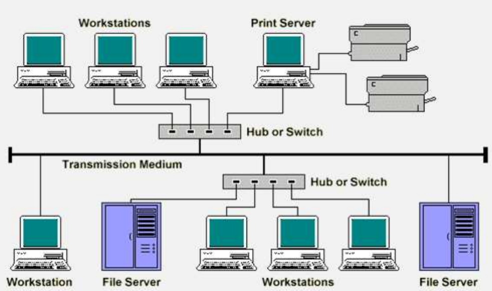
COMMUNICATION & NETWORKING TECHNOLOGIES

Internet of Things

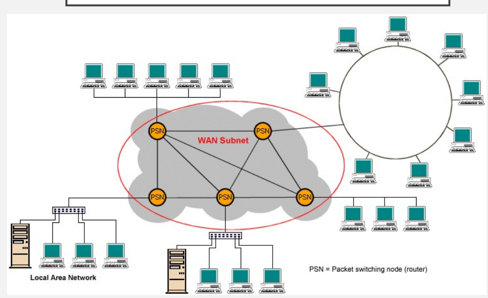
COMPUTER NETWORKS

- Geographical spread –
  - LAN
  - MAN
  - WAN
  - Internetwork

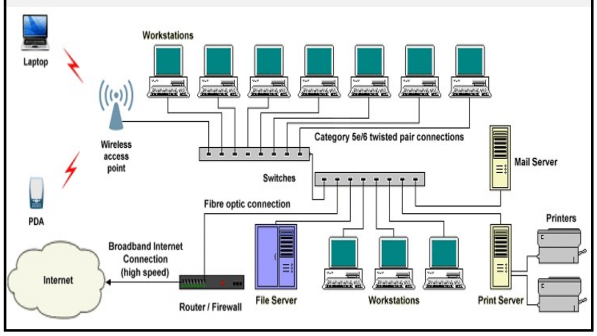
NETWORKS



NETWORKS



NETWORKS



NETWORK MODEL

- ISO –OSI Reference model
- Internet model (TCP/IP)

THE SEVEN LAYERED MODEL

- Application
- Presentation
- Session
- Transport
- Network
- Data link
- Physical

LAYERED MODELS

- The process of breaking up the functions or tasks of networking into layers reduces complexity.
- Each layer provides a service to the layer above it in the protocol specification.
- Each layer communicates with the same layer's software or hardware on other computers.

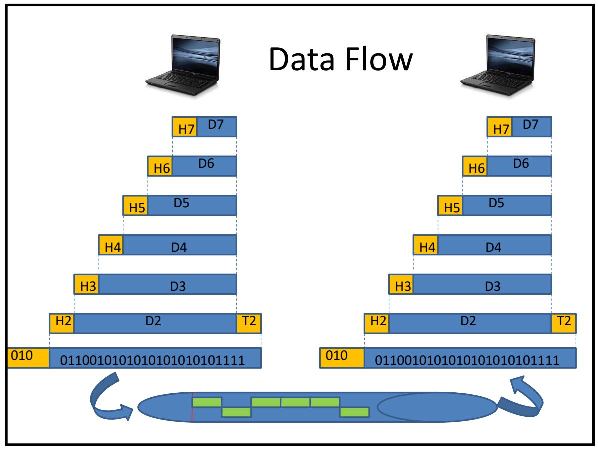
LAYERED MODELS

- Study of layered model means study of their
  - Functions
  - Scope (delivery points)

Delivery points

1) Hop to hop (node to node)
2) Source to destination (end to end delivery)
3) Process to process (port to port)

Data Flow



Physical layer

Physical layer is responsible for transmission of bit stream over the physical medium.

Physical Layer

- Physical layer is the actual interface to the physical transmission medium.
- Implementation varies with the physical medium used. (Twisted pair, coaxial cable, optical fiber or radio waves (wireless).)
- Representation of data (bit-encoding- voltage levels for 0/1 bit transmissions)
- Time-duration of bits (signaling speed).

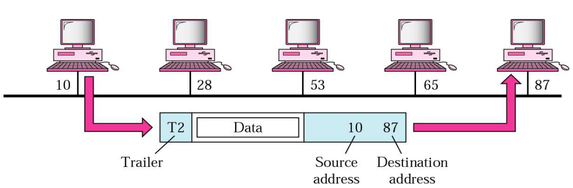
Data link layer

Data link layer is responsible for moving FRAMES from one Hop (Node) to the next. i.e. Hop- to- Hop delivery

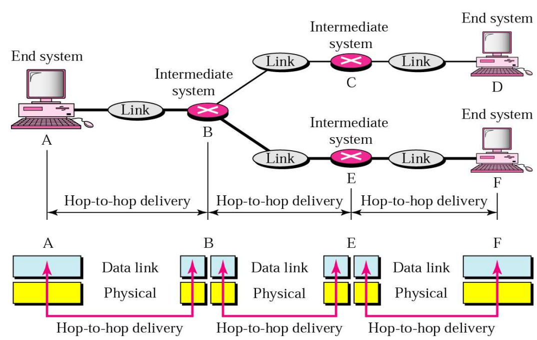
Data link layer

- Framing
- Physical Addressing
- Flow control
- Error control
- Access control

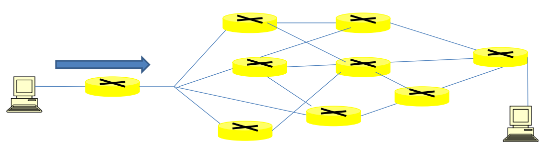
At data link layer…



Hop-to-Hop delivery



Network Layer



- Which path to take?
- Why?
- How to proceed?

ROUTING

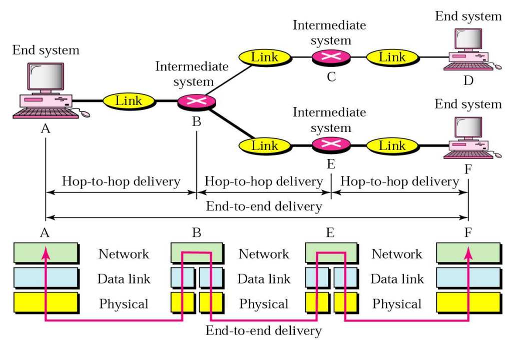
Network Layer

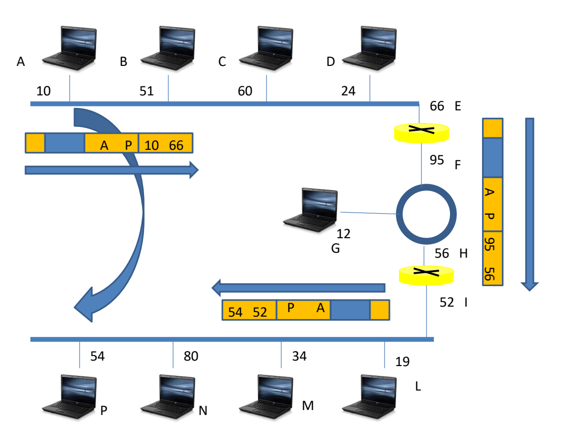
Network layer is responsible for the delivery of individual PACKETS from source to destination

Functions of Network Layer

- Logical Addressing
- Routing

Network Layer

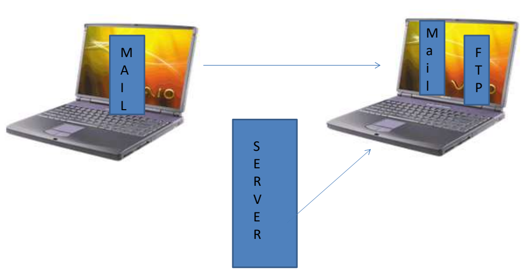




Transport Layer

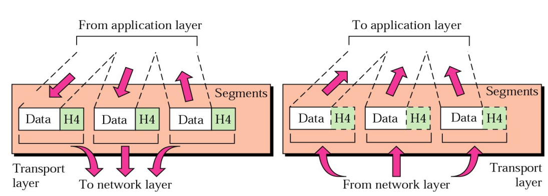
Transport layer is responsible for delivery of message from one process to another.

