Reliable Data Delivery

802.11 physical and MAC layers unreliable
- noise, interference, and other propagation effects result in loss of frames
- even with error-correction codes, frames may not successfully be received

can be dealt with at a higher layer

more efficient to deal with errors at MAC level

802.11 includes frame exchange protocol
- station receiving frame returns acknowledgment (ACK) frame
- exchange treated as atomic unit
- if no ACK within short period of time, retransmit

Four Frame Exchange

RTS alerts all stations within range of source that exchange is under way

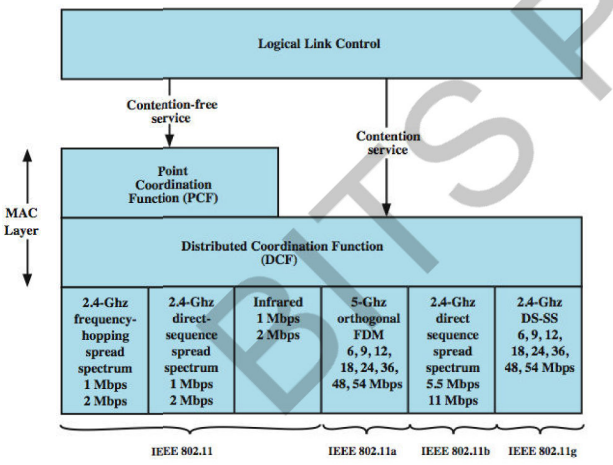
CTS alerts all stations within range of destination

other stations don't transmit to avoid collision

RTS/CTS exchange is required function of MAC but may be disabled

•can use four-frame exchange for better reliability
- source issues a Request to Send (RTS) frame
- destination responds with Clear to Send (CTS)
- after receiving CTS, source transmits data
- destination responds with ACK

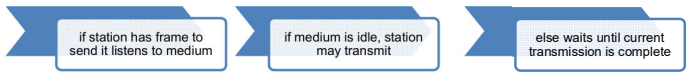
Media Access Control



Distributed Coordination Function

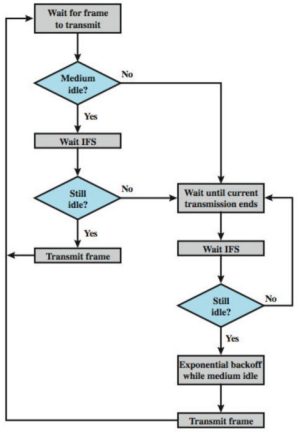
DCF sublayer uses CSMA

no collision detection since on a wireless network
DCF includes delays that act as a priority scheme



innovate achieve lead

IEEE 802.11 Medium Access Control Logic



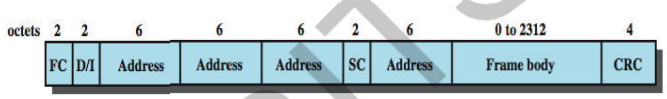
Priority IFS Values

SIFS (short IFS)
- for all immediate response actions

PIFS (point coordination function IFS)
- used by the centralized controller in PCF scheme when issuing polls

DIFS (distributed coordination function IFS)
- used as minimum delay for asynchronous frames contending for access

IEEE 802.11 MAC Frame Format



FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control

Control Frames

Power Save-Poll (PS-Poll)
- request AP transmit buffered frame when in power-saving mode

Request to Send (RTS)
- first frame in four-way frame exchange

Clear to Send (CTS)
- second frame in four-way exchange

Acknowledgment (ACK)
- acknowledges correct receipt

Contention-Free (CF)-end
- announces end of contention-free period part of

CF-End + CF-Ack:
- acknowledges CF-end to end contention-free period and release stations from associated restrictions

innovate achieve lead

Data Frames – Not Data Carrying

- Null Function
  - carries no data, polls, or acknowledgments
  - carries power management bit in frame control field to AP
  - indicates station is changing to low-power state
- other three frames (CF-Ack, CF-Poll, CF-Ack + CF-Poll) same as corresponding frame in preceding list but without data

Management Frames

used to manage communications between stations and Aps

management of associations

- requests, response, reassociation, dissociation, and authentication

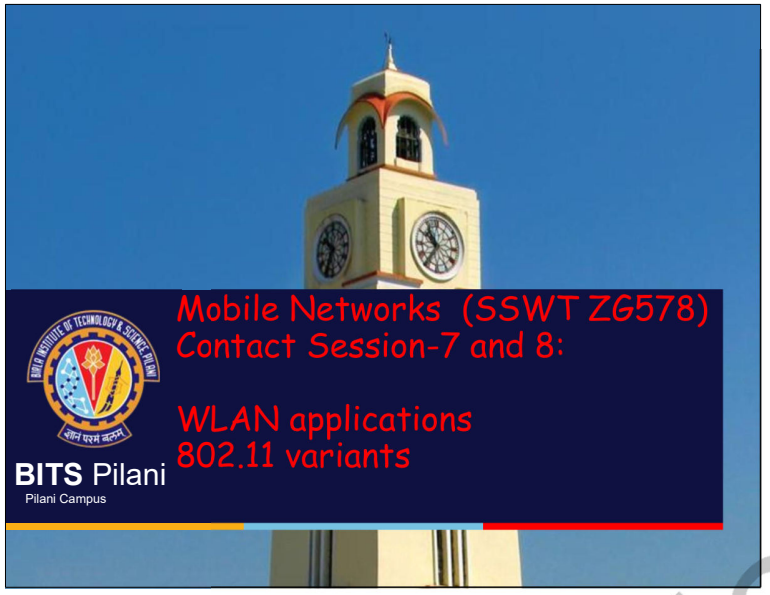
Original 802.11 Physical Layer - DSSS

- Direct-sequence spread spectrum (DSSS)
- 2.4 GHz ISM band at 1 Mbps and 2 Mbps
- up to seven channels, each 1 Mbps or 2 Mbps, can be used
- depends on bandwidth allocated by various national regulations
  - 13 in most European countries
  - one in Japan
- each channel bandwidth 5 MHz
- encoding scheme DBPSK for 1-Mbps and DQPSK for 2-Mbps using an 11-chip Barker sequence

Original 802.11 Physical Layer - FHSS

- Frequency-hopping spread spectrum
  - makes use of multiple channels
  - signal hopping between multiple channels based on a pseudonoise sequence
  - 1-MHz channels are used
- hopping scheme is adjustable
  - 2.5 hops per second in United States
  - 6 MHz in North America and Europe
  - 5 MHz in Japan
- two-level Gaussian FSK modulation for 1 Mbps
- four-level GFSK modulation used for 2 Mbps

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES



Wireless and Mobile Networks

innovate achieve lead

Background:

wireless (mobile) phone subscribers now exceeds # wired phone subscribers!

computer nets: laptops, palmtops, PDAs, Internet-enabled phone promise anytime untethered Internet access

two important (but different) challenges

- *wireless:* communication over wireless link
- *mobility:* handling the mobile user who changes point of attachment to network

Mobile Communication Technology according to IEEE

innovate achieve lead

802.11a → 802.11h
802.11i/e/…/w
802.11b → 802.11g

Personal wireless nw
WPAN 802.15

ZigBee
802.15.4 → 802.15.4a/b
802.15.5
802.15.1
802.15.2
802.15.3 → 802.15.3a/b
Bluetooth

Wireless distribution networks
WMAN 802.16 (Broadband Wireless Access)

WiMAX
+ Mobility
802.20 (Mobile Broadband Wireless Access)

Characteristics of wireless LANs

innovate achieve lead

Advantages
- very flexible within reception area
- Ad-hoc networks do not need planning
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- more robust against disasters like, e.g., earthquakes, fire

Disadvantages
- low bandwidth compared to wired networks (1-10 Mbit/s)
- many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
- many national restrictions for wireless, long time to establish global solutions like, e.g., IMT-2000

innovate achieve lead

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary

Comparison: infrared vs. radio transmission

Infrared
- uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)

Advantages
- simple, cheap, available in many mobile devices
- no licenses needed
- simple shielding possible

Disadvantages
- interference by sunlight, heat sources etc.
- many things shield or absorb IR light
- low bandwidth

Example
- IrDA (Infrared Data Association) interface available everywhere

Radio
- typically using the license free ISM band at 2.4 GHz

Advantages
- experience from wireless WAN and mobile phones can be used
- coverage of larger areas possible (radio can penetrate walls, furniture etc.)

