS received is found to be corrupted, then the node takes a random back-off and retries later.

Busy Tone Multiple Access Protocols

Busy Tone Multiple Access

The busy tone multiple access (BTMA) protocol is one of the earliest protocols proposed for overcoming the hidden terminal problem faced in wireless environments. The transmission channel is split into two: a data channel and a control channel. The data channel is used for data packet transmissions, while the control channel is used to transmit the busy tone signal. When a node is ready for transmission, it senses the channel to check whether the busy tone is active. If not, it turns on the busy tone signal and starts data transmission; otherwise, it reschedules the packet for transmission after some random rescheduling delay. Any other node which senses the carrier on the incoming data channel also transmits the busy tone signal on the control channel. Thus, when a node is transmitting, no other node in the two-hop neighbourhood of the transmitting node is permitted to simultaneously transmit.

Dual Busy Tone Multiple Access Protocol

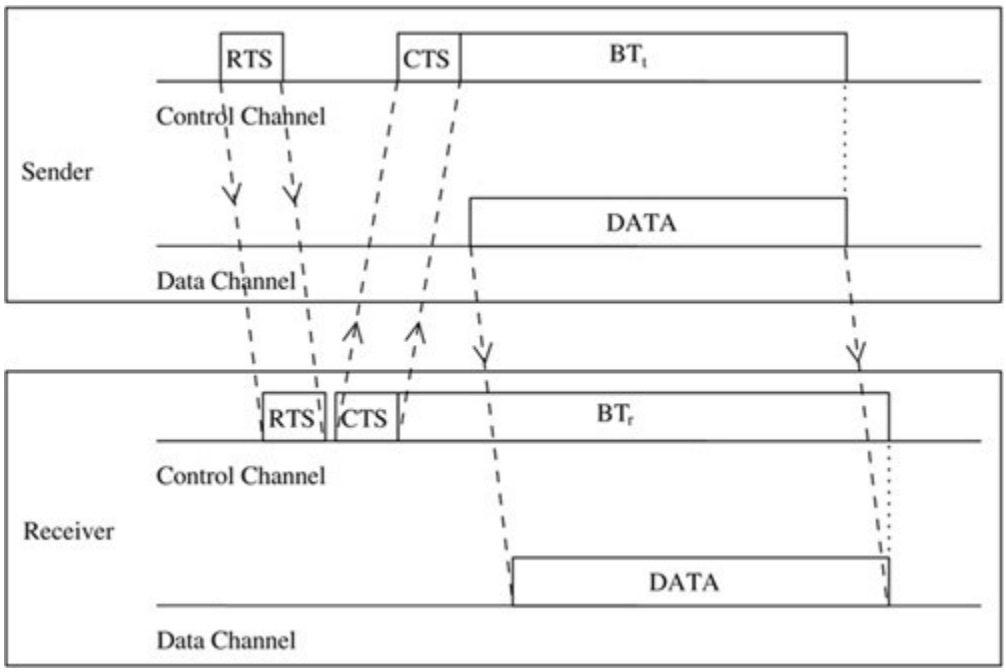
The dual busy tone multiple access protocol (DBTMA) is an extension of the BTMA scheme.Here again, the transmission channel is divided into two: the data channel and the control channel.

As in BTMA, the data channel is used for data packet transmissions. The control channel is used for control packet transmissions (RTS and CTS packets) and also for transmitting the busy tones. DBTMA uses two busy tones on the control channel, BT_t and BT_r. The BT_t tone is used by the node to indicate that it is transmitting on the data channel. The BT_r tone is turned on by a node when it is receiving data on the data channel. The two busy tone signals are two sine waves at different well-separated frequencies.

When a node is ready to transmit a data packet, it first senses the channel to determine whether the BT_r signal is active. An active BT_r signal indicates that a node in the neighbourhood of the ready node is currently receiving packets. If the ready node finds that there is no BT_r signal, it transmits the RTS packet on the control channel. On receiving the RTS packets, the node to which the RTS was destined checks whether the BT_t tone is active in its neighbourhood.

An active BT_t implies that some other node in its neighbourhood is transmitting packets and so it cannot receive packets for the moment. If the node finds no BT_t signal, it responds by

sending a CTS packet and then turns on the BT_r signal. The sender node, on receiving this CTS packet, turns on the BT_t signal and starts transmitting data packets .After completing transmission, the sender node turns off the BT_t signal. The receiver node, after receiving all data packets, turns off the BT_r signal.



Media Access with Reduced Handshake

The media access with reduced handshake protocol (MARCH) [8] is a receiver-initiated protocol. MARCH, unlike MACA-BI [7], does not require any traffic prediction mechanism. The protocol exploits the broadcast nature of traffic from omnidirectional antennas to reduce the number of handshakes involved in data transmission.

In MACA, the RTS-CTS control packets exchange takes place before the transmission of every data packet. But in MARCH, the RTS packet is used only for the first packet of the stream. From the second packet onward, only the CTS packet is used.

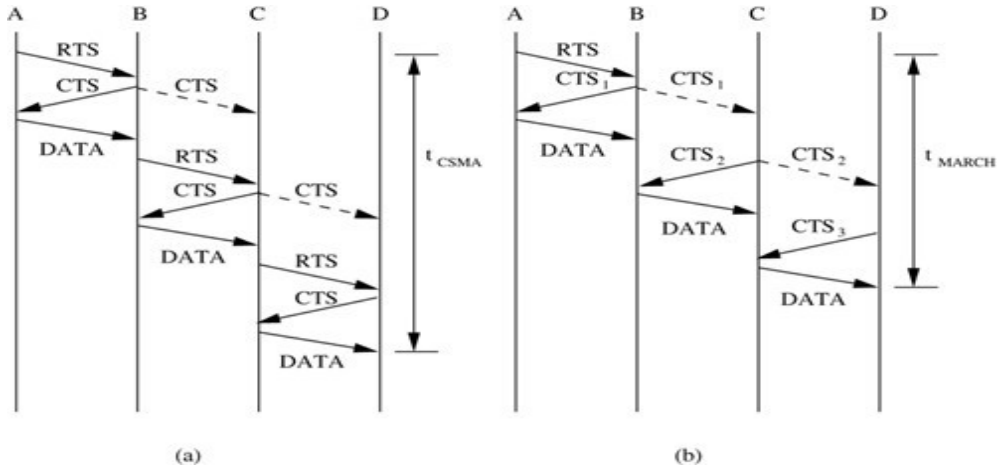


Figure 6.13. Handshake mechanism in (a) MACA and (b) MARCH.

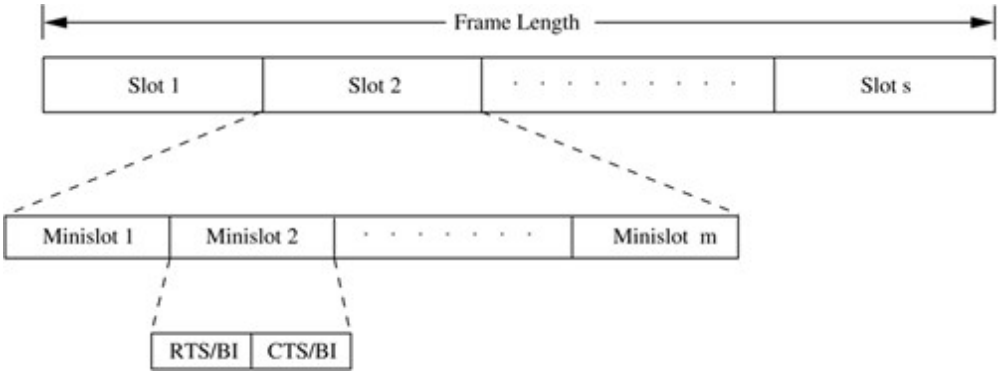
Figure 6.13 (b) shows the handshake mechanism of MARCH. Here, when node B transmits the CTS_1 packet, this packet is also heard by node C. A CTS packet carries information regarding the duration of the next data packet. Node C therefore determines the time at which the next data packet would be available at node B. It sends the CTS_2 packet at that point of time. On receiving the CTS_2packet, node B sends the data packet directly to node C. It can be observed from the figure that the time taken for a packet transmitted by node A to reach node D in MARCH, that is,t_{MARCH}, is less compared to the time taken in MACA, t_{MACA}.

CONTENTION-BASED PROTOCOLS WITH RESERVATION MECHANISMS

Distributed Packet Reservation Multiple Access Protocol

The distributed packet reservation multiple access protocol (D-PRMA) extends the earlier centralized packet reservation multiple access (PRMA) scheme into a distributed scheme that can be used in ad hoc wireless networks. PRMA was proposed for voice support in a wireless LAN with a base station, where the base station serves as the fixed entity for the MAC operation. D-PRMA extends this protocol for providing voice support in ad hoc wireless networks.

D-PRMA is a TDMA-based scheme. The channel is divided into fixed- and equal-sized frames along the time axis (Below Figure). Each frame is composed of *s* slots, and each slot consists of *m* minislots. Each minislot can be further divided into two control fields, RTS/BI and CTS/BI(BI stands for busy indication), as shown in the figure. 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. If no node wins the first minislot, then the remaining minislots are continuously used for contention, until a contending node wins any minislot. Within a reserved slot, communication between the source and receiver nodes takes place by means of either time division duplexing (TDD) or frequency division duplexing (FDD).

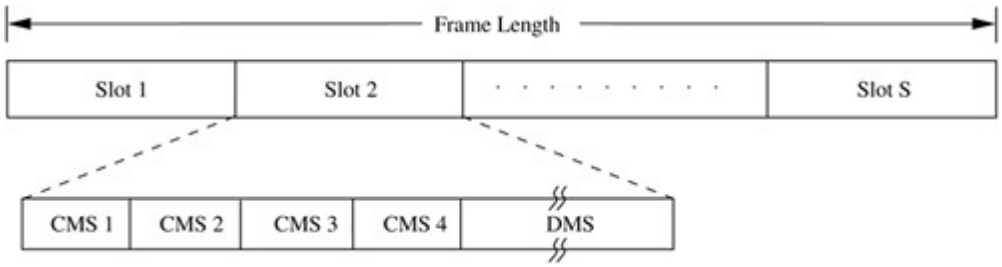
Collision Avoidance Time Allocation Protocol

The collision avoidance time allocation protocol (CATA) [11] is based on dynamic topology dependent transmission scheduling. Nodes contend for and reserve time slots by means of a distributed reservation and handshake mechanism. CATA supports broadcast, unicast, and multicast transmissions simultaneously. The operation of CATA 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.

- Usage of negative acknowledgments for reservation requests, and control packet transmissions.

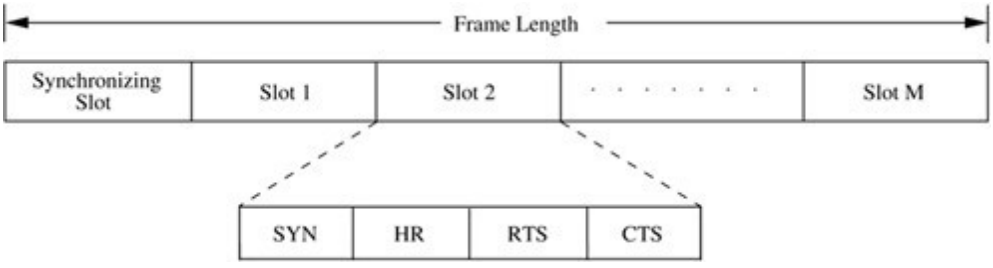
Time is divided into equal-sized frames, and each frame consists of *S* slots (Below Figure). Each slot is further divided into five minislots. The first four minislots are used for transmitting control packets and are called control minislots (CMS1, CMS2, CMS3, and CMS4). The fifth and last minislot, called data minislot (DMS), is meant for data transmission.



Frame format in CATA.

