IMPORTANT QUESTIONS & ANSWERS

Department of CSE

SUBJECT CODE: CS 6003

SUBJECT NAME: AD HOC AND SENSOR NETWORKS

Regulation: 2013 **Semester and Year: 07 and IV**

TABLE OF CONTENT

ANNA UNIVERSITY, CHENNAI-25
SYLLABUS COPY
AD HOC AND SENSOR NETWORKS
REGULATION 2013

CS6003 AD HOC AND SENSOR NETWORKS 3 0 0 3

UNITI INTRODUCTION 9

Fundamentals of Wireless Communication Technology – The Electromagnetic spectrum– Radio propagation Mechanisms – Characteristics of the Wireless Channel –mobile ad hoc networks(MANETs) and wireless sensor networks (WSNs) :concepts and architectures. Applications of Ad Hoc and Sensor networks. Design Challenges in Ad hoc and Sensor Networks.

UNIT II MAC PROTOCOLS FOR AD HOC WIRELESS NETWORKS 9

Issues in designing a MAC Protocol- Classification of MAC Protocols- Contention based protocols- Contention based protocols with Reservation Mechanisms- Contention based protocols with Scheduling Mechanisms – Multi channel MAC-IEEE 802.11

UNIT III ROUTING PROTOCOLS AND TRANSPORT LAYER IN ADHOC WIRELESS NETWORKS 9

Issues in designing a routing and Transport Layer protocol for Ad hoc networks-proactive routing, reactive routing (on-demand), hybrid routing- Classification of Transport Layersolutions-TCPoverAdhocwireless networks

UNIT IV WIRELESS SENSOR NETWORKS (WSNS) AND MAC PROTOCOLS 9

Single node architecture: hardware and software components of a sensor node - WSN Network architecture: typical network architectures-data relaying and aggregation strategies -MAC layer protocols: self-organizing, Hybrid TDMA/FDMA and CSMA based MAC- IEEE 802.15.4.

UNIT V WSN ROUTING, LOCALIZATION & QOS 9

Issues in WSN routing – OLSR- Localization – Indoor and Sensor Network Localization-absolute and relative localization, triangulation-QOS in WSN-Energy Efficient Design-Synchronization-Transport Layer issues.

TOTAL: 45 PERIODS

TEXTBOOK:

1. C. Siva Ram Murthy, and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures andProtocols",Prentice Hall Professional Technical Reference, 2008.

REFERENCES:

1. Carlos De Morais Cordeiro, Dharma Prakash Agrawal “Ad Hoc & Sensor Networks: Theory and Applications”, World Scientific Publishing Company, 2006.

2.Feng Zhao and Leonides Guibas, "Wireless Sensor Networks", Elsevier Publication - 2002.

3.Holger Karl and Andreas Willig “Protocols and Architectures for Wireless Sensor Networks”,Wiley,2005

4.Kazem Sohraby, Daniel Minoli, & Taieb Znati, “Wireless Sensor Networks- Technology, Protocols, and Applications”, John Wiley, 2007. 5. Anna Hac, “Wireless Sensor Network Designs”, John Wiley, 2

AIM AND OBJECTIVE OF THE SUBJECT

AIM:

To discuss the basic principles, design issues, operations and Different protocols used in ad hoc and wireless sensor networks.

OBJECTIVES:

Learn the basic wireless technologies

Understand the classification of MAC protocols and ad hoc routing protocols in WSN.

Be familiar in WSN Hardware and Software components

Understand the issues in Ad Hoc & Sensor network.

To learn the applications of Sensor nodes.

DETAILED LESSON PLAN

Text Book:

C. Siva Ram Murthy, and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols ", Prentice Hall Professional Technical Reference, 2008.

Reference Books:

Carlos De Morais Cordeiro, Dharma Prakash Agrawal “Ad Hoc & Sensor Networks : Theory and Applications”, World Scientific Publishing Company, 2006.

Feng Zhao and Leonides Guibas, "Wireless Sensor Networks", Elsevier Publication2002.

Holger Karl and Andreas Willig “Protocols and Architectures for Wireless SensorNetworks”,Wiley,2005

Kazem Sohraby, Daniel Minoli, & Taieb Znati, “Wireless Sensor Networks-Technology, Protocols, and Applications”, John Wiley, 2007.

Anna Hac, “Wireless Sensor Network Designs”, John Wiley, 2003.

Sl. no	Unit	Topic/Portions to be Covered	Hours Required /Planned	Cumm ulative Hrs	Books Referred
UNIT 1: INTRODUCTION					
1	1	Fundamentals of Wireless Communication Technology	1	1	TB1
2	1	The Electromagnetic Spectrum-Spectrum Allocation	1	2	TB1
3	1	Radio Propagation Mechanisms	1	3	TB1
4	1	Characteristics of the Wireless Channel	1	4	TB1
5	1	Mobile and ad hoc networks(MANETS) and wireless sensor networks(WSNs): concepts and architectures	1	5	TB1
6	1	Applications of Ad Hoc Wireless Networks	1	6	TB1
7	1	Design Challenges in Ad hoc and Sensor Networks	1	7	TB1
8	1	Transport Layer Protocols	2	9	TB1
UNIT II **MAC PRTOCOLS FOR AD HOC WIRELESS NETWORKS**					
8	2	Issues in designing a MAC protocol for ad hoc wireless networks	1	10	TB1

9	2	Classifications of MAC protocols	1	11	TB1
10	2	Contention-based protocols-MACAW,MACA-By Invitation	1	12	TB1
11	2	Contention-based protocols with Reservation Mechanisms-	2	14	TB1
12	2	Contention-based MAC protocols with Scheduling Mechanisms-	2	16	TB1
13	2	Multi channel MAC	1	17	TB1
14	2	IEEE 802.11	1	18	TB1
UNIT III **ROUTING PROTOCOLS AND TRANSPORT LAYER IN ADHOC WIRELESS NETWORKS**					
15	3	Issues in designing a routing protocol for ad hoc wireless networks	1	19	TB1
16	3	Table-driven routing protocols-	2	21	TB1
17	3	On-demand routing protocols-	1	22	TB1
18	3	Location-Aided Routing, Associativity	1	23	TB1
19	3	Hybrid routing protocols	1	24	TB1
20	3	Transport layer and security protocols for ad hoc wireless networks-& design issues.	1	25	TB1
21	3	Classification of Transport layer solutions	1	26	TB1
22	3	TCP over Ad Hoc Wireless Networks	1	27	TB1
UNIT IV **WIRELESS SENSOR NETWORKS(WSNS) AND MAC PROTOCOLS**					
23	4	Introduction to Sensor networks, Single node Architecture	1	28	R2
24	4	Hardware Components	1	29	R2
25	4	Software components	1	30	R2
26	4	WSN Architecture: Layered Architecture	1	31	TB1
27	4	Clustered Architecture	1	32	TB1
28	4	MAC layer protocols: self organizing	1	33	TB1
29	4	Hybrid TDMA /FDMA	1	34	TB1
30	4	CSMA based MAC	1	35	TB1
31	4	IEEE 802.15.4	1	36	R2
UNIT V **WSN ROUTING, LOCALIZATION & QOS**					
32	5	Issues in WSN routing	1	37	TB1

33	5	OLSR	1	38	TB1
34	5	Localization	1	39	TB1
35	5	Indoor and Sensor Network Localization	1	40	TB1
36	5	Absolute and relative localization, triangulation	1	41	TB1
37	5	QOS in WSN	1	42	TB1
38	5	Energy Efficient Design	1	43	TB1
39	5	Synchronization	1	44	TB1
40	5	Transport layer issues	1	45	TB1

UNIT I

INTRODUCTION

Fundamentals of Wireless Communication Technology – The Electromagnetic spectrum– Radio propagation Mechanisms – Characteristics of the Wireless Channel –mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs): concepts and architectures. Applications of Ad Hoc and Sensor networks. Design Challenges in Ad hoc and Sensor Networks.

PART- A

1. What is an ad hoc network?

An ad hoc network is a multi hop, infrastructure less network which has no centralized server to control the communication between the nodes and resources cannot be reserved beforehand. It is used in battlefields and military applications.

2. What are the challenging issues in ad hoc network maintenance?

The challenging issues in ad hoc network are

Medium access scheme

Routing

Multicast routing

Transport layer protocol

Pricing Schemes

Quality of Service Provisioning

Self-Organization

Security

Addressing and Service Discovery

Energy Management

Scalability

Deployment considerations

3. Why are ad hoc networks needed?

Ad hoc networking is often needed where an infrastructure network cannot be deployed and managed. The presence of dynamic and adaptive routing protocols enables quick formation of ad hoc networks and is suitable for emergency situations like natural disasters, spontaneous meetings or military conflicts.

4. List the applications of ad hoc networks.

Ad hoc networks are widely used in

Military applications and battlefields

Collaborative and distributed computing

Emergency search and rescue operations

Wireless sensor and mesh networks

5. List the transmission impediments of wireless channel. (or) List the characteristics of wireless channels.

The characteristics of wireless channel are

Path loss

Fading

Interference

Doppler Shift

rate constraints

6. What is fading? List the different types of fading.

Fading refers to the fluctuations in signal strength, when received at the receiver. It occurs due to multipath propagation. The different types of fading are

1.Slow/long term fading 2.Fast/short term fading

7. List the characteristics and Applications of MANETs.

The characteristics of MANETs are

Dynamic topologies

Bandwidth-constrained and variable capacity links.

Energy-constrained operation.

Limited physical security.

The applications of MANET are

Defense applications.

Crisis-management applications

Telemedicine

Tele-geo processing applications (e)Virtual navigation

Education via the internet

8. Define- MANET.

MANET is defined as an autonomous system of nodes or Mobile Stations (also serving as routers) connected by wireless links, the union that forms a communication networks, modeled in the form of an arbitrarily communication graph.

9. What is scattering?(Nov 2016)

When a radio wave impinges on a rough surface, the reflected energy is spread out in all directions. This is called scattering. It occurs when the wavelength of medium is small when compared to wavelength of travelled wave. e.g. Foliage, lamp post, sharp edges.

10. Define Reflection

When the propagating radio wave hits an object which is very large compared to its wavelength (such as the surface of the Earth, or tall buildings), the wave gets reflected by that object. Reflection causes a phase shift of 180 degrees between the incident and the reflected rays.

11. Write the equation for maximum data rate according to Shannon's theorem.

Shannon's theorem states the maximum data rate possible on a noisy channel. The maximum data rate is

$$\mathbf{C = B \times \log_2 (1+(S/N)) \text{ bits per second}}$$

Where C = maximum data rate, B = bandwidth S/N = signal to noise ratio. The Noise level is represented by SNR – Signal to Noise Ratio.

PART B

1. Explain in detail about Cellular and Ad Hoc Wireless Networks (Nov/Dec 2016)

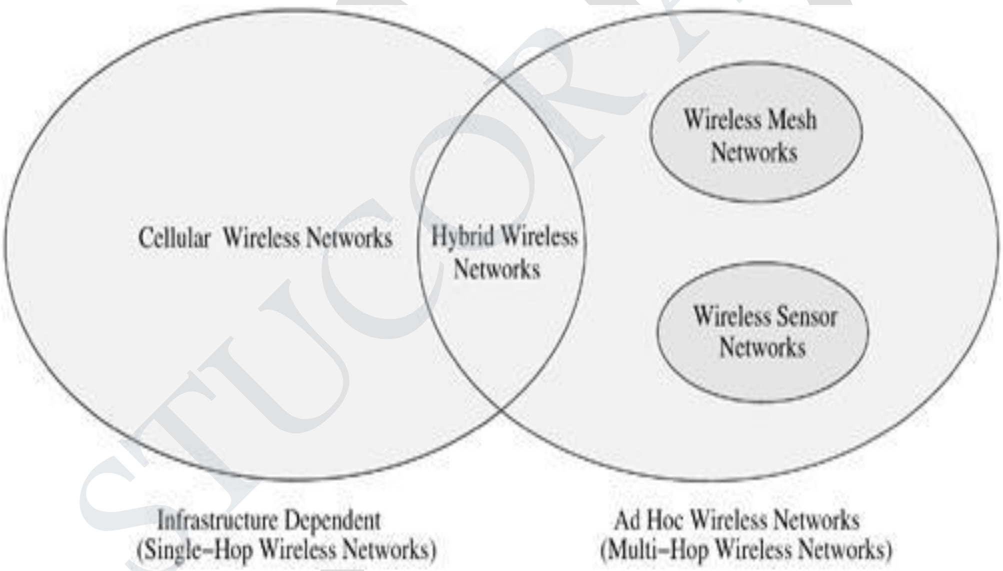

Cellular Wireless Networks
Hybrid Wireless Networks
Wireless Mesh Networks
Wireless Sensor Networks
Infrastructure Dependent (Single-Hop Wireless Networks)
Ad Hoc Wireless Networks (Multi-Hop Wireless Networks)

Figure1.1 Cellular and Ad hoc and wireless networks

The current cellular wireless networks are classified as the infrastructure dependent network. The path setup for a call between two nodes, say, node C to E, is completed through base station as illustrated in the figure 1.2

Ad hoc wireless networks are defined as a category of wireless network that utilize multi-hop radio replaying and are capable of operating without the support of any fixed infrastructure. Absence of any central coordinator or base station makes the routing complex.

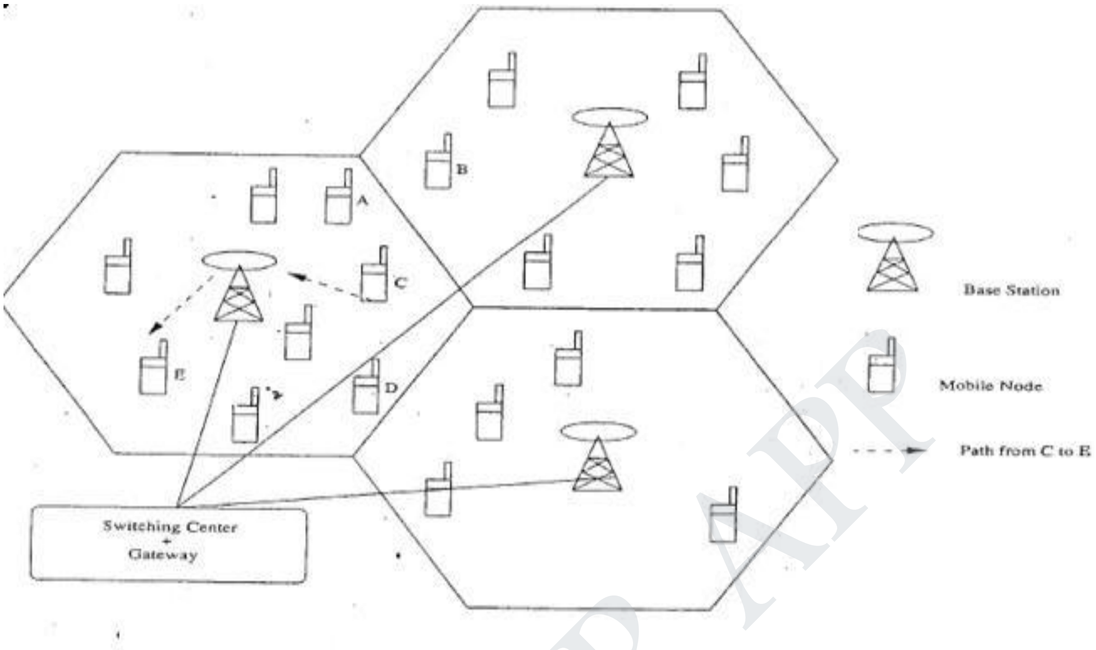


Figure1.2 Cellular networks

Ad hoc wireless network topology for the cellular network shown in above figure is illustrated below.

The path setup for a call between 2 nodes, say, node C to E , is completed through the intermediate mobile node F.

Wireless mesh network and Wireless sensor networks are specific examples of ad hoc wireless networks.

The presence of base station simplifies routing and resource management in a cellular network.

But in ad hoc networks, routing and resource management are done in a distributed manner in which all nodes co-ordinate to enable communication among them.

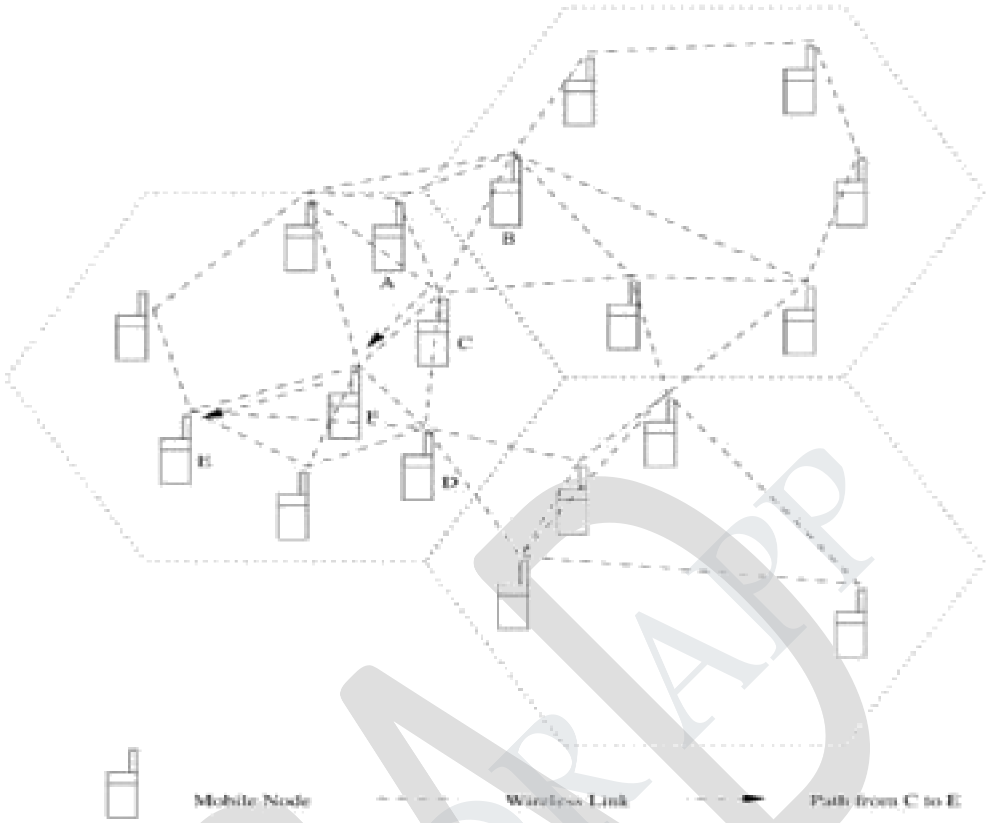


Figure 1.3 An Ad hoc wireless network

Difference between cellular networks and adhoc wireless networks.