Disadvantages
- limited license free frequency bands
- shielding more difficult, electrical interference

Example
- Many different products

WLAN: IEEE 802.11b

Data rate
- 1, 2, 5.5, 11 Mbit/s, depending on SNR
- User data rate max. approx. 6 Mbit/s

Transmission range
- 300m outdoor, 30m indoor
- Max. data rate ~10m indoor

Frequency
- Free 2.4 GHz ISM-band

Security
- Limited, WEP insecure, SSID

Availability
- Many products, many vendors

Connection set-up time
- Connectionless/always on

Quality of Service
- Typ. Best effort, no guarantees (unless polling is used, limited support in products)

Manageability
- Limited (no automated key distribution, sym. Encryption)

Special Advantages/Disadvantages
- Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
- Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

WLAN: IEEE 802.11a

Data rate
- 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
- User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
- 6, 12, 24 Mbit/s mandatory

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-band

Security
- Limited, WEP insecure, SSID

Availability
- Some products, some vendors

Connection set-up time
- Connectionless/always on

Quality of Service
- Typ. best effort, no guarantees (same as all 802.11 products)

Manageability
- Limited (no automated key distribution, sym. Encryption)

Special Advantages/Disadvantages
- Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
- Disadvantage: stronger shading due to higher frequency, no QoS

innovate achieve lead

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

WLAN: IEEE 802.11 – future developments (03/2005)

innovate achieve lead

802.11c: Bridge Support
- Definition of MAC procedures to support bridges as extension to 802.1D

802.11d: Regulatory Domain Update
- Support of additional regulations related to channel selection, hopping sequences

802.11e: MAC Enhancements – QoS
- Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
- Definition of a data flow ("connection") with parameters like rate, burst, period…
- Additional energy saving mechanisms and more efficient retransmission

802.11f: Inter-Access Point Protocol
- Establish an Inter-Access Point Protocol for data exchange via the distribution system
- Currently unclear to which extend manufacturers will follow this suggestion

802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM
- Successful successor of 802.11b, performance loss during mixed operation with 11b

802.11h: Spectrum Managed 802.11a
- Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)

WLAN: IEEE 802.11- future developments (03/2005)

innovate achieve lead

802.11i: Enhanced Security Mechanisms
- Enhance the current 802.11 MAC to provide improvements in security.
- TKIP enhances the insecure WEP, but remains compatible to older WEP systems
- AES provides a secure encryption method and is based on new hardware

802.11j: Extensions for operations in Japan
- Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range

802.11k: Methods for channel measurements
- Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel

802.11m: Updates of the 802.11 standards

802.11n: Higher data rates above 100Mbit/s
- Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
- MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
- However, still a large overhead due to protocol headers and inefficient mechanisms

802.11p: Inter car communications
- Communication between cars/road side and cars/cars
- Planned for relative speeds of min. 200km/h and ranges over 1000m
- Usage of 5.850-5.925GHz band in North America

WLAN: IEEE 802.11– future developments (03/2005)

innovate achieve lead

802.11r: Faster Handover between BSS
- Secure, fast handover of a station from one AP to another within an ESS
- Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
- Handover should be feasible within 50ms in order to support multimedia applications efficiently

802.11s: Mesh Networking
- Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
- Support of point-to-point and broadcast communication across several hops

802.11t: Performance evaluation of 802.11 networks
- Standardization of performance measurement schemes

802.11u: Interworking with additional external networks

802.11v: Network management
- Extensions of current management functions, channel measurements
- Definition of a unified interface

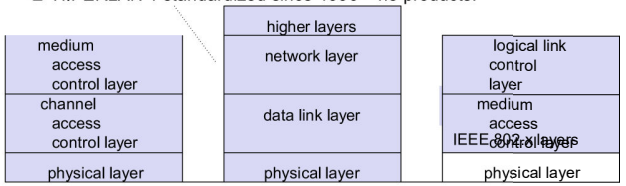
802.11w: Securing of network control
- Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.

Note: Not all "standards" will end in products, many ideas get stuck at working group level
Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/getieee802/

innovate achieve lead

ETSI standard
- European standard, cf. GSM, DECT, ...
- Enhancement of local Networks and interworking with fixed networks
- integration of time-sensitive services from the early beginning

HIPERLAN family
- one standard cannot satisfy all requirements
  - range, bandwidth, QoS support
  - commercial constraints
- HIPERLAN 1 standardized since 1996 – no products!



innovate achieve lead

HiperLan

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

HIPERLAN 1 never reached product status,
the other standards have been renamed/modfied !

HIPERLAN 1 - Characteristics

Data transmission
- point-to-point, point-to-multipoint, connectionless
- 23.5 Mbit/s, 1 W power, 2383 byte max. packet size

Services
- asynchronous and time-bounded services with hierarchical priorities
- compatible with ISO MAC

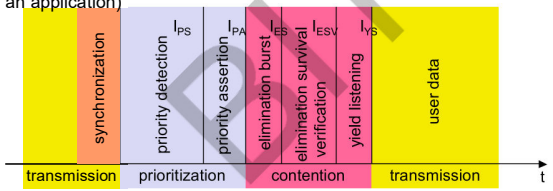
Topology
- infrastructure or ad-hoc networks
- transmission range can be larger then coverage of a single node („forwarding“ integrated in mobile terminals)

Further mechanisms
- power saving, encryption, checksums

HIPERLAN 1 - CAC sublayer

Channel Access Control (CAC)
- assure that terminal does not access forbidden channels
- priority scheme, access with EY-NPMA
- 3 EY-NPMA phases: priority resolution, contention resolution, transmission

Priorities
- 5 priority levels for QoS support
- QoS is mapped onto a priority level with the help of the packet lifetime (set by an application)



Some history: Why wireless ATM?

- seamless connection to wired ATM, a integrated services high-performance network supporting different types a traffic streams
- ATM networks scale well: private and corporate LANs, WAN
- B-ISDN uses ATM as backbone infrastructure and integrates several different services in one universal system
- mobile phones and mobile communications have increasing importance in everyday life
- current wireless LANs do not offer adequate support for multimedia data streams
- merging mobile communication and ATM leads to wireless ATM from a telecommunication provider point of view
- goal: seamless integration of mobility into B-ISDN

Problem: very high complexity of the system – never reached products

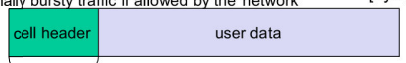
innovate achieve lead

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

ATM

- favored by the telecommunication industry for advanced high-performance networks, e.g., B-ISDN, as transport mechanism
- statistical (asynchronous, on demand) TDM (ATDM, STDM)
- cell header determines the connection the user data belongs to
- mixing of different cell-rates is possible
  - different bit-rates, constant or variable, feasible
- interesting for data sources with varying bit-rate:
  - e.g., guaranteed minimum bit-rate
  - additionally bursty traffic if allowed by the network

ATM cell:



connection identifier, checksum etc.

Cell-based transmission

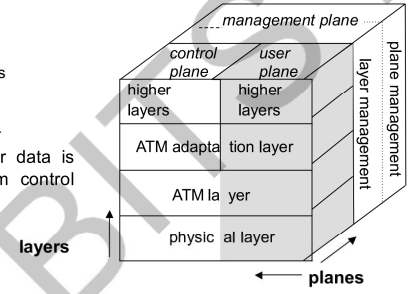
- asynchronous, cell-based transmission as basis for ATM
- continuous cell-stream
- additional cells necessary for operation and maintenance of the network (OAM cells; Operation and Maintenance)
- OAM cells can be inserted after fixed intervals to create a logical frame structure
- if a station has no data to send it automatically inserts idle cells that can be discarded at every intermediate system without further notice

B-ISDN protocol reference model

3 dimensional reference model

- three vertical planes (columns)
  - user plane
  - control plane
  - management plane
- three hierarchical layers
  - physical layer
  - ATM layer
  - ATM adaptation layer

Out-of-Band-Signaling: user data is transmitted separately from control information



ATM Forum Wireless ATM Working Group

- ATM Forum founded the *Wireless ATM Working Group* June 1996
- Task: development of specifications to enable the use of ATM technology also for wireless networks with a large coverage of current network scenarios (private and public, local and global)
- compatibility to existing ATM Forum standards important
- it should be possible to easily upgrade existing ATM networks with mobility functions and radio access
- two sub-groups of work items

Radio Access Layer (RAL) Protocols
- radio access layer
- wireless media access control
- wireless data link control
- radio resource control
- handover issues

Mobile ATM Protocol Extensions
- handover signaling
- location management
- mobile routing
- traffic and QoS Control
- network management

innovate achieve lead

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

WATM services

Office environment
- multimedia conferencing, online multimedia database access

Universities, schools, training centers
- distance learning, teaching

Industry
- database connection, surveillance, real-time factory management

Hospitals
- reliable, high-bandwidth network, medical images, remote monitoring

Home
- high-bandwidth interconnect of devices (TV, CD, PC, ...)

Networked vehicles
- trucks, aircraft etc. interconnect, platooning, intelligent roads

WATM components

WMT (Wireless Mobile ATM Terminal)
RAS (Radio Access System)
EMAS-E (End-user Mobility-supporting ATM Switch - Edge)
EMAS-N (End-user Mobility-supporting ATM Switch - Network)
M-NNI (Network-to-Network Interface with Mobility support)
LS (Location Server)
AUS (Authentication Server)

BRAN – Broadband Radio Access Networks

Motivation
- deregulation, privatization, new companies, new services
- How to reach the customer?
  - alternatives: xDSL, cable, satellite, radio

Radio access
- flexible (supports traffic mix, multiplexing for higher efficiency, can be asymmetrical)
- quick installation
- economic (incremental growth possible)

Market
- private customers (Internet access, tele-xy...)
- small and medium sized business (Internet, MM conferencing, VPN)

Scope of standardization
- access networks, indoor/campus mobility, 25-155 Mbit/s, 50 m-5 km
- coordination with ATM Forum, IETF, ETSI, IEEE, ...

innovate achieve lead

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

Broadband network types

Common characteristics
- ATM QoS (CBR, VBR, UBR, ABR)

HIPERLAN/2
- short range (< 200 m), indoor/campus, 25 Mbit/s user data rate
- access to telecommunication systems, multimedia applications, mobility (<10 m/s)

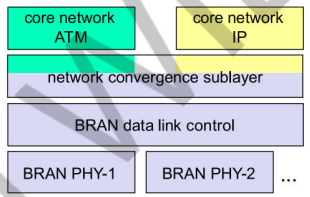
HIPERACCESS
- wider range (< 5 km), outdoor, 25 Mbit/s user data rate
- fixed radio links to customers ("last mile"), alternative to xDSL or cable modem, quick installation
- Several (proprietary) products exist with 155 Mbit/s plus QoS