Hop Reservation Multiple Access Protocol

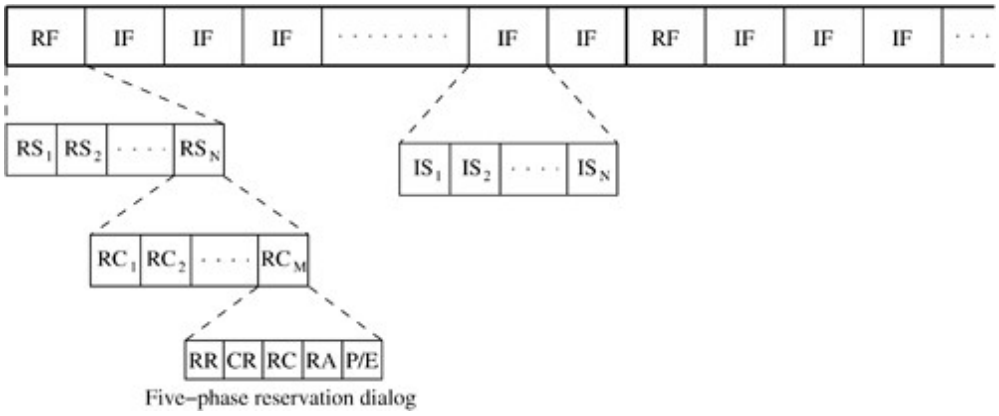
The hop reservation multiple access protocol (HRMA is a multichannel MAC protocol which is based on simple half-duplex, very slow frequency-hopping spread spectrum (FHSS) radios. It uses a reservation and handshake mechanism to enable a pair of communicating nodes to reserve a frequency hop, thereby guaranteeing collision-free data transmission even in the presence of hidden terminals. HRMA can be viewed as a time slot reservation protocol where each time slot is assigned a separate frequency channel.



Frame format of HRMA

Five-Phase Reservation Protocol

The five-phase reservation protocol (FPRP) is 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.



Frame structure in FPRP.

The five phases of the reservation process are as follows:

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.

CONTENTION-BASED MAC PROTOCOLS WITH SCHEDULING MECHANISMS

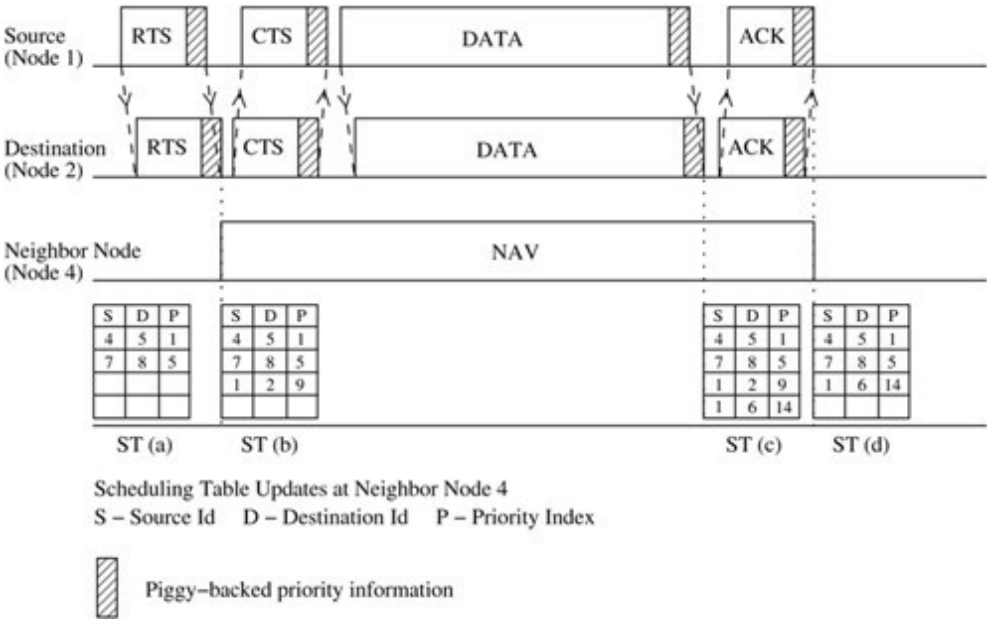
Distributed Priority Scheduling and Medium Access in Ad Hoc Networks

The distributed priority scheduling scheme (DPS) is based on the IEEE 802.11 distributed coordination function. DPS uses the same basic RTS-CTS-DATA-ACK packet exchange mechanism. The RTS packet transmitted by a ready node carries the priority tag/priority index for the current DATA packet to be transmitted. The priority tag can be the delay target for the DATA packet. On receiving the RTS packet, the intended receiver node responds with a CTS packet. The receiver node copies the priority tag from the received RTS packet and piggybacks it along with the source node id, on the CTS packet.

Below Figure illustrates the piggy-backing and table update mechanism. Node 1 needs to transmit a DATA packet (with priority index value 9) to node 2. It first transmits RTS packet carrying piggy-backed information about this DATA packet. The initial state of the ST of node 4 which is a neighbor of nodes 1 and 2 is shown in ST (a). Node 4, on hearing this RTS packet, retrieves the piggybacked priority information and makes a corresponding entry in its ST, as shown in ST (b)..

The destination node 2 responds by sending a CTS packet. The actual DATA packet is sent by the source node once it receives the CTS packet. This DATA packet carries piggy-backed priority information regarding the head-of-line packet at node 1. On hearing this DATA packet, neighbor node 4 makes a corresponding entry for the head-of-line packet of node 1, in its ST.

ST(c) shows the new updated status of the ST at node 4. Finally, the receiver node sends an ACK packet to node 1. When this packet is heard by node 4, it removes the entry made for the corresponding DATA packet from its ST. The state of the scheduling table at the end of this data transfer session is depicted in ST (d).



Distributed Wireless Ordering Protocol

The distributed wireless ordering protocol (DWOP) [19] consists of a media access scheme along with a scheduling mechanism. It is based on the distributed priority scheduling scheme proposed in. DWOP ensures that packets access the medium according to the order specified by an ideal reference scheduler such as first-in-first-out (FIFO), virtual clock, or earliest deadline first.

The key concept in DWOP is that a node is made eligible to contend for the channel only if its locally queued packet has a smaller arrival time compared to all other arrival times in its ST(all other packets queued at its neighbor nodes), that is, only if the node finds that it holds the next region-wise packet in the hypothetical FIFO schedule. Two additional table management techniques, receiver participation and stale entry elimination, are used in order to keep the actual schedule close to the reference FIFO schedule. DWOP may not suffer due to information asymmetry. Since in most networks all nodes are not within the radio range of each other, a transmitting node might not be aware of the arrival times of packets queued at another node which is not within its direct transmission range. This information asymmetry might affect the fair sharing of bandwidth. For example, in Below Figure 6.26 (a), the sender of flow B would be aware of the packets to be transmitted by the sender of flow A, and so it defers its transmission whenever a higher priority packet is queued at the sender of flow A. But the sender of flow A is not aware of the arrival times of packets queued at the sender of

flow B and hence it concludes that it has the highest priority packet in its neighbourhood. Therefore, node 1 unsuccessfully tries to gain access to the channel continuously. This would result in flow B receiving an unfair higher share of the available bandwidth. In order to overcome this information asymmetry problem, the *receiver participation* mechanism is used.

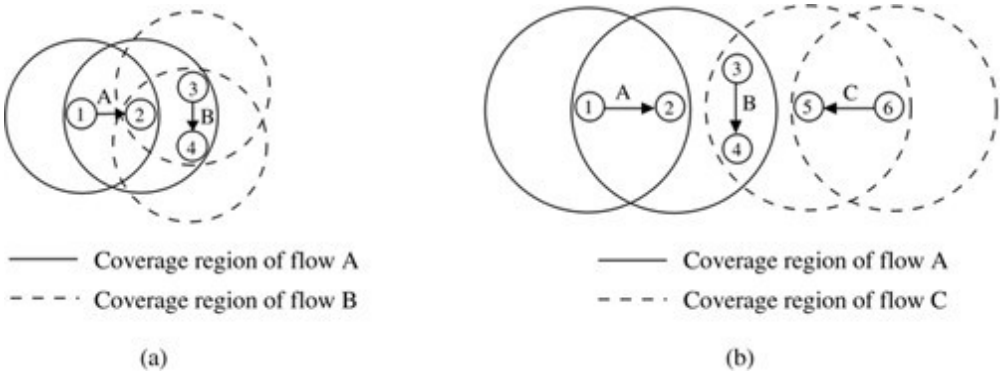


Figure 6.26. (a) Information asymmetry. (b) Perceived collisions.

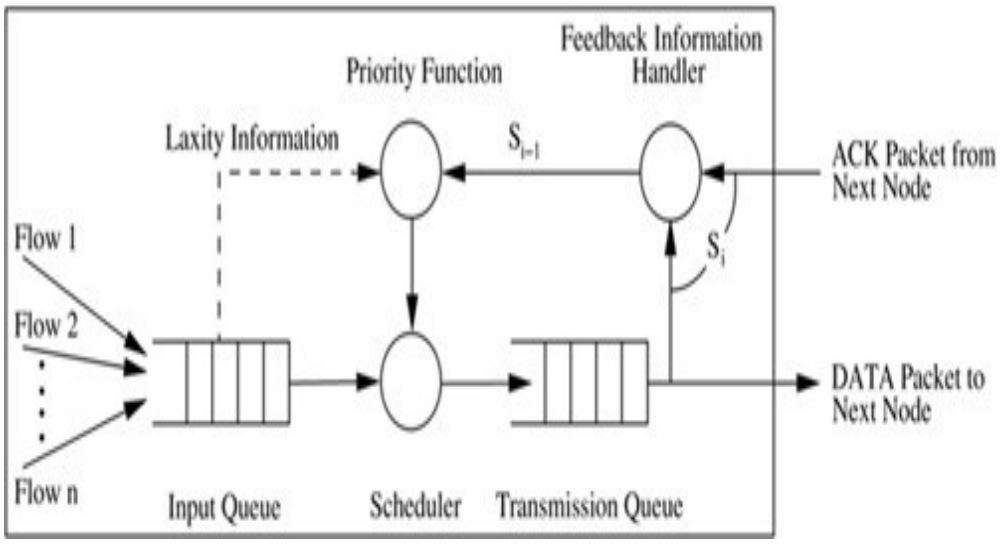
Distributed Laxity-Based Priority Scheduling Scheme

The distributed laxity-based priority scheduling (DLPS) scheme [20] is a packet scheduling scheme, where scheduling decisions are made taking into consideration the states of neighbouring nodes and the feedback from destination nodes regarding packet losses. Packets are reordered based on their uniform laxity budgets (ULBs) and the packet delivery ratios of the flows to which they belong.

Each node maintains two tables: scheduling table (ST) and packet delivery ratio table (PDT). The ST contains information about packets to be transmitted by the node and packets overheard by the node, sorted according to their *priority index* values. Priority index expresses the priority of a packet. The lower the priority index, the higher the packets priority. The PDT contains the count of packets transmitted and the count of acknowledgment (ACK) packets received for every flow passing through the node.

Below Figure depicts the overall functioning of the feedback mechanism. Incoming packets to a node are queued in the node's input queue according to their arrival times. The scheduler sorts them according to their priority values and inserts them into the transmission queue. The highest priority packet from this queue is selected for transmission. The node, after transmitting a packet, updates the count of packets transmitted so far in its PDT. The

destination node of a flow, on receiving data packets, initiates a feedback by means of which the count of DATA packets received by it is conveyed to the source through ACK packets traversing the reverse path.



ISSUES IN AD HOC WIRELESS NETWORKS

The major issues that affect the design, deployment, and performance of an ad hoc wireless system are as follows:

Medium access scheme

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. In the case of polling-based MAC protocols, partial coordination is required**.**

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.

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. In such cases, the hidden terminal can cause collisions at the receiver node.

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.

Access delay: The access delay refers to the average delay that any packet experiences to get transmitted. The MAC protocol should attempt to minimize the delay.

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.

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.

• **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.

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.

Mobility: One of the most important properties of ad hoc wireless networks is the mobility associated with the nodes. The mobility of nodes results in frequent path breaks, packet collisions, transient loops, stale routing information, and difficulty in resource reservation. A good routing protocol should be able to efficiently solve all the above issues.

Bandwidth constraint: Since the channel is shared by all nodes in the broadcast region (any region in which all nodes can hear all other nodes), the bandwidth available per wireless link depends on the number of nodes and the traffic they handle. Thus only a fraction of the total bandwidth is available for every node.

Error-prone and shared channel: The bit error rate (BER) in a wireless channel is very high (of the order of 10^{-5} to 10^{-3}) compared to that in its wired counterparts (of the order of 10^{-12} to 10^{-9}).