Cellular Networks	Ad hoc Wireless network
Fixed Infrastructure based	Infrastructure less
Single hop wireless links	Multi-hop wireless links
Guaranteed Bandwidth(voice traffic)	Shared radio channel(data traffic)
Circuit-switched(evolving toward packet switching)	Packet-switched(evolved toward emulation of circuit switching)
High cost and time of deployment	Quick and cost – effective deployment
Reuse of frequency spectrum through geographical channel reuse	Dynamic frequency reuse based on carrier sense mechanism
Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth.

Cellular Networks	Ad hoc Wireless network
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control and protocols.
Application domains include mainly civilian and commercial sectors	Application domains include battle fields, emergency search and reuse operations and collaborative computing
High cost of network maintenance(backup Power source, staffing)	Self organization and maintenance properties are built into the networks
Mobile hosts are of relatively low complexity	Mobile host requires more intelligence
Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	Main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths.
Widely deployed and currently in the 3rd generation of Evolution	Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense.

2. Explain in detail about Applications of Ad Hoc Wireless

Networks Military Application:

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, ad hoc wireless networks provide required communication mechanism quickly.

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

Collaborative & Distributed computing

Adhoc wireless network helps in collaborative computing, by establishing temporary communication infrastructure for quick communication with minimal configuration among a group of people in a conference.

In distributed file sharing application reliability is of high importance which would be provided by adhoc network.

Other applications such as streaming of multimedia objects among participating nodes in ad hoc wireless networks require support for soft real-time communication

Devices used for such applications could typically be laptops with add-on wireless interface cards, enhanced personal digital assistants (PDAs) or mobile devices with high processing power

Emergency Operations

Ad hoc wireless networks are very useful in emergency operations such as search and rescue, crowd control and commando operations.

The major factors that favour ad hoc wireless networks for such tasks are self-configuration of the system with minimal overhead, independent of fixed or centralized 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 ad hoc wireless networks would be a good solution for co-ordinating rescue activities.

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

Wireless Mesh Network

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

It provides many alternate paths for a data transfer session between a source & destination, resulting in quick reconfiguration of the path when the existing path fails due to node failure.

Since the infrastructure built is in the form of small radio relaying devices, the investment required in wireless mesh networks is much less than what is required for the cellular network counterpart.

The possible deployment scenarios of wireless mesh networks include: residential zones, highways, business zones, important civilian regions and university campuses

Wireless mesh networks should be capable of self-organization and maintenance.

It operates at license-free ISM band around 2.4 GHz & 5 GHz.

It is scaled well to provide support to large number of points.

Major advantage is the support for a high data rate, quick & low cost of deployment, enhanced services, high scalability, easy extend ability, high availability & low cost per bit.

Wireless Sensor Networks:

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

Sensor nodes are tiny devices that have capability of sensing physical parameters processing the data gathered, & communication to the monitoring system. The issues that make sensor network a distinct category of ad hoc 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 :

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.

3. Explain in detail about Issues in Ad Hoc Wireless Networks.(Apr/May 2017)

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

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

1. Medium Access Scheme

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

a. Distributed Operation:

The ad hoc wireless networks need to operate in environments where no centralized coordination is possible.

The MAC protocol design should be fully distributed involving minimum control overhead.

b. Synchronization:

The MAC protocol design should take into account the requirement of time synchronization. Synchronization is mandatory for TDMA-based systems for management of transmission and reception slots.

c. Hidden Terminals:

Hidden terminals are nodes that are hidden(or not reachable) from the sender of a data transmission session, but are reachable to the receiver of the session.

d. Exposed terminals:

Exposed terminals, the nodes that are in the transmission range of the sender of an on-going session, are prevented from making a transmission.

e. Throughput:

The MAC protocol employed in adhoc wireless networks should attempt to maximize the throughput of the system.

f. Access delay:

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

g. **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.

h. 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.

i. 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.

j. 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.

k. 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.

l. 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.

m. Use of directional antennas:

This has many advantages that include

Increased spectrum reuse.

Reduction in interference and

Reduced power consumption

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}].

Consideration of the state of the wireless link, signal-to-noise ratio, and path loss for routing in ad hoc wireless networks can improve the efficiency of the routing protocol.

Location-dependent contention :

The load on the wireless channel varies with the number of nodes present in a given geographical region.

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

Efficiency

Control overhead

Quality of Service

Efficient group management

Scalability

Security

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.

Pricing Scheme

Assume that an optimal route from node A to node B passes through node C, & node C is not powered on.

Then node A will have to set up a costlier & non-optimal route to B.

The non-optimal path consumes more resources & affects the throughput of the system.

As the intermediate nodes in a path that relay the data packets expend their resources such as battery charge & computing power, they should be properly compensated.

Hence, pricing schemes that incorporate service compensation or service reimbursement are required.

6. Quality of Service Provisioning (QoS)

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

QoS-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.

Path loss.

QoS framework :

A framework for QoS is a complete system that attempts to provide the promised services to each user or application.

The key component of QoS framework is a QoS service model which defines the way user requirements are served.

7. 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)

8. Security

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

Attacks against network are of 2 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 of 2 types :

External attack: The active attacks that are executed by nodes outside the network.

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

9. 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.

10. 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.

11. 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.

12. Deployment Considerations

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

Low cost of deployment

Incremental deployment

Short deployment time

Reconfigurability

4. Explain in detail about Electromagnetic spectrum.

Wireless communication is based on the principles of broadcast and reception of electromagnetic waves. These waves can be characterized by their frequency (*f*) or their wavelength (λ). Frequency is the number of cycles (oscillations) per second of the wave and is measured in Hertz (Hz), in honor of Heinrich Hertz, the German physicist who discovered radio, and wavelength is the distance between two consecutive maxima or minima in the wave. The speed of propagation of these waves (*c*) varies from medium to medium, except in a vacuum where all electromagnetic waves travel at the same speed, the speed of light. The relation between the above parameters can be given as

$$\mathbf{C=\lambda*f}$$

where *c* is the speed of light (3 × 108*m*/*s*), *f* is the frequency of the wave in Hz, and λ is its wavelength in meters.

ITU, located in Geneva and a sub organization of the United Nations, coordinates wired and wireless telecommunication activities worldwide. There are no official names for the bands in which the very high-frequency X-rays and Gamma rays fall.

The low-frequency bands comprised of the radio, microwave, infrared, and visible light portions of the spectrum can be used for information transmission by modulating the amplitude, frequency, or the phase of the waves.

The high frequency waves such as X-rays and Gamma rays, though theoretically better for information propagation, are not used due to practical concerns such as the difficulty to generate and modulate these waves, and the harm they could cause to living things.

Radio waves are easy to generate and are widely used for both indoor and outdoor communication due to properties such as their ability to pass through buildings and ability to travel long distances. Since radio transmission is omni directional (when radio waves are generated, they spread out from the transmitting antenna in all directions) in nature, the need to physically align the transmitter and receiver also does not arise.

The frequency of the radio wave determines many of the characteristics of the transmission.

At low frequencies the waves can pass through obstacles easily, but their power falls with an inverse-squared relation with respect to the distance. The higher frequency waves are more prone to absorption by rain drops, and they get reflected by obstacles.

In the VLF, LF, and MF bands the propagation of waves, also called as ground waves The maximum transmission ranges of these waves are of the order of a few hundred kilometers. They are used for low bandwidth transmissions such as amplitude modulated (AM) radio broadcasting

The HF and VHF band transmissions are absorbed by the atmosphere near the Earth’s surface.

However, a portion of the radiation, called the sky wave, radiates outward and upward to the ionosphere in the upper atmosphere.

SNR is the ratio of the signal power to the noise power on a transmission medium, and is used to categorize the quality of a transmission. However, because of the higher frequency of operation they do not pass through buildings.

Infrared waves and waves in the EHF band (also known as millimeter waves) are used for short-range communication.

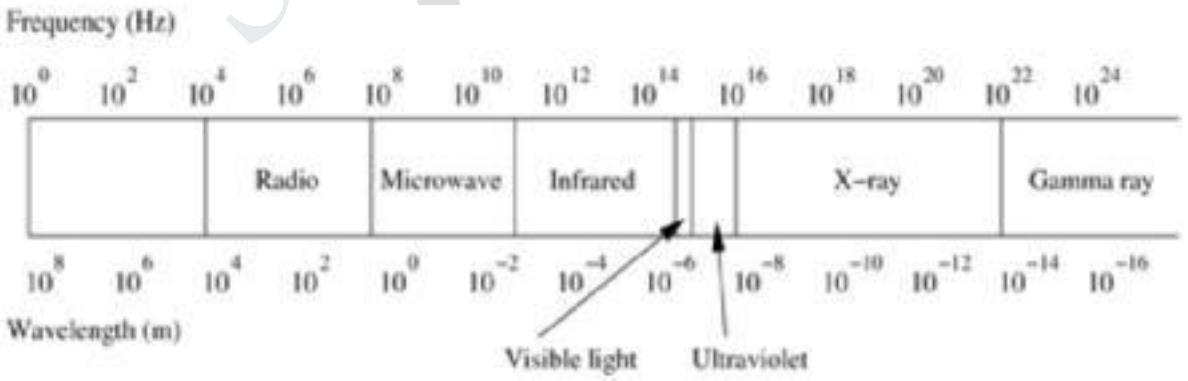


Figure 1.4 Frequency Spectrum

Spectrum Allocation

Worldwide, an agency of the International Telecommunications Union Radio communication (ITU-R) Bureau called World Administrative Radio Conference (WARC) tries to coordinate the spectrum allocation by the various national governments, so that communication devices that can work in multiple countries can be manufactured. Methods used for this frequency allocation are comparative bidding, lottery system and auctioning method.

5. Explain in detail about Radio Propagation Mechanisms (April/May 2017)

Radio waves generally experience the following three propagation mechanisms:

- **Reflection:**

  When the propagating radio wave hits an object which is very large compared to its wavelength (such as the surface of the Earth, or tall buildings), the wave gets reflected by that object. Reflection causes a phase shift of 180 degrees between the incident and the reflected rays.

- **Diffraction:**

  The propagation effect is undergone by a wave when it hits an impenetrable object. The wave bends at the edges of the object, thereby propagating in different directions. This phenomenon is termed as diffraction. The dimensions of the object causing diffraction are comparable to the wavelength of the wave being diffracted. The bending causes the wave to reach places behind the object which generally cannot be reached by the line-of-sight transmission. The amount of diffraction is frequency-dependent, with the lower frequency waves diffracting more.

- **Scattering:**

  When the wave travels through a medium, which contains many objects with dimensions small when compared to its wavelength, scattering occurs. The wave gets scattered into several weaker outgoing signals. In practice, objects such as street signs, lamp posts, and foliage cause scattering.

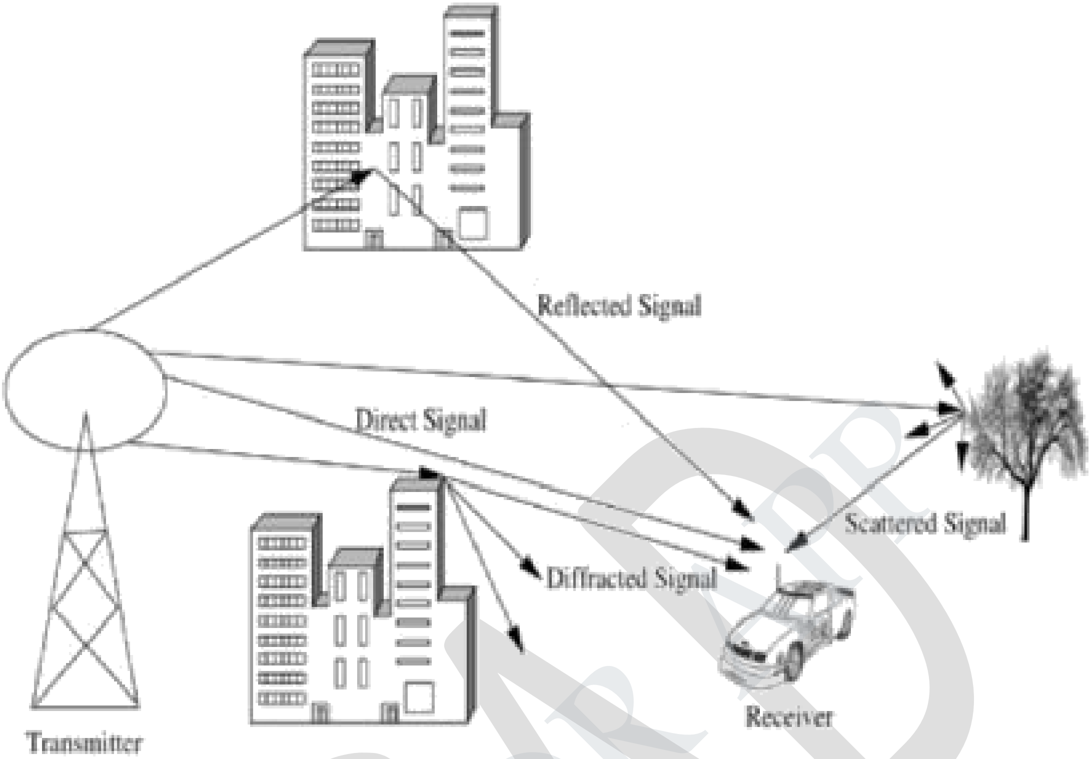


Figure 1.5 Radio Propagation mechanism.

UNIT II

MAC PROTOCOL FOR AD HOC WIRELESS NETWORKS

Issues in designing a MAC Protocol- Classification of MAC Protocols- Contention based protocols- Contention based protocols with Reservation Mechanisms- Contention based protocols with Scheduling Mechanisms – Multi channel MAC-IEEE 802.11

1. List the design goals of a MAC protocol for ad-hoc networks.

Design goals of a MAC protocol for ad-hoc networks are

The operation of the protocol should be distributed.

The protocol should provide QoS support for real-time traffic.

The access delay, which refers to the average delay experienced by any packet to get transmitted, must be kept low.

The available bandwidth must be utilized efficiently.

The protocol should ensure fair allocation of bandwidth to nodes.

Control overhead must be kept as low as possible.

The protocol should minimize the effects of hidden and exposed terminal problems.

The protocol must be scalable to large networks.

The protocol should have power control mechanisms.

The protocol should have mechanisms for adaptive data rate control.

The protocol should try to use directional antennas.

The protocol should provide synchronization among nodes.

2. List the issues of designing a MAC protocol for ad-hoc networks

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

Bandwidth efficiency

Bandwidth must be utilized in efficient manner

Quality of service support

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

Synchronization

MAC protocol must consider synchronization between nodes in the network Synchronization is very important for BW (time slot) reservation by nodes

Exchange of control packets may be required for achieving time synchronization among nodes.

Hidden and exposed terminal problems

The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender but are within the transmission range of the receiver.

Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other.

3. List the five phases of FPRP.

The five phases of FPRP are

Reservation request phase

Collision report phase

Reservation confirm phase

Reservation acknowledge phase

Packing/elimination phase

4. What are the mechanisms used in the MAC layer?

The mechanisms used in the MAC layer are

- Contention based protocols
- Contention based protocols with reservation mechanisms

Contention based protocols with scheduling mechanisms

Protocols with directional antennas.

5. List out the types of Contention-based protocols with reservation Mechanisms.

Synchronous protocols: All nodes need to be synchronized. Global time synchronization is difficult to achieve.

Asynchronous protocols: These protocols use relative time information for effecting reservations.

6. List the services provided by IEEE 802.11.

The services provided by IEEE 802.11 are

Association

De authentication

Disassociation

Integration

MSDU Delivery

Privacy

Re association

7. List out the types of Contention-based protocols

Sender-initiated protocols:

Packet transmissions are initiated by the sender node.Single-channel sender-initiated protocols: A node that wins the contention to the channel can make use of the entire bandwidth. Multichannel sender-initiated protocols: The available bandwidth is divided into multiple channels.

Receiver-initiated protocols:

The receiver node initiates the contention resolution protocol.

8. Define MARCH Protocol .

Media Access with Reduced Handshake Protocol (MARCH)

It is a receiver-initiated protocol.

It doesn’t require any traffic prediction mechanism.

It exploits the broadcast nature of traffic from Omni-directional antennas to reduce the number of handshakes involved in the data transmission.

9.Define the term PCL in Multichannel MAC.

Each node maintains a data structure called PCL (PreferableChannelList).

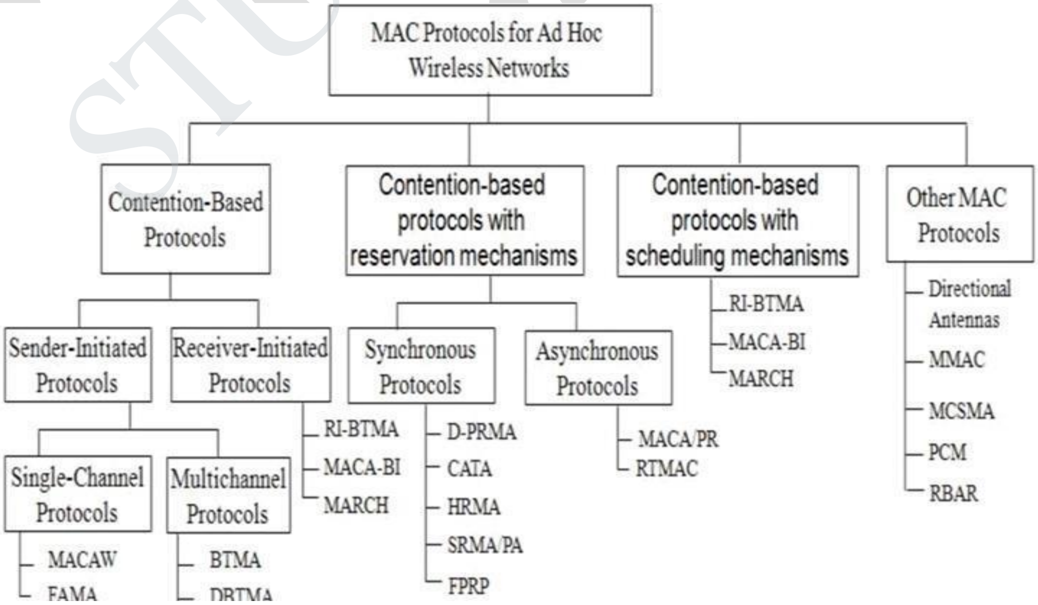
PCL contains the usage of the channels within the transmission-range of the node. Based on their usage, channels can be classified into three types:

1) High preference channel (HIGH): The channel has been selected by the current node and is being used by the node in the current beacon-interval.