HIPERLINK – currently no activities
- intermediate link, 155 Mbit/s
- connection of HIPERLAN access points or connection between HIPERACCESS nodes

BRAN and legacy networks

Independence
- BRAN as access network independent from the fixed network
- Interworking of TCP/IP and ATM under study

Layered model
- Network Convergence Sub-layer as superset of all requirements for IP and ATM



Coordination
- IETF (TCP/IP)
- ATM forum (ATM)
- ETSI (UMTS)
- CEPT, ITU-R, ... (radio frequencies)

HiperLAN2 (historical)

Official name: BRAN HIPERLAN Type 2
- H/2, HIPERLAN/2 also used

High data rates for users
- More efficient than 802.11a

Connection oriented QoS support

Dynamic frequency selection

Security support
- Strong encryption/authentication

Mobility support

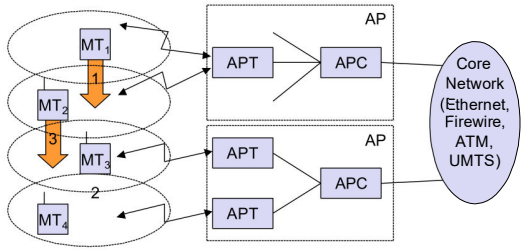
Network and application independent
- convergence layers for Ethernet, IEEE 1394, ATM, 3G

Power save modes

Plug and Play

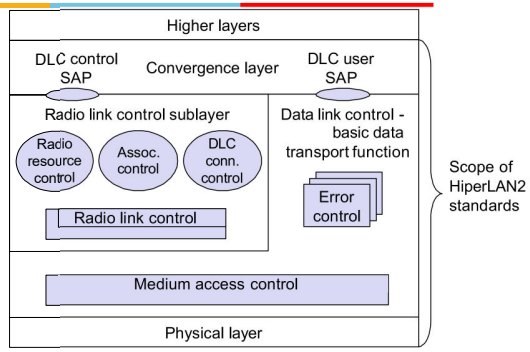
No products – but several mechanisms have been Adopted by other standards (e.g. 802.11a)

HiperLAN2 architecture and handover scenarios

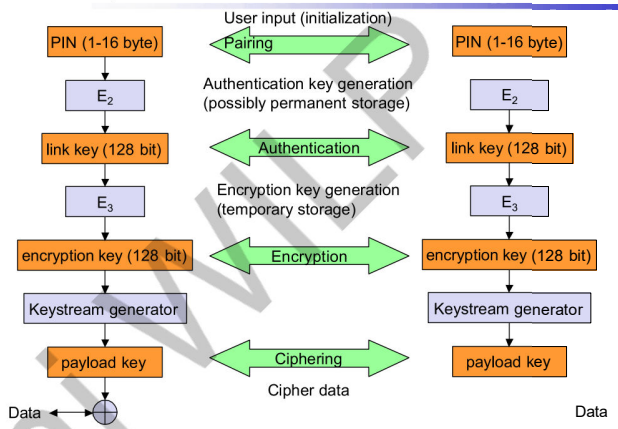


innovate achieve lead

HiperLAN2 protocol stack



Security



SDP – Service Discovery Protocol

Inquiry/response protocol for discovering services

- Searching for and browsing services in radio proximity
- Adapted to the highly dynamic environment
- Can be complemented by others like SLP, Jini, Salutation, …
- Defines discovery only, not the usage of services
- Caching of discovered services
- Gradual discovery

Additional protocols to support legacy protocols/apps.

RFCOMM

- Emulation of a serial port (supports a large base of legacy applications)
- Allows multiple ports over a single physical channel

Telephony Control Protocol Specification (TCS)

- Call control (setup, release)
- Group management

OBEX

- Exchange of objects, IrDA replacement

WAP

- Interacting with applications on cellular phones

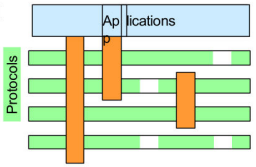
innovate achieve lead

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

Profiles

Represent default solutions for a certain usage model
- Vertical slice through the protocol stack
- Basis for interoperability

Generic Access Profile
Service Discovery Application Profile
Cordless Telephony Profile
Intercom Profile
Serial Port Profile
Headset Profile
Dial-up Networking Profile
Fax Profile
LAN Access Profile
Generic Object Exchange Profile
Object Push Profile
File Transfer Profile
Synchronization Profile



Additional Profiles
Advanced Audio Distribution
PAN
Audio Video Remote Control
Basic Printing
Basic Imaging
Extended Service Discovery
Generic Audio Video Distribution
Hands Free
Hardcopy Cable Replacement

WPAN: IEEE 802.15-1 – Bluetooth

innovate achieve lead

Data rate
- Synchronous, connection-oriented: 64 kbit/s
- Asynchronous, connectionless
  - 433.9 kbit/s symmetric
  - 723.2 / 57.6 kbit/s asymmetric

Transmission range
- POS (Personal Operating Space) up to 10 m
- with special transceivers up to 100 m

Frequency
- Free 2.4 GHz ISM-band

Security
- Challenge/response (SAFER+), hopping sequence

Availability
- Integrated into many products, several vendors

Connection set-up time
- Depends on power-mode
- Max. 2.56s, avg. 0.64s

Quality of Service
- Guarantees, ARQ/FEC

Manageability
- Public/private keys needed, key management not specified, simple system integration

Special Advantages/Disadvantages
- Advantage: already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer to peer, scatternets
- Disadvantage: interference on ISM-band, limited range, max. 8 devices/network&master, high set-up latency

WPAN: IEEE 802.15 – future developments 1

innovate achieve lead

802.15-2: Coexistence
- Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference

802.15-3: High-Rate
- Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
- Data Rates: 11, 22, 33, 44, 55 Mbit/s
- Quality of Service isochronous protocol
- Ad hoc peer-to-peer networking
- Security
- Low power consumption
- Low cost
- Designed to meet the demanding requirements of portable consumer imaging and multimedia applications

WPAN: IEEE 802.15 – future developments 3

innovate achieve lead

802.15-4: Low-Rate, Very Low-Power
- Low data rate solution with multi-month to multi-year battery life and very low complexity
- Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
- Data rates of 20-250 kbit/s, latency down to 15 ms
- Master-Slave or Peer-to-Peer operation
- Up to 254 devices or 64516 simpler nodes
- Support for critical latency devices, such as joysticks
- CSMA/CA channel access (data centric), slotted (beacon) or unslotted
- Automatic network establishment by the PAN coordinator
- Dynamic device addressing, flexible addressing format
- Fully handshaked protocol for transfer reliability
- Power management to ensure low power consumption
- 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band

Basis of the ZigBee technology – www.zigbee.org

innovate achieve lead

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

ZigBee

Relation to 802.15.4 similar to Bluetooth / 802.15.1

Pushed by Chipcon, ember, freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung

More than 150 members
- Promoter (40000$/Jahr), Participant (9500$/Jahr), Adopter (3500$/Jahr)

No free access to the specifications (only promoters and

participants) ZigBee platforms comprise
- IEEE 802.15.4 for layers 1 and 2
- ZigBee protocol stack up to the applications

802.15.5: Mesh Networking
- Partial meshes, full meshes
- Range extension, more robustness, longer battery live

Some more IEEE standards for mobile communications

innovate achieve lead

IEEE 802.16: Broadband Wireless Access / WirelessMAN / WiMax
- Wireless distribution system, e.g., for the last mile, alternative to DSL
- 75 Mbit/s up to 50 km LOS, up to 10 km NLOS; 2-66 GHz band
- Initial standards without roaming or mobility support
- 802.16e adds mobility support, allows for roaming at 150 km/h
  - Unclear relation to 802.20, 802.16 started as fixed system…

IEEE 802.20: Mobile Broadband Wireless Access (MBWA)
- Licensed bands < 3.5 GHz, optimized for IP traffic
- Peak rate > 1 Mbit/s per user
- Different mobility classes up to 250 km/h and ranges up to 15 km

IEEE 802.21: Media Independent Handover Interoperability
- Standardize handover between different 802.x and/or non 802 networks

IEEE 802.22: Wireless Regional Area Networks (WRAN)
- Radio-based PHY/MAC for use by license-exempt devices on a non-interfering basis in spectrum that is allocated to the TV Broadcast Service

WLAN: Home RF – yet another standard, no success

innovate achieve lead

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

Cost
- Adapter 130€, base station 230€

Availability
- Several products from different vendors, no more support

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

RFID – Radio Frequency Identification (1)

innovate achieve lead

Data rate
- Transmission of ID only (e.g., 48 bit, 64kbit, 1 Mbit)
- 9.6 – 115 kbit/s

Transmission range
- Passive: up to 3 m
- Active: up to 30-100 m
- Simultaneous detection of up to, e.g., 256 tags, scanning of, e.g., 40 tags/s

Frequency
- 125 kHz, 13.56 MHz, 433 MHz, 2.4 GHz, 5.8 GHz and many others

Security
- Application dependent, typ. no crypt. on RFID device

Cost
- Very cheap tags, down to 1€ (passive)

Availability
- Many products, many vendors

Connection set-up time
- Depends on product/medium access scheme (typ. 2 ms per device)

Quality of Service
- none

Manageability
- Very simple, same as serial interface

Special Advantages/Disadvantages
- Advantage: extremely low cost, large experience, high volume available, no power for passive RFIDs needed, large variety of products, relative speeds up to 300 km/h, broad temp. range
- Disadvantage: no QoS, simple denial of service, crowded ISM bands, typ. one- way (activation/ transmission of ID)

innovate achieve lead

BITS Pilani
Pilani | Dubai | Goa | Hyderabad | Mumbai
WORK INTEGRATED LEARNING PROGRAMMES

RFID – Radio Frequency Identification (2)

innovate achieve lead

Function
- Standard: In response to a radio interrogation signal from a reader (base station) the RFID tags transmit their ID
- Enhanced: additionally data can be sent to the tags, different media access schemes (collision avoidance)

Features
- No line-of sight required (compared to, e.g., laser scanners)
- RFID tags withstand difficult environmental conditions (sunlight, cold, frost, dirt etc.)
- Products available with read/write memory, smart-card capabilities

Categories
- Passive RFID: operating power comes from the reader over the air which is feasible up to distances of 3 m, low price (1€)
- Active RFID: battery powered, distances up to 100 m

RFID – Radio Frequency Identification (3)

innovate achieve lead

Applications
- Total asset visibility: tracking of goods during manufacturing, localization of pallets, goods etc.
- Loyalty cards: customers use RFID tags for payment at, e.g., gas stations, collection of buying patterns
- Automated toll collection: RFIDs mounted in windshields allow commuters to drive through toll plazas without stopping
- Others: access control, animal identification, tracking of hazardous material, inventory control, warehouse management, ...