Multicasting

The major issues in designing multicast routing protocols are as follows:

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

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

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

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

Scalability: The multicast routing protocol should be able to scale for a network with a large number of nodes.

•**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 and maintaining end-to end connections, reliable end-to-end delivery of data packets, flow control, and congestion control.

Pricing scheme

Ad hoc wireless networks employed for special tasks such as military missions, rescue operations, and law enforcement do not require such pricing schemes, whereas the successful commercial deployment of ad hoc wireless networks requires billing and pricing.

Quality of service provisioning

Quality of service (QoS) is the performance level of services offered by a service provider or a network to the user. QoS provisioning often requires negotiation between the host and the network, resource reservation schemes, priority scheduling, and call admission control. Rendering QoS in ad hoc wireless networks can be on a per flow, per link, or per node basis. The QOS depends on three factors QoS parameters, QoS-aware routing, and QoS frameworks.

Security

The security of communication in ad hoc wireless networks is very important, especially in military applications. The attacks against ad hoc wireless networks are generally classified into two types: passive and active attacks. Passive attacks refer to the attempts made by malicious nodes to perceive the nature of activities and to obtain information transacted in the network without disrupting the operation. Active attacks disrupt the operation of the network. The major security threats that exist in ad hoc wireless networks are as follows:

- **Denial of service**
- **Resource consumption**
- **Information disclosure**
- **Interference**

Energy management

Energy management is defined as the process of managing the sources and consumers of energy in a node or in the network as a whole for enhancing the lifetime of the network. Energy management can be classified into the following categories:

- **Transmission power management:**
- **Battery energy management**
- **Processor power management**

- **Devices power management**
- Scalability

Deployment considerations

The deployment of ad hoc wireless networks involves actions different from those of wired networks. It requires a good amount of planning and estimation of future traffic growth over any link in the network.

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

Scenario of deployment

Military deployment

Emergency operations deployment

Commercial wide-area deployment

Home network deployment

UNIT -4

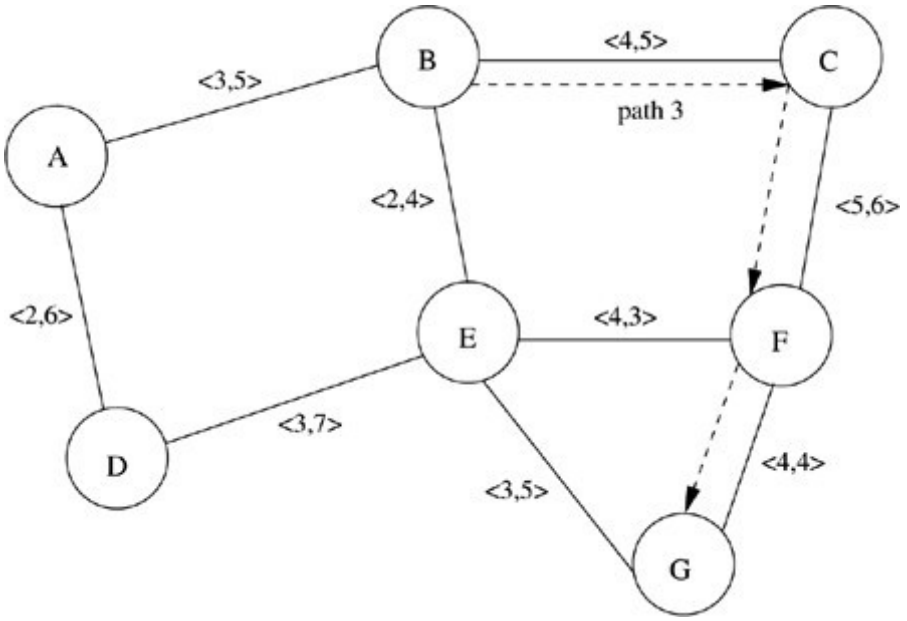
QUALITY OF SERVICE

INTRODUCTION

Quality of service (QoS) is the performance level of a service offered by the network to the user. The goal of QoS provisioning is to achieve a more deterministic network behavior, so that information carried by the network can be better delivered and network resources can be better utilized.After accepting a service request from the user, the network has to ensure that the service requirements of the user's flow are met.

After receiving a service request from the user, the first task is to find a suitable loop-free path from the source to the destination that will have the necessary resources available to meet the QoS requirements of the desired service. This process is known as QoS routing. After finding a suitable path, a resource reservation protocol is employed to reserve necessary resources along that path.

For example, consider the network shown in Figure 10.1. The attributes of each link are shown in a tuple < *BW, D* >,where *BW* and *D* represent available bandwidth in Mbps and delay1 in milliseconds. Suppose a packet-flow from node *B* to node *G* requires a bandwidth guarantee of 4 Mbps.



An example of QoS routing in ad hoc wireless network

QoS routing selects path 3 (*i.e.,* $B \rightarrow C \rightarrow F \rightarrow$ G) because, out of the available paths, path 3 alone meets the bandwidth constraint of 4 Mbps for the flow.

No.	Path	Hop Count	End-to-end Bandwidth (Mbps)	End-to-end Delay (milliseconds)
1	$B \rightarrow E \rightarrow G$	2	2	9
2	$B \rightarrow E \rightarrow F \rightarrow G$	3	2	11
3	$B \rightarrow C \rightarrow F \rightarrow G$	3	4	15
4	$B \rightarrow C \rightarrow F \rightarrow E \rightarrow G$	4	3	19
5	$B \rightarrow A \rightarrow D \rightarrow E \rightarrow G$	4	2	23
6	$B \rightarrow A \rightarrow D \rightarrow E \rightarrow F \rightarrow G$	5	2	25

Available paths from node *B* to node *G*

ISSUES AND CHALLENGES IN PROVIDING QOS IN AD HOC WIRELESS NETWORKS

Dynamically varying network topology: Since the nodes in an ad hoc wireless network do not have any restriction on mobility, the network topology changes dynamically. Hence, the admitted QoS sessions may suffer due to frequent path breaks, thereby requiring such sessions to be re-established over new paths.

Imprecise state information: In most cases, the nodes in an ad hoc wireless network maintain both the link-specific state information and flow-specific state information. The link-specific state information includes bandwidth, delay,delay jitter, loss rate, error rate, stability, cost, and distance values for each link.The flow-specific information includes session ID, source address, destination Address. The state information is inherently imprecise due to dynamic changes in network topology and channel characteristics.

Lack of central coordination: Unlike wireless LANs and cellular networks, ad hoc wireless networks do not have central controllers to coordinate the activity of nodes.

Error-prone shared radio channel: The radio channel is a broadcast medium by nature. During propagation through the wireless medium, the radio waves suffer from several impairments such as attenuation, multipath propagation, and interference.

Hidden terminal problem: The hidden terminal problem is inherent in ad hoc wireless networks. This problem occurs when packets originating from two or more sender nodes, which are not within the direct transmission range of each other, collide at a common receiver node. It necessitates the retransmission of the packets.

Limited resource availability: Resources such as bandwidth, battery life, storage space, and processing capability are limited in ad hoc wireless networks. Out of these, bandwidth and battery life are critical resources, the availability of which significantly affects the

performance of the QoS provisioning mechanism. Hence, efficient resource management mechanisms are required for optimal utilization of these scarce resources.

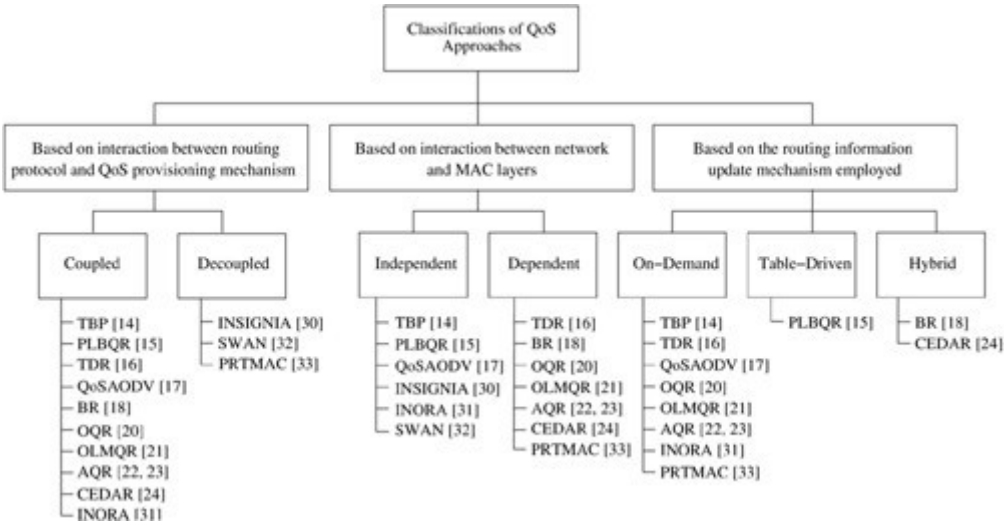
Insecure medium: Due to the broadcast nature of the wireless medium, communication through a wireless channel is highly insecure. Therefore, security is an important issue in ad hoc wireless networks, especially for military and tactical applications.

CLASSIFICATIONS OF QOS SOLUTIONS

The QoS solutions can be classified in two ways. One classification is based **on the QoS approach employed**, Other one classifies **QoS solutions based on the layer**.

Classifications of QoS Approaches

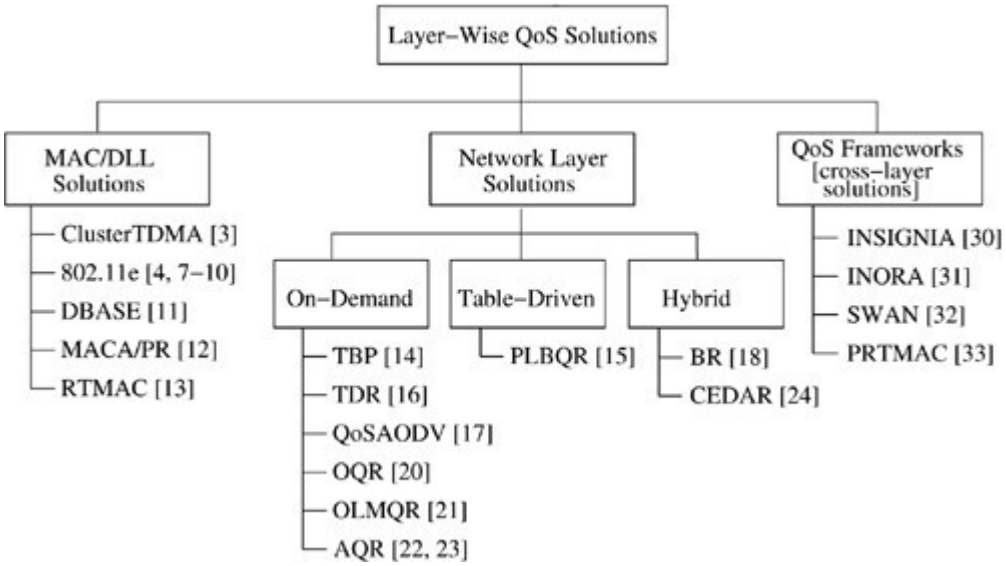
several criteria are used for classifying QoS approaches. The QoS approaches can be classified based on the interaction between the routing protocol and the QoS provisioning mechanism. Based on the interaction between the network and the MAC layers, or based on the routing information update mechanism.



Classifications of QoS approaches

Layer-Wise Classification of Existing QoS Solutions

The existing QoS solutions can also be classified based on which layer in the network protocol stack they operate in. Following figure gives a layer-wise classification of QoS solutions. The figure also shows some of the cross-layer QoS solutions proposed for ad hoc wireless networks.



NETWORK LAYER SOLUTIONS

Existing network layer solutions that support QoS provisioning are

QoS Routing Protocols

QoS routing protocols search for routes with sufficient resources in order to satisfy the QoS requirements of a flow. The information regarding the availability of resources is managed by a resource management module which assists the QoS routing protocol in its search for QoS feasible paths. The QoS routing protocol should find paths that consume minimum resources.