Transport Layer

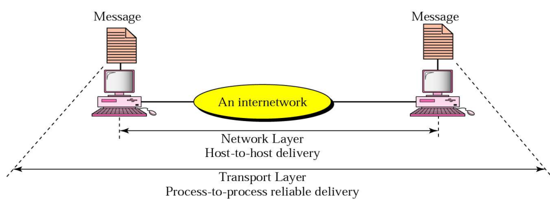


PROCESS TO PROCESS OR
PORT TO PORT DELEVERY

Transport Layer



Transport Layer



Transport Layer

- Process to process delivery – it requires service point address i.e port addresses
- What are port addresses?
- Port number 20 –FTP DATA
- Port number 23 – TELNET
- Port number 25 – SMTP
- Port number 80 – HTTP

Functions of transport layer

- Service point addressing
- Segmentation and reassembly
- Flow control
- Error control
- Connection control

SESSION LAYER

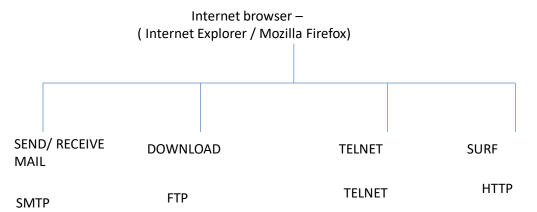
- To establish, manage and terminate session
- Functions like Dialog control, Synchronization

PRESENTATION LAYER

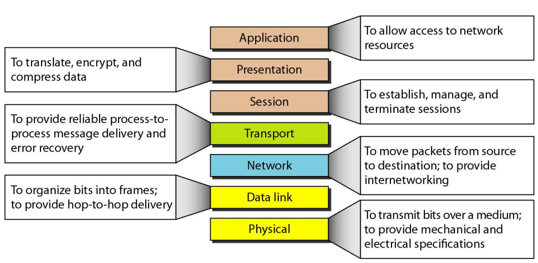
- Sender or receiver may be using different syntax, semantics for information
- Hence, message from above (appl layer) is transferred to common format at sender's side and converted to receiver's required format at his side using corresponding presentation layers.
- So, functions like translation, compression, encryption

APPLICATION LAYER

- It enables user/software to access network



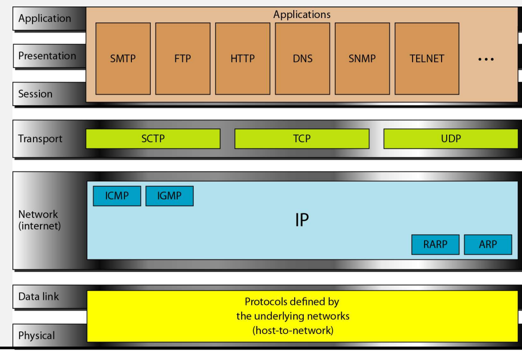
Summary

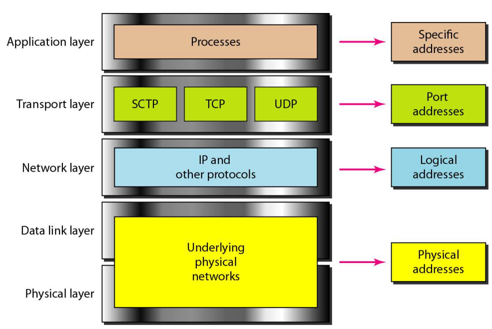


COMMUNICATION & NETWORKING TECHNOLOGIES

Internet of Things

OSI &TCP/IP COMPARISON

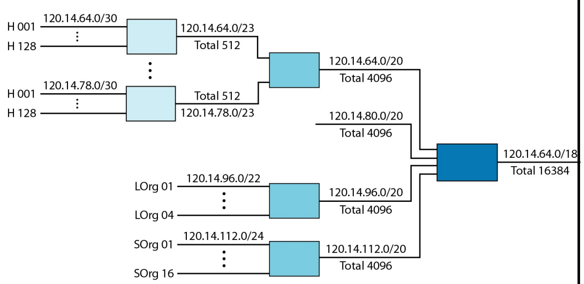




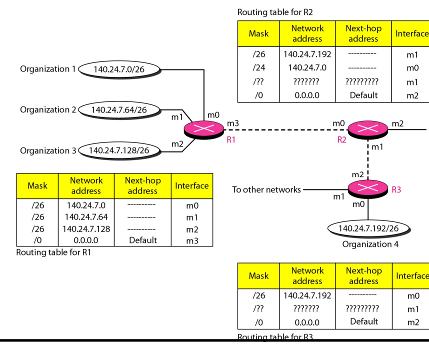
ROUTING

IPv4

Addresses in IPv4



Routers and tables



Routing table for R2

Mask	Network address	Next-hop address	Interface
/26	140.24.7.192	----------	m1
/24	140.24.7.0	----------	m0
/??	???????	?????????	m1
/0	0.0.0.0	Default	m2

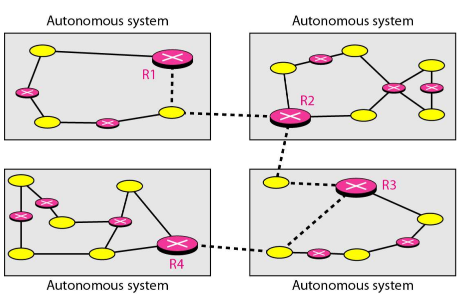
Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/0	0.0.0.0	Default	m3

Routing table for R1

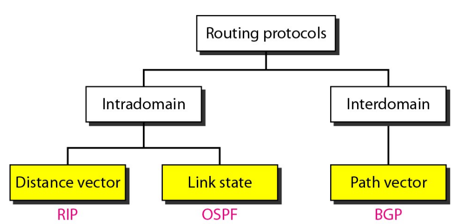
Mask	Network address	Next-hop address	Interface
/26	140.24.7.192	----------	m0
/??	???????	?????????	m1
/0	0.0.0.0	Default	m2

Routing table for R3

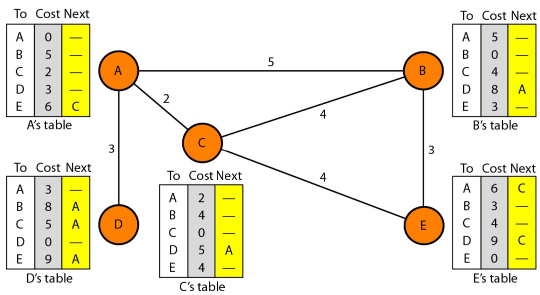
Autonomous system



Routing protocols



Distance vector routing protocols



A's table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

B's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	8	A
E	3	—

D's table

To	Cost	Next
A	3	—
B	8	A
C	5	A
D	0	—
E	9	A

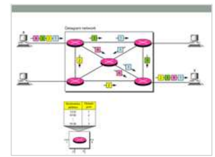
C's table

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	5	A
E	4	—

E's table

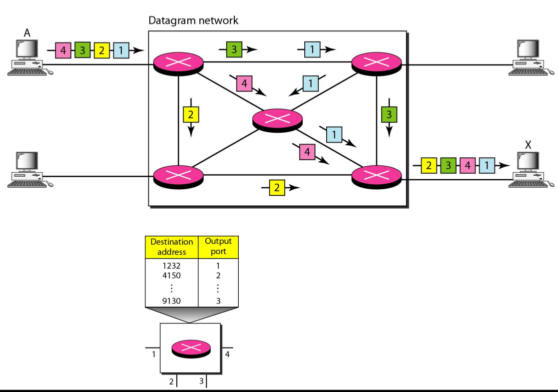
To	Cost	Next
A	6	C
B	3	—
C	4	—
D	9	C
E	0	—

Internet Protocol (IP)



- Transmission mechanism
- Connectionless, Unreliable
- Best-Effort delivery

- No error checking, tracking
- No track of routes
- No reassembly of datagrams at destination
- Will do best to get the transmission through, but no guarantees



Other protocols

- ARP (Address Resolution Protocol)

  Logical address → Physical address

- RARP(Reverse Address Resolution Protocol)

  Physical address → Logical address

- ICMP (Internet Control Message Protocol)

- IGMP (Internet Group Message Protocol)

TRANSPORT LAYER PROTOCOLS

TCP and UDP

Transmission Control Protocol

- Full Duplex communication
- Connection-oriented service
  - Creates stream oriented environment in which it accepts the responsibility of delivering bytes in order
- Reliable
  - Uses a mechanism to check safe and sound arrival of data
- Flow control
  - Rx controls amt of data to be sent by the sender
  - Byte oriented flow control
- Error control
  - Byte oriented
- Congestion control
  - Senders data tx is controlled by congestion in n/w

User Datagram Protocol

- Simple protocol with Minimum Overhead
- Connectionless
- Unreliable
- Requires less interaction between sender and Rx

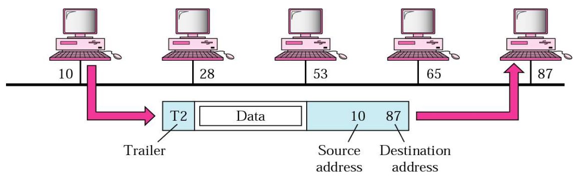
WIRED AND WIRELESS NETWORKS

From Communication and MAC perspective

Wired and Wireless Communication

- Wired
  - Guided Medium
- Wireless
  - Unguided transmissions
    - Multipath, Fading, Interferences, reflections..
    - (Higher) Path loss
  - Spectrum usage
  - Offers easy mobility