Local Positioning Systems
- GPS useless indoors or underground, problematic in cities with high buildings
- RFID tags transmit signals, receivers estimate the tag location by measuring the signal's time of flight

RFID – Radio Frequency Identification (4)

innovate achieve lead

Security
- Denial-of-Service attacks are always possible
  - Interference of the wireless transmission, shielding of transceivers
- IDs via manufacturing or one time programming
- Key exchange via, e.g., RSA possible, encryption via, e.g., AES

Future Trends
- RTLS: Real-Time Locating System – big efforts to make total asset visibility come true
- Integration of RFID technology into the manufacturing, distribution and logistics chain
- Creation of „electronic manifests" at item or package level (embedded inexpensive passive RFID tags)
- 3D tracking of children, patients

ISM band interference

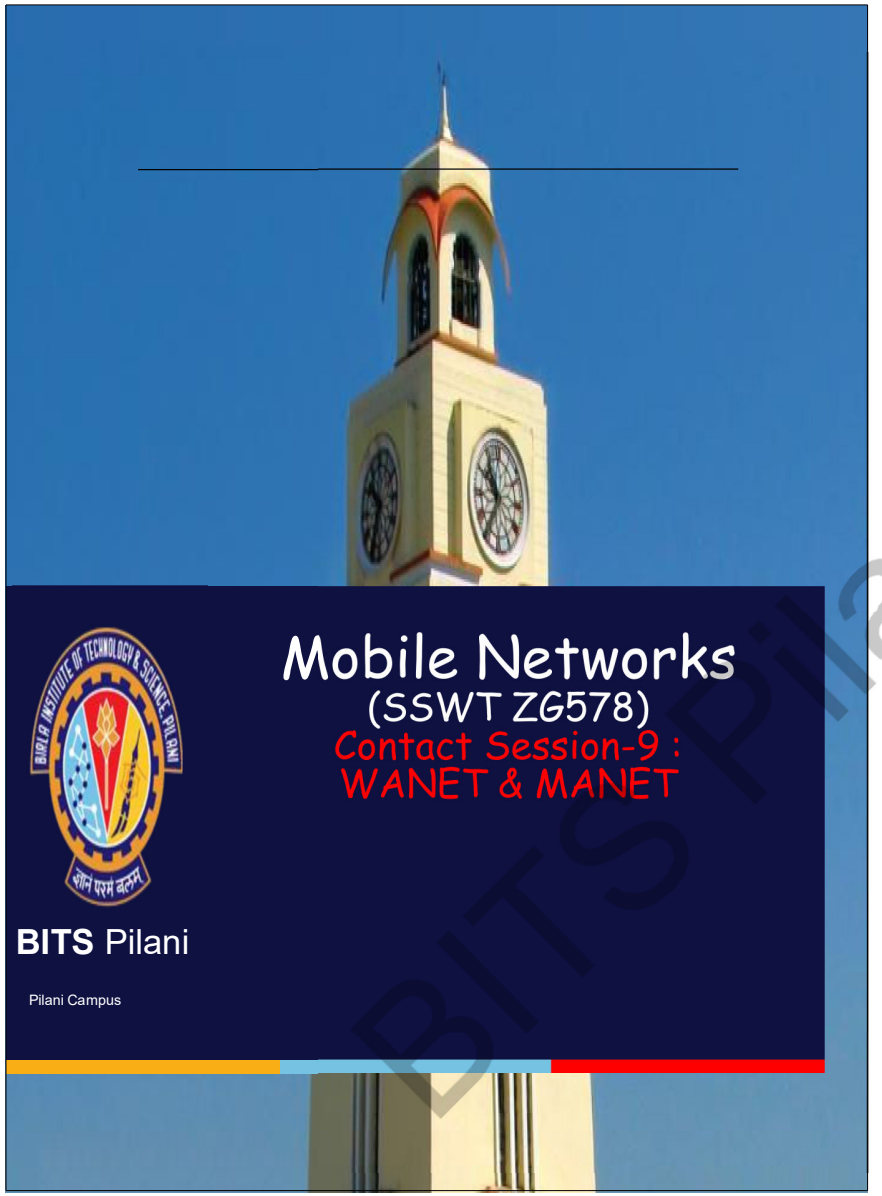
innovate achieve lead

Levels of interference
- Physical layer: interference acts like noise
  - Spread spectrum tries to minimize this
  - FEC/interleaving tries to correct
- MAC layer: algorithms not harmonized
  - E.g., Bluetooth might confuse 802.11

© Fusion Lighting, Inc.

Bluetooth may act like a rogue member of the 802.11 network
IEEE 802.15-2 discusses these problems
- Proposal: Adaptive Frequency Hopping

innovate achieve lead



AD HOC NETWORKS INTRODUCTION

innovate achieve lead

TABLE OF CONTENTS

1. Introduction
2. Elements of Ad hoc Wireless Networks
3. Issues in Ad hoc wireless networks
4. Commercial Applications of Ad Hoc Networking
5. Ad hoc wireless Internet
6. Mobile Adhoc Wireless Networks

innovate achieve lead

- The computer network uses distributed processing in which task is divided among several computers. Instead, a single computer handles an entire task, each separate computer handles a subset

Advantages of Distributed processing

- **Security:** It provides limited interaction that a user can have with the entire system. For example, a bank allows the users to access their own accounts through an ATM without allowing them to access the bank's entire database.
- **Faster problem solving:** Multiple computers can solve the problem faster than a single machine working alone.
- **Security through redundancy:** Multiple computers running the same program at the same time can provide the security through redundancy. For example, if four computers run the same program and any computer has a hardware error, then other computers can override it.

Applications of Distributed Systems

- E-mail
- Online Ticket Reservation
- Banking, etc.,

1.1.2 Types of Communication

- Communication medium refers to the physical channel through which data is sent and received. Data is sent in the form of voltage levels which make up the digital signal. A digital signal consists of 0s and 1s. There are basically two types of networks:
  - **Wired network**
- **Wireless network Wired Network**
- In a wired network, data is transmitted over a physical medium.
- There are three types of physical cables used in a wired network.
  - Twisted Pair
  - Coaxial Cable
  - Fiber Optic

  Examples: Cable TV, Broadband Telephone Communication.

Wireless Network

- A wireless network uses radio waves as the sole medium for transmitting and receiving data. There are no wires involved.
- Radio waves are electromagnetic waves which are transverse in nature and they have the longest wavelength on the electromagnetic spectrum. **Examples**: Infrared, Bluetooth, WiFi.

Elements of Ad hoc Wireless Networks

The word "ad hoc" comes from Latin Language, which means 'for this purpose only', Ad hoc Networks are the small area networks, especially designed with Wireless/Temporary connections to the different computer assisted nodes.

A wireless ad-hoc network (WANET) is a type of local area network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring a central device, such as a router or access point. When Wi- Fi networks are in ad-hoc mode, each device in the network forwards data to the others.

- Since the devices in the ad-hoc network can access each other's resources directly through a basic point-to-point wireless connection, central servers are unnecessary for functions such as file shares or printers.
- In a wireless ad-hoc network, a collection of devices (or nodes) is responsible for network operations, such as routing, security, addressing and key management. Figure 1.1 shows, multi-hop wireless ad hoc networks, it defined as a collection of nodes that communicate with each other wirelessly by using radio signals with a shared common channel.

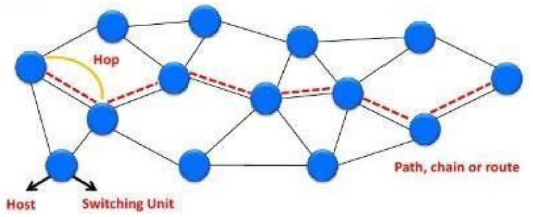


Figure 1.1 Multi- Hop Wireless Ad-Hoc Networks

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

Types of Wireless Ad Hoc Networks

Wireless ad hoc networks are categorized into different classes. They are:

- **Mobile ad hoc network (MANET)**: An ad hoc network of mobile devices.
- **Vehicular ad hoc network (VANET)**: Used for communication between vehicles. Intelligent VANETs use artificial intelligence and ad hoc technologies to communicate what should happen during accidents.
- **Smartphone ad hoc network (SPAN)**: Wireless ad hoc network created on smartphones via existing technologies like Wi-Fi and Bluetooth.
- **Wireless mesh network**: A mesh network is an ad hoc network where the various nodes are in communication directly with each other to relay information throughout the total network.
- **Army tactical MENT**: Used in the army for "on-the-move" communication, a wireless tactical ad hoc network relies on range and instant operation to establish networks when needed.
- **Wireless sensor network**: Wireless sensors that collect everything from temperature and pressure readings to noise and humidity levels, can form an ad hoc network to deliver information to a home base without needing to connect directly to it.
- **Disaster rescue ad hoc network**: Ad hoc networks are important when disaster strikes and established communication hardware isn't functioning properly.