2) Medium preference channel (MID): The channel is free and is not being currently used in the transmission-range of the node.

3) Low preference channel (LOW): The channel is already being used in the transmission-range of the node by other neighboring nodes. A counter is associated with each LOW state channel.

List out Classification Of Mac Protocols



PART- B

1. a) Explain in detail about Issues in Designing Mac Protocol for Ad Hoc Wireless Network. (April/May 2017) (Nov/Dec 2016)

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

Bandwidth efficiency

Bandwidth must be utilized in efficient

manner Minimal Control overhead

BW = ratio of BW used for actual data transmission to the total available BW

Quality of service support

Essential for supporting time-critical traffic sessions

They have resource reservation mechanism that takes into considerations

The nature of wireless channel and the mobility of nodes

Synchronisation

MAC protocol must consider synchronisation between nodes in the network Synchronisation is very important for BW (time slot) reservation by nodes.

Exchange of control packets may be required for achieving time synchronisation among nodes

Hidden and exposed terminal problems

The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender but are within the transmission range of the receiver.

Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other.

S1 and S2 are hidden from each other & they transmit simultaneously to R1 which leads to collision

The exposed terminal problem refers to the inability of a node, which is blocked due to transmission by a nearby transmitting node, to transmit to another node.

If S1 is already transmitting to R1, then S3 cannot interfere with on-going transmission & it cannot transmit to R2.

The hidden & exposed terminal problems reduce the throughput of a network when traffic load is high.

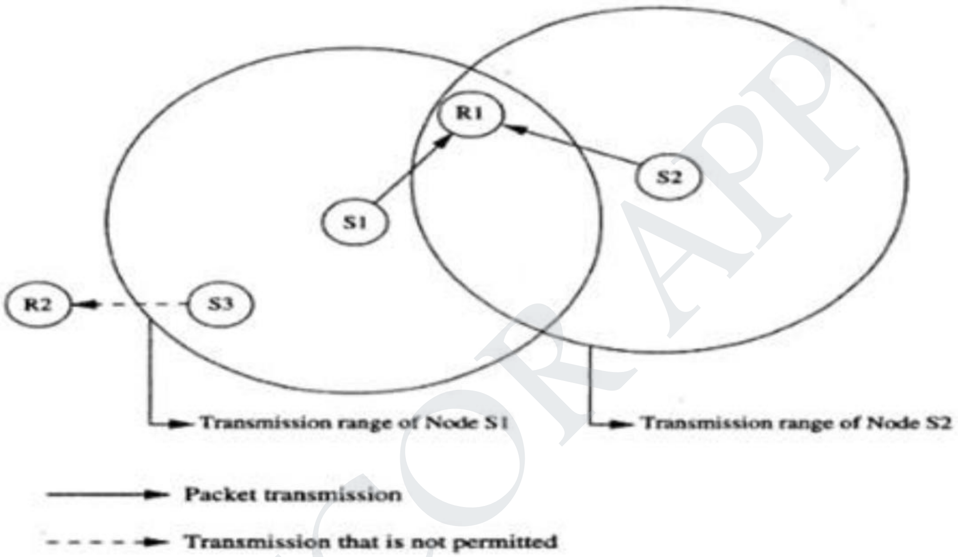

R1
S2
S1
R2
S3
Transmission range of Node S1
Transmission range of Node S2
Packet transmission
Transmission that is not permitted

Figure 2.1 Hidden and exposed terminal problem

Error-prone shared broadcast channel

When a node is receiving data, no other node in its neighborhood should transmit data. A node should get access to the shared medium only when its transmission do not affect any ongoing session

MAC protocol should grant channel access to nodes in such a manner that collisions are minimized. Protocol should ensure fair BW allocation.

Distributed nature/lack of central coordination

Do not have centralized coordinators

Nodes must be scheduled in a distributed fashion for gaining access to the channel

MAC protocol must make sure that additional overhead, in terms of BW consumption, incurred due to this control information is not very high.

Mobility of nodes

Nodes are mobile most of the time

The protocol design must take this mobility factor into consideration so that the performance of the system is not affected due to node mobility.

1b) Explain the Design Goals of a Mac Protocol for Ad Hoc Wireless Networks

The operation of a protocol should be distributed

The protocol should provide QoS support for real-time traffic

The access delay, which refers to the average delay experienced by any packet to get transmitted, must be kept low

The available bandwidth must be utilized efficiently

The protocol should ensure fair allocation of bandwidth to nodes

Control overhead must be kept as low as possible

The protocol should minimize the effects of hidden and exposed terminal problems.

The protocol must be scalable to large networks

It should have power control mechanisms in order to efficiently manage energy consumption of the nodes

The protocol should have mechanisms for adaptive data rate control.

1c). Explain different Classification of Mac Protocols. (April/May 2017)

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

Contention-based protocols

Contention-based protocols with reservation mechanisms

Contention-based protocols with scheduling mechanisms

Contention-based protocols:

Sender-initiated protocols:

Packet transmissions are initiated by the sender node.

Single-channel sender-initiated protocols:

A node that wins the contention to the channel can make use of the entire bandwidth.

Multichannel sender-initiated protocols:

The available bandwidth is divided into multiple channels.

Receiver-initiated protocols:

The receiver node initiates the contention resolution protocol.

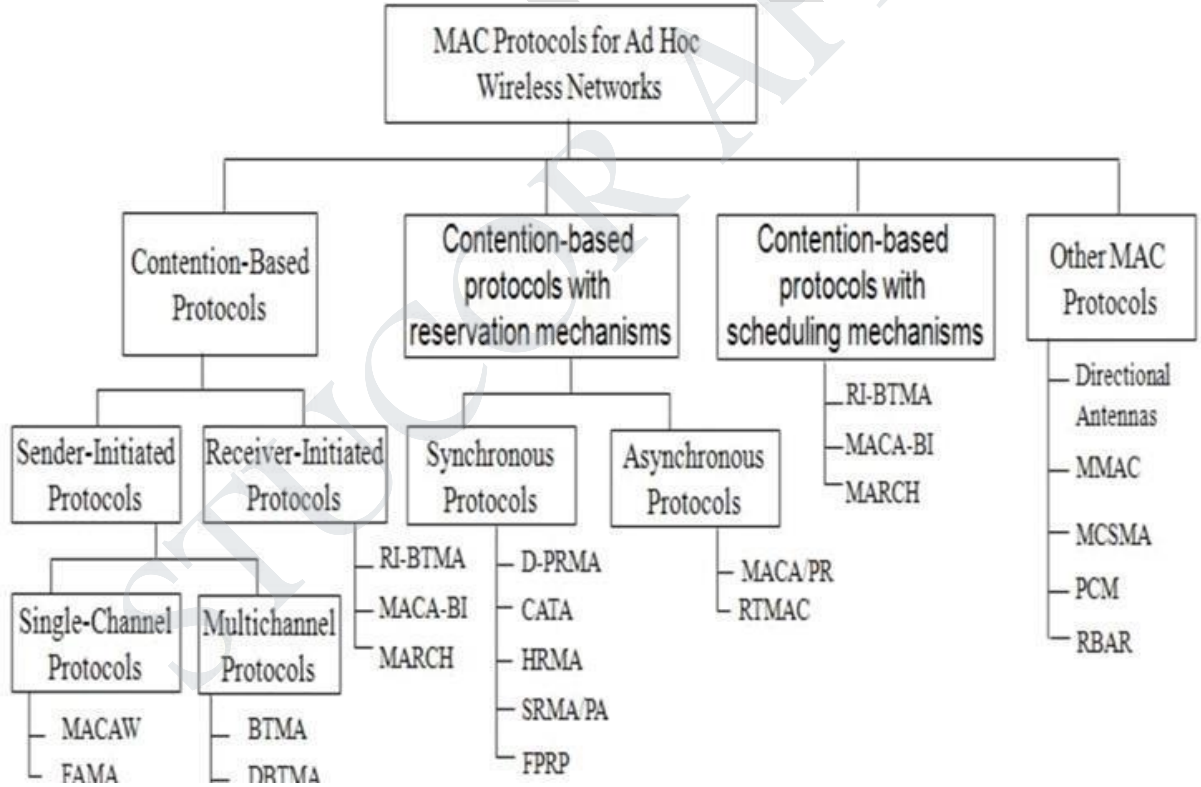


Figure 2.2 Classification of MAC protocols

Contention-based protocols with reservation mechanisms

Synchronous protocols: All nodes need to be synchronized. Global time synchronization is difficult to achieve.

Asynchronous protocols: These protocols use relative time information for effecting reservations.

Contention-based protocols with scheduling mechanisms

Node scheduling is done in a manner so that all nodes are treated fairly and no node is starved of bandwidth.

Scheduling-based schemes are also used for enforcing priorities among flows whose packets are queued at nodes.Some scheduling schemes also consider battery characteristics.

Other protocols are those MAC protocols that do not strictly fall under the above categories.

3. Explain in Detail about Contention Based Protocols With Reservation Mechanisms

a)Distributed Packet Reservation Multiple Access Protocol (D-PRMA)

It extends the centralized packet reservation multiple access (PRMA) scheme into a distributed scheme that can be used in ad hoc wireless networks.

PRMA was designed in a wireless LAN with a base station.

D-PRMA extends PRMA protocol in a wireless LAN.D-PRMA is a TDMA-based scheme. The channel is divided into fixed- and equal-sized frames along the time axis.

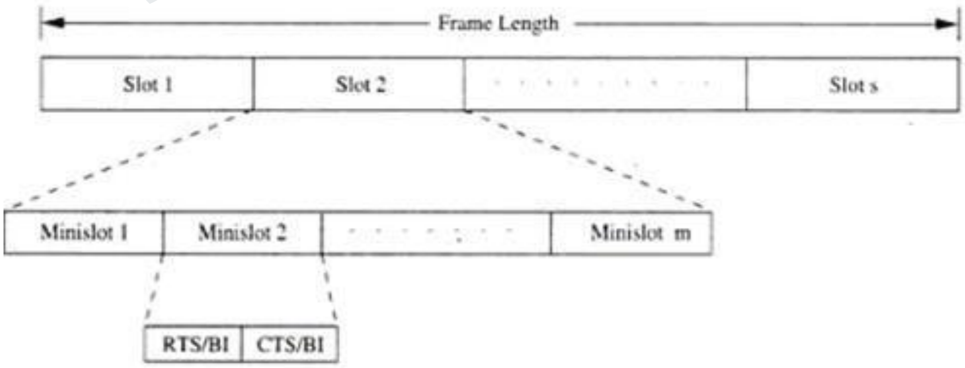


Figure 2.3 Frame structure in D-PRMA

Each frame is composed of s slots and each slot consists of m minislots.

Each minislot is further divided into two control fields, RTS/BI and CTS/BI

These control fields are used for slot reservation and for overcoming the hidden terminal problem

All nodes having packets ready for transmission contend for the first minislot of each slot

The remaining (m-1) minislots are granted to the node that wins the contention.Also, the same slot in each subsequent frame can be reserved for this winning terminal until it completes its packet transmission session

Within a reserved slot, communication between the source and receiver nodes takes by means of either time division duplexing (TDD) or frequency division duplexing (FDD)

Any node that wants to transmit packets has to first reserve slots.

A certain period at the beginning of each minislot is reserved for carrier sensing

In order to prioritize nodes transmitting voice traffic over nodes transmitting normal data traffic, two rules are followed in D-PRMA

1st rule : voice nodes are allowed to start contending from minislot 1 with probability p=1. Others with p<1 2nd rule :only if the node winning the minislot contention is a voice node, it is permitted to reserve the same slot in each subsequent frame until the end of the session.

In order to avoid the hidden terminal problem, all nodes hearing the CTS sent by the receiver are not allowed to transmit during the remaining period of that same slot

In order to avoid the exposed terminal problem, a node hearing the RTS but not the CTS is still allowed to transmit

Requirement 1 when a node wins the contention in minislot 1, other terminals must be prevented from using any of the remaining (m-1) minislots in the same

slot for contention

Requirement 2 when a slot is reserved in subsequent frames, other nodes should be prevented from contending for those reserved slots

D-PRMA is more suited for voice traffic than for data traffic applications

Collision Avoidance Time Allocation Protocol (CATA)

It is based on dynamic topology-dependent transmission scheduling.Nodes contend for and reserve time slots by means of a distributed reservation and handshake mechanism.

It Support broadcast, unicast, and multicast transmissions.

The operation is based on two basic principles:

The receiver(s) of a flow must inform the potential source nodes about the reserved slot on which it is currently receiving packets.

The source node must inform the potential destination node(s) about interferences in the slot.

Usage of negative acknowledgements for reservation requests, and control packet transmissions at the beginning of each slot, for distributing slot reservation information to senders of broadcast or multicast sessions.

Time is divided into equal-sized frames, and each frame consists of S slots.

Each slot is further divided into five mini slots.

The first 4 mini slots are used for transmitting control packets and are called control mini slots (CMS)

The last mini slot is called data mini slot (DMS).

While the last mini slot is used for data transmission and is called data mini slot(DMS).

CMS1: Slot Reservation (SR)
CMS2: RTS
CMS3: CTS
CMS4: not to send (NTS)
DMS: Data transmission

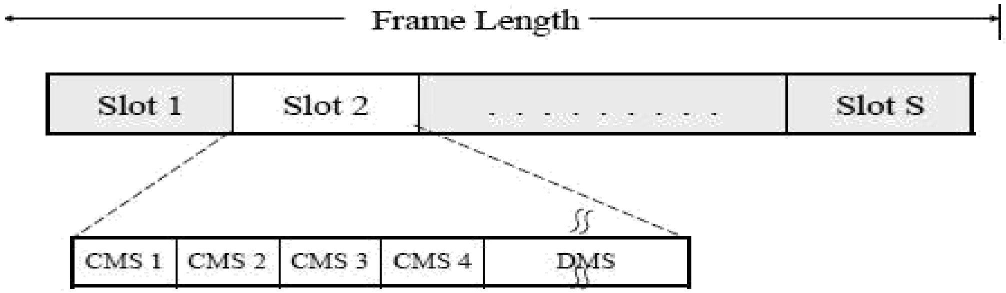


Figure 2.4 Frame format in CATA

The CMS1 and CMS2 are used to inform neighbors about the current reservation. While CMS3 and CMS4 are used for channel reservation.

Each node that receives data during the DMS of current slot transmits an SR in CMS1.This serves to inform other neighbouring potential sender nodes about the currently active reservations.

Every node that transmits data during the DMS of current slot transmits an RTS in CMS2, CMS3 and CMS4 are used as follows:

The sender of an intend reservation, if it senses the channel is idle in CMS1, transmits an RTS in CMS2 Then the receiver transmits a CTS in CMS3.

If the reservation was successful, the data can be transmitted in current slot and the same slot in subsequent frames.

Once the reservation was successfully, in the next slot both the sender an receiver do not transmit anything during CMS3.
During CMS4, the sender transmits a NTS(NTS serves as a negative ack)

A potential multicast source node that receives the NTS packet understands that its reservation is failed.

Advantages:

It works well with simple single-channel half-duplex radios

It is simple and provides support for collision-free broadcast and multicast traffic.

Hop Reservation Multiple Access Protocol (HRMA)

It is a time slot-reservation protocol where each slot is assigned a separate frequency channel.

A handshake mechanism is used for reservation to enable node pairs to reserve a frequency hop, thus providing collision-free communication and avoiding the hidden terminal problem.

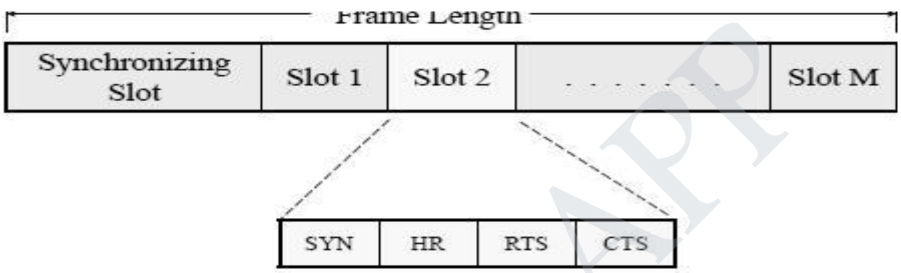


Figure 2.5 Frame format in HRMA

One frequency channel is a dedicated synchronizing channel where nodes exchange synchronization information.

The remaining frequency channels are paired, one channel in each pair is used for hop-reservation packets(RTS & CTS) & data packets, the other one is used for acknowledgement (ACK).

Time is slotted and each slot is assigned a separate frequency hop.

Each time slot is divided into four periods, namely, synchronizing period, HR period, RTS period, and CTS period.

Each period meant for transmitting or receiving the synchronizing packet, FR packet, RTS packet, and CTS packet respectively.

After the handshaking is over, the two nodes communicate by sending data and ACKs on the very same frequency channels. All idle nodes hop to the synchronizing frequency *f0* and exchange synchronization information.

Synchronizing slot is used to identify the beginning of a frequency hop and the frequency to be used in the immediately following hop

A node ready to transmit data, it senses the HR period of the current slot .If the channel is idle during HR period; it transmits an RTS during RTS period and waits for CTS during CTS period.

On receiving the RTS, the destination node transmits the CTS packet during the CTS period of the same slot and waits for the data packet.

If the source node receives the CTS packet correctly, it implies that the source and receiver nodes have successfully reserved the current hop. If the channel is busy during HR period, it backs off for a randomly multiple slots.

Suppose the sender needs to transmit data across multiple frames, it informs the receiver through the header of the data packet. The receiver node transmits an HR packet during the HR period of the same slot in next frame to inform its neighbors.

The sender receiving the HR packet, it sends an RTS during the RTS period and jams other RTS packets. Both receivers remain silent during the CTS period.

Soft Reservation Multiple Access with Priority Assignment (SRMA/PA)

It is developed with the main objective of supporting integrated services of real-time and non-real-time application in ad hoc networks.