The QoS metrics can be classified as **additive metrics, concave metrics, and multiplicative metrics.**

An additive metric A_m is defined as $\sum_{i=1}^{h} L_i(m)$, where $L_i(m)$ is the value of metric m over link L_i and $L_i \times$ P. The hop length of path P is h. A concave metric represents the minimum value over a path P and is formally defined as $C_m = min(L_i(m))$, $L_i(m)$ ε P. A multiplicative metric represents the product of QoS metric values and is defined as $M_m = \prod_{i=1}^{h}(L_i(m))$, $L_i(m)$ ε P. To find a QoS

Ticket-Based QoS Routing Protocol

Ticket-based QoS routing is a distributed QoS routing protocol for ad hoc wireless networks. This protocol has the following features:

• It can tolerate imprecise state information during QoS route computation and exhibits good performance even when the degree of imprecision is high.

• It probes multiple paths in parallel for finding a QoS feasible path. This increases the chance of finding such a path. The number of multiple paths searched is limited by the number of tickets issued in the probe packet by the source node. State information maintained at intermediate nodes is used for more accurate route probing. An intelligent hop-by-hop selection mechanism is used for finding feasible paths efficiently.
• The optimality of a path among several feasible paths is explored. A low-cost path that uses minimum resources is preferred when multiple feasible paths are available.
• A primary-backup-based fault-tolerant technique is used to reduce service disruption during path breaks that occur quite frequently in ad hoc wireless networks.

Trigger-Based Distributed QoS Routing Protocol

The trigger-based (on-demand) distributed QoS routing (TDR) protocol was proposed by De *et al.* for supporting real-time applications in ad hoc wireless networks. It operates in a distributed fashion. Every node maintains only the local neighbourhood information in order to reduce computation overhead and storage overhead.

Database Management

All nodes in the network maintain the local neighborhood information. For each neighbor, every node maintains *received power level,* current geographic coordinates, velocity, and direction of motion in the database.

Initial Route Discovery

If the source *S* has enough *ResiBWS* to satisfy the MaxBW for the session, the required bandwidth is temporarily reserved for a certain duration within which it expects an acknowledgment from the destination *D.* If the source knows the location of the destination, it performs route discovery through selective forwarding.

In this approach, the source node takes advantage of location information of its neighbors and forwards route requests to only selective neighbours that are lying closely toward the destination node and satisfying QoS requirements of the connection request.

Route/Reroute Acknowledgment

After accepting the route, the destination node *D* builds *DTD* table with the NodActv flag set to 1 (*i.e.,*active) and sends an ACK to the source *S* along the selected route.

Route Deactivation

In case of session completion or termination, the source node purges its corresponding *ST* table and sends a route deactivation packet toward the destination. Upon receiving a deactivation request, each node which was part of that session updates its *ResiBW* and purges the activity table for that session.

QoS-Enabled Ad Hoc On-Demand Distance Vector Routing Protocol

Perkins *et al.* have extended the basic ad hoc on-demand distance vector (AODV) routing protocol to provide QoS support in ad hoc wireless networks .

Several modifications have been carried out for the routing table structure and *RouteRequest* and *RouteReply* messages in order to support QoS routing. Each routing table entry corresponds to a different destination node. The following fields are appended to each routing table entry:

- Maximum delay
- Minimum available bandwidth
- List of sources requesting delay guarantees
- List of sources requesting bandwidth guarantees

Maximum Delay Extension Field

The maximum delay extension field is interpreted differently for *RouteRequest* and *RouteReply*messages. In a *RouteRequest* message, it indicates the maximum time (in seconds) allowed for a transmission from the current node to the destination node. In a *RouteReply* message, it indicates the current estimate of cumulative delay from the current intermediate node forwarding the *RouteReply,*to the destination.

Using this field the source node finds a path (if it exists) to the destination node satisfying the maximum delay constraint.

Minimum Bandwidth Extension Field

In a *RouteRequest* message, this field indicates the minimum bandwidth (in Kbps) that must be available along an acceptable path from the source to the destination. In a *RouteReply* message, it indicates the minimum bandwidth available on the route between the node forwarding the *RouteReply*and the destination node. Using this field, the source node finds a path (if it exists) to the destination node satisfying the minimum bandwidth constraint.

Advantages and Disadvantages

The advantage of QoS AODV protocol is the simplicity of extension of the AODV protocol that can potentially enable QoS provisioning. However, as no resources are reserved along the path from the source to the destination, this protocol is not suitable for applications that require hard QoS guarantees.

Bandwidth Routing Protocol

The bandwidth routing (BR) protocol consists of an end-to-end path bandwidth calculation algorithm to inform the source node of the available bandwidth to any destination in the ad hoc network, a bandwidth reservation algorithm to reserve a sufficient number of free slots for the QoS flow, and a standby routing algorithm to reestablish the QoS flow in case of path breaks. Here, only bandwidth is considered to be the QoS parameter.

Bandwidth Calculation

Since the network is multi-hop in nature, the free slots recorded at each node may be different. The set of common free slots between two adjacent nodes denotes the link bandwidth between them. The path bandwidth between two nodes is the maximum bandwidth available in the path between them. If the two nodes are adjacent, the path bandwidth between them equals their link bandwidth. For example, consider two adjacent nodes, node A and node B, having free slots {2,5,6,8} and {1,2,4,5}, respectively. The link bandwidth $linkBW(A, B) = freeslot(A) \cap freeslot(B) = \{2, 5\}$. It means that only slots 2 and 5 can be used by nodes A and B for transmitting data packets to each other.

Advantages and Disadvantages

The BR protocol provides an efficient bandwidth allocation scheme for CDMA over-TDMA-based ad hoc wireless networks. The standby routing mechanism can reduce the packet loss during path breaks. But the CDMA-over-TDMA channel model that is used in this protocol requires assigning a unique control slot in the control phase of superframe for each node present in the network. This assignment has to be done statically before commissioning the network. Due to this, it is not possible for a new node to enter into the network at a later point of time.

On-Demand Link-State Multipath QoS Routing Protocol ***(imp)*

The on-demand link-state multipath QoS routing (OLMQR) protocol searches for multiple paths which collectively satisfy the required QoS. The original bandwidth requirement is split into sub-bandwidth requirements.

On-Demand Link-State Discovery

For each call request, the source node floods a QRREQ packet toward the destination. Each packet records the path history and all link-state information along its route. A QRREQ packet contains the following fields: source ID, destination ID, node history, free time-slot list, bandwidth requirement, and time to live (TTL). The node history field records the path from source to the current traversed node.

The source *S* floods a QRREQ packet into the network toward the destination D, if the given requirement is *BW*. An intermediate node *N* receiving a QRREQ packet performs the following operations:

1. Node *N* checks the node history field of the QRREQ packet for its address. If it is present, the node discards this QRREQ packet.
2. Otherwise,

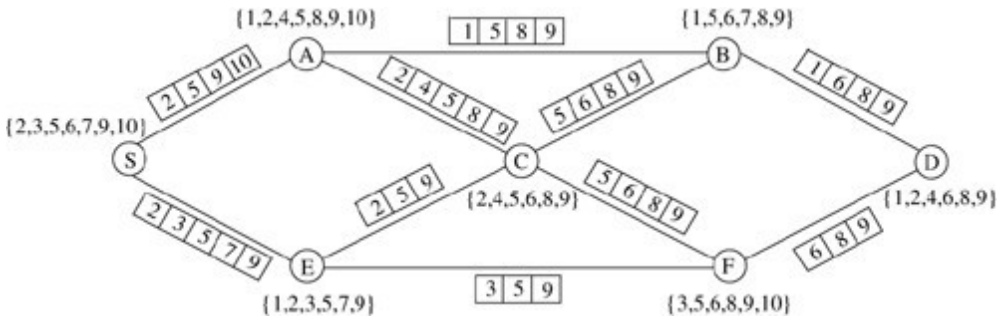
• Node *N* decrements TTL by one. If TTL counts down to zero, it discards this QRREQ packet.

• Node *N* adds itself into the node history field, appends the free timeslots of the link between itself and the last node recorded in the node history field into the free time-slot list field, and rebroadcasts this QRREQ packet.

In following Figure. The source *S* floods the network with a QRREQ packet by setting *BW* and *TTL* fields to 3 and 4, respectively.

The destination *D*receives six QRREQ packets, which have traversed along the paths: $S \rightarrow A \rightarrow B \rightarrow D$, $S \rightarrow E \rightarrow F \rightarrow D$, $S \rightarrow A \rightarrow C \rightarrow B \rightarrow D$,$S \rightarrow A \rightarrow C \rightarrow F \rightarrow D$, $S \rightarrow E \rightarrow C \rightarrow F \rightarrow D$, and $S \rightarrow E \rightarrow C \rightarrow B \rightarrow D$.

Using this information, a partial view of the network is constructed at the destination *D*.



An example network.

QOS FRAMEWORKS FOR AD HOC WIRELESS NETWORKS

A framework for QoS is a complete system that attempts to provide required/promised services to each user or application. All components within this system cooperate in providing the required services.

The key components

- Routing protocol
- QoS resource reservation signaling
- Admission control
- Packet scheduling

- It is used to find a path from the source to the destination and to forward the data packet to the next intermediate relay node. QoS routing describes the process of finding suitable path(s).
- Once a path with the required QoS is found, the next step is to reserve the required resources along that path. This is done by the resource reservation signalling protocol.
- It is a validation process in communication systems where a check is performed before a connection is established to see if current resources are sufficient for the proposed connection.
- When multiple QoS connections are active at the same time through a link, the decision on which QoS flow is to be served next is made by the scheduling scheme.

QoS Models

A QoS model defines the nature of service differentiation. In wired network QoS frameworks, several service models have been proposed. Two of these models are the

integrated services (IntServ) model and the differentiated services (DiffServ) model . The IntServ model provides QoS on a per flow.

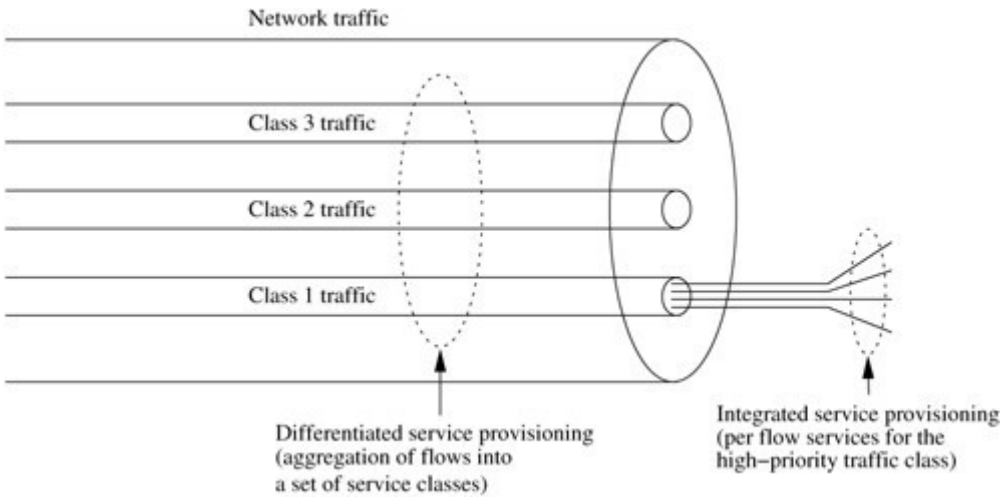
The DiffServ model was proposed in order to overcome the difficulty in implementing and deploying IntServ model and RSVP in the Internet. In this model, flows are aggregated into a limited number of service classes.

The above two service models cannot be directly applied to ad hoc wireless networks because of the inherent characteristics of ad hoc wireless networks such as continuously varying network topology, limited resource availability, and error-prone shared radio channel.

Flexible QoS Model for Mobile Ad Hoc Networks

The flexible QoS model for mobile ad hoc networks (FQMM) takes advantage of the per flow granularity of IntServ and aggregation of services into classes in DiffServ. In this model the nodes are classified into three different categories, namely, *ingress* node (source), *interior* node (intermediate relay node), and *egress* node (destination) on a per flow basis.

The FQMM model provides per flow QoS services for the high-priority flows while lower priority flows are aggregated into a set of service classes as illustrated in Figure .