Advantages of Ad Hoc Networks

- Ad-hoc networks can have more flexibility.
- It is better in mobility.
- It can be turn up and turn down in a very short time.
- More economical
- It considered as a robust network because of its non-hierarchical distributed control and management mechanisms.

Disadvantages of Ad Hoc Networks

- Unpredictable Topology
- Limited Bandwidth
- Lose of data
- Interference
- Limited Security
- Energy Constraints

1.3 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 Control (MAC)
- Routing
- Multicasting
- Transport layer protocol
- Quality of Service (QOS)
- Self-organization
- Security
- Energy management
- Addressing and service discovery
- Scalability
- Deployment considerations

1.3.1 Medium Access Control

The purpose of this protocol is to achieve a distributed FIFO schedule among multiple nodes in an ad hoc network. When a node transmits a packet, it adds the information about the arrival time of queued packets. It provide fair access to shared broadcast radio channel. The major issues in MAC protocol are as follows:

- **Distributed Operation:** The MAC protocol design should be fully distributed involving minimum control overhead, because it need to operate in environment without centralized device.
- **Synchronization:** The synchronization is mandatory for TDMA-based systems for management of transmission and reception slots.
- **Hidden Terminals Problem:** 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. (Figure 1.2)

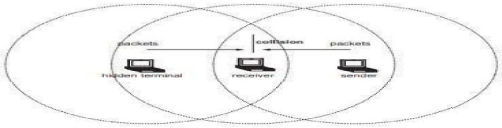


Figure 1.2 Hidden Terminal Problem

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- Collisions at receiver node -> inefficient bandwidth utilization, reduce throughput.

- **Exposed Terminals Problem:** The nodes that are in the transmission range of the sender of an on-going session, are prevented from making a transmission. The exposed nodes should be allowed to transmit in a controlled fashion without causing collision to the on-going data transfer. (Figure 1.3)

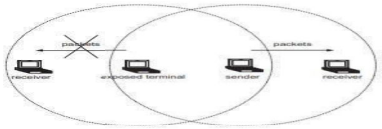


Figure 1.3 Exposed Terminal Problem

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- **Throughput:** The MAC protocol employed in ad hoc wireless networks should attempt to maximize the throughput of the system. The important considerations for throughput enhancement are
  - Minimizing the occurrence of collisions.
  - Maximizing channel utilization
  - Minimizing control overhead.
- **Access delay:** 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.
- **Ability to measure resource availability:** In order to handle the resources such as bandwidth efficiently and perform call admission control based on their availability, the MAC protocol should be able to provide an estimation of resource availability at every node. This can also be used for making congestion control decisions.
- **Capability for power control:** The transmission power control reduces the energy consumption at the nodes, causes a decrease in interference at neighboring nodes, and increases frequency reuse.
- **Adaptive rate control:** This refers to the variation in the data bit rate achieved over a channel. A MAC protocol that has adaptive rate control can make use of a high data rate when the sender and receiver are nearby & adaptively reduce the data rate as they move away from each other.

1.3.2 Routing

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

- **Mobility:** The Mobility of nodes results in frequent path breaks, packet collisions, transient loops, stale routing information, and difficulty in resource reservation.
- **Bandwidth constraint:** Since the channel is shared by all nodes in the broadcast region, the bandwidth available per wireless link depends on the number of nodes & traffic they handle.
- **Error-prone and shared channel:** The Bit Error Rate (BER) in a wireless channel is very high [10^{-5} to 10^{-3}] compared to that in its wired counterparts [10^{-12} to 10^{-9}].
- **Location-dependent contention:** The load on the wireless channel varies with the number of nodes present in a given geographical region. This makes the contention for the channel high when the number of nodes increases. The high contention for the channel results in a high number of collisions & a subsequent wastage of bandwidth.

- **Other resource constraints:** The constraints on resources such as computing power, battery power, and buffer storage also limit the capability of a routing protocol.

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

- **Minimum route acquisition delay**
- **Quick route reconfiguration**
- **Loop-free routing**
- **Distributed routing approach**
- **Minimum control overhead**
- **Scalability**
- **Provisioning of QoS**
- **Support for time-sensitive traffic**
- **Security and privacy**

1.3.3 Multicasting

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

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

- **Efficient group management:** Group management refers to the process of accepting multicast session members and maintaining the connectivity among them until the session expires.
- **Scalability:** The multicast routing protocol should be able to scale for a network with a large number of node
- **Security:** Authentication of session members and prevention of non-members from gaining unauthorized information play a major role in military communications.

1.3.4 Transport Layer Protocol

The main objectives of the transport layer protocols include :

- Setting up & maintaining end-to-end connections,
- Reliable end-to-end delivery of packets,
- Flow control &
- Congestion control.

Examples of some transport layers protocols are,

a) UDP (User Datagram Protocol) :

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

b) TCP (Transmission Control Protocol):

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

1.3.5 Quality of Service (QoS)

➢ QoS is the performance level of services offered by a service provider or a network to the user.

- QoS provisioning often requires,
  - Negotiation between host & the network.
  - Resource reservation schemes.
  - Priority scheduling &
  - Call admission control.
- **QoS parameters**

Applications	Corresponding QoS parameter
1.Multimedia application	1. Bandwidth & Delay.
2.Military application	2.Security & Reliability.
3.Defense application	3.Finding trustworthy intermediate hosts & routing
4.Emergency search and rescue operations	4.Availability.
5.Hybrid wireless network	5.Maximum available link life, delay, bandwidth & channel utilization.
6.communication among the nodes in a sensor network	6.Minimum energy consumption, battery life & energy conservation

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

1.3.6 Self-Organization

One very important property that an ad hoc wireless network should exhibit is organizing & maintaining the network by itself.

The major activities that an ad hoc wireless network is required to perform for self- organization are,

- Neighbour discovery.
- Topology organization &
- Topology reorganization (updating topology information)

1.3.7 Security

Security is an important issue in ad hoc wireless network as the information can be hacked.

Attacks against network are two types

- Passive attack → Made by malicious node to obtain information transacted in the network without disrupting the operation.
- Active attack → They disrupt the operation of network.

Further active attacks are two types

- External attack: The active attacks that are executed by nodes outside the network.
- Internal attack: The active attacks that are performed by nodes belonging to the same network.

The major security threats that exist in ad hoc wireless networks are as follows :

- **Denial of service** – The attack affected by making the network resource unavailable for service to other nodes, either by consuming the bandwidth or by overloading the system.
- **Resource consumption** – The scarce availability of resources in ad hoc wireless network makes it an easy target for internal attacks, particularly aiming at consuming resources available in the network. The major types of resource consumption attacks are,
  - Energy depletion
    - ✓ Highly constrained by the energy source
    - ✓ Aimed at depleting the battery power of critical nodes.
  - Buffer overflow
    - ✓ Carried out either by filling the routing table with unwanted routing entries or by consuming the data packet buffer space with unwanted data.

- ✓ Lead to a large number of data packets being dropped, leading to the loss of critical information.

- **Host impersonation** – A compromised internal node can act as another node and respond with appropriate control packets to create wrong route entries, and can terminate the traffic meant for the intended destination node.
- **Information disclosure** – A compromised node can act as an informer by deliberate disclosure of confidential information to unauthorized nodes.
- **Interference** – A common attack in defense applications to jam the wireless communication by creating a wide spectrum noise.

8. **Addressing and Service Discovery**

Addressing & service discovery assume significance in ad hoc wireless network due to the absence of any centralised coordinator.

An address that is globally unique in the connected part of the ad hoc wireless network is required for a node in order to participate in communication.

Auto-configuration of addresses is required to allocate non-duplicate addresses to the nodes.

9. **Energy Management**

Energy management is defined as the process of managing the sources & consumers of energy in a node or in the network for enhancing the lifetime of a network.

Features of energy management are:

- Shaping the energy discharge pattern of a node's battery to enhance battery life.
- Finding routes that consumes minimum energy.
- Using distributed scheduling schemes to improve battery life.
- Handling the processor & interface devices to minimize power consumption.

➢ Energy management can be classified into the following categories:

- **Transmission power management**
  - The power consumed by the Radio Frequency (RF) module of a mobile node is determined by several factors such as
    - ✓ The state of operation.
    - ✓ The transmission power and
    - ✓ The technology used for the RF circuitry.

- **Battery energy management**
  - The battery management is aimed at extending the battery life of a node by taking advantage of its chemical properties, discharge patterns, and by the selection of a battery from a set of batteries that is available for redundancy.
- **Processor power management**
  - The clock speed and the number of instructions executed per unit time are some of the processor parameters that affect power consumption.
  - The CPU can be put into different power saving modes during low processing load conditions.
  - The CPU power can be completely turned off if the machines is idle for a long time.
- **Devices power management**
  - Intelligent device management can reduce power consumption of a mobile node significantly.
  - This can be done by the operating system (OS) by selectively powering down interface devices that are not used or by putting devices into different power saving modes, depending on their usage.