At data link layer…



MAC protocols

MAC protocols

- Contention based (Random access)
  - ALOHA
  - Slotted ALOHA
  - CSMA/CD
  - CSMA/CA
- Contention Free /Scheduling based/ Fixed assignment
  - FDMA
  - TDMA
  - CDMA
  - Polling
  - Token passing

CSMA

- All stations are required to sense the medium before trying to use it
- Reduces possibility of collision but cannot eliminate it.
- Reason for it – “propagation delay”

COMMUNICATION & NETWORKING TECHNOLOGIES

Internet of Things

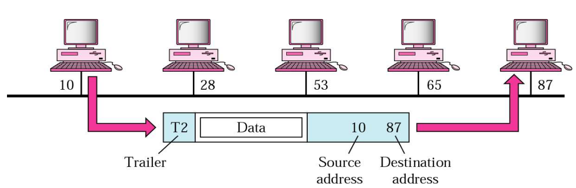
WIRED AND WIRELESS NETWORKS

From Communication and MAC perspective

Wired and Wireless Communication

- Wired
  - Guided Medium
- Wireless
  - Unguided transmissions
    - Multipath, Fading, Interferences, reflections..
    - (Higher) Path loss
  - Spectrum usage
  - Offers easy mobility

At data link layer…



MAC protocols

MAC protocols

Contention based (Random access)

- ALOHA
- Slotted ALOHA
- CSMA/CD
- CSMA/CA

Contention Free /Scheduling based/ Fixed assignment

- FDMA
- TDMA
- CDMA

- Polling
- Token passing

CSMA

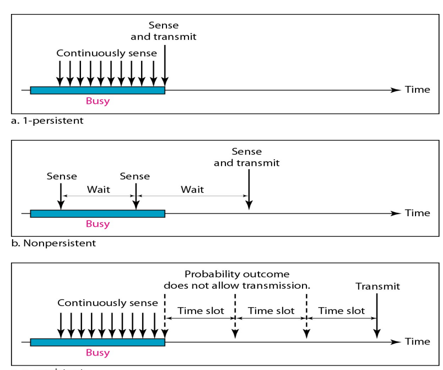
- All stations are required to sense the medium before trying to use it
- Reduces possibility of collision but cannot eliminate it.
- Reason for it – “propagation delay”

Protocol Decisions

- What to do if the medium is busy
- What to do if channel is idle

Persistence methods

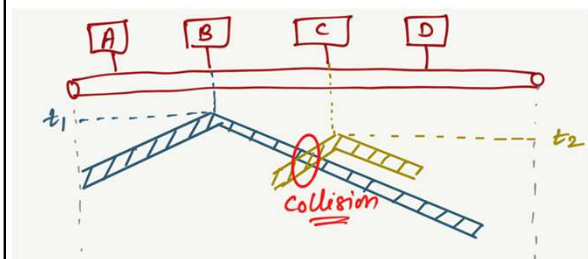
1) 1-persistence
2) Non-persistence
3) p- persistence

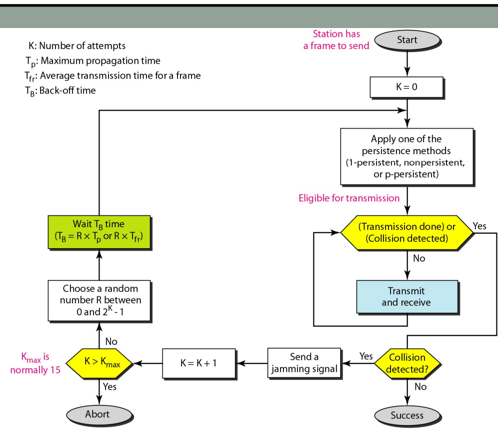


CSMA/CD

- Carrier sense multiple access – collision detection
- Augmentation of algorithm to handle collision
- Monitors medium while sending frame

Collision on shared medium

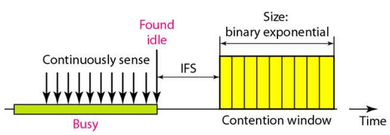


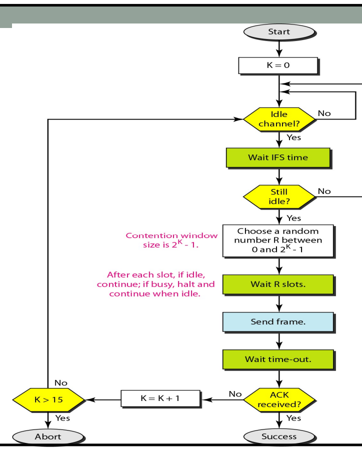


Wireless LAN - CSMA/CA

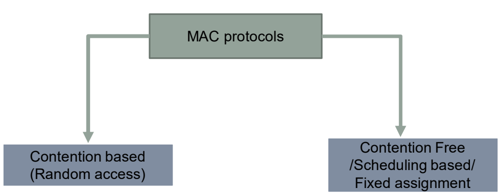
- Carrier Sense Multiple Access – Collision Avoidance
- A mechanism is used to avoid collision rather than detecting it.
- Detecting collision based on energy change might be difficult.

Timing in CSMA/CA





MAC protocols

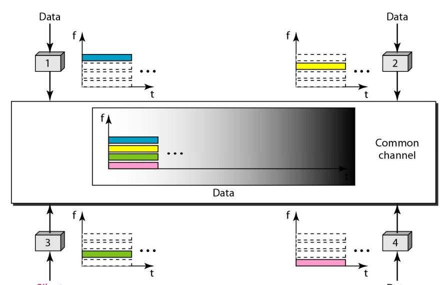


- ALOHA
- CSMA/CD
- CSMA/CA

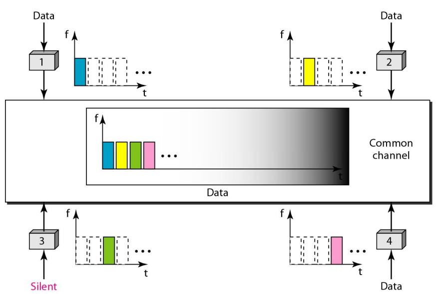
- FDMA
- TDMA
- CDMA

- Polling
- Token passing

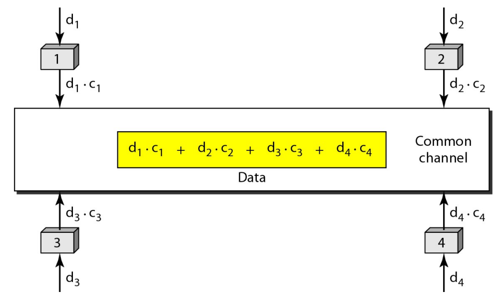
FDMA



TDMA



CDMA



IEEE special project 802 (Yr. 1985)

- IEEE 802.2 : Logical Link Control (LLC)
- IEEE 802.3 : CSMA/CD (Ethernet)
- IEEE 802.11 : Wireless LAN
- IEEE 802.15 : Wireless PAN

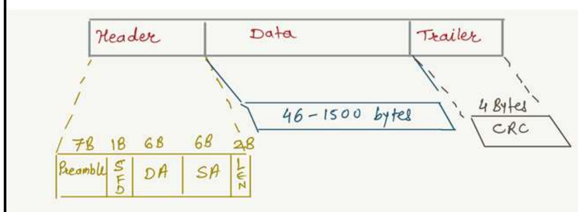
LLC

- Single data link control protocol for all IEEE LAN.
- Provides services to Network layer independent of the physical medium –enables access to different types of physical network.
- Provides interconnectivity between different LANs.
- Functions – flow control, error control, part of framing.