QoS Resource Reservation Signaling

The QoS resource reservation signalling scheme is responsible for reserving the required resources and informing the corresponding applications, which then initiate data transmission. Signalling protocol consists of three phases, namely, connection establishment, connection maintenance, and connection termination.

On establishing a connection, it monitors the path and repairs/reconfigures it if the connection suffers from any violation in its QoS guarantees. On completion/termination of a session, it releases the resources that had been reserved for that session.

INSIGNIA

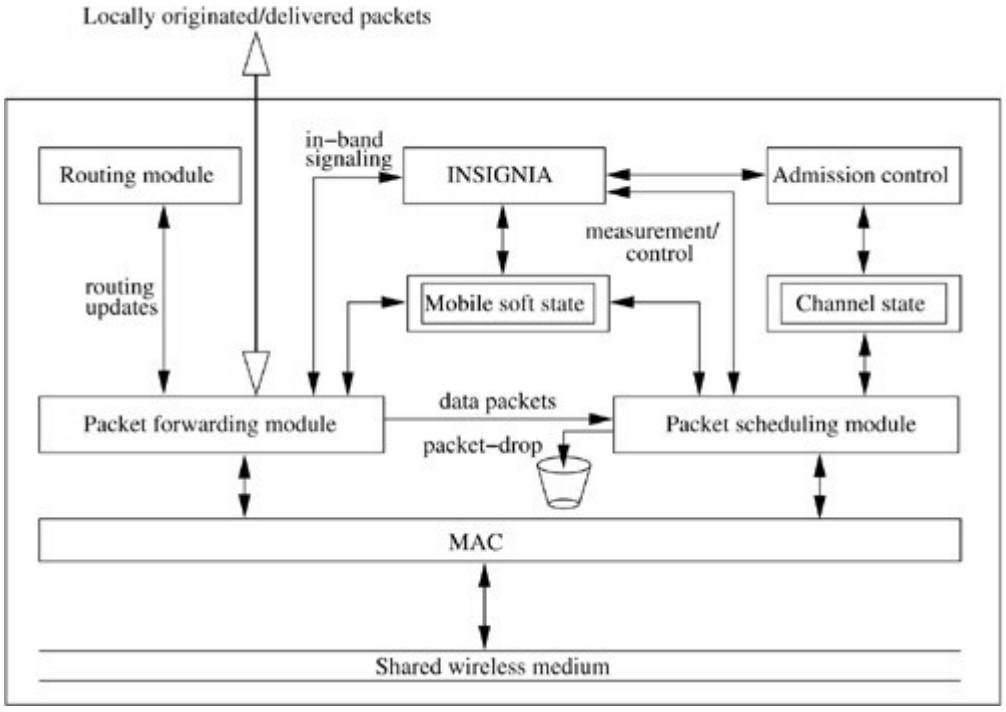
The INSIGNIA QoS framework was developed to provide adaptive services in ad hoc wireless networks. Adaptive services support applications that require only a minimum quantitative QoS guarantee (such as minimum bandwidth) called *base QoS.*

The key design issues in providing adaptive services are as follows:

• How fast can the application service level be switched from *base QoS* to *enhanced QoS* .

• How and when is it possible to operate on the *base QoS* or *enhanced QoS* level.

As depicted in Figure, the INSIGNIA framework has the following key components for supporting adaptive real-time services:



Routing module: The routing protocol finds a route from the source to the destination. It is also used to forward a data packet to the next intermediate relay node.

In-band signaling: This module is used to establish, adapt, restore, and tear down adaptive services between source-destination pairs. It is not dependent on any specific link layer protocol. In in-band signaling systems, the control information is carried along with data packets and hence no explicit control channel is required.

Admission control: This module allocates bandwidth to flows based on the maximum/minimum bandwidth requested. Once the bandwidth is reserved, the reservation must be refreshed periodically by a soft state mechanism.

Packet forwarding: This module classifies the incoming packets and delivers them to the appropriate module. If the current node is the destination of the packet, then the packet is delivered to the local application.

Packet scheduling: Packets that are to be routed to other nodes are handled by the packet-scheduling module. The packets to be transmitted by a node are scheduled by the scheduler based on the forwarding policy.

Medium access control (MAC): The MAC protocol provides QoS-driven access to the shared wireless medium for adaptive real-time services.

INORA

INORA is a QoS framework for ad hoc wireless networks that makes use of the INSIGNIA in-band signaling mechanism.

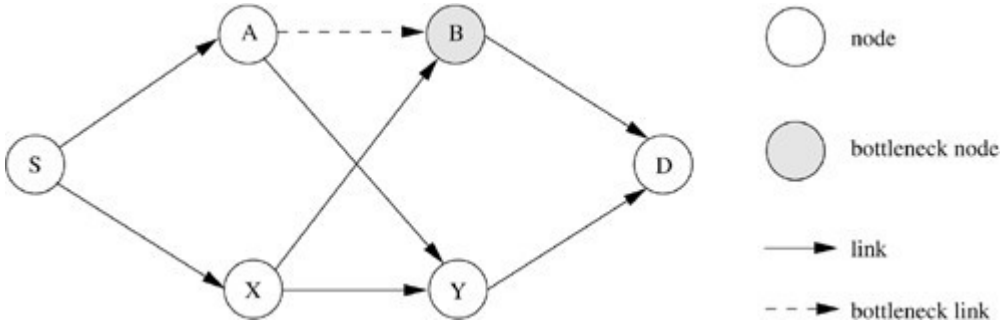
INORA can be classified into two schemes: *coarse feedback scheme* and *class-based fine feedback scheme.*

Coarse Feedback Scheme

In this scheme, if a node fails to admit a QoS flow either due to lack of minimum required bandwidth (*BWmin*) or because of congestion at the node, it sends an out-of-band *admission control failure* (ACF) message to its upstream node. After receiving the ACF message, the upstream node reroutes the flow through another downstream node provided by the TORA routing protocol. If none of its neighbors is able to admit the flow, it in turn sends an ACF message to its upstream node.

The operations of the coarse feedback scheme are explained through the following example. Here a QoS flow is being initiated by the source node *S* to the destination node *D.* Let the DAG created by the TORA protocol be as shown in Following Figure.

1. Let $S \rightarrow A \rightarrow B \rightarrow D$ be the path chosen by the TORA routing protocol.



2. INSIGNIA tries to establish soft state reservations for the QoS flow along the path. Assume that node A has admitted the flow successfully and node *B* fails to admit the flow due to lack of sufficient resources. Node *B* sends an ACF message to node *A*.

3. Node *A* tries to reroute the flow through neighbor node *Y* provided by TORA.

4. If node *Y* admits the flow, the flow gets the required reservation all along the path. The new path is $S \rightarrow A \rightarrow Y \rightarrow D$.

5. If node *Y* fails to admit the flow, it sends an ACF message to node *A*,which in turn sends an ACF message to node *S*.

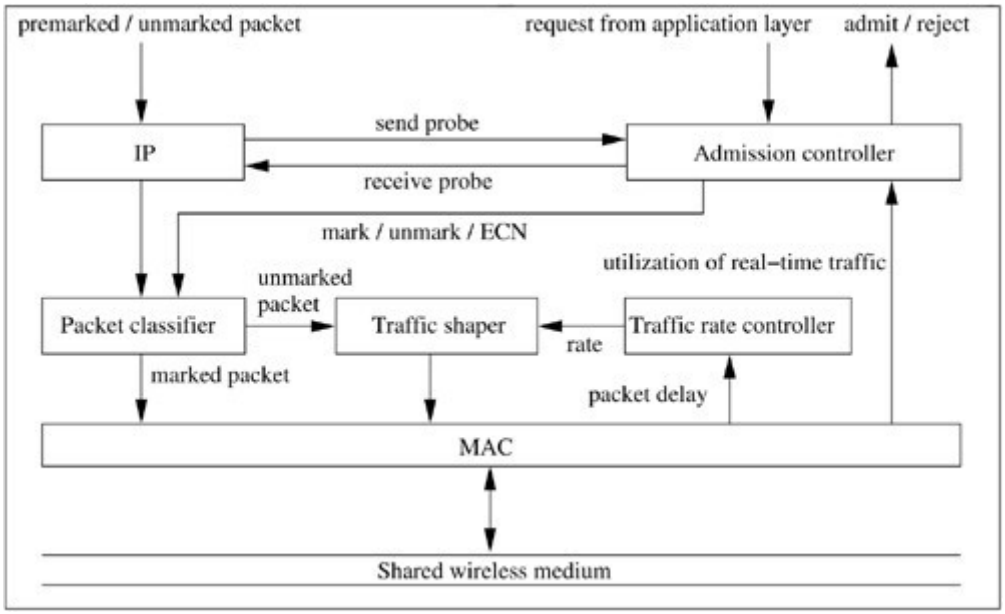
6. Node *S* tries with its other downstream neighbors to find a QoS path for the flow.

7. If no such neighbour is available, node *S* rejects the flow.

SWAN

SWAN Model

The SWAN model has several control modules which are depicted in below Figure. Upon receiving a packet from the IP layer, the *packet classifier* module checks whether it is marked (*i.e.,* real-time packet) or not (*i.e.,* best-effort packet). If it is a best-effort packet, it is forwarded to the *traffic-shaper* for regulation. If it is a real-time packet, the module forwards it directly to the MAC layer, bypassing the *traffic shaper*. The *traffic shaper* represents a simple leaky bucket traffic policy. The traffic shaper delays best-effort packets in conformance with the rate calculated by the *traffic rate controller*. The *call admission controller* module is responsible for admitting or rejecting new real-time sessions. The decision on whether to admit or reject a real-time session is taken solely by the source node based on the result of an end-to-end request/response probe.



ENERGY MANAGEMENT IN AD HOC WIRELESS NETWORKS

NEED FOR ENERGY MANAGEMENT IN AD HOC WIRELESS NETWORKS

The main reasons for energy management in ad hoc wireless networks are listed below:

• **Limited energy reserve:** The main reason for the development of ad hoc wireless networks is to provide a communication infrastructure in environments where the setting up of a fixed infrastructure is impossible. Ad hoc wireless networks have very limited energy resources. Advances in battery technologies have been negligible as compared to the recent advances that have taken place in the field of mobile computing and communication.

Difficulties in replacing the batteries: Sometimes it becomes very difficult to replace or recharge the batteries. In situations such as battlefields, this is almost impossible.

Constraints on the battery source: Batteries tend to increase the size and weight of a mobile node. Reducing the size of the battery results in less capacity which, in turn, decreases the active lifespan of the node. Hence, in addition to reducing the size of the battery, energy management techniques are necessary to utilize the battery capacity in the best possible way.

Selection of optimal transmission power: The transmission power selected determines the reachability of the nodes. The consumption of battery charge increases with an increase in the transmission power.

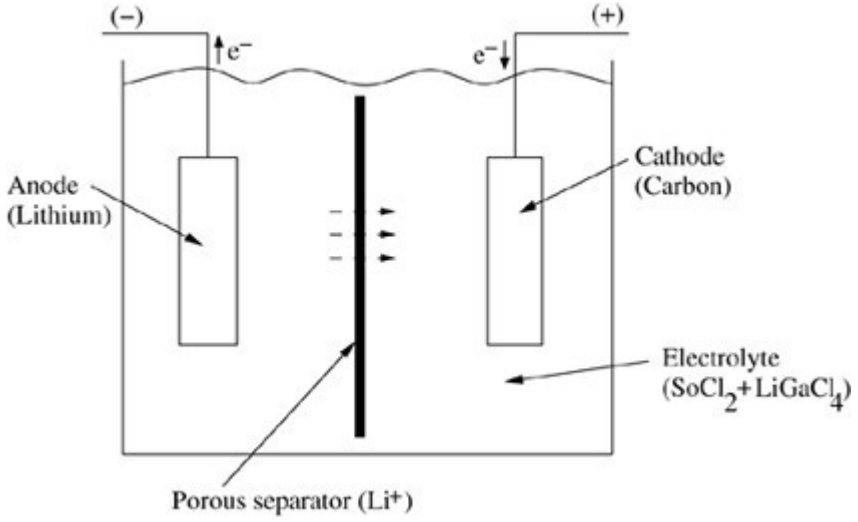
Channel utilization: A reduction in the transmission power increases frequency reuse, which leads to better channel reuse. Power control becomes very important for CDMA-based systems in which the available bandwidth is shared among all the users. Hence, power control is essential to maintain the required signal to interference ratio (SIR) at the receiver and to increase the channel reusability.