1.3.10 Scalability

➢ Scalability is the ability of the routing protocol to scale well in a network with a large number of nodes.

➢ It requires minimization of control overhead & adaptation of the routing protocol to the network size.

1.3.11 Deployment Considerations

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

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

- **Incremental deployment**
  - Deployment can be performed incrementally over geographical regions of the city.
  - The deployed part of the network starts functioning immediately after the minimum configuration is done.
- **Short deployment time**
  - Compared to wired networks, the deployment time is considerably less due to the absence of any wired links.
- **Reconfigurability**
  - The cost involved in reconfiguring a wired network covering a Metropolitan Area Network (MAN) is very high compared to that of an ad hoc wireless network covering the same service area.

4. Commercial Applications of Ad Hoc Networking

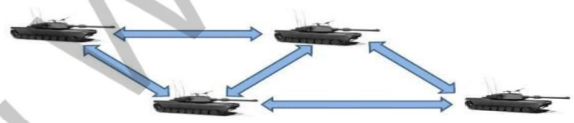
Ad Hoc wireless networks, due to their quick and economically less demanding deployment, find applications in several areas. Some important applications are:

- Military Applications
- Collaborative and Distributed computing
- Energy Operations
- Wireless Mesh Networks
  - Wireless Sensor Networks
  - Hybrid Wireless Networks

1.4.1 Military Applications

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

- The primary nature of the communication required in a military environment enforces certain important requirements on adhoc wireless networks namely, Reliability, Efficiency, Secure communication & Support for multicast routing.



Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

1.4.2 Collaborative & Distributed computing

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

1.4.3 Emergency Operations

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

- In environments, where the conventional infrastructure based communication facilities are destroyed due to a war or due to natural calamities, immediate deployment of adhoc wireless networks would be a good solution for co-ordinating rescue activities.

  They require minimum initial network configuration with very little or no delay

1.4.4 Wireless Mesh Network

Wireless mesh networks are adhoc wireless network that are formed to provide an alternate communication infrastructure for mobile or fixed nodes/users, without the spectrum reuse constraint & requirement of network planning of cellular network.(Figure 1.4)

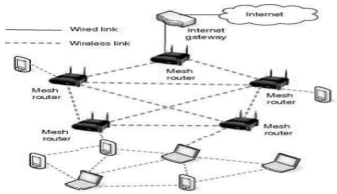


Figure 1.4 Wireless Mesh Netowrks

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- It provides many alternate paths for a data transfer session between a source & destination, resulting in quick reconfiguration of the path when the existing path fails due to node failure.
- Since the infrastructure built is in the form of small radio relaying devices, the investment required in wireless mesh networks is much less than what is required for the cellular network counterpart.
- The possible deployment scenarios of wireless mesh networks include: residential zones, highways, business zones, important civilian regions and university campuses
- Wireless mesh networks should be capable of self-organization and maintenance.
- It operates at license-free ISM band around 2.4 GHz & 5 GHz.

- It is scaled well to provide support to large number of points.
- Major advantage is the support for a high data rate, quick & low cost of deployment, enhanced services, high scalability, easy extendibility, high availability & low cost per bit.

1.4.5 Wireless Sensor Networks

- The Wireless Sensor Networks (WSN) are special category of Adhoc wireless network that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.(Figure 1.5)
- Sensor nodes are tiny devices that have capability of sensing physical parameters processing the data gathered, & communication to the monitoring system.

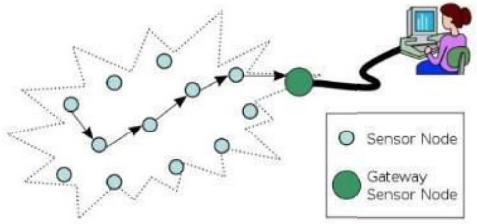


Figure 1.5 Wireless Sensor Networks

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- The issue that make sensor network a distinct category of adhoc wireless network are the following:

Mobility of nodes

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

Size of the network

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

Density of deployment

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

Power constraints

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

Data / Information fusion

- Data fusion refers to the aggregation of multiple packets into one before relaying it.

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

Traffic Distribution

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

1.4.6 Hybrid Wireless Networks

- One of the major application area of ad hoc wireless network is in the hybrid wireless architecture such as Multi-hop Cellular Network [MCN] & Integrated Cellular Adhoc Relay [iCAR].
- The primary concept behind cellular networks is geographical channel reuse.
- Several techniques like cell sectoring, cell resizing and multi-tier cells increase the capacity of cellular networks.
- MCNs combine the reliability & support of fixed base station of cellular network with flexibility & multi - hop relaying adhoc wireless networks.
- Major advantages are:
  - Higher capacity than cellular networks due to the better channel reuse.
  - Increased flexibility & reliability in routing.
  - Better coverage & connectivity in holes of a cell can be provided by means of multiple hops through intermediate nodes in a cell.

1.5 Ad hoc wireless Internet

Ad hoc wireless internet extends the services of the internet to the end users over an ad hoc wireless network. It shows in figure 1.6.

Some of the applications of ad hoc wireless internet are :

- Wireless mesh network.
- Provisioning of temporary internet services to major conference venues.
- Sports venues.
- Temporary military settlements.
- Battlefields
- Broadband internet services in rural regions.

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

- **Gateway**
  - They are the entry points to the wired internet.
  - Generally owned & operated by a service provider.
  - They perform following tasks ,
    - ✓ Keeping track of end users.
    - ✓ Bandwidth management.
    - ✓ Load balancing.
    - ✓ Traffic shaping.
    - ✓ Packet filtering.
    - ✓ Width fairness &
    - ✓ Address, service & location discovery.
- **Address mobility**
  - This problem is worse here as the nodes operate over multiple wireless hops.
  - Solution such as Mobile IP can provide temporary alternative.

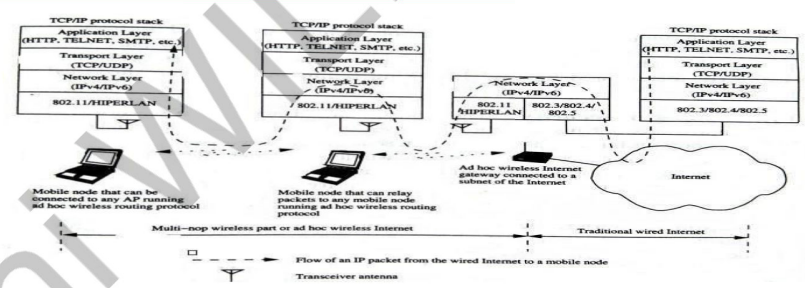


Figure 1. 6 Ad Hoc Wireless Internet
Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- **Routing**
  - It is a major problem in ad hoc wireless internet, due to dynamic topological changes, the presence of gateways, multi-hop relaying, & the hybrid character of the network.
  - Possible solution is to use separate routing protocol for the wireless part of ad hoc wireless internet.
- **Transport layer protocol**
  - Several factors are to be considered here, the major one being the state maintenance overhead at the gateway nodes.
- **Load balancing**
  - They are essential to distribute the load so as to avoid the situation where the gateway nodes become bottleneck nodes.
- **Pricing / Billing**
  - Since internet bandwidth is expensive, it becomes very important to introduce pricing/billing strategies for the ad hoc wireless internet.

- **Provisioning of security**
  - Security is a prime concern since the end users can utilize the ad hoc wireless internet infrastructure to make e-commerce transaction.
- **QoS support**
  - With the widespread use of Voice Over IP (VOIP) & growing multimedia applications over the internet, provisioning of QoS support in the ad hoc wireless internet becomes a very important issue.
- **Service, address & location discovery**
  - Service discovery refers to the activity of discovering or identifying the party which provides service or resource.
  - Address discovery refers to the services such as those provided by Address Resolution Protocol (ARP) or Domain Name Service (DNS) operating within the wireless domain.
  - Location discovery refers to different activities such as detecting the location of a particular mobile node in the network or detecting the geographical location of nodes.

1.6 Routing Protocols for Ad Hoc Wireless Networks

- Routing is the exchange of information from one station of networks to other and Protocol is the set of standard or rules to exchange data between two devices.
- An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network.
- An ad hoc wireless network consists of a set of mobile nodes (hosts) that are connected by wireless links. The network topology (the physical connectivity of the communication network) in such a network may keep changing randomly.
- Routing protocols that find a path to be followed by data packets from a source node to a destination node used in traditional wired networks cannot be directly applied in ad hoc wireless networks due to their highly dynamic topology absence of established infrastructure for centralized administration (e.g., base stations or access points), bandwidth-constrained wireless links, and resource (energy)-constrained nodes.

innovate achieve lead

1.7 Issues in Designing a Routing Protocol for Ad Hoc Wireless Networks

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

- Mobility of nodes
- Bandwidth Constraints
- Error-Prone channel state
- Hidden Terminal Problem
- Exposed Terminal Problems
- Resource Constraints

1.7.1 Mobility

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

1.7.2 Bandwidth Constraint

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

innovate achieve lead

- The limited bandwidth availability also imposes a constraint on routing protocols in maintaining the topological information.

1.7.3 Error-prone shared broadcast radio channel

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

1.7.4 Hidden Terminal Problem

- The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the receiver, but are within the transmission range of the receiver.
- Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other.