WIRED LAN

ETHERNET

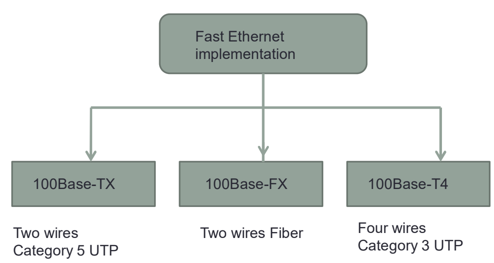
802.3 Frame format



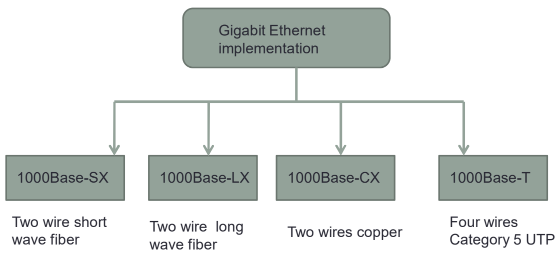
IEEE 802.3 10Mbps physical layer medium alternative

	10 BASE 5	10 BASE 2	10 BASE T	10 BASE-F
Transmission medium	Coaxial cable	Coaxial cable	UTP	850nm optical fiber pair
Signaling Technique	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)
Topology	Bus	Bus	Star	Star
Maximum segment length	500 m	185 m	100 m	2000 m
Cable diameter	10 mm	5mm	0.4 to 0.6mm	62.5/125 micrometers

Implementation

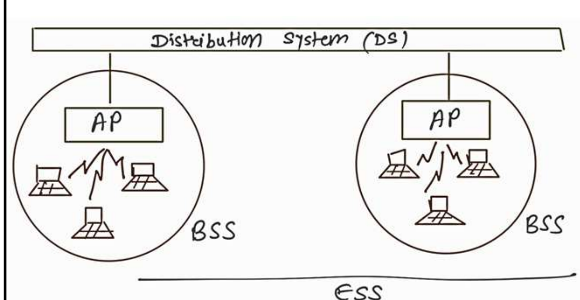


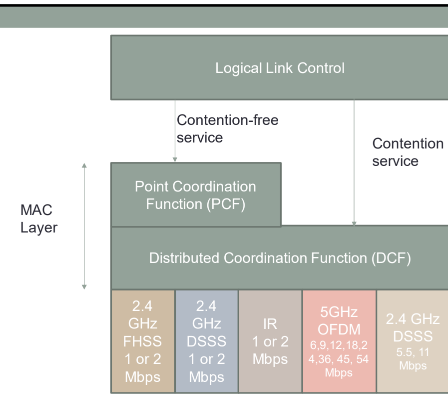
Implementation



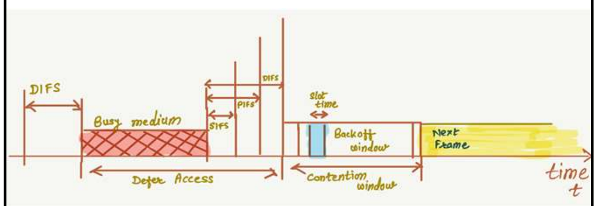
WIRELESS LAN

802.11

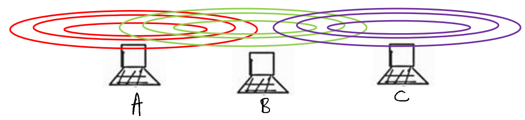




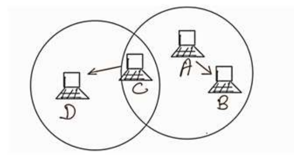
Basic Access Method



Hidden terminal problem

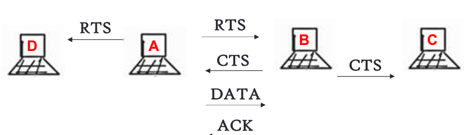


Exposed terminal problem

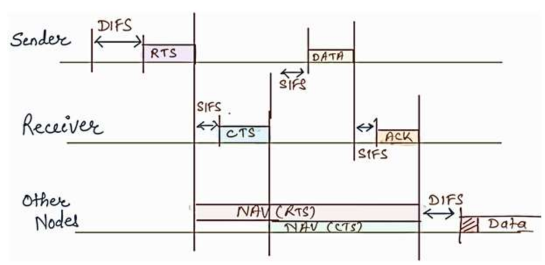


Use of handshaking

Reliability



802.11 –RTS/CTS

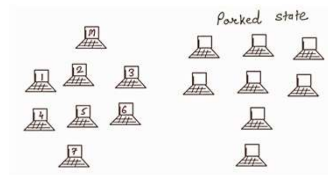


COMMUNICATION & NETWORKING TECHNOLOGIES

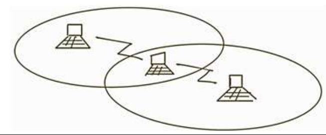
Internet of Things

Bluetooth IEEE 802.15.1 (Wireless PAN)

Piconet



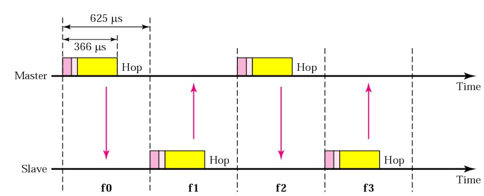
Scatternet



Bluetooth

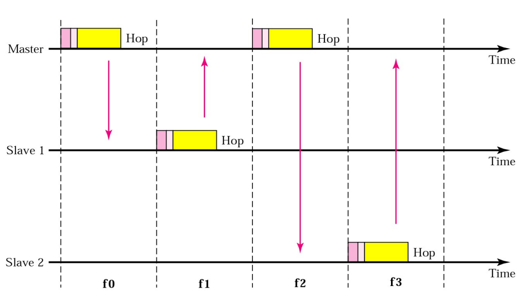
- FHSS – 2.4 GHz
- Modulation technique – GFSK
- Data rate- 1 Mbps
- Power – 1mW – 100 mW
- Range ~ 20-30 m

Single Secondary communication



Here, length of Time slot of TDMA is same as Dwell time (1600 hops/sec)

Multiple Secondary communication



Links

- SCO – Sync connection oriented
  - Useful to avoid latency
  - Time slots are reserved
  - No retransmission done
- ACL – Async connectionless
  - Useful for data integrity
  - Retransmissions are done

IEEE 802.15.4 and Zigbee

- The IEEE 802.15.4 (LRWPAN) standard defines the physical layer (PHY) and Media Access Control (MAC) layer.

PHY covers frequency band, power, data-rate, modulation techniques

- Frequency bands -868MHz / 915MHz / 2.4GHz
- Data rate – 20 kbps to 250 kbps
- Range – 10 to 75 m

MAC –

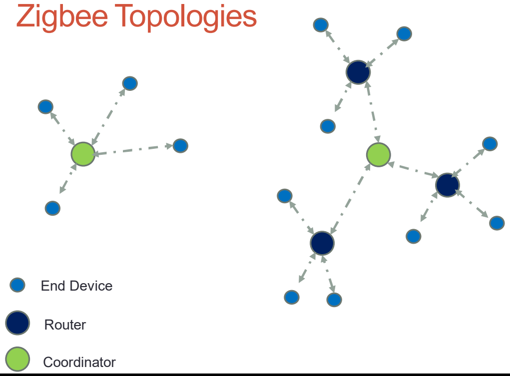
- Beaconless mode(uses CSMA/CA, short data messages)
- Beacon-enabled Mode (mix of contention free and contention based access)

Zigbee

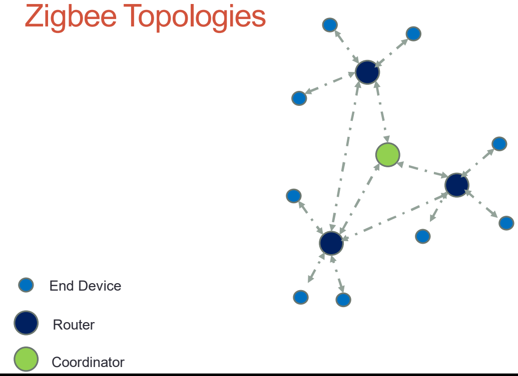
- ZigBee technology is a low data rate, low power consumption.
- Created by a set of companies which form the ZigBee Alliance.
- Defines layer 3 and above.
- Provides more flexible network topologies, intelligent message routing and enhanced security measures.
- Topologies – Star, mesh, cluster-tree.

https://zigbeealliance.org/

Zigbee Topologies



Zigbee Topologies



Mesh Network

- Nodes may be connected to each other via multiple connections.
- In routing tables, connections are dynamically updated and optimized.
- Re-configuration of routing paths is possible (in case of nodes appearing, disappearing and re-appearing in the network).
- Self-healing and stability of the network.