Nodes use

a collision-avoidance handshake mechanism and

a soft reservation mechanism

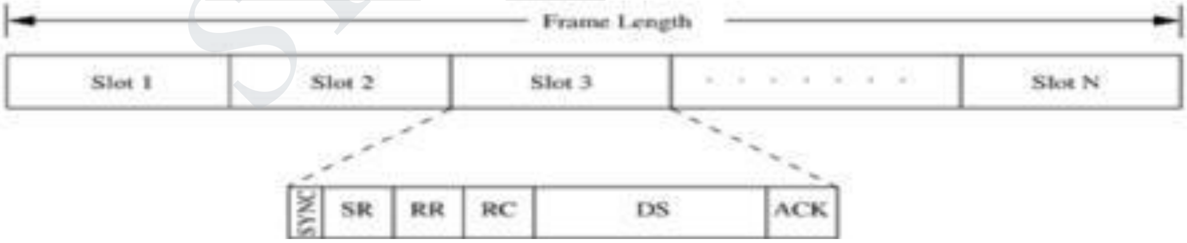


Figure 2.6 Frame structure in (SRMA/PA)

Time is divided into frames, with each frame consisting of a fixed number of slots.Each slot is further divided into 6 different fields namely SYNC, soft reservation (SR), reservation request (RR), reservation confirm (RC), data sending (DS) and acknowledgement (ACK).

The SYNC field is used for synchronization purposes

The SR, RR, RC, & ACK fields are used for transmitting & receiving the corresponding control packets

The DS field is used for data transmission

The SR packet serves as a busy tone. It informs the nodes about the reservation of the slot. It also carries the access priority value assigned to the node that has reserved the slot

A node determines whether or not a slot is free through the SR field of that slot. When an idle node receives a data packet for transmission, the node waits for a free slot and transmits the RR packet in the RR field of that slot.

In case of a voice terminal node, the node tries to take control of the slot already reserved by a data terminal if it finds it priority level to be higher than that of the data terminal. This process is called soft reservation.

Priority levels are initially assigned to nodes based on the service classes in a static manner.

It is required that priority of voice terminal pv(R) > priority of data terminal pd(R).

A node can be in one of the two states:

A node is said to be in the active state if it is currently transmitting

A node is said to be in the idle state if it does not have any packet to be transmitted

In the active state itself, nodes can be in one of the two states: access state and reserved state. Access state is one in which the node is backlogged and is trying to reserve a slot for transmission.In order to avoid collisions,a binary exponential back-off algorithm is used for non-real time connections and a modified binary exponential back-off algorithm is used for real time connection

E)Five-Phase Reservation Protocol (FPRP)

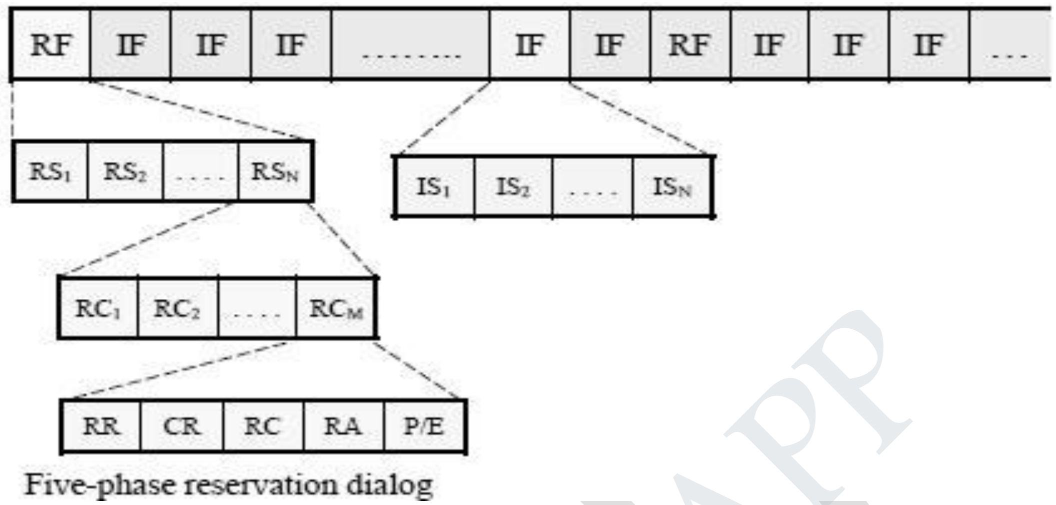


Figure 2.7 Frame structure in FPRP

It is a single-channel TDMA-based broadcast scheduling protocol.

The protocol is fully distributed, that is, multiple reservations can be simultaneously made throughout the network.

The protocol assumes the availability of global time at all nodes.

No ordering among nodes is followed

Nodes need not wait for making time slot reservations.

Time is divided into frames:

Reservation frame (RF) and

Information frame (IF).

Each RF has N reservation slots (RS) and each IF has N information slots (IS). Each RS is composed of M reservation cycles (RCs). Each RF is followed by a sequence of IFs. In order to reserve an IS, a node needs to contend during the corresponding RS.

Based on these contentions, a TDMA schedule is generated in the RF and is used in the subsequent Ifs until the next RF.

During the corresponding IS, a node would be in one of the three states: transmit(T), receive(R) or blocked(B)

The reservation takes following five phases:

1. Reservation request phase:

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

2. Collision report phase:

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

3. Reservation confirmation phase:

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

4. Reservation acknowledgment phase:

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

5. Packing and elimination (P/E) phase:

Two types of packets are transmitted during this phase: packing packet and elimination packet.

MACA with Piggy-Backed Reservation (MACA/PR)

It is based on the MACAW protocol with non-persistent CSMA

The main components are:

A MAC protocol

A reservation protocol

A QoS routing protocol

It differentiates real-time packets from the best-effort packets. It provides guaranteed bandwidth support for real-time packets.Also, it provides reliable transmission of best efforts packets.

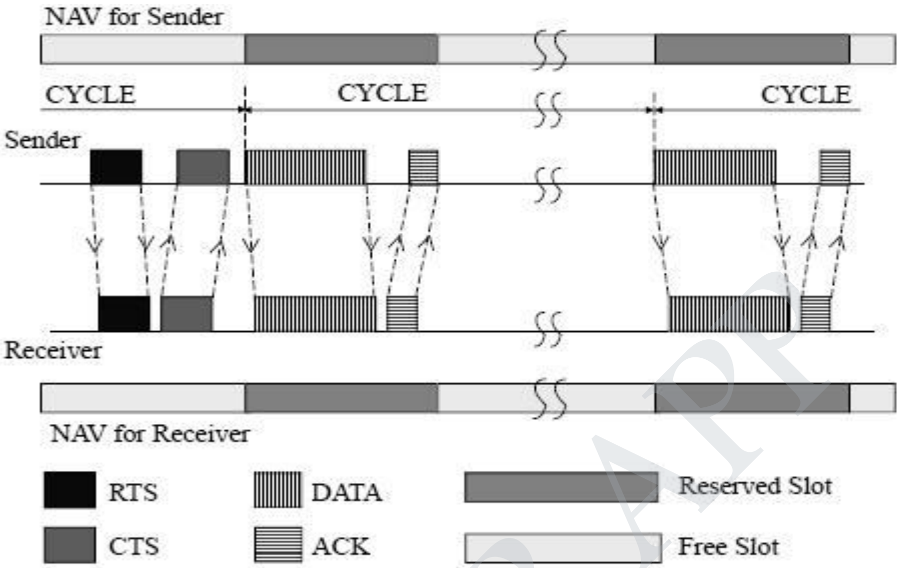


Figure 2.8 Packet transmission in MACA/PR

Time is divided into slots. Each node records the transmit and receive reservations of its neighbors in a reservation-table(RT). For real-time traffic the source first sends an RTS packet, for which the receiver responds with a CTS packet. Now the source sends the first DATA packet of the real-time session.

Reservation information for the next DATA packet is piggy-backed on this current DATA packet.

On receiving this DATA packet, the receiver updates its reservation table with the piggy-backed reservation information

The receiver then sends ACK packet back to the source,Receiver piggy-backs the reservation confirmation information on the ACK packet

Advantage: It does not require global synchronization among nodes

Drawback: A free slot can be reserved only if it can fit the entire RTS-CTS-DATA-ACK exchange.

G) Real-Time Medium Access Control Protocol (RTMAC)

It provides a bandwidth reservation mechanism for supporting real-time traffic. It has two components:

1) QoS routing protocol is responsible for end-to-end reservation & release of bandwidth resources

MAC protocol is responsible for medium access for best effort traffic & reservation for real time traffic.

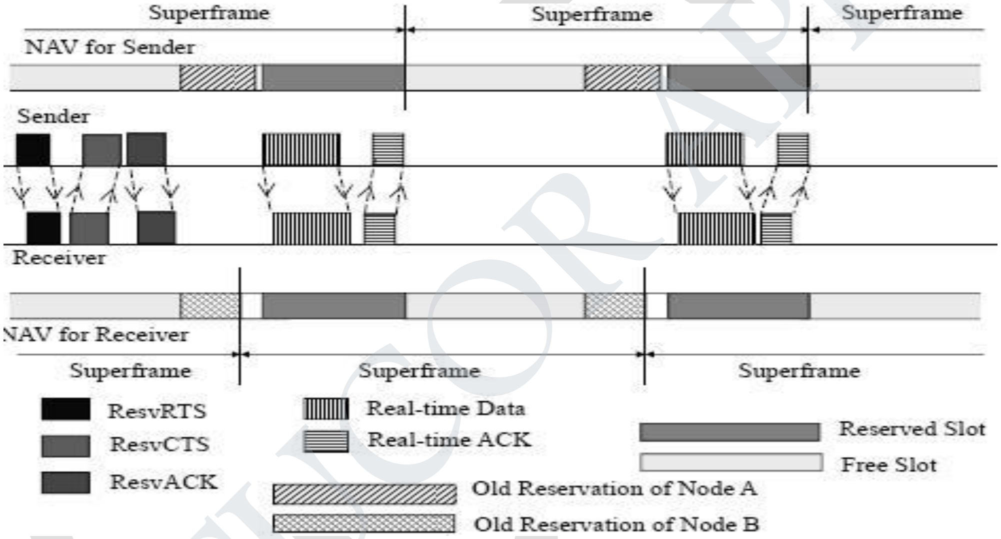


Figure 2.9 Packet transmission in RTMAC

For transmitting best effort packets: RTS, CTS, and ACK are used.For transmitting real time packets: ResvRTS, ResvCTS, and ResvACK are used

Time is divided into super frames. Each superframe consists of a number of reservation-slots (resv).A node that needs to transmit real-time packets, first reserves a set of resv-slots.

The set of resv-slots reserved by a node for a connection on a superframe is called a connection-slot.

The duration of each resv-slot is twice the maximum propagation delay. Each node maintains a reservation table (RT). RT contains information such as sender-id & receiver-id.starting and ending times of active reservation.

NAV indicates the network allocation vector maintained at each node.

Advantages:

Bandwidth efficiency

Asynchronous mode of operation where nodes do not require any global time synchronization

Flexibility of slot placement in the super frame.

4. Explain in detail about Contention Based Protocols. (Nov/Dec 2016)

MACAW (MACA for Wireless)

Back-off mechanism used in MACA starves flows

To prevent large variations in the back-off values, a multiplicative increase and linear decrease (MILD) is used in MACAW.

On Collision: back-off is increased by a multiplicative factor (1.5)

On Successful transmission: back-off is decreased by one

The sender senses the carrier to see and transmits a RTS (Request To Send) frame if no nearby station transmits a RTS.

The receiver replies with a CTS (Clear To Send) frame. Sender sends DATA, for which receiver responds with ACK. RTS/CTS packets carry the expected duration of the data transmission.

A node near the receiver on hearing the CTS packet, defers its transmission till the receiver receives the data packet. This overcomes hidden node problem.

A node near the sender that only hears the RTS is free to transmit simultaneously when the sender is transmitting data. This overcomes exposed node problem

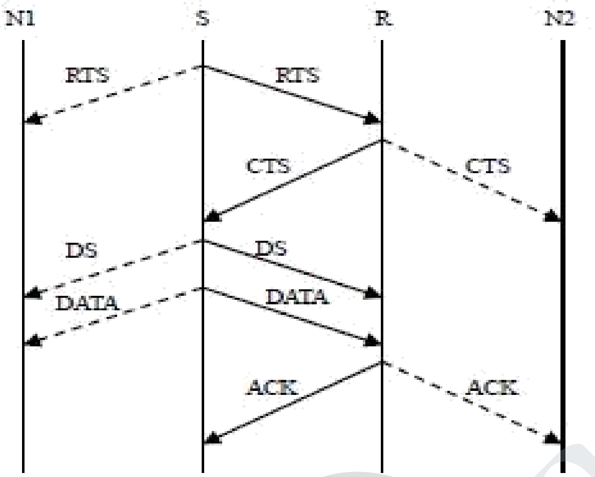


Figure 2.10 Packet exchange in MACAW

.

The receiver sends an ACK when receiving a frame.

→ Neighbors keep silent until see ACK.

Collision handling: If a packet is lost (collision), the node uses the binary exponential back-off (BEB) algorithm to back off for a random time interval before retrying.

RTS/CTS mechanism does not solve the exposed terminal problem.

Solution: New control packet called data-sending (DS) can be used. DS contains information such as the duration of the forthcoming data transmission.

The protocol uses one more control packet called the request-for-request-to-send (RRTS)

Synchronization information needs to be propagated to the concerned nodes.

If a node had received an RTS previously for which it was not able to respond because there exists on-going transmission, then it waits for the next contention period and transmits RRTS.

B)Floor Acquisition Multiple Access Protocols (FAMA)

- It is based on a channel access discipline which consists of
  - a carrier-sensing operation and

a collision-avoidance dialog between the sender and the intended receiver of a packet

Floor acquisition refers to the process of gaining control of the channel.

At any time, only one node is assigned to use the channel.

Carrier-sensing by the sender,

followed by the RTS-CTS control packet exchange,

enables the protocol to perform as efficiently as MACA

Data transmission to be collision free, the duration of an RTS must be at least twice the maximum channel propagation delay

Two variations of FAMA

RTS-CTS exchange with no carrier-sensing uses the ALOHA protocol for transmitting RTS packets (MACA).

RTS-CTS exchange with non-persistent carrier-sensing uses non-persistent CSMA for the same purpose(FAMA-NTR).

FAMA-NTR

Before sending a packet, the sender senses the channel.

If channel is busy, the sender back-off a random time and retries later.

If the channel is free, the sender sends RTS and waits for a CTS packet.

If the sender cannot receive a CTS, it takes a random back-off and retries later.

If the sender receives a CTS, it can start transmission data packet.

In order to allow the sender to send a burst of packets, the receiver is made to wait a time duration τ seconds after a packet is received.

C)Busy Tone Multiple Access Protocols (BTMA)

- The transmission channel is split into two:
  - ○ → a data channel for data packet transmissions
  - ○ → a control channel used to transmit the busy tone signal

When a node is ready for transmission, it senses the channel to check whether the busy tone is active. If not, it turns on the busy tone signal and starts data transmissions.Otherwise, it reschedules the packet for transmission after some random rescheduling delay.

When a node is transmitting, no other node in the two-hop neighborhood of the transmitting node is permitted to simultaneously transmit.

Drawback: very poor bandwidth utilization

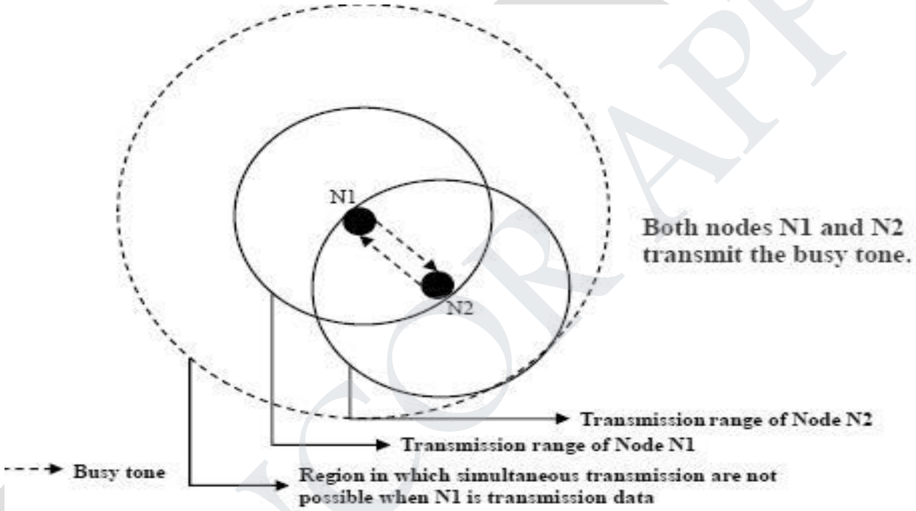

N1
N2
Both nodes N1 and N2 transmit the busy tone.
Transmission range of Node N2
Transmission range of Node N1
Busy tone
Region in which simultaneous transmission are not possible when N1 is transmission data

Figure 2.11Transmission in BTMA

Dual Busy Tone Multiple Access Protocol (DBTMAP)

The transmission channel is divided into:

The data channel is used for data packet transmission

The control channel is used for RTS, CTS, busy tones

Use two busy tones on the control channel, BTt and BTr.

BTt: indicate that it is transmitting on the data channel

BTr: indicate that it is receiving on the data channel

Two busy tone signals are two sine waves at different Frequencies

When a node is ready to transmit a data packet

- First, it senses the channel to determine whether the BTr signal is active
- If there is no BTr signal, then it transmit RTS packet

On receiving the RTS packets, receiver checks whether the BTt tone is active

If there is no BTt signal, Receiver Sends CTS packet and turns on the BTr signal

Sender receives CTS, turns on BTt signal, starts data transmission and turns off BTt signal

Receiver receives data and turn off BTr signal

DBTMA has better network utilization than RTS/CTS based protocol.

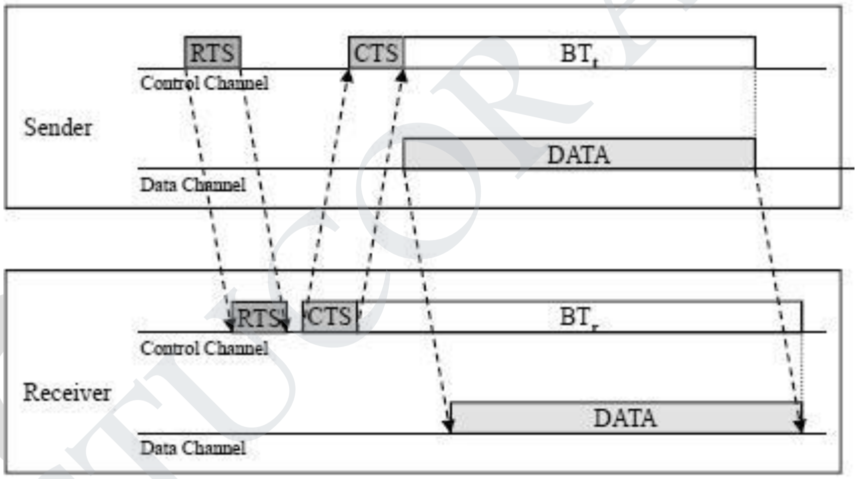


Figure 2.12 Packet transmission in DBTMA

Receiver-Initiated Busy Tone Multiple Access Protocol (RI-BTMA)

The transmission channel is split into two:

a data channel for data packet transmissions

a control channel used for transmitting the busy tone signa

A node can transmit on the data channel only if it finds the busy tone to be absent on the control channel.