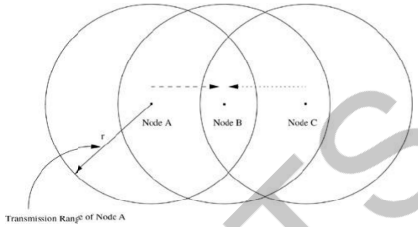


Figure 1. 7 Hidden Terminal Problem

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- For example, consider figure 1.7. Here, if both node A and node C transmit to node B at the same time, their packets collide at node B. This is due to the fact that both node A and C are hidden from each other, as they are not within the direct transmission range of each other and hence do not know about the presence of each other.

Solution for this problem (figure 1.8), include medium access collision avoidance (MACA)

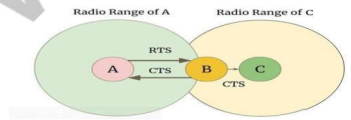


Figure 1.8 Solution for Hidden Terminal Problem

- Transmitting node first explicitly notifies all potential hidden nodes about the forthcoming transmission by means of a two way handshake control protocol called RTS-CTS protocol exchange. This may not solve the problem completely but it reduces the probability of collisions.

1.7.5 Exposed Terminal Problem

- The exposed terminal problem refers to the inability of a node which is blocked due to transmission by a nearby transmitting node to transmit to another node.
- For example, consider the figure 1.9, Here, if a transmission from node B to another node A is already in progress, node C cannot transmit to node D, as it concludes that its neighbor node B, is in transmitting mode and hence should not interfere with the on-going transmission. Thus, reusability of the radio spectrum is affected.

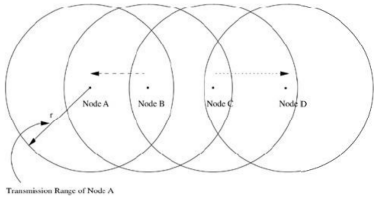


Figure 1. 9 Exposed Terminal Problem

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

- Solution for this problem, illustrated in figure 1.10. In this case, node A did not successfully receive the CTS originated by node R and hence assumes that there is no on- going transmission in the neighborhood. Since node A is hidden from node T, any attempt to originate its own RTS would result in collision of the on-going transmission between nodes T and R.

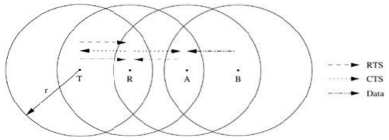


Figure 1. 10 Solution for Exposed Terminal Problem

Source : Ad Hoc Wireless Networks Architectures and Protocol by C. Siva Ram Murthy and B. S. Manoj

1.7.6 Resource Constraints

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

1.8 Characteristics of an Ideal Routing Protocol for Ad Hoc Wireless Networks

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

- It must be fully distributed as centralized routing involves high control overhead and hence is not scalable.
- It must be adaptive to frequent topology changes caused by the mobility of nodes.
- Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired.
- It must be localized, as global state maintenance involves a huge state propagation control overhead.
- It must be loop-free and free from state routes.

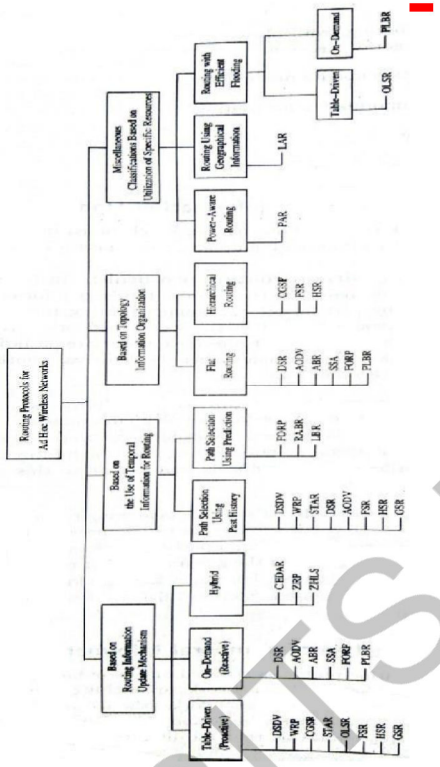
- The number of packet collisions must be kept to a minimum by limiting the number of broadcasts made by each node. The transmissions should be reliable to reduce message loss and to prevent the occurrence of state routes.
- It must converge to optimal routes once the network topology becomes stable. The convergence must be quick.
- It must optimally use scarce resources such as bandwidth, computing power, memory, and battery power.
- Every node in the network should try to store information regarding the stable local topology only. Changes in remote parts of the network must not cause updates in the topology information maintained by the node.
- It should be able to provide a certain level of quality of service (QoS) as demanded by the applications, and should also offer support for time-sensitive traffic.
- Routing information update mechanism.
- Use of temporal information for routing
- Routing topology
- Utilization of specific resources.

1. Based on the routing information update mechanism

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

- **Proactive or table-driven routing protocols**
  - Every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.
  - Routing information is generally flooded in the whole network.
  - Whenever a node requires a path to a destination, it runs an appropriate path- finding algorithm on the topology information it maintains.
- **Reactive or on-demand routing protocols**
  - Do not maintain the network topology information.
  - Obtain the necessary path when it is required, by using a connection establishment process.

Figure 1.11 Classification of Sensor Network Protocols



innovate achieve lead

Mobile Ad hoc Networks

I. Introduction

Wireless Networks

- Need: Access computing and communication services, on the move
- Infrastructure-based Networks
  - traditional cellular systems (base station infrastructure)
- Wireless LANs
  - typically radio links (802.11, etc), can be Infrared
  - very flexible within the reception area; ad-hoc networks possible
  - lower bandwidth than wired networks (1-54 Mbit/s)
- Ad hoc Networks
  - useful when infrastructure not available, impractical, or expensive
  - originally military applications, rescue, home networking
  - interesting potential for Metro-area networking

4

innovate achieve lead

innovate achieve lead

Cellular Wireless

- Single hop wireless connectivity to the wired world
  - Space divided into cells
  - A base station is responsible to communicate with hosts in its cell
  - Mobile hosts can change cells while communicating
  - Hand-off occurs when a mobile host starts communicating via a new base station

5

Mobile Ad Hoc Networks (MANETs)

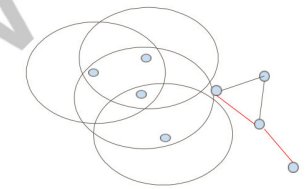
- Formed by wireless hosts which may be mobile
- Without (necessarily) using a pre-existing infrastructure
- Routes between nodes may potentially contain multiple hops

6

innovate achieve lead

Mobile Ad Hoc Networks (MANETs)

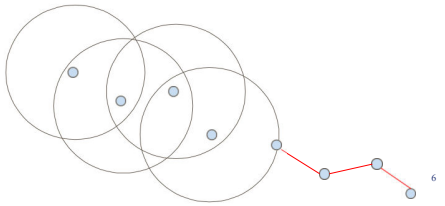
- May need to traverse multiple links to reach destination



7

Mobile Ad Hoc Networks (MANETs)

- Mobility causes route changes



6

innovate achieve lead

innovate achieve lead

Why Ad Hoc Networks ?

- Setting up of fixed access points and backbone infrastructure is not always viable
  - Infrastructure may not be present in a disaster area or war zone
  - Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m)
- Ad hoc networks:
  - Do not need backbone infrastructure support
  - Are easy to deploy
  - Self-configure
  - Useful when infrastructure is absent, destroyed or impractical

9

Many Applications

- Personal area networking
  - cell phone, laptop, ear phone, wrist watch
- Military environments
  - soldiers, tanks, planes
- Civilian environments
  - taxi cab network
  - meeting rooms
  - sports stadiums
  - boats, small aircraft
- Emergency operations
  - search-and-rescue
  - policing and fire fighting

6

innovate achieve lead

Many Variations

- Fully Symmetric Environment
  - all nodes have identical capabilities and responsibilities
- Asymmetric Capabilities
  - transmission ranges and radios may differ
  - battery life of different nodes may differ
  - processing capacity may be different at different nodes
  - speed of movement
- Asymmetric Responsibilities
  - only some nodes may route packets
  - some nodes may act as leaders of nearby nodes (e.g., cluster head)

11

Many Variations

- Traffic characteristics may differ in different ad hoc networks
  - bit rate
  - timeliness constraints
  - reliability requirements
  - unicast / multicast / geocast
  - host-based addressing / content-based addressing / capability-based addressing
- May co-exist (and co-operate) with an infrastructure-based network

12

BITS Pilani, Pilani Campus

innovate achieve lead

innovate achieve lead

Many Variations

- Mobility patterns may be different
  - people sitting at an airport lounge
  - New York taxi cabs
  - kids playing
  - military movements
  - personal area network
- Mobility characteristics
  - speed
  - predictability
    - direction of movement
    - pattern of movement
  - uniformity (or lack thereof) of mobility characteristics among different nodes

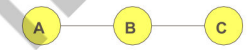
13

Challenges in Design & Operation of MANETs

- Lack of a centralized entity
- ALL communications is carried over the wireless medium
  - Limited wireless transmission range
  - Broadcast nature of the wireless medium
    - Hidden terminal problem (see next slide)
    - Exposed terminal problem
    - Ease of snooping on wireless transmissions (security hazard)
- Packet losses due to transmission errors
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Potentially frequent network partitions

14

innovate achieve lead



Nodes A and C cannot hear each other

Transmissions by nodes A and C can collide at node B

Nodes A and C are hidden from each other

15

Challenges in Design & Operation of MANETs

- Given all these challenges, the design of ad-hoc should allow for a high degree of
  - Reliability
  - Survivability
  - Availability
  - Manageability of the network