Near Field Communication (NFC)

- Short range wireless communication (radio waves -13.56 Mhz)
- Applications –
  - Mobile (cashless) payments
  - Smart ticketing system
  - Data sharing
  - Information exchange (ex. Smart Business cards)
  - Targeted marketing (Smart Adv. Posters)
  - Access control

https://nfc-forum.org/

Mode of operation

- Peer-to-peer communication mode
- Reader/Writer mode
- Card-Emulation mode

- Standards- NFC-A, NFC-B, NFC-F, and NFC-V
- Defines the coding scheme, modulation tech & data rate
- Low data rate (~ 200 kbps)

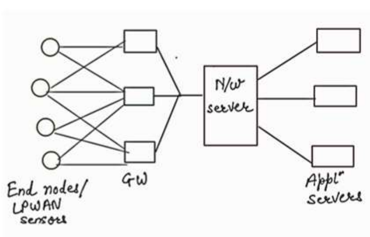
LoRa and LoRaWAN

- LoRa – Covers Physical layer
- Enables the low-power, long-range communication link
- Utilizes Chirp Spread Spectrum modulation technique
- License free band - 865 MHz to 867 MHz (India)
- Data rate – 290 bps – 50 kbps
- Range ~ 10 KM+
- Very high power efficiency Battery lifetime – 105 months (2000 mAh)
- Low cost, high capacity
- Interference immunity

https://lora-alliance.org/

LoRaWAN

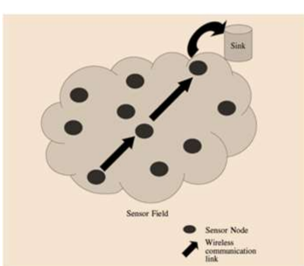
- LoRaWAN defines the communication protocol and system architecture for the network.



WIRELESS SENSOR NETWORK

WSN

Wireless Sensor Networks



- Sensor Node
  - Sensing
  - Processing/Computation
  - Comm/networking

Sensor networks are built using a large number of densely deployed sensor nodes

Wireless Sensor Networks

Deployments

- On the ground
- Underground
- Air
- Underwater
- On human bodies
- In vehicles
- Inside building structures

Collection of data

- Periodic
- Threshold based
- Query based
- Event triggered
- Combination of above

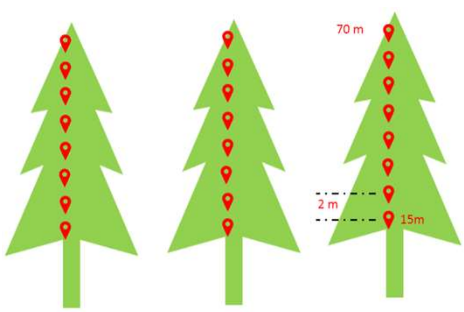
WSN applications

- Monitoring Space
- Monitoring Objects
- Monitoring Interaction between Space & Objects

Monitoring Space

- Environmental and Habitat Monitoring
- Precision Agriculture
- Indoor Climate Control
- Military Surveillance
- Intelligent Alarms

Redwood climate monitoring

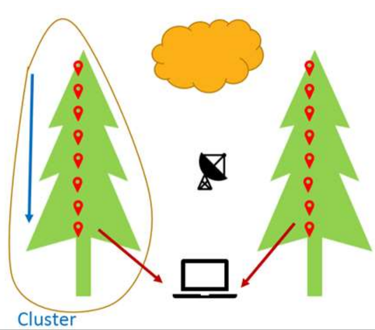


Parameters Monitored

- Temperature
- Humidity
- Solar Radiation
- Light Levels
- Photosynthetically active radiation

Interval of 5 mins

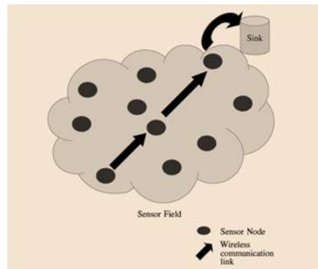
Network structure



WIRELESS SENSOR NETWORK

WSN

Wireless Sensor Networks



- Sensor Node
  - Sensing
  - Processing/Computation
  - Comm/networking

Sensor networks are built using a large number of densely deployed sensor nodes.

Wireless Sensor Networks

Deployments

- On the ground
- Underground
- Air
- Underwater
- On human bodies
- In vehicles
- Inside building structures

Collection of data

- Periodic
- Threshold based
- Query based
- Event triggered
- Combination of above

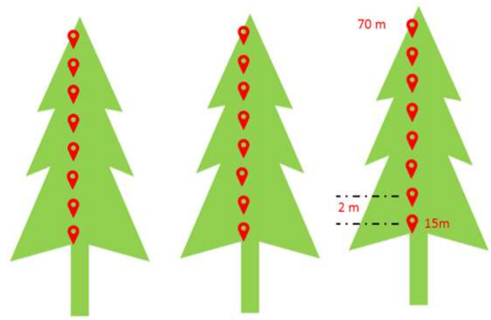
WSN applications

- Monitoring Space
- Monitoring Objects
- Monitoring Interaction between Space & Objects

Monitoring Space

- Environmental and Habitat Monitoring
- Precision Agriculture
- Indoor Climate Control
- Military Surveillance
- Intelligent Alarms

Redwood climate monitoring

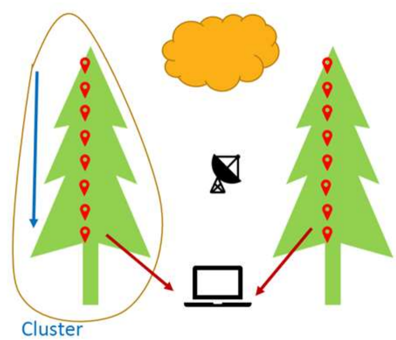


Parameters Monitored

- Temperature
- Humidity
- Solar Radiation
- Light Levels
- Photosynthetically active radiation

Interval of 5 mins

Network structure

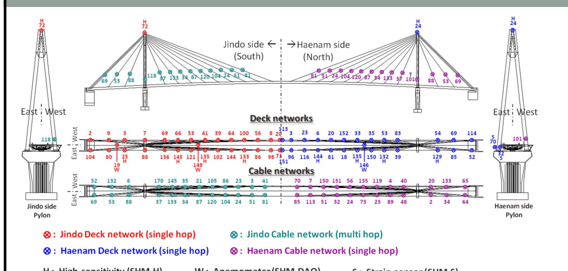


Monitoring objects

- Structural monitoring
- Condition based maintenance
- Medical Diagnostics

Bridge monitoring system

Jindo Bridge in South Korea



- 113 sensor nodes measuring a total of 661 channels of data.
- All 113 nodes are self–powered using solar or wind energy harvesting.
- Nodes can communicate in either single-hop or multi-hop ways with two base-station computers that are remotely accessible via the Internet.
- Aerodynamic and aeroelastic properties of bridges are estimated based on data.

https://spie.org/news/4043-bridge-monitoring-using-wireless-smart-sensors?SSO=1

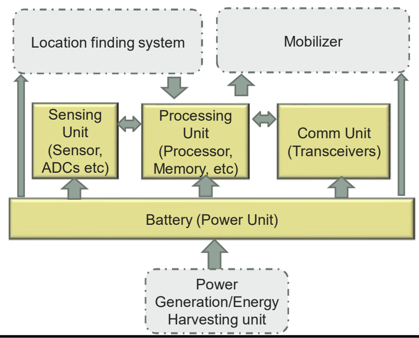
Monitoring Interaction between Space & Objects

- Wildlife Habitats
- Disaster Management
- Asset Tracking
- Manufacturing Process Flows

Zebranet (Kenya)

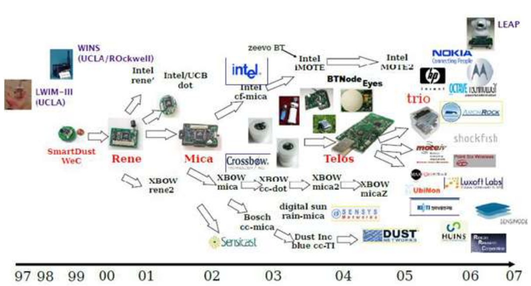
- GPS position samples every 3 minutes
- Wide range – hundred's or thousands of kms
- Parameters
  - Moving (Mobility patterns)
  - Sleep patterns
  - Drinking habits

Node structure



- Limited Battery power
  Ex. 2 AA batteries
- Limited storage capacity
  Ex. 128KB-1MB
- Limited processing powers
  Ex. 8/16 bit processors
- Low data rate/bandwidth
  Ex. 1Kbps - 1Mbps, 3-100 Meters

Glimpse at available motes



- Node's characteristics
  - Power
  - Range
  - Timing mechanism
  - Size
  - Cost
  - Flexibilities
  - Processing capacity
  - Mote should have Individual Chars that satisfy a Distributed Environment
- System's characteristics
  - Lifetime
  - Coverage
  - Response time
  - Temporal accuracy
  - Effective sampling rate
  - Ease of deployment
  - Overall cost
  - Map overall design requirement to Individual Device Capability

Challenges of Sensor Networks

- Random deployment – self configuring and maintaining networks required.
- Heterogeneity (of nodes)
- Different types of sensors and interfacing
- Mobility of nodes
- Wireless communication channel (temporally and spatially varying, Unreliable)
- Large scale coordination
- Distributed processing
- Real-time computation