The data packet is divided into two portions: a preamble and the actual data packet.The busy tone serves two purposes:

Acknowledges the sender the successful of receiving preamble

Inform the nearby hidden nodes the impending transmission

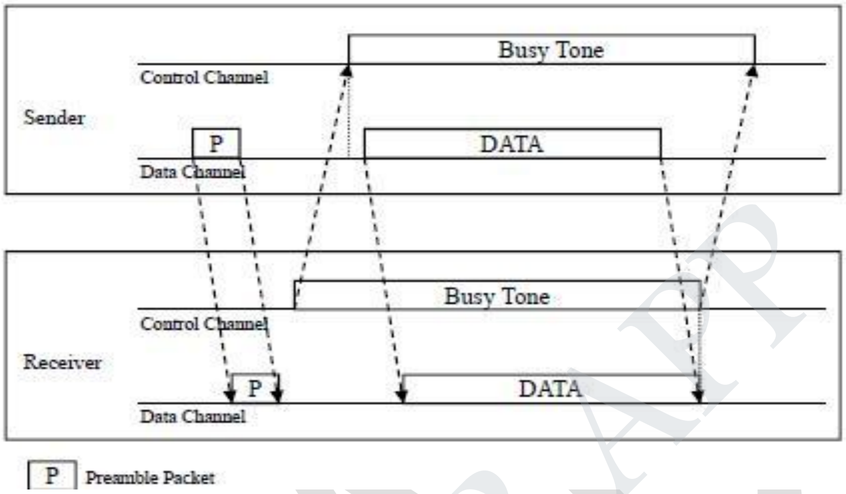


Figure 2.13 Packet transmission in RI-BTMA The operation of the RI-BTMA protocol contains two types

→The basic protocol

No backlog buffers: packets that suffer collisions cannot be retransmitted

→The controlled protocol

Backlogged mode: backlog buffer is non-empty

Backlog buffers: transmitting a backlogged packet in next idle slot with a probability q.Non-backlogged mode: transmitting a non-backlogged packet in the next idle slot with a probability p.

MACA-By Invitation Protocol (MAC BI)

It is a receiver-initiated protocol.

It reduces the number of control packets used in the MACA protocol.

It eliminated the need for the RTS packet.

The receiver node initiates data transmission by transmitting a ready-to-receive(RTR) control packet to the sender.

If it is ready to transmit, the sender node responds by sending a DATA packet. Thus, data transmission occurs through a two way handshake mechanism.

The efficiency of the MACA-BI scheme is mainly dependent on

→the ability of the receiver node to predict accurately the arrival rates of traffic at the sender nodes.

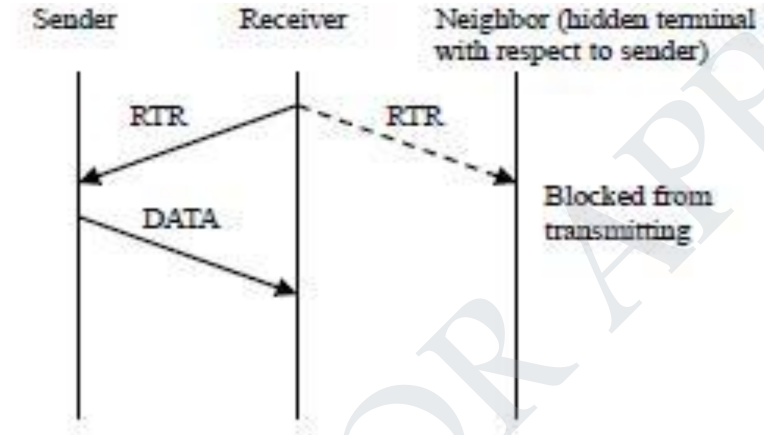

Sender
Receiver
Neighbor (hidden terminal with respect to sender)
RTR
RTR
DATA
Blocked from transmitting

Figure 2.14 Packet transmission in MACA-BI

Media Access with Reduced Handshake Protocol (MARCH)

It is a receiver-initiated protocol.

It doesn't require any traffic prediction mechanism.

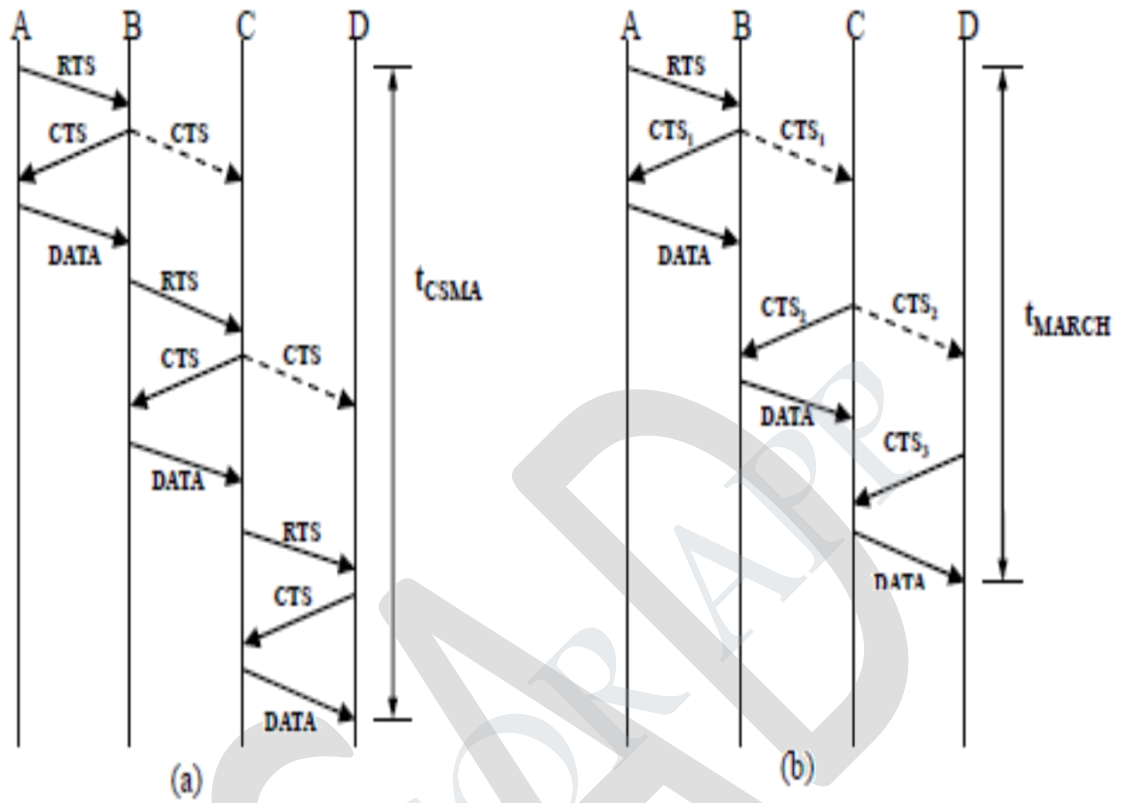
It exploits the broadcast nature of traffic from omni-directional antennas to reduce the number of handshakes involved in the data transmission. A node obtains information about the data packet arrivals at its neighbouring nodes by overhearing the CTS packets transmitted by them.

It then sends a CTS packet to the concerned neighbour node for relaying data from that node.

The throughput of MARCH is significantly high compared to MACA.

Control overhead is much less.

Less BW is consumed for control traffic.



Handshake mechanism in (a) MACA and (b) MARCH

Figure 2.15 Handshake mechanism

5. Explain in detail about Contention Based Mac Protocols With Scheduling Mechanisms.

A)Distributed Priority Scheduling (DPS)

It uses the basic RTS-CTS-DATA-ACK packet exchange mechanism .The protocol works as follows:

When source transmits a RTS, priority-tag of current DATA is piggy-backed on RTS.

On receiving RTS, the receiver responds with CTS.

iii) The receiver copies priority-tag from the received-RTS and piggy-backs it along Neighbors receive the RTS or CTS , retrieve the piggy-backed information and make a corresponding entry in their scheduling-tables.

When source transmits a DATA, its head-of-line(HOL) packet information is piggy-backed on DATA (HOL packet of a node refers to the packet to be transmitted next by the node).

On receiving DATA, the receiver responds with ACK.

The receiver copies the HOL-information from the received-DATA and piggy-backs it along Neighbors, receive the DATA or ACK retrieve the piggy-backed information and make a corresponding entry in their STs.

When a node hears an ACK, it removes from its ST any entry made earlier for corresponding DATA.

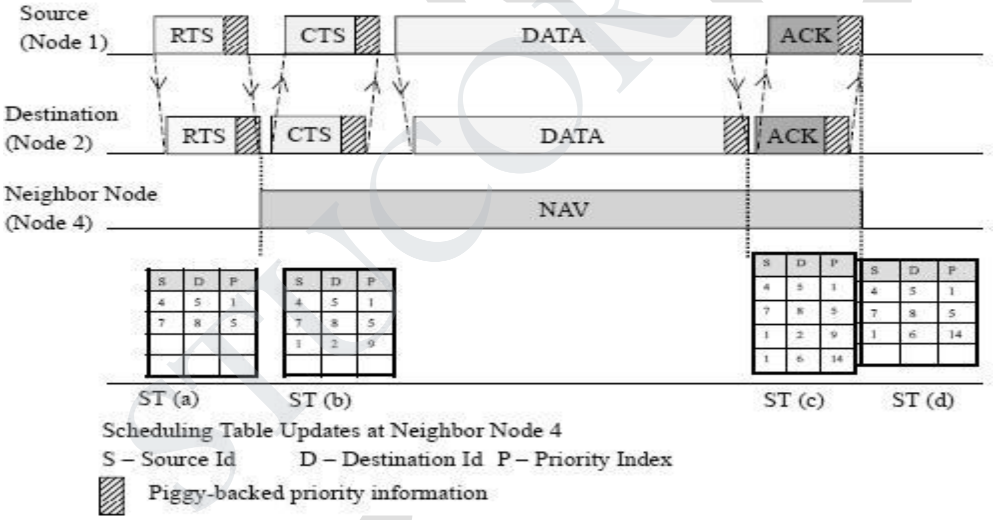


Figure 2.16 Piggy – backing and scheduling table update mechanism in DPS

Multi-Hop Coordination

The excess delay incurred by a packet at the upstream-nodes is compensated for at the downstream-nodes. When a node receives a packet, it would have already received the priority-index of the packet piggy-backed on the previous RTS packet. In case the node is an intermediate-node (which has to further forward the packet), the node calculates the new priority-index of the DATA packet based on the received value of the priority-index.If a packet suffers due to excess delay at the upstream-nodes, then the downstream-node increase priority of packet so that packet is able to meet its end-to-end delay target Similarly, if a packet arrives very early due to lack of contention at the upstream- nodes, then the priority of that packet would be reduced at the downstream-nodes.

B) Distributed Wireless Ordering Protocol (DWOP)

Packets access the medium according to order specified by an ideal reference scheduler such as FIFO (or earliest deadline first).In FIFO, packet priority-indices are set to the arrival-times of packets. Each node builds up a scheduling-table (ST) ordered according to the overheard arrival- times. It may not suffer due to information asymmetry (Since in most networks, all nodes are not within the radio range of each other, a transmitting node might not be aware of the arrival times of packets queued at another node which is not within its direct transmission range).Control packets (RTS/CTS) are used to piggy-back priority-information regarding HOL-packets of nodes.

Receiver Participation Mechanism

When receiver finds that the source is transmitting out-of-order (i.e. the reference FIFO schedule is being violated), an out-of-order notification(OON) is piggy-backed by the receiver on the control packets (CTS/ACK) and it sends to the source.

On receiving this OON, the source goes into a back-off state after completing the transmission of its current packet.

The back-off period Tback-off is given by ,

Tback-off = R*(EIFS+DIFS+Tsuccess+CWmin)

where Tsuccess = longest possible time required to transmit a packet successfully.

Stale Entry Elimination

This makes sure that the STs are free of stale entries.

An entry is deleted from the ST only after an ACK packet for the corresponding entry is heard by the node.

C)Distributed Laxity Based Priority Scheduling Scheme (DLPS)

It is a packet scheduling scheme, where scheduling decisions are made taking into consideration

- ○ the states of neighboring nodes &
- ○ the feedback from destination nodes regarding packet losses

Each node maintains following 2 tables:

The scheduling table(ST) contains information about

Packets to be transmitted by the node &

Packets overheard by the node

The packet delivery ratio table(PDT) contains

The count of DATA packets transmitted &

The count of ACK packets received

Incoming packets to a node are queued in the node's input-queue according to their arrival-times

The scheduler sorts packets according to their priority values and inserts them into the transmission queue

The highest priority packet from this queue is selected for transmission.

The destination node (on receiving data packets) initiates a feedback by means of which the count of DATA packets received by it is conveyed to the source through ACK packets.

These two pieces of information (denoted by Si) are received by the feedback information handler (FIH).

The FIH sends the previous state information Si-1 to the priority function module (PFM)

The ULB of each packet in ST is available at the node. This information is also sent to

PFM, which uses the information fed to it to calculate the priority-indices of packets in the ST.PDR(packet delivery ratio) of the flow at any given time is computed by

$$PDR = \frac{acksRcvd}{pktsSent}$$

- Priority index of a packet is defined as

$$PI = \frac{PDR}{M} \times ULB$$

Where ULB is the uniform laxity budget of the packet.

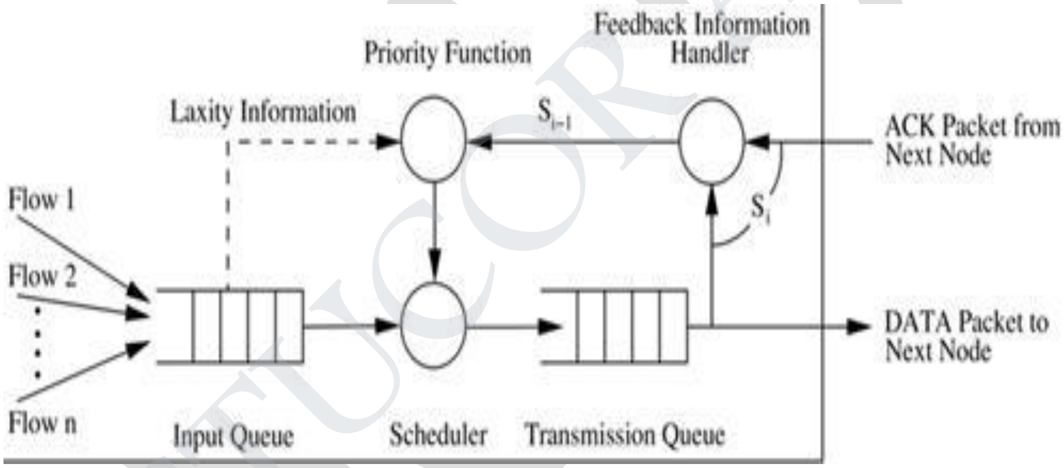


Figure 2.17 Feedback mechanism

6. Explain in detail about Multichannel Mac Protocol (MMAC)

Each node maintains a data structure called PCL (Preferable Channel List).

PCL contains the usage of the channels within the transmission-range of the node. Based on their usage, channels can be classified into three types:

High preference channel (HIGH): The channel has been selected by the current node and is being used by the node in the current beacon-interval.

Medium preference channel (MID): The channel is free and is not being currently used in the transmission-range of the node.

Low preference channel (LOW): The channel is already being used in the transmission-range of the node by other neighboring nodes.

A counter is associated with each LOW state channel.Time is divided into beacon-intervals & every node is synchronized by periodic beacon transmissions

At the start of every beacon-interval, there exists a time interval called the adhoc traffic indication messages (ATIM) window.

ATIM window is used by the nodes to negotiate for channels for transmission during the current beacon-interval. The protocol works as follows

A source sends an ATIM to the intended receiver. The ATIM carries the PCL of the source.

On receiving this ATIM, the receiver uses the PCL carried on the ATIM and its own PCL to select a channel. It includes this channel information in the ATIM-ACK packet & sends to the source.

Then, source determines whether it can transmit on the channel indicated in the ATIM-ACK message. If so, it responds by sending the receiver an ATIM-RES(reservation) packet.

At the end of the ATIM window, the source and receiver switch to the agreed-upon channel and start communicating by exchanging RTS/CTS.

If a receiver node R receives an ATIM packet from a source S, it selects a channel as below.

If there exists a HIGH state channel in the node R's PCL, then that channel is selected.

if there exists a HIGH state channel in the PCL of node S, then that channel is selected.

if there exists a common MID state channel in the PCLs of both node S and node R, then that channel is selected.

if there exists a channel which is in the MID state at only one of the two nodes, then that channel is chosen.

5) If all channels in both PCLs are in the LOW state, the counters of the corresponding channels at nodes S and R are added, and the channel with the least count is selected.

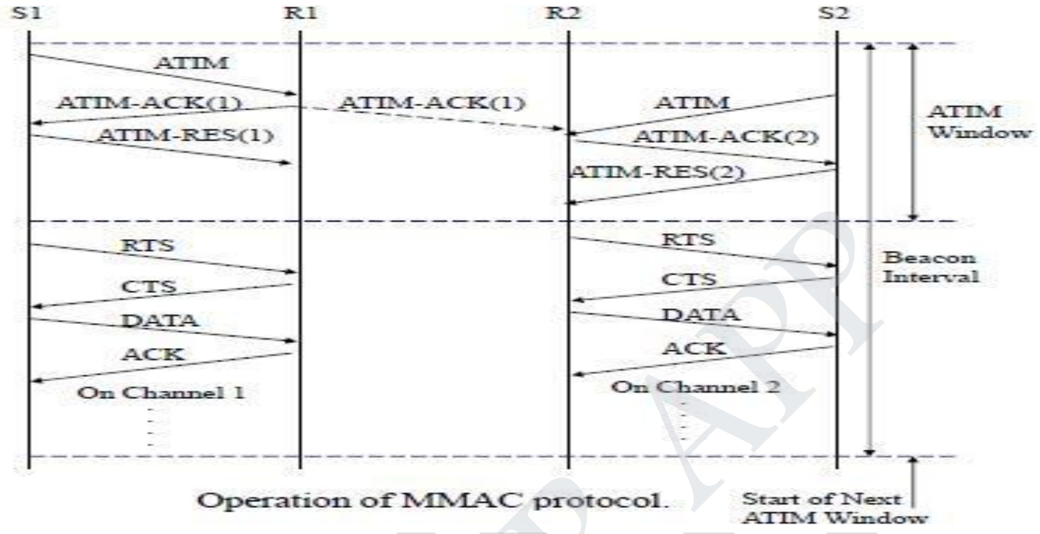


Figure 2.18 Operation of MMAC protocol

Multichannel CSMA Mac Protocol (M-CSMA)

It employs the notion of soft channel reservation, where preference is given to the channel that was used for the previous successful transmission.