BATTERY MANAGEMENT SCHEMES

Overview of Battery Characteristics

Battery technologies: The most popular rechargeable battery technologies developed over the last two decades are comprised of nickel-cadmium, lithium ion, nickel metal-hydride, reusable alkaline, and lithium polymer.

Principles of battery discharge: A battery typically consists of an array of one or more cells. Hence, in the subsequent sections, the terms "battery" and "cell" are used interchangeably. The three main voltages that characterize a cell are: (1) the open circuit voltage (*Voc*), that is, the initial voltage under a no-load condition of a fully charged cell, (2) the operating voltage (*Vi*), that is, the voltage under loaded conditions, and (3) the cut-off voltage (*Vcut*) at which the cell is said to be discharged.



Basic structure of a lithium chloride battery

.

Device-Dependent Schemes

The lifetime of a node is determined by the capacity of its energy source and the energy required by the node. the battery life can be improved by introducing techniques which make efficient utilization of the battery power.

Following are the device dependent approaches that increase the battery lifetime by exploiting its internal characteristics.

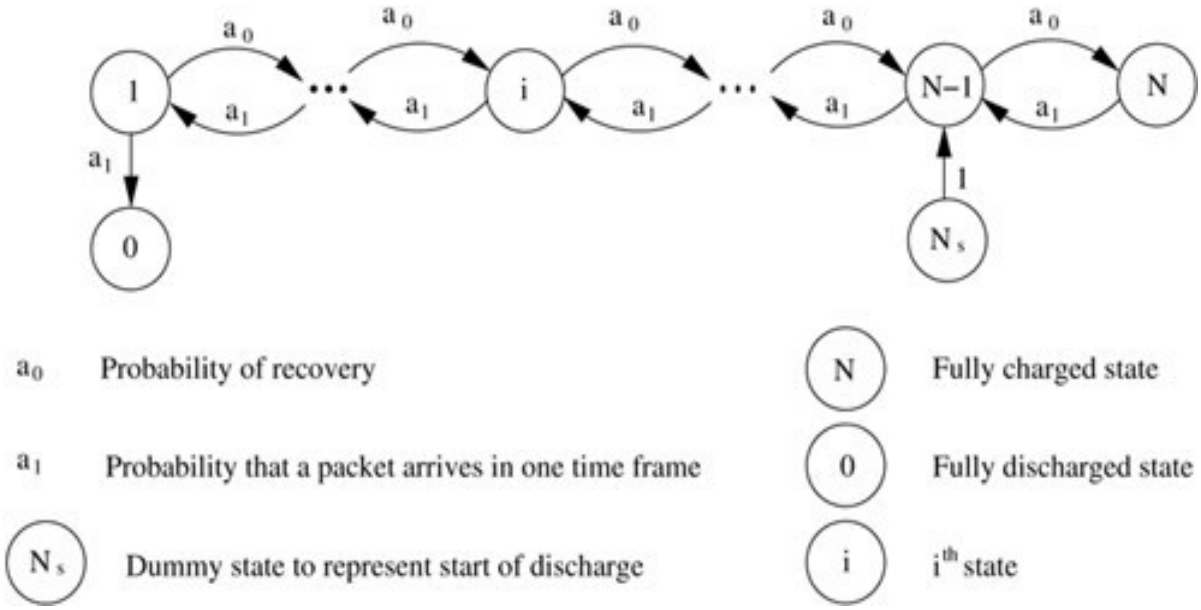
Effect of Battery Pulsed Discharge

Recent works shows that pulsed current discharge applied for bursty stochastic transmissions improves the battery lifetime. If pulsed current discharge is applied to a cell, significant improvement in the specific energy delivered is realized. In such an environment, higher specific power can be obtained for a constant specific energy.

Binary Pulsed Discharge

In this mode, if there are packets in the queue, transmission of a packet occurs in one time slot; one charge unit is recovered if the queue is empty. The current required for transmission is drained during the entire time frame.

The Markov chain for binary pulsed discharge is shown in following Figure.



An additional dummy state is added to the Markov chain representing the cell behavior, which represents the start of the discharge. The cell is modelled as a transient process and the packet arrival follows a Bernoulli process. If the probability that a packet arrives in one time frame is stated as $a1 = q$ and the probability for transmitting a packet in a time slot is given by $a1$, then the probability of recovery is given by $a0 = (1 - q)$. The cell can never cross the charge state of N. The gain obtained in this scheme is given by , where mp is the total expected number of packets transmitted and N is the amount of charge in a fully charged battery. The gain, however, cannot exceed C/N where C is the theoretical capacity.

TRANSMISSION POWER MANAGEMENT SCHEMES

The components used in the communication module consume a major portion of the energy in ad hoc wireless networks. Increasing the transmission range not only increases coverage, but also the power consumption rate at the transmitter.

Data Link Layer Solutions

As stated earlier, transmitter power greatly influences the reachability of the node and thus the range covered by it. Power control can be affected at the data link layer by means of topology control and constructing a power control loop.

Some of the solutions proposed to calculate the optimum transmission range are as follows:

1• Dynamic power adjustment policies

2• Distributed topology control algorithms

3 constructing distributed power control loop

4• Centralized topology control algorithm

1) Ad hoc wireless networks are prone to constant link failures due to node mobility; hence the stability of routes cannot be assured in such situations. But frequent link failures lead to reduced throughput. A parameter called *affinity* that decides the stability of a route.

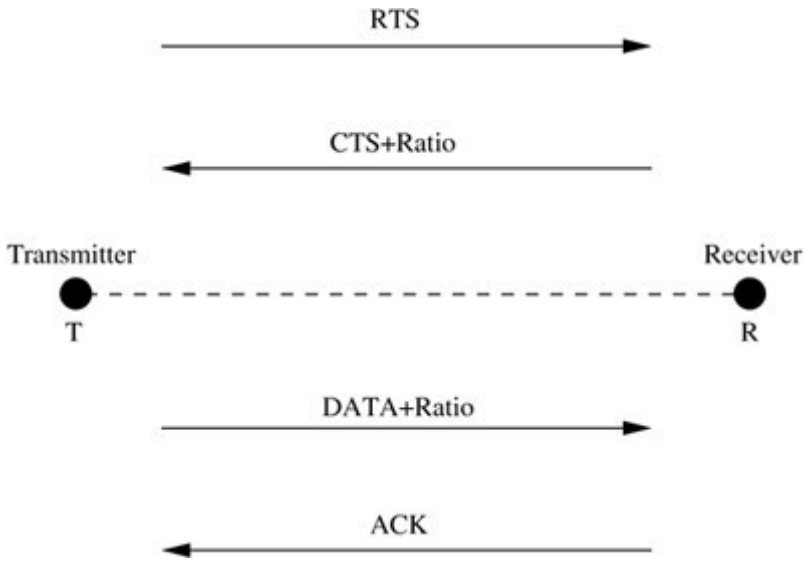
2) Distributed Topology Control Mechanisms

   According to this algorithm, each node of the ad hoc wireless network independently runs a localized algorithm and decides the appropriate power level to be used by that node. A node increases the power directionally until it finds one node in all the

directions. Then it tries to increase the lifetime of the nodes to a greater extent by reducing the transmission power and having less coverage of the nodes while guaranteeing the same connectivity as the one achieved when the nodes are maximally powered. The principle behind this algorithm is that the topology of the network can be changed by choosing the appropriate power level.

3) The power control algorithm has been incorporated into the IEEE 802.11 MAC protocol. We now discuss the modifications made to the 802.11 MAC protocol. Unlike the usual IEEE 802.11 DCF protocol which uses only one common power level, the modified algorithm uses ten different power levels varying with a step size of one tenth of the maximum power level available.

The format of the message header is also modified as shown in Figure.
The headers of the CTS and Data frames are modified to include the information of the ratio of the signal strength of the last received message to the minimum acceptable signal strength of the node under consideration. When the receiver receives the RTS signal from the transmitter, it attaches to the CTS the ratio information calculated and sends it back to the sender. Similarly, when the sender gets the CTS packet, it includes the ratio in the Data frame and sends it to the receiver. Thus in a single transmission of RTS-CTS-Data-ACK exchange, both the sender and the receiver learn about the transmit power levels of each other.



Modifications to IEEE 802.11.

SYSTEM POWER MANAGEMENT SCHEMES

This power can be conserved significantly by applying the following schemes:

- Processor power management schemes
- Device power management schemes

Processor Power Management Schemes

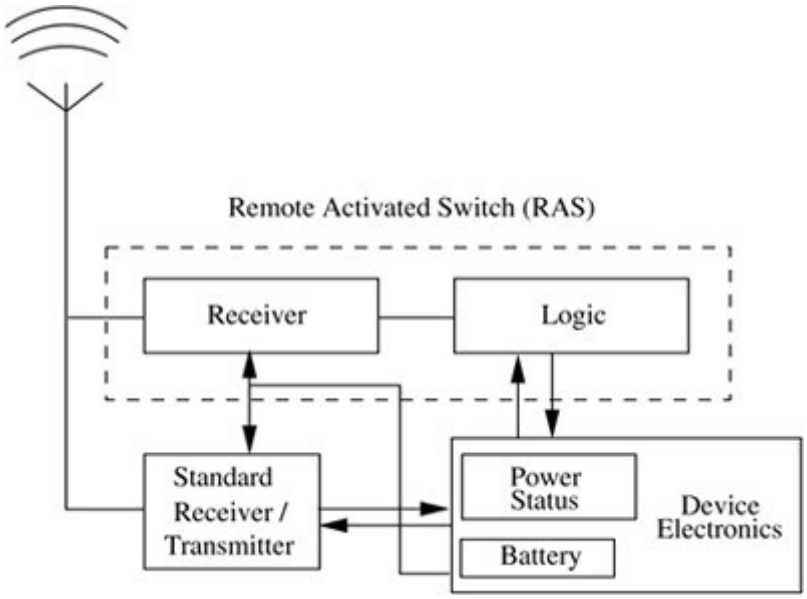
Processor power management schemes deal with techniques that try to reduce the power consumed by the processor, such as reducing the number of calculations performed.

Power-Saving Modes

The nodes in an ad hoc wireless network consume a substantial amount of power even when they are in an idle state since they keep listening to the channel, awaiting request packets from the neighbours. In order to avoid this, the nodes are switched off during idle conditions and switched on only when there is an arrival of a request packet.

This primarily has two advantages: **reducing the wastage in power** consumed when the node is in the listen mode, and **providing idle time** for the batteries of the node to recover charges.

To implement the remote activation of the nodes, a switch called remote activated switch (RAS) is used, as shown in Figure. As soon as the node enters the idle state, it is switched off by the RAS switch. The receiver of the RAS switch still listens to the channel. It is designed to be either fully passive or powered by the battery. The remote neighbours send the wake-up signal and a sequence. The receiver, on receiving the wake-up signal, detects the sequence. The logic circuit compares it with the standard sequence for the node. It switches on the node only if both the sequences match.



Remote activated switch.

Device Power Management Schemes

Some of the major consumers of power in ad hoc wireless networks are the hardware devices present in the nodes. Various schemes have been proposed in the design of hardware that minimizes the power consumption.

Low-Power Design of Hardware

Low-power design of hardware results in a significant improvement in the energy conservation. Some of the low-power design suggestions include varying clock speed CPUs, disk spin down, and flash memory.

We now look into some of the sources of power consumption in the ad hoc wireless networks and the corresponding solutions to reduce power consumption.

CPU Power Consumption

The energy required for the CPU operation depends largely on the clock frequency (F). As the clock rate increases, frequent switching of the logic gates between different voltage levels (V), that is, the ground voltage and the peak voltage, takes place, which leads to higher power consumption.

The larger the capacitance (*C*) of these transistors, the higher the energy required. Hence, the total power required by the CPU is proportional to *CV2F*. **The solution suggested is as follows**:

• The parameter *C* can be set during the chip design.
• The values of *F* and *V* can be set dynamically at run-time which, along with power-aware CPU scheduling policies, reduces the power consumption significantly.