Challenges of Sensor Networks

- Limited Resources –Energy, processing power, bandwidth, storage
- Harsh environment – not easily accessible
- Failure of nodes (Extreme environment and limited battery) - redundancy and fault tolerance required
- Applications requirements –
  - Varying latency bounds
  - Duration of deployment
  - Resolution (density of deployment)
  - Cost

Types of deployments

- Simpler – ex. of indoor –warehouse monitoring
  - Power supply available
  - Nodes are accessible
- Outdoor – Glacier monitoring
  - Energy consumption -Several months to years
  - Need redundancy – no accessibility
- Large scale – Habitat monitoring, ocean
  - Large no of nodes
  - Mobility - more frequent reconfiguration
  - Long duration - Energy optimization required

Deployment objectives

- Coverage
  - Sensing range, sampling rate
  - Resolution required
- Connectivity
  - Communication range
  - Partitioning or voids formations
- Topology
  - Direct comm -Star
  - Multi-hop
  - Hierarchy –Cluster formation

PROTOCOL STACK FOR WSN

Considerations of Protocol stack

- WSN design has to consider -
  - Environmental conditions
  - Application's requirements
  - Limited available resources
- Network architecture and entire protocol stack needs to be critically examined and modified for optimization.
- Ideally, the network protocol stack is expected to be channel-aware and application-aware leading to optimal network performance with efficient use of resources.

Physical Layer

It is more efficient to transmit a signal using multi-hop network composed of short-range radios rather than using a long-range link.

- Need **simpler** radio technology with
  - High-spectral efficiency
  - Min energy consumption
  - Low cost and size
- Immunity from interference and noise
- Reliability/Robustness from multipath and fading effects
- Licensed and unlicensed bands of operation
- Options- Narrowband, Spread-spectrum, UWB

Data Link Layer

Sensor nodes can follow sleep/Wake patterns

- Energy efficient
- Avoid collisions, Idle listening, overhearing, over-emitting
- Small code size and memory requirements
- Scalability
- Adaptability to changes in topology
- Other issues – Throughput/channel utilization, Latency, fairness etc.

Network layer

Data aggregation can be used to avoid traffic of redundant data on the network.

- Energy efficient operations
- End-to-end delay bounds
- Void/disconnections happening due to
  - Node failure
  - Depletion of battery
  - Unforeseen mobility
  - Obstacles
  - Nodes may follow sleep/wake patterns
- Routing decisions based on geographic co-ordinates and/or data semantics instead of node IDs.

Upper layers

- **Transport Layer** – would be needed (at gateway) when WSN is connected to Internet.
- In a WSN environment, hop-by-hop reliability of data transfer is a preferable approach than the conventional end-to-end reliability.
- **Application Layer -** WSN technologies are designed to realize a particular application.

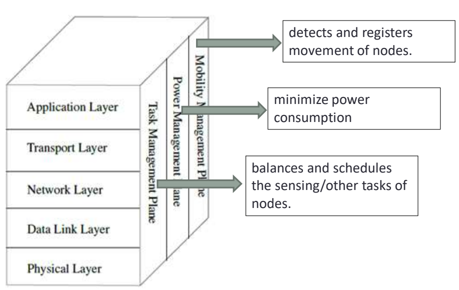
WIRELESS SENSOR NETWORK

WSN

Approaches of protocol stack design

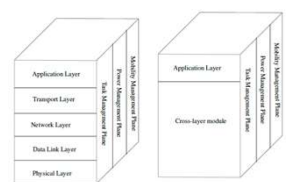
- WSN’s provide functionalities which are not present in the traditional networks.
- Various approaches of protocol stack design have been proposed.
- Blocks needed to build WSN might span several layers of OSI model.
- For ex. Localization

Management planes in WSN



Cross-layer approach

- Joint optimization and design of networking layers.
- Functionalities of two or more layers can be combined to form a single coherent framework.
- Results in significant improvement in terms of energy conservation.



Traditional approach for WSN protocol stack design

Cross-layer solution for WSN protocol stack design

TIME SYNCHRONIZATION

Time Synchronization

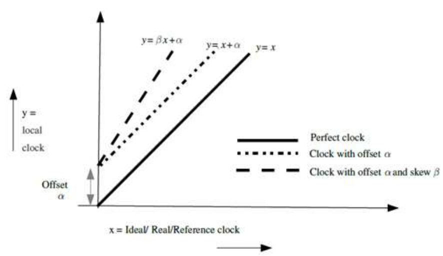
- The process of achieving and maintaining a common time-base throughout the network is called as time synchronization.

- Correct timing information is required in situations such as
  - Absolute time stamp - Event monitoring application
  - Right chronology of the events -Target Tracking applications
  - TDMA MAC protocols, Localization, sleep/wake scheduling, task scheduling

Issues

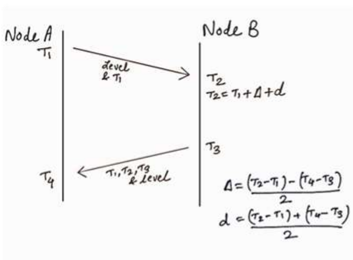
- Timing information available to node from the local clock.
- Most common clock hardware on nodes is not very accurate because the frequency (that makes time increase) is never exactly right.
- Accuracies are affected by temperature, supply voltage fluctuations, aging and so on.
- For TelosB motes, the upper bound on clock drift is 40 ppm. This means a clock in mote can loose up to 40 microseconds in a second.

Characteristics of clock



Timing-sync Protocol for Sensor Networks

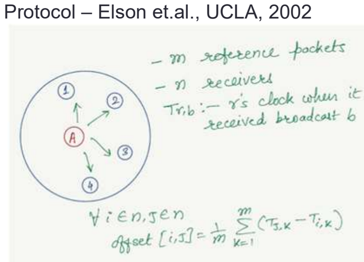
- TPSN Protocol – Ganeriwal et.al, UCLA, 2003



Assumption – Clock drift and prop delay do not change in small span of time.

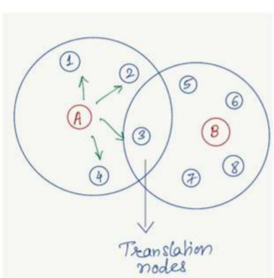
Time Synchronization using Reference Broadcasts

- RBS Protocol – Elson et.al., UCLA, 2002



RBS broadcast is always used as a *relative* time reference, never to communicate an absolute time value.

RBS - Multi-Hop Time Synchronization



LOCALIZATION PROTOCOLS

Need?

- Sensed data need a geo-stamp
- Certain applications – Target tracking, speed estimation
- Geographical routing depends on location information
- Aids in self-organization and self-healing of the WSN
- GPS is expensive (cost, size and energy required)
- GPS systems may not be available in some cases

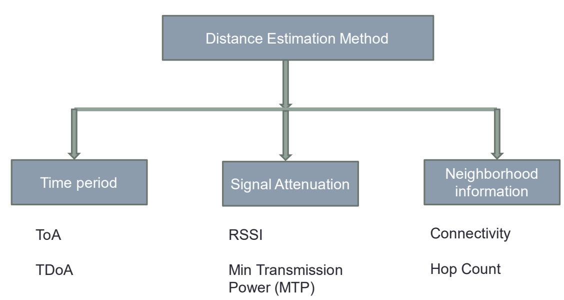
Requirements of localization

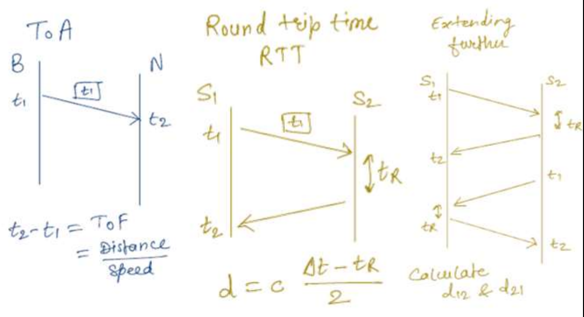
- Precision as per the application.
- Efficient in utilizing resources – If beacon hardware is required-should be minimal.
- Distributed algorithm (processing).
- Adaptive to the changing environment.
- Fast – Localization is needed immediately after deployment of network, many other protocols depend on it.
- Mobile networks might need repetitive process.