The available bandwidth is divided into several channels.

The channels may be created in the frequency domain (FDMA) or in the code domain(CDMA).

An idle node continuously monitors all the channels. A channel whose TRSS(total received signal strength) is below the ST(sensing threshold) of the node is marked IDLE by the node. Such channels are put in the free-channels list (FCL).

When an idle node receives a packet to be transmitted, it does the following.

If FCL is empty, it waits for any channel to become IDLE.

In case FCL is non-empty, the node first checks whether the channel it used for its most recent successful transmission is included in the list. If so, the node uses this channel for its new transmission.

Otherwise, one among the IDLE channels available in the FCL is randomly chosen.

Drawback:

If the number of channels is very large, then the protocol results in very high packet transmission time.

UNIT III

ROUTING PROTOCOLS AND TRANSPORT LAYER IN AD HOC WIRELESS NETWORKS

Issues in designing a routing and Transport Layer protocol for Ad hoc networks- proactive routing, reactive routing (on-demand), hybrid routing- Classification of Transport Layer solutions-TCP over Ad hoc wireless Networks.

PART-A

1. Differentiate proactive and reactive routing protocols. Write examples for each.

S.No.	Proactive	Reactive
1	Route is pre-established	Route establishment is on-demand
2	Continuously discover the routes	Route discovery by some global search
3	Updates topology information	No information update is done
4	No latency in route discovery	longer delay due to latency of route discovery
5	Large capacity is needed to update network information	Large capacity is not needed
6	A lot of routing information may never be used	May not be appropriate for real-time communication
7	Eg: DSDV, WRP	Eg: AODV, ABR

2. How does energy aware routing work?

The energy aware routing works based on the routing metrics such as low energy, cost and remaining battery charge. It aims mainly at increasing the lifetime of the network.

3.Define Message Retransmission List (MRL).

It contains entry for every updated message.

Maintain counter for each entry.

4. List the advantages and disadvantages of DSDV routing protocols.

The advantages and disadvantages of DSDV routing protocols are

Advantages:

Less Delay is involved in route setup process.

DSDV protocol guarantees loop free paths.

Incremental updates with sequence number tags make the existing wired network protocols adaptable to ad-hoc wireless networks. Count to infinity problem is reduced in DSDV.

Path Selection: DSDV maintains only the best path instead of maintaining multiple paths to every destination. With this, the amount of space in routing table is reduced.

Disadvantages:

Updates due to broken links lead to heavy control overhead during mobility.

The control overhead is directly proportional to the number of nodes.

Small network with high mobility or large network with low mobility can choke the available bandwidth.

Wastage of bandwidth due to unnecessary advertising of routing information even if there is no change in the network topology.

Delay in obtaining information about a node could result in stale routing at the nodes.

5. What is the approach used to find link stability in ABR?

Associativity-based routing (ABR) protocol selects route based on the stability of the wireless link. A link is classified as stable or unstable based on its temporal stability. Temporal stability is determined based on number of beacon signal that node receives from its neighbors.

Large number of beacon signals implies stable link

Lesser number of beacon signals implies unstable link .

6.Give the classifications of routing protocol in MANET.

The classifications of routing protocol in MANET are

Proactive protocols: This protocol attempt to evaluate continuously the routes within the network, so that when a packet needs to be forwarded, the router is already known and can be immediately used.

Reactive protocols: This protocol invokes a route determination procedure only on demand.

The routing protocols may also be categorized as follows:

Table-driven protocols.

Source-initiated on-demand protocols

7. Is hop – length always the best metric for choosing paths in MANETs? Defend your answer.

No, hop length is not always the best metric for choosing paths in MANETs. It is the best metric only in the shortest path protocol. For secure routing, all the nodes along the path must be secure nodes else security is compromised. For energy aware routing, low power consumption and remaining battery backup must also be considered for choosing path.

8. Why does TCP not work well in ad hoc network?

The TCP does not work well in ad hoc network because of the following reasons

Misinterpretation of packet loss

Frequent path breaks

Effect of path length

Misinterpretation of congestion window

Asymmetric link behavior

Uni-directional path

Multipath routing

Network partitioning and remerging

Use of sliding-window-based transmission.

9.What are not supported by the traditional TCP for handling Ad hoc network?

The features that are not supported by the traditional TCP for handling ad hoc network are

Throughput

Power consumption

Path break handling mechanisms

Scheduling of packet loss and rate of transmission

Bandwidth consumption due to RTS-CTS-DATA-ACK

10.What are the advantages and disadvantages of TCP-F? Advantages

TCP-F provides a simple FB based solution to minimize the problem arising out of frequent path breaks in ad hoc wireless networks.

At the same time, it also permits the TCP congestion control mechanism to respond to congestion in the n/w.

Disadvantages

If the route to the sender is not available at the FP then additional control packets may need to be generated for routing the RFN packet.

TCP-F has an additional state compared to the traditional TCP state m/c, and hence its implementation requires modifications to the existing TCP libraries.

Congestion window used after a new route is obtained may not reflect the achievable transmission rate to the n/w and the TCP-F receiver.

11.What are the issues in designing a transport layer protocol for ad hoc wireless Networks?

Induced traffic

Induced throughput unfairness

Separation of congestion control, reliability, and flow control

Power and bandwidth constraints

Misinterpretation of congestion

Completely decoupled transport layer

Dynamic topology.

PART-B

1. Discuss the issues in designing a routing protocol for ad hoc wireless networks and describe the classification of routing protocols. (nov/Dec 2016)

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

Mobility

Network topology is highly dynamic due to movement of nodes. Hence, an ongoing session suffers frequent path breaks.

Disruption occurs due to the movement of either intermediate nodes in the path or end nodes.

Wired network routing protocols cannot be used in ad hoc wireless networks because the nodes are here are not stationary and the convergence is very slow in wired networks.

Mobility of nodes results in frequently changing network topologies

Routing protocols for ad hoc wireless networks must be able to perform efficient and effective mobility management.

Bandwidth Constraint

Abundant bandwidth is available in wired networks due to the advent of fiber optics and due to the exploitation of wavelength division multiplexing (WDM) technologies.

In a wireless network, the radio band is limited, and hence the data rates it can offer are much less than what a wired network can offer.

This requires that the routing protocols use the bandwidth optimally by keeping the overhead as low as possible.

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

Error-prone shared broadcast radio channel

The broadcast nature of the radio channel poses a unique challenge in ad hoc wireless networks.

The wireless links have time-varying characteristics in terms of link capacity and link-error probability.

This requires that the ad hoc wireless network routing protocol interact with the MAC layer to find alternate routes through better-quality links.

Transmissions in ad hoc wireless networks result in collisions of data and control packets.

Therefore, it is required that ad hoc wireless network routing protocols find paths with less congestion.

Hidden and exposed terminal problems

The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the receiver, but are within the transmission range of the receiver.

Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other.

Ex: consider figure (3.1). Here, if both node A and node C transmit to node B at the same time, their packets collide at node B. This is due to the fact that both node A and C are hidden from each other, as they are not within the direct transmission range of each other and hence do not know about the presence of each other.

Solution for this problem include medium access collision avoidance (MACA):

- Transmitting node first explicitly notifies all potential hidden nodes about the forthcoming transmission by means of a two way handshake control protocol called RTS-CTS protocol exchange.

  This may not solve the problem completely but it reduces the probability of collisions.

Medium access collision avoidance for wireless (MACAW):

An improved version of MACA protocol.

- Introduced to increase the efficiency.
- Requires that a receiver acknowledges each successful reception of data packet.

Other solutions include floor acquisition multiple access (FAMA) and Dual busy tone multiple access (DBTMA). The exposed terminal problem refers to the inability of a node which is blocked due to transmission by a nearby transmitting node to transmit to another node.

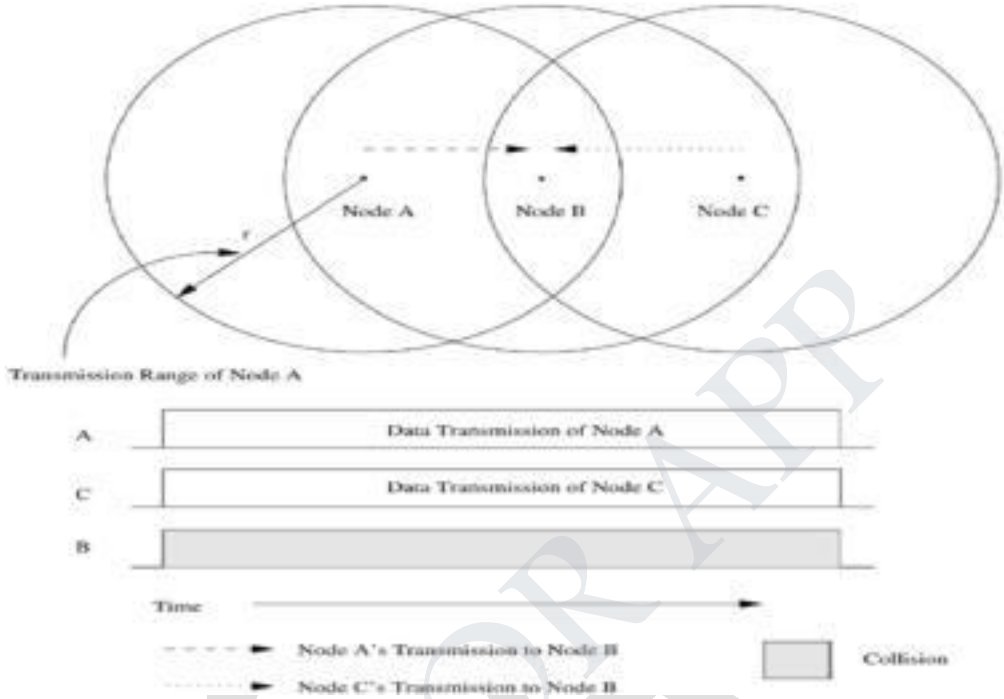

Node A
Node B
Node C
r
Transmission Range of Node A
A
Data Transmission of Node A
C
Data Transmission of Node C
B
Time
Node A's Transmission to Node B
Node C's Transmission to Node B
Collision

Figure 3.1: Hidden Terminal Problem

Successful transmission is a four-way exchange mechanism, RTS-CTS-Data-ACK, as illustrated in figure (3.2)

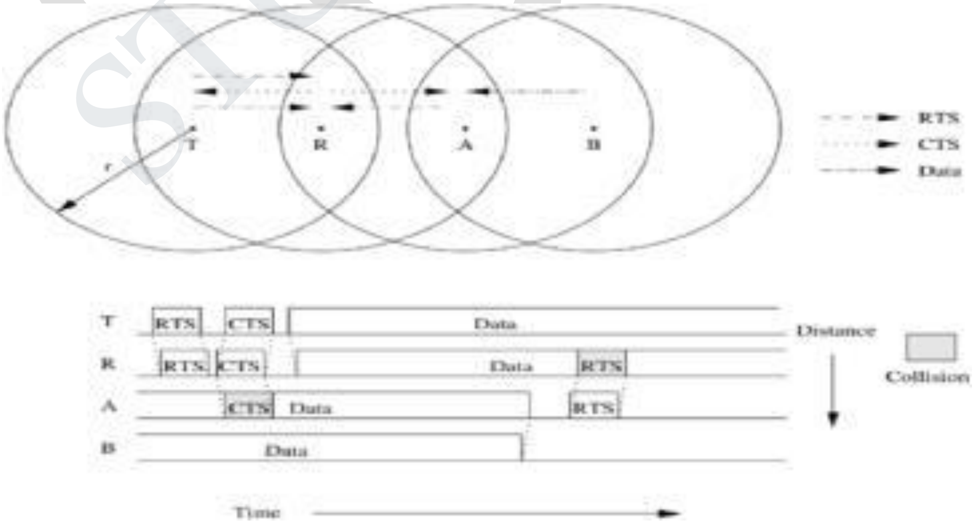


Figure 3.2: Hidden terminal problem with RTS-CTS-Data-ACK scheme.

Ex: consider the figure (3.3). Here, if a transmission from node B to another node A is already in progress, node C cannot transmit to node D, as it concludes that its neighbor node B, is in transmitting mode and hence should not interfere with the on-going transmission. Thus, reusability of the radio spectrum is affected.

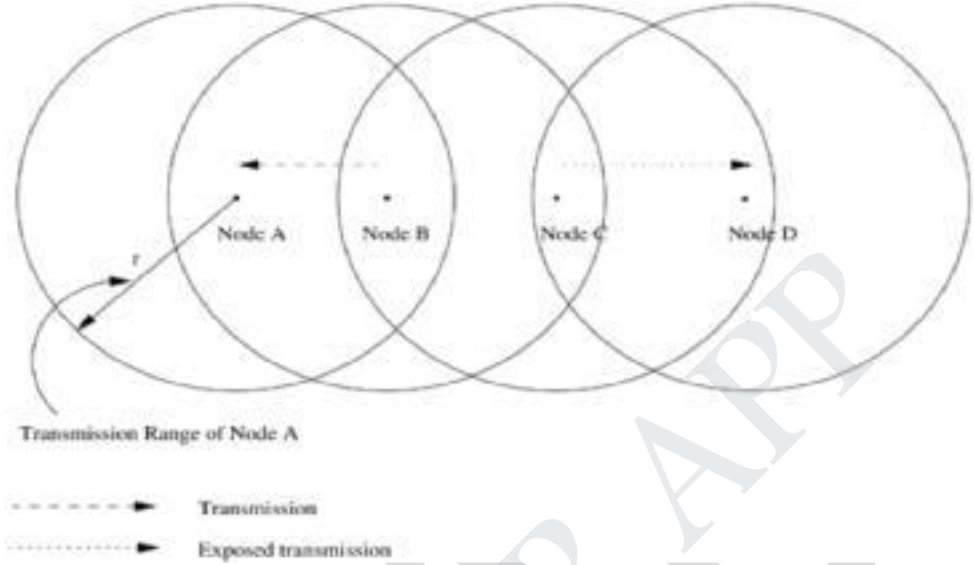


Figure 3.3: Exposed Terminal Problem

5. Resource Constraints

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

Characteristics of an Ideal Routing Protocol for ad hoc wireless networks

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

It must be fully distributed as centralized routing involves high control overhead and hence is not scalable.

It must be adaptive to frequent topology changes caused by the mobility of nodes.

Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired.

It must be localized, as global state maintenance involves a huge state propagation control overhead.

It must be loop-free and free from state routes.

The number of packet collisions must be kept to a minimum by limiting the number of broadcasts made by each node. The transmissions should be reliable to reduce message loss and to prevent the occurrence of state routes.

It must converge to optimal routes once the network topology becomes stable. The convergence must be quick.

It must optimally use scarce resources such as bandwidth, computing power, memory, and battery power.

Every node in the network should try to store information regarding the stable local topology only. Changes in remote parts of the network must not cause updates in the topology information maintained by the node.

It should be able to provide a certain level of quality of service (QoS) as demanded by the applications, and should also offer support for time-sensitive traffic.

Classification of Routing Protocols:

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

Routing information update mechanism.

Use of temporal information for routing

Routing topology

Utilization of specific resources.

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

They are:

Proactive or table-driven routing protocols :

- Every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.
- Routing information is generally flooded in the whole network.
- Whenever a node requires a path to a destination, it runs an appropriate path finding algorithm on the topology information it maintains.

Reactive or on-demand routing protocols:

- Do not maintain the network topology information.
- Obtain the necessary path when it is required, by using a connection establishment process.

Hybrid routing protocols:

- Combine the best features of the above two categories.
- Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node.
- For routing within this zone, a table-driven approach is used.
- For nodes that are located beyond this zone, an on-demand approach is used.

Based on the use of temporal information for routing:

The protocols that fall under this category can be further classified into two types

Routing protocols using past temporal information:

Use information about the past status of the links or the status of links at the time of routing to make routing decisions.

Routing protocols that use future temporal information:

Use information about the about the expected future status of the wireless links to make approximate routing decisions.

Apart from the lifetime of wireless links, the future status information also includes information regarding the lifetime of the node, prediction of location, and prediction of link availability.

Based on the routing topology

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

- Flat topology routing protocols:

  Make use of a flat addressing scheme similar to the one used in IEEE 802.3 LANs.

  It assumes the presence of a globally unique addressing mechanism for nodes in an ad hoc wireless network.

Hierarchical topology routing protocols:

Make use of a logical hierarchy in the network and an associated addressing scheme.

The hierarchy could be based on geographical information or it could be based on hop distance.

Based on the utilization of specific resources

Power-aware routing:

- Aims at minimizing the consumption of a very important resource in the ad hoc wireless networks: the battery power.
- The routing decisions are based on minimizing the power consumption either logically or globally in the network.

- Geographical information assisted routing :
  - Improves the performance of routing and reduces the control overhead by effectively utilizing the geographical information available.

2. (a) Illustrate the process of route establishment and route maintenance in Destination Sequenced Distance-Vector Routing Protocol (DSDV) by taking an example.

Destination sequenced distance-vector routing protocol:

It is an enhanced version of the distributed Bellman -Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network.

It incorporates table updates with increasing sequence number tags to prevent loops, to counter the count-to-infinity problem, and for faster convergence.

As it is a table-driven routing protocol, routes to all destinations are readily available at every node at all times.

The tables are exchanged between neighbors at regular intervals to keep an up -to-date view of the network topology.

The table updates are of two types:

Incremental updates: Takes a single network data packet unit (NDPU). These are used when a node does not observe significant changes in the local topology.

Full dumps: Takes multiple NDPUs. It is done either when the local topology changes significantly or when an incremental update requires more than a single NDPU.

Table updates are initiated by a destination with a new sequence number which is always greater than the previous one.