Hard Disk Drive (HDD) Power Consumption

As mentioned earlier, the basic source for power consumption in hard disks is the disk spin. Various approaches have been suggested for turning off the drives and to bring down the speed of spinning. We now see how the spin-down can be performed on the disk drives.

By using historical data: One method suggested is based on the traces of disk usage collected over a long period of time. By analyzing various spin-down thresholds, an optimal value for threshold has to be agreed upon, which acts as a balance between the two contradictory requirements of reducing power consumption and reducing the access delays.

UNIT-5

WIRELESS SENSOR NETWORKS

Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity.

Each node of the sensor network consists of three subsystems: the sensor subsystem which senses the environment, the processing subsystem which performs local computations on the sensed data, and the communication subsystem which is responsible for message exchange with neighboring sensor nodes.

Applications of Sensor Networks

Sensor nodes are used in a variety of applications which require constant monitoring and detection of specific events. The military applications of sensor nodes include battlefield surveillance and monitoring, guidance systems of intelligent missiles, and detection of attack by weapons of mass destruction, such as chemical, biological, or nuclear.

Sensors are also used in environmental applications such as forest fire and flood detection, and habitat exploration of animals. Sensors can be extremely useful in patient diagnosis and monitoring. Patients can wear small sensor devices that monitor their physiological data such as heart rate or blood pressure.

Comparison with Ad Hoc Wireless Networks

While both ad hoc wireless networks and sensor networks consist of wireless nodes communicating with each other, there are certain challenges posed by sensor networks. The number of nodes in a sensor network can be several orders of magnitude larger than the number of nodes in an ad hoc network. Sensor nodes are more prone to failure and energy drain, and their battery sources are usually not replaceable or rechargeable. Sensor nodes may not have unique global identifiers, so unique addressing is not always feasible in sensor networks.

Issues and Challenges in Designing a Sensor Network

Sensor networks pose certain design challenges due to the following reasons:

• Sensor nodes are randomly deployed and hence do not fit into any regular topology. Once deployed, they usually do not require any human intervention. Hence, the setup and maintenance of the network should be entirely autonomous.

• Sensor networks are infrastructure-less. Therefore, all routing and maintenance algorithms need to be distributed.

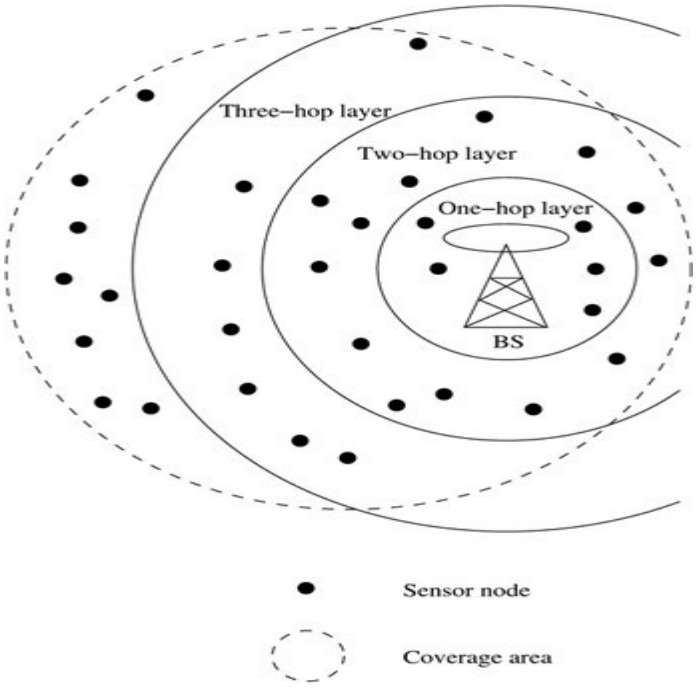
- Hardware design for sensor nodes should also consider energy efficiency as a primary requirement.
- Provisions must be made for secure communication over sensor networks, especially for military applications which carry sensitive data.

SENSOR NETWORK ARCHITECTURE

The two basic kinds of sensor network architecture are layered and clustered.

Layered Architecture

A layered architecture has a single powerful base station (BS), and the layers of sensor nodes around it correspond to the nodes that have the same hop-count to the BS.



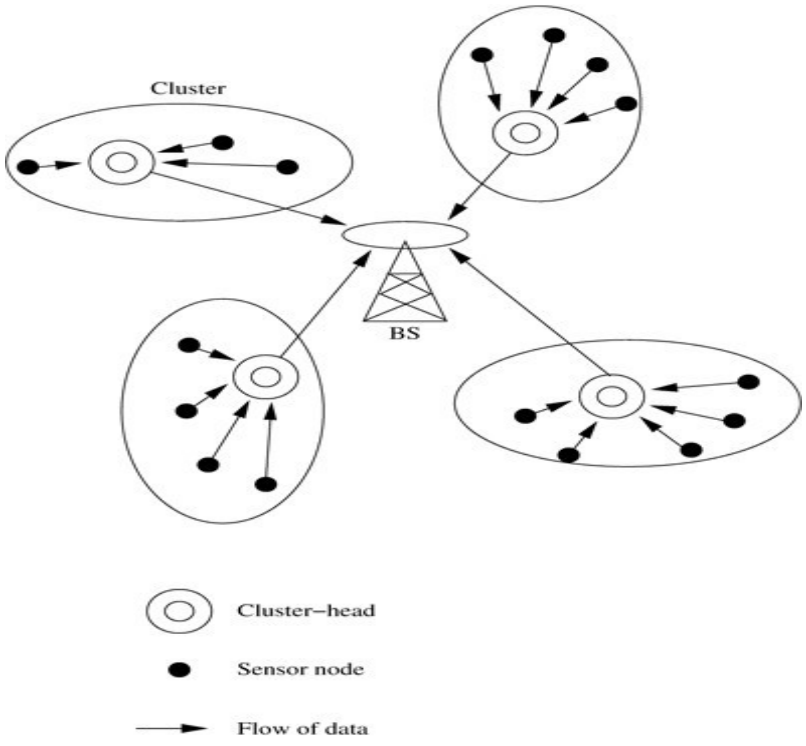
Layered architecture

Layered architectures have been used with in-building wireless backbones, and in military sensor-based infrastructure, such as the multi-hop infrastructure network architecture (MINA). In the in-building scenario, the BS acts an an access point to a wired network, and small nodes form a wireless backbone to provide wireless connectivity. The users of the network have hand-held devices such as PDAs which communicate via the small nodes to the BS. Similarly, in a military operation, the BS is a data-gathering and processing entity with a communication link to a larger network. A set of wireless sensor nodes is accessed by the hand-held devices of the soldiers. The advantage of a layered architecture is that each node is involved only in short-distance, low-power transmissions to nodes of the neighboring layers.

Unified Network Protocol Framework is a set of protocols for complete implementation of a layered architecture for sensor networks.

Clustered Architecture

A clustered architecture organizes the sensor nodes into clusters, each governed by a cluster-head. The nodes in each cluster are involved in message exchanges with their respective cluster-heads, and these heads send messages to a BS, which is usually an access point connected to a wired network.



Clustered architecture.

Clustered architecture is especially useful for sensor networks because of its inherent suitability for data fusion. The data gathered by all members of the cluster can be fused at the cluster-head, and only the resulting information needs to be communicated to the BS.

DATA DISSEMINATION

Data dissemination is the process by which queries or data are routed in the sensor network. The data collected by sensor nodes has to be communicated to the BS or to any other node interested in the data. The node that generates data is called a *source* and the information to be reported is called an *event.* A node which is interested in an event and seeks information about it is called a *sink.* Traffic models have been developed for sensor networks such as the data collection and data dissemination (diffusion) models.

In the data collection model, the source sends the data it collects to a collection entity such as the BS.This could be periodic or on demand. The data is processed in the central collection entity.

Some data dissemination techniques are,

Flooding

In flooding, each node which receives a packet broadcasts it if the maximum hop-count of the packet is not reached and the node itself is not the destination of the packet. This technique does not require complex topology maintenance or route discovery algorithms.

Gossiping

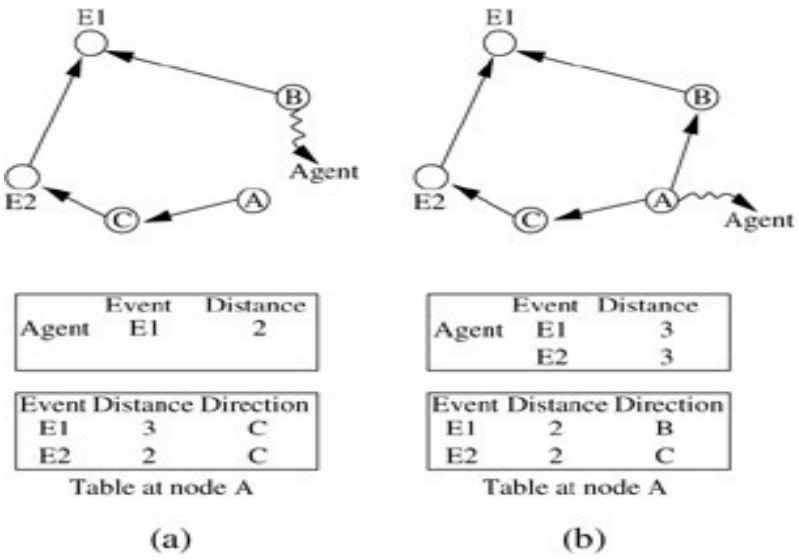
Gossiping is a modified version of flooding, where the nodes do not broadcast a packet, but send it to a randomly selected neighbor. This avoids the problem of implosion, but it takes a long time for a message to propagate throughout the network.

Rumor Routing

Rumor routing is an agent-based path creation algorithm. These are basically packets which are circulated in the network to establish shortest paths to events that they encounter. They can also perform path optimizations at nodes that they visit. When an agent finds a node whose path to an event is longer than its own, it updates the node's routing table.

Figure illustrates the working of the rumor routing algorithm. In Figure 12.4 (a), the agent has initially recorded a path of distance 2 to event $E1$. Node A's table shows that it is at a distance 3 from event $E1$ and a distance 2 from $E2$. When the agent visits node A, it updates

its own path state information to include the path to event *E*2. The updating is with one hop greater distance than what it found in *A,* to account for the hop between any neighbor of *A* that the agent will visit next, and *A*. It also optimizes the path to *E*1 recorded at node *A* to the shorter path through node *B*. The updated status of the agent and node table is shown in Figure 12.4 (b).



DATA GATHERING

The objective of the data-gathering problem is to transmit the sensed data from each sensor node to aBS. One round is defined as the BS collecting data from all the sensor nodes once. The goal of algorithms which implement data gathering is to maximize the number of rounds of communication before the nodes die and the network becomes inoperable.

A few algorithms that implement data gathering are discussed below.

Direct Transmission

All sensor nodes transmit their data directly to the BS. This is extremely expensive in terms of energy consumed, since the BS may be very far away from some nodes. Also, nodes must take turns while transmitting to the BS to avoid collision, so the media access delay is also large.

Power-Efficient Gathering for Sensor Information Systems

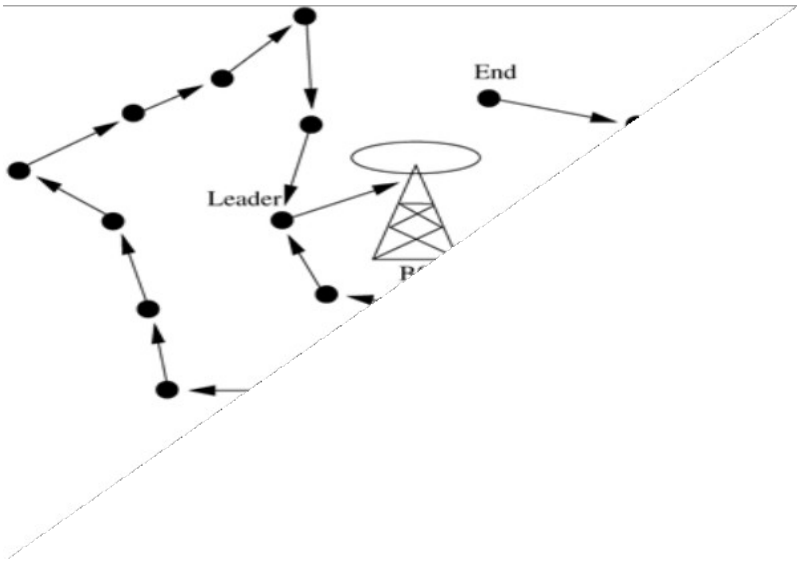
Power-efficient gathering for sensor information systems (PEGASIS) is a data-gathering protocol based on the assumption that all sensor nodes know the location of every other node, that is, the topology information is available to all nodes.