Classification of algorithm

- Approximate Vs Precise
- Central Vs Distributed
- Range based Vs Range Free
- Relative Vs Absolute
- Indoor Vs Outdoor
- Beacon-Free Vs Beacon based

Distance estimation methods





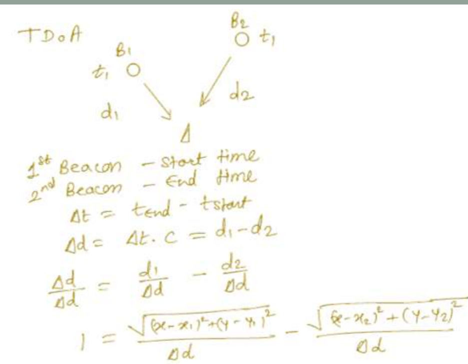
Small distances may need high time resolution.

One may use sound signal or combination of two.

RTT may include reaction time and clock drifts.

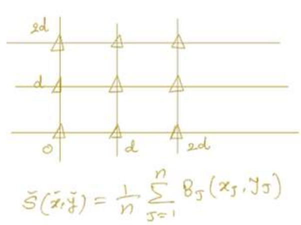
RSSI

$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2$



Examples of localization algorithm

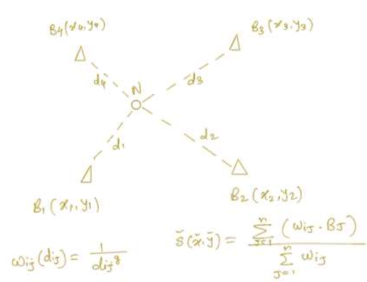
- Centroid Algorithm – Authors Bulusu et.al, USC, 2000



- Coarse-grained localization
- Avoids explicit distance measurements

Examples of localization algorithm

- Weighted centroid algorithm – Blumenthal et.al, Rostock Univ, 2005



WIRELESS SENSOR NETWORK

WSN

MEDIUM ACCESS CONTROL

MAC protocols

MAC - Attributes

- Energy Efficiency
- Throughput – Goodput
- Bandwidth Utilization
- Latency
- Fairness
- Scalability

MAC protocols

Contention based (Ex. CSMA/CA)

- Simpler to implement
- Scalable
- Flexible

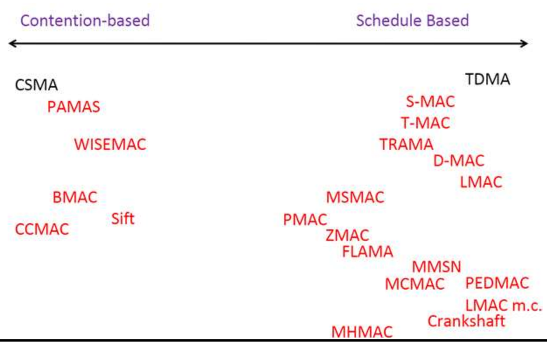
- Collisions can occur
- Energy consumed in idle listening, overhearing, collision and retransmission.

Scheduled Based (Ex. TDMA)

- Since data transmissions are scheduled, node can turn-off radio and sleep.
- Collision, idle listening, overhearing can be avoided.
- Energy efficient
- Ensures Fairness

- Slots might be wasted – Poor channel utilization
- Limits scalability and flexibility to handle mobile nodes and topology changes
- Requires precise time-sync

MAC protocols in WSN



S-MAC

- Authors – Ye et.al, USC & UCLA, 2002
- Milestone among energy-efficient MAC protocols

- Periodic listen and sleep
  - Synchronizer and follower
  - SYNC pulse
- Collision and Overhearing avoidance
  - RTS/CTS handshake
  - ACK for reliability
  - NAV period used for snoozing
- Message Passing
  - Duration field to indicate time required for tx of all data fragments

- Issues
  - Sleep delay introduces latency

ROUTING PROTOCOLS

Simple approaches of relaying data

- Flooding
  - Each packet received by sensor node is broadcast to all its neighbors, until the destination is reached.
  - Large number of duplicate packets will be generated on network.
  - Multiple nodes may send same data to the same destination node.

- Gossiping
  - Select a random neighbor (other than the source of packet), at every hop, until the packet reaches the destination.
  - May have large end-to-end delays in data delivery.

- Both approaches do not consider power consumption criteria.

Design aspects for routing protocols

- Data delivery models
  - Periodic data transmission to the Base-station
  - Query-response or event triggered transmissions
- Direct or multi-hop routing
- Performance matrices
  - Packet delivery ratio
  - Avg delay per packet
  - Energy consumption
  - Product of Energy* delay as Criteria
  - Network lifetime
    - First node dies
    - Half of nodes dies
    - Last node dies

Topology management protocols

- Topology management protocols select which nodes can turn off the radios without compromising network capacity.
- Co-ordinate the sleep transitions of all nodes while ensuring adequate network connections.

Categories of Routing protocols in WSN

- Optimization-based Routing protocols
  - Use optimization techniques to find minimum cost path
  - “Optimal” routes that avoid low-energy nodes and balances traffic
  - Optimal paths may get depleted sooner – choose set of “good” routes (sub-optimal) paths in probabilistic manner
  - Maintain network connectivity as long as possible
- Data centric based Routing protocols
  - Reduce data redundancy by performing data aggregation
  - Use signal processing techniques to perform data fusion

Categories of Routing protocols in WSN

- Cluster-based Routing protocols
  - Introduces hierarchy in the network
  - Special nodes termed as “Cluster-head” nodes form a wireless backbone to the sink
  - Energy optimization can be done at time of cluster formation, cluster-head election, data aggregation at CH etc.
- Location-based routing protocols
  - Uses position information for data relaying
  - Query can be sent to particular region
  - Offers significant reduction in number of transmissions
- QoS enabled Routing protocols
  - QoS in terms of end-to-end average delay, Deadline-miss ratio

Low Energy Adaptive Cluster Hierarchy protocol (LEACH)

- LEACH, Heinzelman et.al, MIT, 2000
- Milestone for cluster-based protocols in WSNs
- Designed for WSNs where BS is fixed and distant from sensor nodes.
- Design principles
  - Localized co-ordination and control for both set-up and operational phases
  - Random rotation of Cluster-Heads
  - Data aggregation to reduce communication cost

LEACH

- Cluster-head election mechanism is totally distributed – Knowledge of topology not required.
- Cluster-head election is performed at defined time intervals.
- Time between two elections is fixed – Round
- In each round, not only does cluster-head change, but also clusters are totally rebuild.
- Each round consists of set-up phase and data transmission phase.
- Data transmission phase is longer than set-up phase.

LEACH

- Advertisement phase
- Cluster set-up phase
- Schedule creation
- Data transmission

LEACH – Advertisement phase

- Node n decides whether or not to become cluster-head, by generating a random number in the interval [0-1] and comparing it with the threshold T(n) as follows –

$$T(n) = \begin{cases} \frac{p}{1 - p\left(r.mod\frac{1}{p}\right)} & if\ n\ \in G \\ 0 & Otherwise \end{cases}$$

- Here,
  - p is the desired percentage of CH nodes in network
  - r – current round number
  - G – Set of nodes that were not CH nodes during last 1/p rounds
- Using this, each node can be a cluster-head approximately once every 1/p rounds.
- Self-elected CH node sends ADV message to other nodes using fixed transmission power and CSMA MAC
- Non-CH nodes collect all ADV messages and select CH with best signal strength.

LEACH

- Cluster set-up phase
  - Nodes have chose the cluster to join in earlier phase.
  - Nodes communicate the choice to the relative CH node using CSMA MAC protocol.
- Schedule Creation
  - CH calculates TDMA schedule for all nodes for communication inside cluster and broadcasts it to nodes
  - CH also gives CDMA code to be used by nodes to avoid interference with adjacent clusters.
- Data transmission
  - Nodes transmit to CH only during allotted time slots with appropriate transmission power
  - Nodes can sleep at other times
  - CH is active during whole round. CH does data aggregation and sends data to BS directly.

LEACH

- Reduces average energy consumption of nodes.
- Because of CH rotation, energy usage is fairly distributed.
- Issues
  - Periodic rebuild of clusters
  - Single hop transmission strategy of CH nodes.

MANET

Mobile Ad-hoc Networks

MANET

- Distributed, Dynamic, Self Configurable Wireless Network.
- No Infrastructure support.
- Network's wireless topology may dynamically change in an unpredictable manner since nodes are free to move.
- Information is transmitted in a store-and forward manner using multi hop routing.

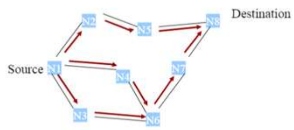
Protocol Stack

- Needs to be mobility-aware.
- Protocols should be able to adapt to the frequent change of topology.
- For ex. Routing – Needs to be dynamic routing with minimal overhead.
- Mobile nodes in MANET might be slightly more powerful compared to WSN nodes.
- Deployment may not always be dense.