Consider the example as shown in figure 3.4 (a). Here node 1 is the source node and node 15 is the destination. As all the nodes maintain global topology information, the route is already available as shown in figure3.4 (b).Here the routing table node 1 indicates that the shortest route to the destination node is available through node 5 and the distance to it is 4 hops, as depicted in figure 3.4 (b)

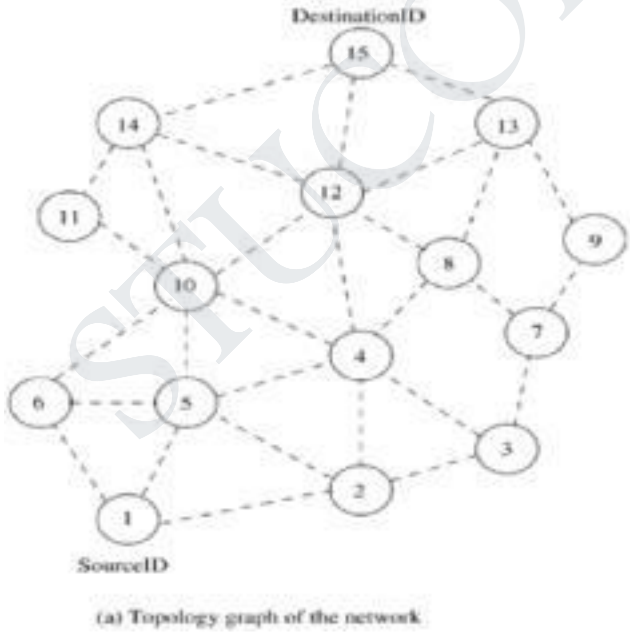
The reconfiguration of a path used by an on-going data transfer session is handled by the protocol in the following way.The end node of the broken link initiates a table update message with the broken link’s weight assigned to infinity (∞) and with a sequence number greater than the stored sequence number for that destination.

Each node upon receiving an update with weight ∞, quickly disseminates it to its neighbors in order to propagate the broken-link information to the whole network.

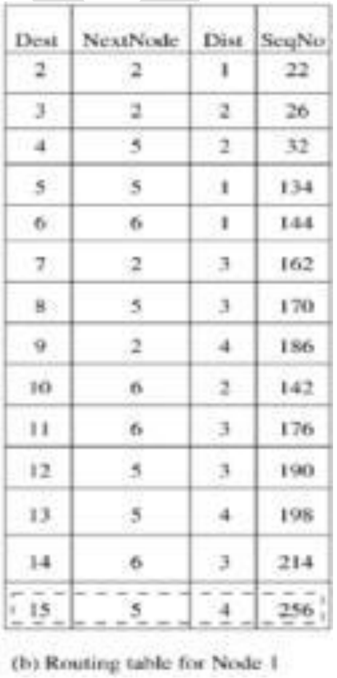
A node always assign an odd number to the link break update to differentiate it from the even sequence number generated by the destination.

The below figure 3.4(a) shows the case when node 11 moves from its current position.

Route Establishment in DSDV:



(a) Topology graph of the network



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

(b) Routing table for Node 1

Figure 3.4(a) Topology graph of the network

Figure 3.4(b) Routing for Node 1

Advantages:

Less delay involved in the route setup process.

Mechanism of incremental update with sequence number tags makes the existing wired network protocols adaptable to ad hoc wireless networks.

The updates are propagated throughout the network.

Disadvantages

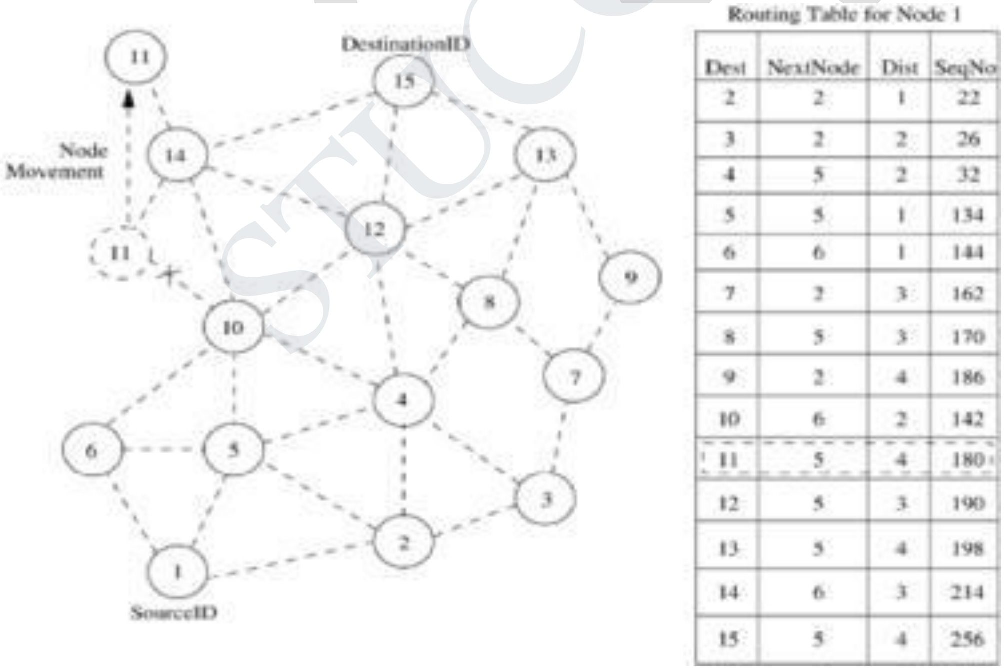
The updates due to broken links lead to a heavy control overhead during high mobility.

Even a small network with high mobility or a large network with low mobility can completely choke the available bandwidth.

Suffers from excessive control overhead.

In order to obtain information about a particular destination node, a node has to wait for a table update message initiated by the same destination node.This delay could result in state routing information at nodes.

Route maintenance in DSDV.



Routing Table for Node 1

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

Figure 3.5 Route Maintenance in DSDV

2. b) Explain in detail about CGSR.

Uses a hierarchical network topology.

CGSR organizes nodes into clusters, with coordination among the members of each cluster entrusted to a special node named cluster-head.

This cluster-head is elected dynamically by employing a least cluster change (LCC) algorithm.According to this algorithm, a node ceases to be a cluster-head only if it comes under the range of another cluster-head, where the tie is broken either using the lowest ID or highest connectivity algorithm.

Clustering provides a mechanism to allocate bandwidth, which is a limited resource, among different clusters, thereby improving reuse.

A token-based scheduling is used within a cluster for sharing the bandwidth among the members of the cluster.

CGRS assumes that all communication passes through the cluster-head. Communication between 2 clusters takes place through the common member nodes that are members of both the cluster are called gateways.

A gateway is expected to be able to listen to multiple spreading codes that are currently in operation in the clusters in which the node exist as a member.

A gateway conflict is said to occur when a cluster-head issues a token to a gateway over spreading code while the gateway is tuned to another code.

Gateways that are capable of simultaneously communicating over two interfaces can avoid gateway conflicts.

The performance of routing is influenced by token scheduling and code scheduling that is handled at cluster-heads and gateways, respectively.

Every member node maintains a routing table containing the destination cluster-head for every node in the network.

In addition to the cluster member table, each node maintains a routing table which keeps the list of next-hop nodes for reaching every destination cluster.

Figure 3.6 shows the cluster head, cluster gateways, and normal cluster member nodes in an ad hoc wireless network.

Route Establishment in CGSR:

Advantages:

CGSR is a hierarchical routing scheme which enables partial coordination between nodes by electing cluster-heads.

Better bandwidth utilization is possible.

Easy to implement priority scheduling schemes with token scheduling and gateway code scheduling.

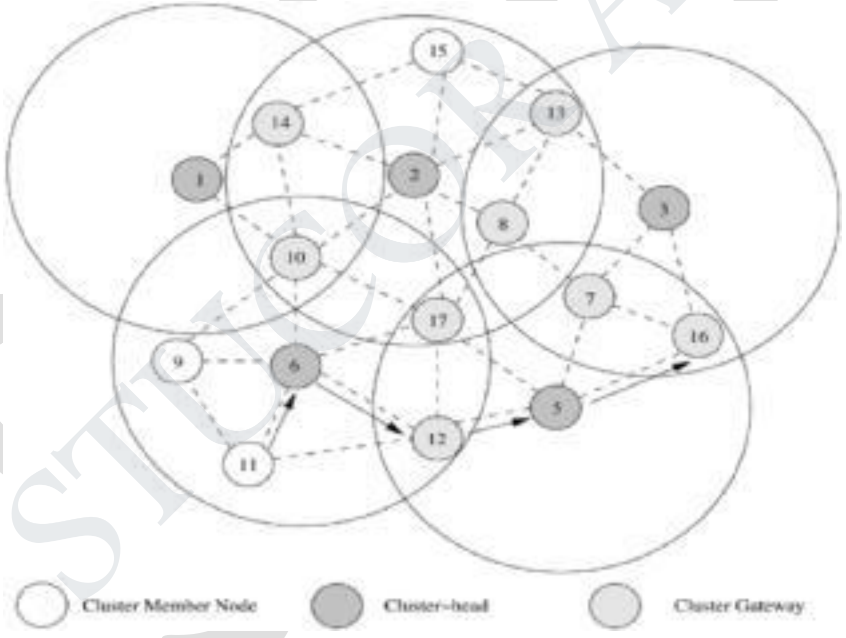


Figure 3.6 Route Establishment in CGSR

Disadvantages:

Increase in path length and instability in the system at high mobility when the rate of change of cluster-head is high.

In order to avoid gateway conflicts, more resources are required.

The power consumption at the cluster-head node is also a matter of concern.

Lead to Frequent changes in the cluster-head, which may result in multiple path breaks.

3. Explain in detail about WRP and STAR. DSDV (nov/Dec 2016)

Wireless Routing Protocol (WRP):

WRP is similar to DSDV, it inherits the properties of the distributed bellman-ford algorithm.

To counter the count-to-infinity problem and to enable faster convergence, it employs a unique method of maintaining information regarding the shortest distance to every destination node in the network and penultimate hop node on the path to every destination node.

Maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network.

It differs from DSDV in table maintenance and in the update procedures.

While DSDV maintains only one topology table, WRP uses a set of tables to maintain more accurate information.

The table that are maintained by a node are :

Distance table (DT): contains the network view of the neighbors of a node. It contains a matrix where each element contains the distance and the penultimate node reported by the neighbor for a particular destination.

Routing table (RT): contains the up-to-date view of the network for all known destinations. It keeps the shortest distance, the predecessor/penultimate node, the successor node, and a flag indicating the status of the path. The path status may be a simplest (correct) path or a loop (error), or destination node not marked (null).

Link cost table (LCT): contains the cost of relaying messages through each link. The cost of broken link is ∞.it also contains the number of update periods passed since the last successful update was received from that link.

iv) **Message retransmission list (MRL):** contains an entry for every update message that is to be retransmitted and maintains a counter for each entry.

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

Consider the example shown in figure 3.7(a) , where the source of the route is node 1 and destination is node 15. As WRP proactively maintains the route to all destinations, the route to any destination node is readily available at the source node.

From the routing table shown, the route from node 1 to node 15 has the next node as node 2. The predecessor node of 15 corresponding to this route is route 12. The predecessor information helps

WRP to converge quickly during link breaks.

When a node detects a link break, it sends an update message to its neighbors with the link cost of the broken link set to ∞. After receiving the update message; all affected nodes update their minimum distances to the corresponding nodes. The node that initiated the update message then finds an alternative route, if available from its DT. Below figure3.7(b) shows route maintenance in WRP.

Advantages:

WRP has the same advantages as that of DSDV.

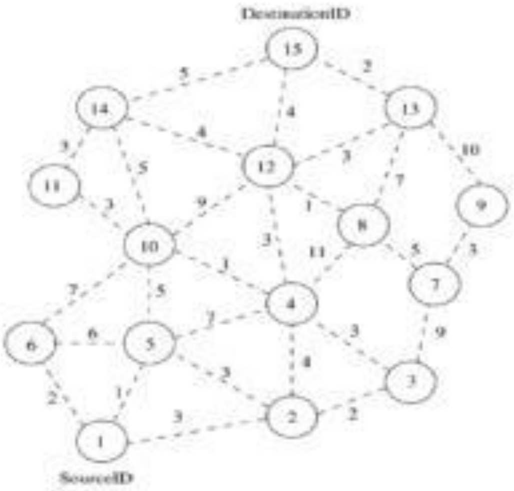
It has faster convergence and involves fewer table updates.

Disadvantages:

The complexity of maintenance of multiple tables demands a larger memory and greater processing power from nodes in the adhoc wireless network.

It is not suitable for highly dynamic and also for very large ad hoc wireless networks.

- **Route establishment in WRP:**

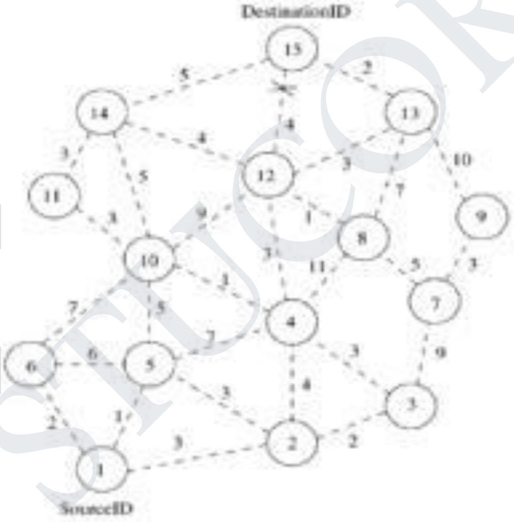


Routing Entry at Each Node for DestinationID 15

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

Figure 3.7(a) Route establishment in WR

Route maintenance in WRP:



Routing Entry at Each Node for DestinationID 15

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

Figure 3.7(b) Route maintenance in WRP

Source-Tree Adaptive Routing Protocol (STAR):

Key concept least overhead routing approach (LORA)

This protocol attempts to provide feasible paths that are not guaranteed to be optimal

Involves much less control overhead.

In STAR protocol, every node broadcasts its source tree information

The source tree of a node consists of the wireless links used by the node

Every node builds a partial graph of the topology

During initialization, a node sends an update message to its neighbors

Each node will have a path to every destination node

The path would be sub-optimal

The data packet contains information about the path to be traversed in order to prevent the possibility of routing loop formation

In the presence of a reliable broadcast mechanism, STAR assumes implicit route maintenance. In addition to path breaks, the intermediate nodes are responsible for handling the routing loops. The Route Repair packet contains the complete source tree of node k and the traversed path of the packet

When an intermediate node receives a Route Repair update message, it removes itself from the top of the route repair path and reliably sends it to the head of the route repair path.

Advantages:

Very low communication overhead

Reduces the average control overhead.

4. Explain On Demand routing protocol in detail.

They execute the path-finding process and exchange routing information only When a path is required by a node to communicate with a destination.

Dynamic Source Routing Protocol (DSR)

Designed to restrict the bandwidth consumed by control packets in adhoc wireless networks by eliminating the periodic table update messages.

It is beacon-less and does not require periodic hello packet transmissions

Basic approach to establish a route by flooding Route Request packets in the network.

Destination node responds by sending a Route Reply packet back to the source

Each RouteRequest carries a sequence number generated by the source node and the path it has traversed

A node checks the sequence number on the packet before forwarding it

The packet is forwarded only if it is not a duplicate RouteRequest

The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions

Thus, all nodes except the destination forward a RouteRequest packet during the route construction phase

In figure 3.8 (a) source node 1 initiates a RouteRequest packet to obtain a path for destination node 15

This protocol uses a route cache that stores all possible information extracted from the source route contained in a data packet

During network partitions, the affected nodes initiate RouteRequest packets

DSR also allows piggy-backing of a data packet on the RouteRequest

As a part of optimizations, if the intermediate nodes are also allowed to originate RouteReply packets, then a source node may receive multiple replies from intermediate nodes

In figure 3.8(a) if the intermediate node 10 has a route to the destination via node 14, it also sends the RouteReply to the source node

The source node selects the latest and best route and uses that for sending data packets

Each data packet carries the complete path to its destination

If a link breaks, source node again initiates the route discovery process

Advantages:

Uses a reactive approach which eliminates the need to periodically flood the network with table update messages

Route is established only when required

Reduce control overhead

Disadvantages

Route maintenance mechanism does not locally repair a broken link

Stale route cache information could result in inconsistencies during route construction phase.

Route Establishment in DSR:

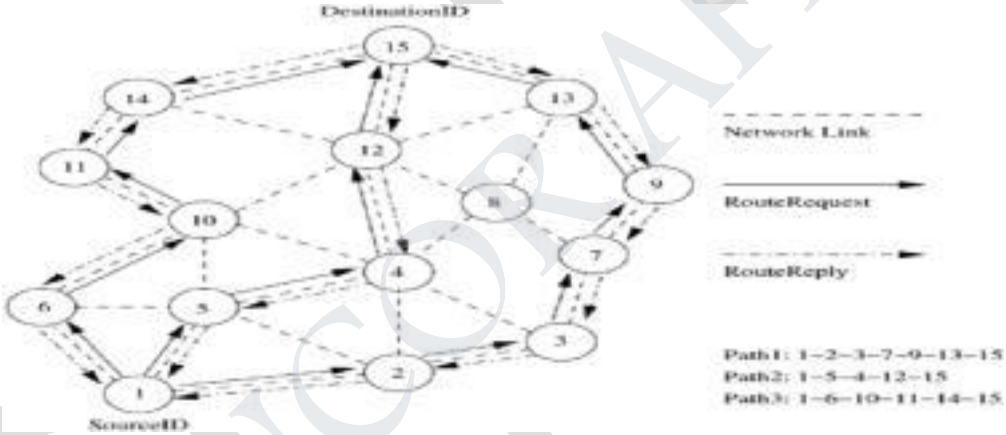


Figure 3.8(a) Route Establishment in DSR

Route maintenance in DSR:

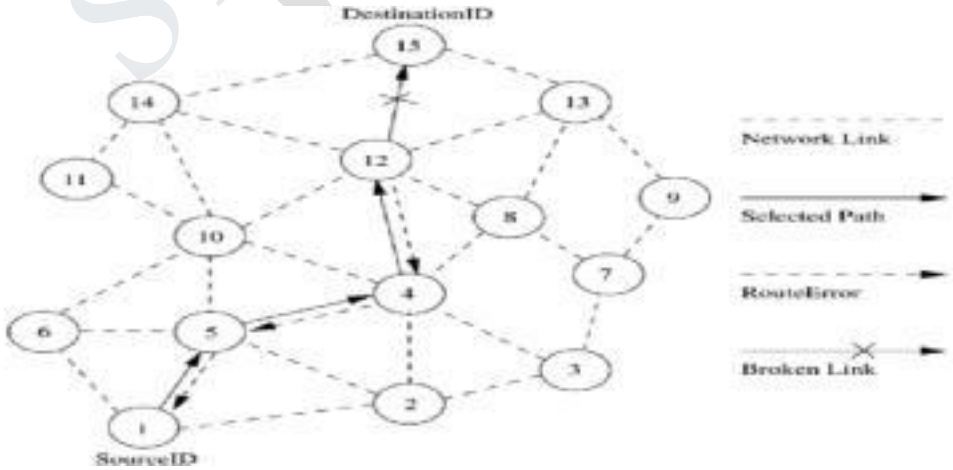


Figure 3.8(b) Route maintenance in DSR

Ad Hoc On-Demand Distance Vector Routing Protocol:

Route is established only when it is required by a source node for transmitting data packets

It employs destination sequence numbers to identify the most recent path

Source node and intermediate nodes store the next hop information corresponding to each flow for data packet transmission

Uses DestSeqNum to determine an up-to-date path to the destination

A RouteRequest carries the source identifier, the destination identifier, the source sequence number, the destination sequence number, the broadcast identifier and the time to live field

DestSeqNum indicates the freshness of the route that is accepted by the source

When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination

The validity of the intermediate node is determined by comparing the sequence numbers

If a RouteRequest is received multiple times, then duplicate copies are discarded

Every intermediate node enters the previous node address and its BcastID

A timer is used to delete this entry in case a RouteReply packet is not received

AODV does not repair a broken path locally

When a link breaks, the end nodes are notified

Source node re-establishes the route to the destination if required

Advantage:

Routes are established on demand and DestSeqNum are used to find latest route to the destination.