16

innovate achieve lead

innovate achieve lead

Mobile Ad hoc Networks

II. Medium Access Control Protocols

Motivation

- Can we apply media access methods from fixed networks?
- Example CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - Send as soon as the medium is free, listen into the medium if a collision occurs (original method in IEEE 802.3)
- Medium access problems in wireless networks
  - Signal strength decreases proportional to the square of the distance
  - Sender would apply CS and CD, but the collisions happen at the receiver
  - Sender may not "hear" the collision, i.e., CD does not work
  - CS might not work, e.g. if a terminal is "hidden"

18

innovate achieve lead

Multiple Access with Collision Avoidance

MACA uses signaling packets for collision avoidance

- RTS (request to send)
  - sender request the right to send from a receiver with a short RTS packet before it sends a data packet
- CTS (clear to send)
  - receiver grants the right to send as soon as it is ready to receive
- Signaling packets contain
  - sender address
  - receiver address
  - packet size
- Variants of this method are used in IEEE 802.11

19

Multiple Access with Collision Avoidance

MACA avoids the problem of hidden terminals

- A and C want to send to B
- A sends RTS first
- C waits after receiving CTS from B

- MACA avoids the problem of exposed terminals
  - B wants to send to A, C to another terminal
  - now C does not have to wait, as it cannot receive CTS from A

20

BITS Pilani, Pilani Campus

innovate achieve lead

innovate achieve lead

Unicast Routing Protocols

- Many protocols have been proposed
- Some specifically invented for MANET
- Others adapted from protocols for wired networks
- No single protocol works well in all environments
  - some attempts made to develop adaptive/hybrid protocols
- Standardization efforts in IETF
  - MANET, MobileIP working groups
  - http://www.ietf.org

25

Unicast Routing Protocols

- Proactive Protocols
  - Traditional distributed shortest-path protocols
  - Maintain routes between every host pair at all times
  - Based on periodic updates; High routing overhead
  - Example: DSDV (destination sequenced distance vector)
- Reactive Protocols
  - Determine route if and when needed
  - Source initiates route discovery
  - Example: DSR (dynamic source routing)
- Hybrid Protocols
  - Adaptive; Combination of proactive and reactive
  - Example : ZRP (zone routing protocol)

26

innovate achieve lead

Protocol Trade-offs

- Proactive Protocols
  - Always maintain routes
  - Little or no delay for route determination
  - Consume bandwidth to keep routes up-to-date
  - Maintain routes which may never be used
- Reactive Protocols
  - Lower overhead since routes are determined on demand
  - Significant delay in route determination
  - Employ flooding (global search)
  - Control traffic may be bursty
- Which approach achieves a better trade-off depends on the traffic and mobility patterns

27

Mobile Ad hoc Networks

III. Routing Protocols

1. Reactive protocols

BITS Pilani, Pilani Campus

innovate achieve lead

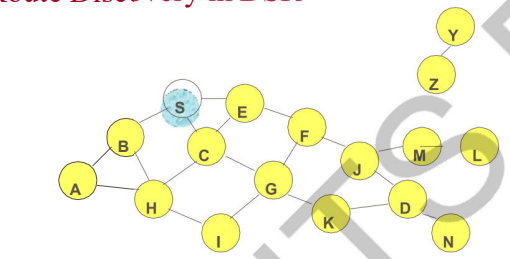
innovate achieve lead

Dynamic Source Routing (DSR)

- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ

29

Route Discovery in DSR



Represents a node that has received RREQ for D from S

30

innovate achieve lead

Ad Hoc On-Demand Distance Vector (AODV) Routing

DSR includes source routes in packet headers

- Resulting large headers can sometimes degrade performance
  - particularly when data contents of a packet are small
- AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes
- AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate

45

AODV

- Route Requests (RREQ) are forwarded in a manner similar to DSR
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
  - AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending a Route Reply
- Route Reply travels along the reverse path set-up when Route Request is forwarded

46

innovate achieve lead

innovate achieve lead

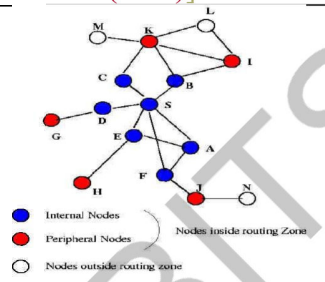
Zone Routing Protocol (ZRP)

ZRP combines proactive and reactive approaches

- All nodes within hop distance at most *d* from a node X are said to be in the routing zone of node X
- All nodes at hop distance exactly *d* are said to be peripheral nodes of node X's routing zone
- Intra-zone routing: Proactively maintain routes to all nodes within the source node's own zone.
- Inter-zone routing: Use an on-demand protocol (similar to DSR or AODV) to determine routes to outside zone.

59

Zone Routing Protocol (ZRP)]



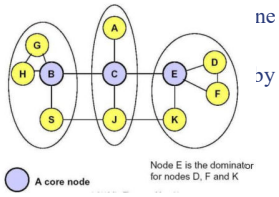
60

innovate achieve lead

Core-Extraction Distributed Ad hoc Routing

A subset of nodes in the network is identified as the *core*

- Each node in the network i ne node in the core
- Each core node determines oy means of a localized broadcast



61

Location-Aided Routing (LAR)

Exploits location information to limit scope of route request flood

- Location information may be obtained using GPS

- *Expected Zone* is determined as a region that is expected to hold the current location of the destination
  - Expected region determined based on potentially old location information, and knowledge of the destination's speed

- Route requests limited to a *Request Zone* that contains the Expected Zone and location of the sender node

60

innovate achieve lead

LAR

- Only nodes within the request zone forward route requests
  - Node A does not forward RREQ, but node B does (see previous slide)
- Request zone explicitly specified in the route request
- Each node must know its physical location to determine whether it is within the request zone

65

LAR

- Only nodes within the request zone forward route requests
- If route discovery using the smaller request zone fails to find a route, the sender initiates another route discovery (after a timeout) using a larger request zone
  - the larger request zone may be the entire network
- Rest of route discovery protocol similar to DSR

66

innovate achieve lead

User Datagram Protocol (UDP)

- UDP provides unreliable delivery
- Studies comparing different routing protocols for MANET typically measure UDP performance
- Several performance metrics are often used
  - Routing overhead per data packet
  - Packet loss rate
  - Packet delivery delay

69

UDP Performance

- Several relevant studies [Broch98Mobicom,Das9ic3n,Johansson99Mobicom,Das00Infocom,Jacquet00Inria]
- Results comparing a specific pair of protocols do not always agree, but some general (and intuitive) conclusions can be drawn
  - Reactive protocols may yield lower routing overhead than proactive protocols when communication density is low
  - Reactive protocols tend to loose more packets (assuming than network layer drops packets if a route is not known)
  - Proactive protocols perform better with high mobility and dense communication graph

70

innovate achieve lead

innovate achieve lead

UDP Performance

- Many variables affect performance
  - Traffic characteristics
    - one-to-many, many-to-one, many-to-many
    - small bursts, large file transfers, real-time, non-real-time
  - Mobility characteristics
    - low/high rate of movement
    - do nodes tend to move in groups
  - Node capabilities
    - transmission range (fixed, changeable)
    - battery constraints
  - Performance metrics
    - delay
    - throughput
    - latency
    - routing overhead
  - Static or dynamic system characteristics (listed above)

71

UDP Performance

- Difficult to identify a single scheme that will perform well in all environments
- Holy Grail: Routing protocol that dynamically adapts to all environments so as to optimize "performance"
  - Performance metrics may differ in different environments

72

innovate achieve lead

Mobile Ad hoc Networks

V. Security Issues

Security Issues in Mobile Ad Hoc Networks

- Not much work in this area as yet
- Many of the security issues are same as those in traditional wired networks and cellular wireless
- What's new ?

100

innovate achieve lead

innovate achieve lead

What's New ?

- Wireless medium is easy to snoop on
- Due to ad hoc connectivity and mobility, it is hard to guarantee access to any particular node (for instance, to obtain a secret key)
- Easier for trouble-makers to insert themselves into a mobile ad hoc network (as compared to a wired network)

101

Resurrecting Duckling

- Battery exhaustion threat: A malicious node may interact with a mobile node often with the goal of draining the mobile node's battery
- Authenticity: Who can a node talk to safely?
  - Resurrecting duckling: Analogy based on a duckling and its mother. Apparently, a duckling assumes that the first object it hears is the mother
  - A mobile device will trust first device which sends a secret key

102

innovate achieve lead

Secure Routing

- Attackers may inject erroneous routing information
- By doing so, an attacker may be able to divert network traffic, or make routing inefficient
- Suggests use of digital signatures to protect routing information and data both
- Such schemes need a Certification Authority to manage the private-public keys

103

Secure Routing

- Establishing a Certification Authority (CA) difficult in a mobile ad hoc network, since the authority may not be reachable from all nodes at all times
- Suggests distributing the CA function over multiple nodes

104

innovate achieve lead

innovate achieve lead

MANET Authentication Architecture

- Digital signatures to authenticate a message
- Key distribution via certificates
- Need access to a certification authority
- Specifies message formats to be used to carry signature, etc.

105

Intrusion Detection

- Detection of abnormal routing table updates
  - Uses "training" data to determine characteristics of normal routing table updates (such as rate of change of routing info)
  - Efficacy of this approach is not evaluated, and is debatable
- Similar abnormal behavior may be detected at other protocol layers
  - For instance, at the MAC layer, *normal* behavior may be characterized for access patterns by various hosts
  - Abnormal behavior may indicate intrusion

108

innovate achieve lead