Types of 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:
    - AODV (Ad-hoc On-demand Distance Vector)
    - DSR (Dynamic Source Routing)
- **Hybrid protocols**
  - Adaptive; Combination of proactive and reactive
  - Example : ZRP (Zone Routing Protocol)

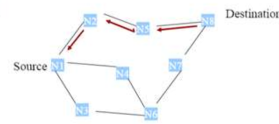
AODV



RREQ

- Source node floods the RREQ (Route request) packet in the network if the route to destination is not available.
- RREQ contains – SrcID, DestID, SrcSeqNum, DestSeqNum, BcastID and TTL.
- DestSeqNum indicates freshness of the route (up-to-date path).
- Intermediate node either forwards the RREQ or replies with RREP.
- Path info is updated if DestSeqNum of received packet > DestSeqNum stored at the Node.
- Duplicate packets are identified by SrcID-BcastID pair and can be discarded.

AODV



RREP

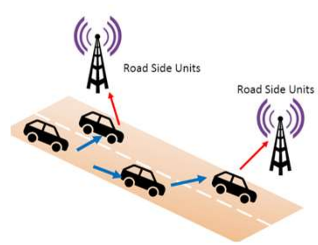
- Every intermediate node enters the previous node address and its Bcast ID while forwarding the RREQ.
- If the RREP not received, timer (TTL) is used to delete the entry.
- In AODV, source node and intermediate nodes store the next-hop information corresponding to each flow for data packet transmission.
- If any link breaks, route error messages are sent to end nodes. Nodes re-initiates the path finding process.

VANET

Vehicular Ad-hoc Networks

VANETS

- Intra-Vehicular communication
- V2I/V2R
- V2V



Applications

- Navigation safety applications
  - crash prevention,
  - road problem warnings,
  - conditions of the driver,
- Navigation efficiency
  - Intelligent Transport Sys,
  - Road congestion avoidance,
  - personalized navigator,
  - pollution mitigation
- Vehicle monitoring
  - Carbon emission level,
- Emergency
  - Evacuations in case of disasters
- urban sensing
  - congestion, pollution sensing
- Entertainment:
  - download multimedia;
  - multiuser games
- Social networking;
  - proximity and correlated motion driven acquisition of friends/peers;
  - blog uploading

- Traffic management
- Automated toll payment
- Location-based services

VANET Vs MANET

- High speed mobility – but regular and predictable
- Topology is very dynamic
- No significant power constraints
- Localization information might be available

Types of Traffic

- Inter vehicle Communication
  - Multicast/Broadcast to transmit traffic related information over multiple hops to a group of receivers.
  - Emergency message dissemination.
- Vehicle to roadside
  - Single hop broadcast from RSU to all equipped vehicles in the vicinity.
  - High bandwidth link.
- Routing-based communications
  - Unicast multi-hop communication between vehicles.

MAC protocol

- Dedicated Short Range Communications (DSRC) is a short to medium range communications service that was developed to support vehicle-to-vehicle and vehicle-to-roadside communications.
- Wireless connectivity between moving vehicles can be provided by existing 802.11a compliant devices – but it has high overhead and complexity.
- In vehicular network, timely communication is essential.
- DSRC effort was migrated to the IEEE 802.11 standard group which renamed the DSRC to IEEE 802.11p –WAVE.
- Wireless Access in Vehicular Environments (WAVE) can be used for both Safety & Non- Safety Applications.

802.11p - Physical Layer

- IEEE802.11P adopts the OFDM PHY on 10-MHz channels in the 5.9 GHz frequency band.
- Wi-Fi industry normally implements the OFDM PHY on the 20-MHz channels, even though 5/10/20 MHz channels have been specified in IEEE802.11-2007 (2.4/5 GHz band).
- Modulation, channel coding etc. remains same.
- Supported Data rate -3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps
- Seven channels of 10 MHz bandwidth with various purposes -
  - Critical safety of life
  - High Power public safety
  - Control Channel (CCH) - safety communications only
  - Service Channel (SCH) -available for both safety and non-safety usage

802.11p

- V2I links –active only for short amount of time.
- Exchange data without the need to establish a basic service set (BSS).
- No need to wait for the association and authentication procedures to complete before exchanging data.
- Uses the wildcard BSSID (a value of all 1s) in the header of the frame.
- Start sending and receiving data frames as soon as they arrive on the communication channel.

Routing protocol - peculiarities

- Network topology.
- Mobility patterns.
- Density of vehicles at different times of the day.
- Rapid changes in vehicles arriving and leaving the VANET

Position based routing

- Position-based routing protocols require info about the physical position of the participating nodes.
- This position is made available to the direct neighbors in the form of periodically transmitted beacons.
- A sender can request the position of a receiver by means of a location service.
- The routing decision at each node - based on destination’s position contained in the packet & position of forwarding node’s neighbors.
- Position-based routing does not require the establishment / maintenance of routes.

Why PBR is suitable?

- Frequent topology changes.
- Short connectivity time.
- Availability of positioning systems.
- Use GPS technology enables forwarding to be decoupled from a node's identity and therefore the position of the destination node is used rather than a route to it.
- Position-based routing provides a more scalable and efficient forwarding mechanism appropriate for highly volatile ad hoc networks.

PBR - Mechanism

- Beaconing
- Location service
- Forwarding
  - geographic unicast
  - geographic broadcast

PBR- Beaconing

- Nodes periodically broadcast short packets with their ID and current geographic position.
- On reception of a beacon, a node stores the information in its location table.

PBR – Location service

- When a node needs to know the position of another node currently not available in its location table, it issues a location query message with the sought node ID, sequence number and hop limit.
- Neighboring nodes rebroadcast this message until it reaches the sought node (or the hop limit).
- sought node answers with a location reply message carrying its current position and timestamp.
- On reception of the location reply, the originating node updates its location table.

Geographic Unicast

- It provides packet transport between two nodes via multiple wireless hops.
- When a node wishes to send a unicast packet, it first determines the destination position (by location table look-up or the location service).
- Then, it executes a greedy forwarding algorithm, sending the packet to its neighbor with the minimum remaining distance to the destination.
- The algorithm is executed at every node along the forwarding path until the packet reaches the destination.

Geographic Broadcast

- It distributes data packets by flooding, where nodes re-broadcast the packets if they are located in the geographic area determined by the packet.
- Also, advanced broadcasting algorithms ensure avoidance of the so-called 'broadcast storms' minimize overhead.

Types

- Position based
  - DTN
  - Non-DTN
- Cluster-Based
- Geocast based
- Mobicast based
- Topology based
  - Proactive
  - Reactive
  - Hybrid
- Broadcast based

Broadcast protocols in VANET

- Highway scenario
  - BROADCOMM –Broadcast communication
- Urban Scenario
  - UMB - Urban multi-hop broadcast protocol
- Hybrid
  - RBLSM -Reliable Broadcasting of Life Safety Messages

Urban Multi-hop Broadcast

- Korkmaz et.al, Ohio State Univ, 2004
- IEEE 802.11 based multi-hop broadcast protocol (UMB) which is designed to address the broadcast storm, hidden node, and reliability problems of multi-hop broadcast in urban areas.
- Message dissemination to locations beyond the transmission range requires multi-hopping.
- Interference, packet collisions, and hidden nodes can stop the message dissemination during multi-hop broadcast.
- Multi-hop broadcast can consume significant amount of wireless resources because of unnecessary retransmissions.
- Message dissemination to different road segments at intersections.

Mechanism

- Sender nodes try to select the furthest node in the broadcast direction to assign the duty of forwarding and acknowledging the packet.
- Protocol divides the road portion inside the transmission range into segment (in the direction of broadcast).
- RTB/CTB handshake is performed with the selected node – Includes transmission duration, source node position, intended direction of broadcast.

Detection of farthest node

- Length of the black-burst signal in the 1st iteration.

$$L_1 = \left\lfloor \frac{d}{Range} * N_{max} \right\rfloor * SlotTime$$

  - L1 is the black-burst length in the 1st iteration,
  - D is the distance between the source and the vehicle,
  - Range is the transmission range,
  - Nmax is the number of segments created, and
  - SlotTime is the length of one slot.
- As a result of this computation, the furthest node sends the longest black-burst.

Data transmission and ACK

- After receiving a successful CTB, the source node sends its broadcast packet – ID of the selected node is included in packet.
- This corresponding node is now responsible for forwarding the broadcast packet and sending an ACK to the source.
- Although all other nodes between the source and the ACK sender receive the broadcast packet, they do not rebroadcast or acknowledge it.

Intersection broadcast

- At intersection, new directional broadcasts should be initiated to all road directions.
- Protocol assumes that there is repeater available at intersection to perform intersection broadcast.