The goals of PEGASIS are as follows:

- Minimize the distance over which each node transmits
- Minimize the broadcasting overhead
- Minimize the number of messages that need to be sent to the BS
- Distribute the energy consumption equally across all nodes.

A greedy algorithm is used to construct a chain of sensor nodes, starting from the node farthest from the BS. At each step, the nearest neighbor which has not been visited is added to the chain. The chain is constructed *a priori*, before data transmission begins, and is reconstructed when nodes die out. At every node, data fusion or aggregation is carried out, so that only one message is passed on from one node to the next.

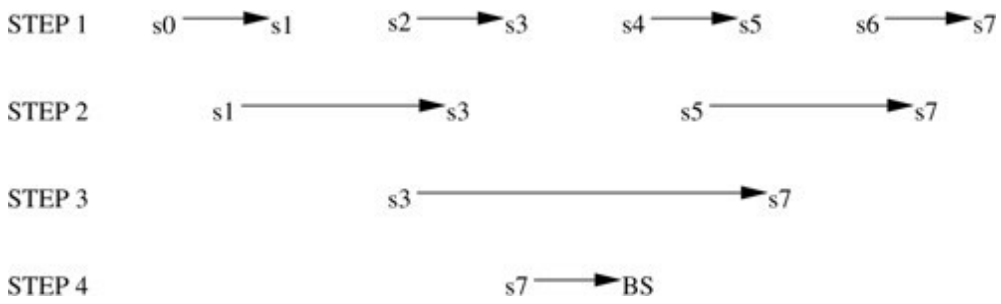
A node which is designated as the leader finally transmits one message to the BS. Leadership is transferred in sequential order, and a token is passed so that the nodes know in which direction to pass messages in order to reach the leader. A possible chain formation is illustrated in below Figure.



Binary Scheme

This is also a chain-based scheme like PEGASIS, which classifies nodes into different levels. All nodes which receive messages at one level rise to the next. The number of nodes is halved from one level to the next. For instance, consider a network with eight nodes labeled *s*0 to *s*7.

As Figure shows, the aggregated data reaches the BS in four steps, which is $O(log2N)$, where N is the number of nodes in the network. This scheme is possible when nodes communicate using CDMA, so that transmissions of each level can take place simultaneously.



MAC PROTOCOLS FOR SENSOR NETWORKS

There are three basic kinds of MAC protocols used in sensor networks: fixed allocation, demand-based, and contention-based.

Fixed-allocation protocols provide a bounded delay for each node. However, in the case of bursty traffic, where the channel requirements of each node may vary over time, a fixed allocation may lead to inefficient usage of the channel.

Demand based MAC protocols are used in such cases, where the channel is allocated according to the demand of the node.

Finally, the contention based MAC protocols involve random-access-based contention for the channel when packets need to be transmitted.

Some of the popular sensor network MAC protocols are,

Self-OrganizingMAC for Sensor Networks

Self-organizing MAC for sensor (SMACS) networks and eavesdrop and register (EAR) are two protocols which handle network initialization and mobility support, respectively. In this

protocol, neighbor discovery and channel assignment take place simultaneously in a completely distributed manner.

Hybrid TDMA/FDMA

This is a centrally controlled scheme which assumes that nodes communicate directly to a nearby BS. A pure TDMA scheme minimizes the time for which a node has to be kept on, but the associated time synchronization costs are very high. A pure FDMA scheme allots the minimum required bandwidth for each connection.

CSMA-Based MAC Protocols

Traditional CSMA-based schemes are more suitable for point-to-point stochastically distributed traffic flows. On the other hand, sensor networks have variable but periodic and correlated traffic.

The sensing periods of CSMA are constant for energy efficiency, while the back-off is random to avoid repeated collisions. Binary exponential back-off is used to maintain fairness in the network. An adaptive transmission rate control (ARC) is also used, which balances originating and route-through traffic in nodes.

Hence, CSMA based MAC protocols are contention-based and are designed mainly to increase energy efficiency and maintain fairness.

LOCATION DISCOVERY

Two basic mechanisms of location discovery are now described.

Indoor Localization

Indoor localization techniques use a fixed infrastructure to estimate the location of sensor nodes. Fixed beacon nodes are strategically placed in the field of observation, typically indoors, such as within a building. The randomly distributed sensors receive beacon signals from the beacon nodes and measure the signal strength, angle of arrival, and time difference between the arrival of different beacon signals. Using the measurements from multiple beacons, the nodes estimate their location.

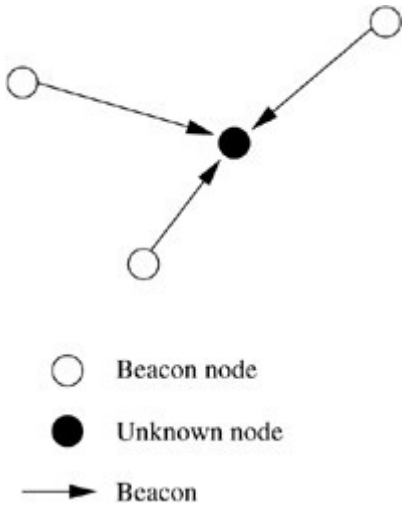
Sensor Network Localization

In situations where there is no fixed infrastructure available and prior measurements are not possible, some of the sensor nodes themselves act as beacons. They have their location information, using GPS, and these send periodic beacons to other nodes. In the case of communication using RF signals, the received signal strength indicator (RSSI) can be used to estimate the distance.

Localization algorithms require techniques for location estimation depending on the beacon nodes' location. These are called multi-lateration (ML) techniques. Some simple ML techniques are,

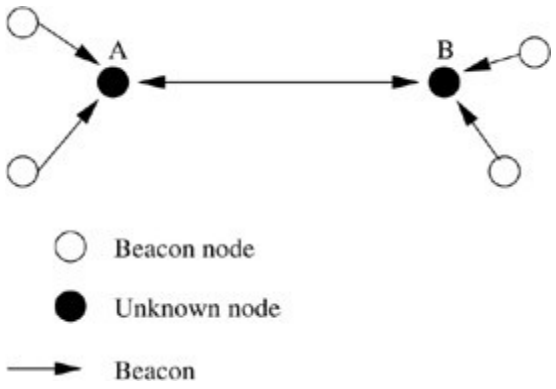
- Atomic ML
- Iterative ML
- Collaborative ML

Atomic ML: If a node receives three beacons, it can determine its position by a mechanism similar to GPS.



Iterative ML: Some nodes may not be in the direct range of three beacons. Once a node estimates its location, it sends out a beacon, which enables some other nodes to now receive at least three beacons. Iteratively, all nodes in the network can estimate their location.

Collaborative ML: When two or more nodes cannot receive at least three beacons each, they collaborate with each other.



QUALITY OF A SENSOR NETWORK

The purpose of a sensor network is to monitor and report events or phenomena taking place in a particular area. Hence, the main parameters which define how well the network observes a given area are "coverage" and "exposure."

Coverage

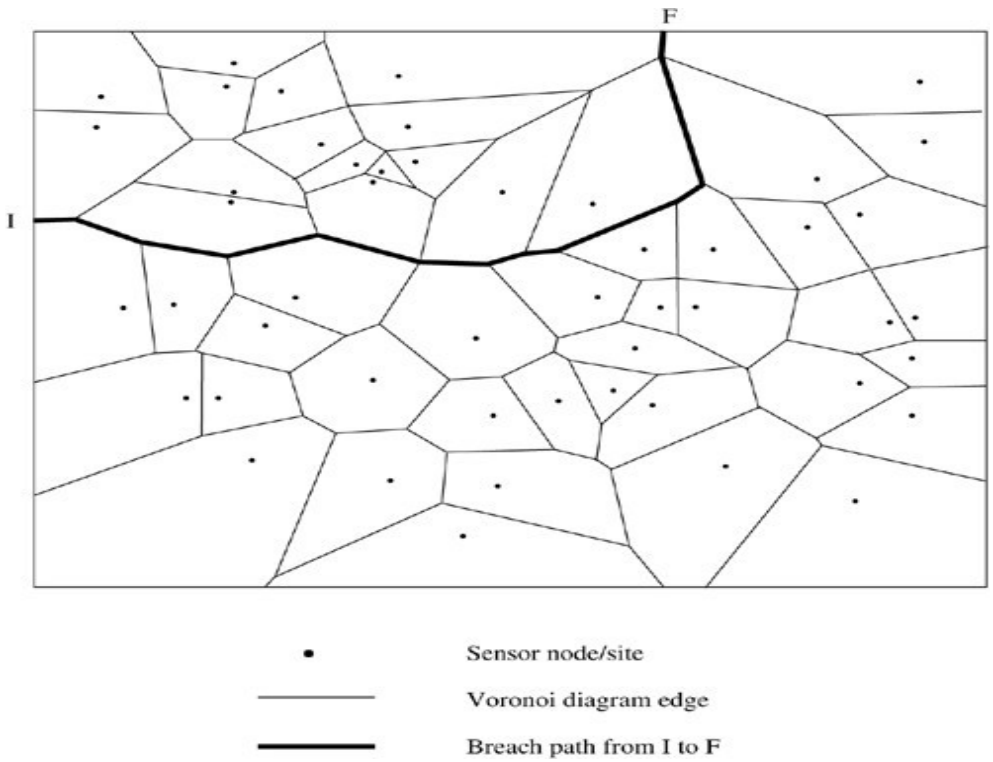
Coverage is a measure of how well the network can observe or cover an event. Coverage depends upon the range and sensitivity of the sensing nodes, and the location and density of the sensing nodes in the given region.

The *worstcase* coverage defines areas of breach, that is, where coverage is the poorest. The*best-case* coverage, on the other hand, defines the areas of best coverage.

The coverage problem is formally defined as follows: Given a field *A* with a set of sensors *S* = {*s*1 , *s*2 , ...,*sn*}, where for each sensor *si* in *S*, its location coordinates (*xi* , *yi*) are known, based on localization techniques.

Areas *I* and *F* are the initial and final locations of an intruder traversing the field. The problem is to identify *PB* , the maximal breach path starting in *I* and ending in *F*. *PB* is defined as the locus of points *p* in the region *A*, where *p* is in *PB* if the distance from *p* to the closest sensor is maximized.

A mathematical technique to solve the coverage problem is the Voronoi diagram. It can be proved that the path *PB* will be composed of line segments that belong to the Voronoi diagram corresponding to the sensor graph. In two dimensions, the Voronoi diagram of a set of sites is a partitioning of the plane into a set of convex polygons such that all points inside a polygon are closest to the site enclosed by the polygon, and the polygons have edges equidistant from the nearby sites. A Voronoi diagram for a sensor network, and a breach path from *I* to *F,* are shown in Figure.



The algorithm to find the breach path *PB* is:

• Generate the Voronoi diagram, with the set of vertices *V* and the set of edges *E.* This is done by drawing the perpendicular bisectors of every line segment joining two sites, and using their points of intersection as the vertices of the convex polygons.
• Create a weighted graph with vertices from *V* and edges from *E,* such that the weight of each edge in the graph is the minimum distance from all sensors in *S.* The edge weights represent the distance from the nearest sensor. Smaller edge weights imply better coverage along the edge.
• Determine the maximum cost path from *I* to *F,* using breadth-first search.

The maximum cost implies least coverage.

EVOLVING STANDARDS

Standards for sensor networks are at an incipient stage. The IEEE 802.15.4 low rate wireless personal area networks (LR-WPANs) standard [24] investigates a low data rate solution with multi-month to multi-year battery life and very low complexity. It is intended to operate in an unlicensed, international frequency band.

This standard aims to define the physical and MAC layer specifications for sensor and other WPANnetworks. Low power consumption is an important feature targeted by the standard. This requires reduced transmission rate, power efficient modulation techniques, and strict power management techniques such as sleep modes.