- Connection setup delay is less.

Disadvantages:

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

Multiple RouteReply packets to single RouteRequest packet can lead to heavy control overhead.

Periodic beaconing leads to unnecessary bandwidth consumption.

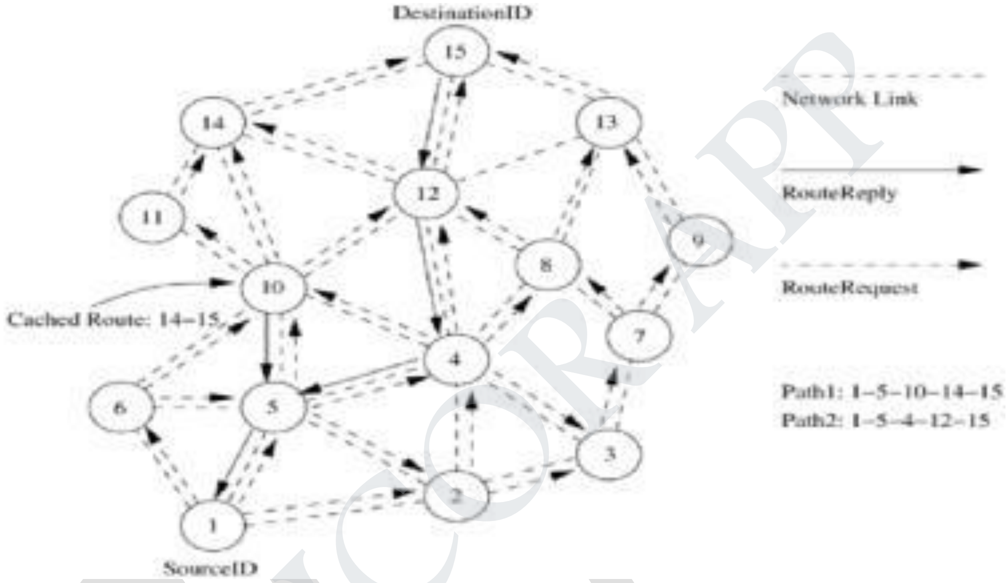


Figure 3.9(a) Route establishment in AODV

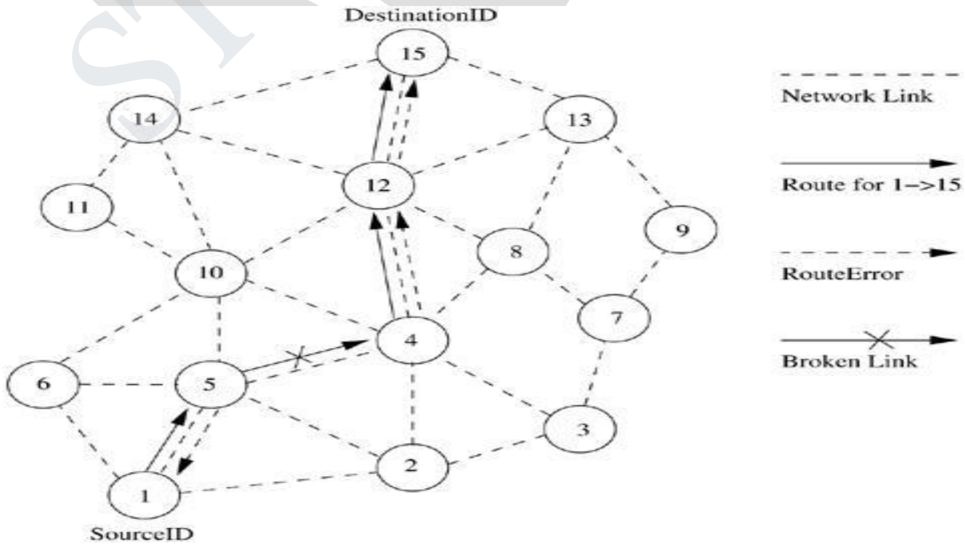


Figure 3.9(b) Route maintenance in AODV

3.Temporally Ordered Routing Algorithm (TORA)

Source-initiated on-demand routing protocol

Uses a link reversal algorithm

Provides loop free multi path routes to the destination

Each node maintains its one-loop local topology information

Has capability to detect partitions

Unique property limiting the control packets to a small region during the reconfiguration process initiated by a path break

TORA has 3 main functions: establishing, maintaining and erasing routes The route establishment function is performed only when a node requires a path to a destination but does not have any directed link

This process establishes a destination-oriented directed acyclic graph using a query/update mechanism

Once the path to the destination is obtained, it is considered to exist as long as the path is available, irrespective of the path length changes due to the re-configurations that may take place during the course of data transfer session

If the node detects a partition, it originated a clear message, which erases the existing path information in that partition related to the destination

Illustration of temporal ordering in TORA.

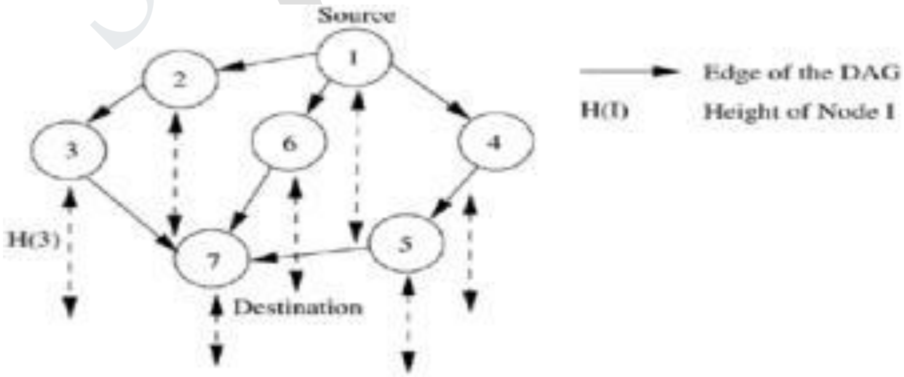
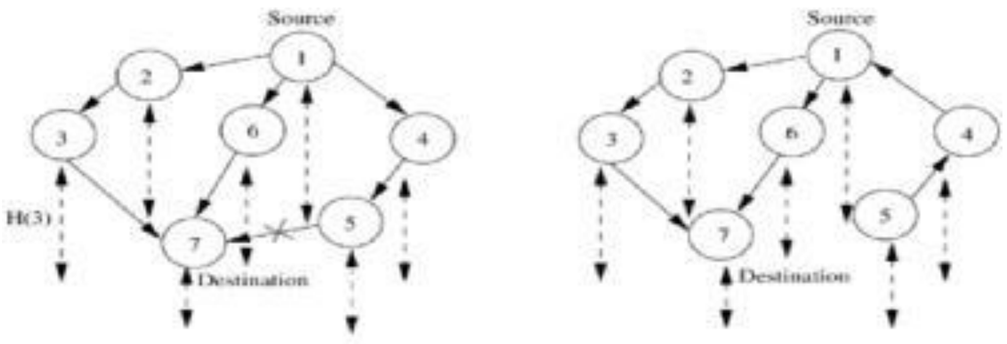


Figure 3.10 Temporal ordering in TORA

Illustration of Route Maintenance in TORA.



Link break beween Nodes 5 and 7

Nodes 4 and 5 reverse their links in order to update the path

Figure 3.11 Route Maintenance in TORA

Advantages:

Incur less control overhead

Concurrent detection of partitions

Subsequent deletion of routes

Disadvantages:

Temporary oscillations and transient loops

Local reconfiguration of paths result in non-optimal routes

Location-Aided Routing (LAR):

It utilizes the location information for improving the efficiency of routing by reducing the control overhead

LAR assumes the availability of the global positioning system (GPS) for obtaining the geographical position information necessary for routing

LAR designates two geographical regions for selective forwarding of control packets, namely, ExpectedZone and RequestZone

The ExpectedZone is the region in which the destination node is expected to be present, given information regarding its location in the past and its mobility information

The RequestZone is a geographical region within which the path-finding control packets are permitted to be propagated

This area is determined by the sender of a data transfer session.

The control packets used for path-finding are forwarded by nodes which are present in the RequestZone and are discarded by nodes outside the zone

LAR uses flooding, but here flooding is restricted to a small geographical region

The nodes decide to forward or discard the control packets based on two algorithms, namely, LAR1 &LAR2

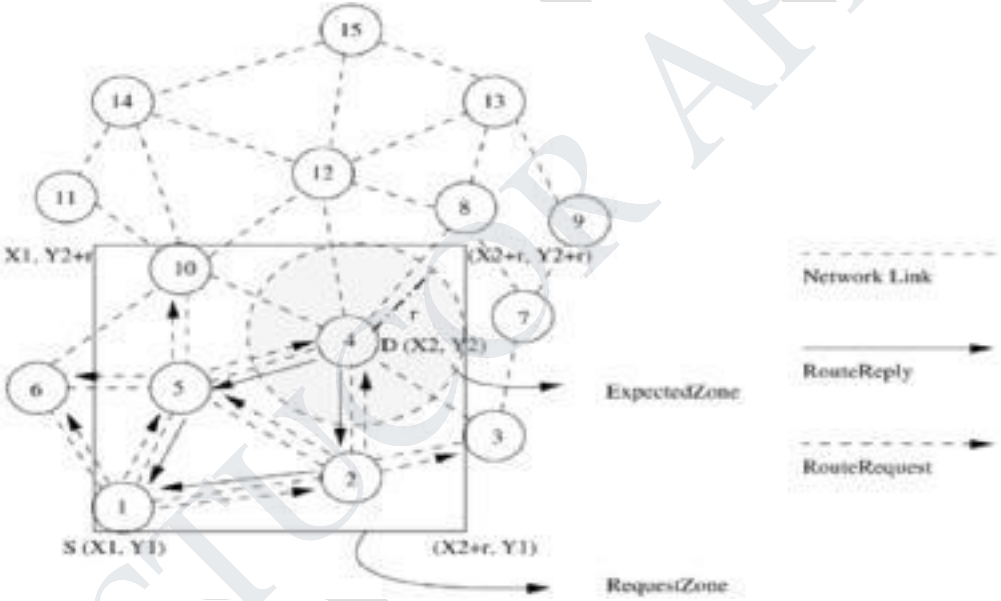


Figure 3.12(a) :RequestZone and ExpectedZone in LAR1.

In the LAR1 algorithm figure 3.12(a), the source node explicitly specifies the RequestZone in the RouteRequest packet which is broadcast to its neighbors.

These nodes verify their own geographical locations to check whether they belong to the ExpectedZone.

Finally, when the RouteRequest reaches the destination node, it originates a RouteReply that contains the current location and current time of the node.

In LAR2 algorithm figure 3.12 (b), the source node includes the distance between itself and the destination node

When the intermediate node receives this RouteRequest packet, it computes the distance to the node D.

A RouteRequest packet is forwarded only once and the distance between the forwarding node and D is updated in the RouteRequest packet for further relaying

In order to compensate for the location error, a larger RequestZone that can accommodate the amount of error that occurred is considered.

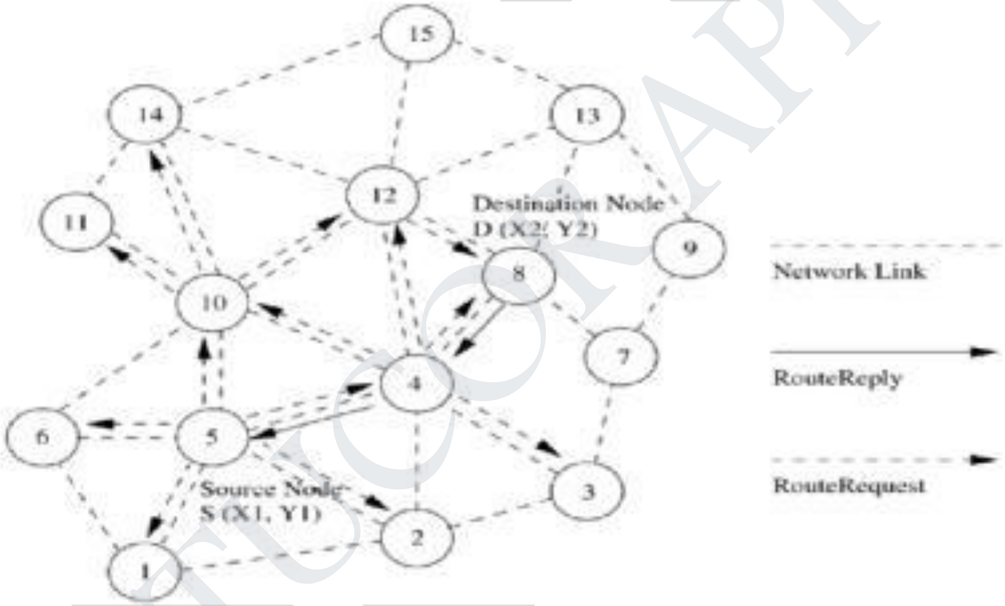


Figure 3.12 (b): Route establishment in LAR2.

Advantage

LAR reduces the control overhead by limiting the search area for finding a path

Efficient use of geographical position information

Reduced control overhead

Increased utilization of bandwidth.

Disadvantage

Depends heavily on the availability of GPS infrastructure.

Hence, cannot be used in situations where there is no access to such information.

Associativity-Based Routing (ABR)

It is a distributed routing protocol that selects routes based on the stability of the wireless links

It is a beacon-based on-demand routing protocol

A link is classified as stable or unstable based on its temporal stability

The temporal stability is determined by counting the periodic beacons that a node receives from its neighbors

Each node maintains the count of its neighbor's beacons and classifies each link as stable or unstable

The link corresponding to a stable neighbor is termed as a stable link, while a link to an unstable neighbor is called an unstable link

A source node floods RouteRequest packets throughout the network if a route is not available in its route cache

All intermediate nodes forward the RouteRequest packet

A RouteRequest packet carries the path it has traversed and the beacon count for the corresponding nodes in the path

When the first RouteRequest reaches the destination, the destination waits for a time period T to receive multiple RouteRequests through different paths

If two paths have the same proportion of stable links, the shorter of them is selected

If more than one path is available, then a random path among them is selected as the path between source and destination.

In figure 3.13(a), source node initiates the RouteRequest to the flooded for finding a route to the destination node

- Solid lines represent stable links
- Dotted lines represent unstable links

ABR uses stability information only during the route selection process at the destination node

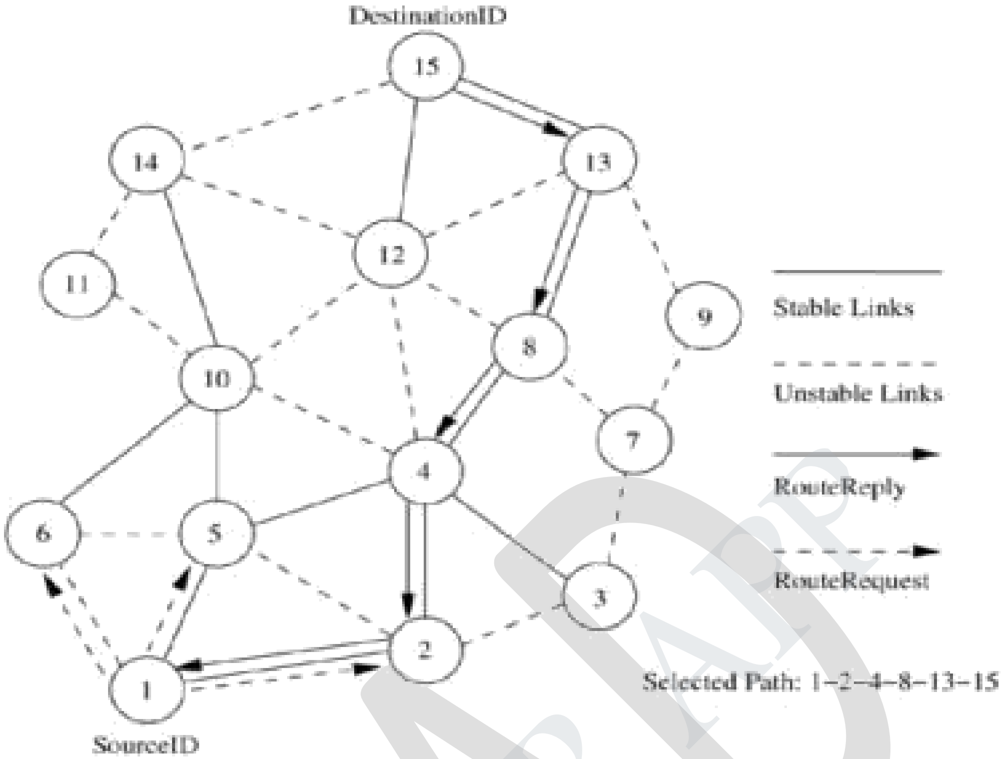


Figure 3.13(a): Route establishment in ABR.

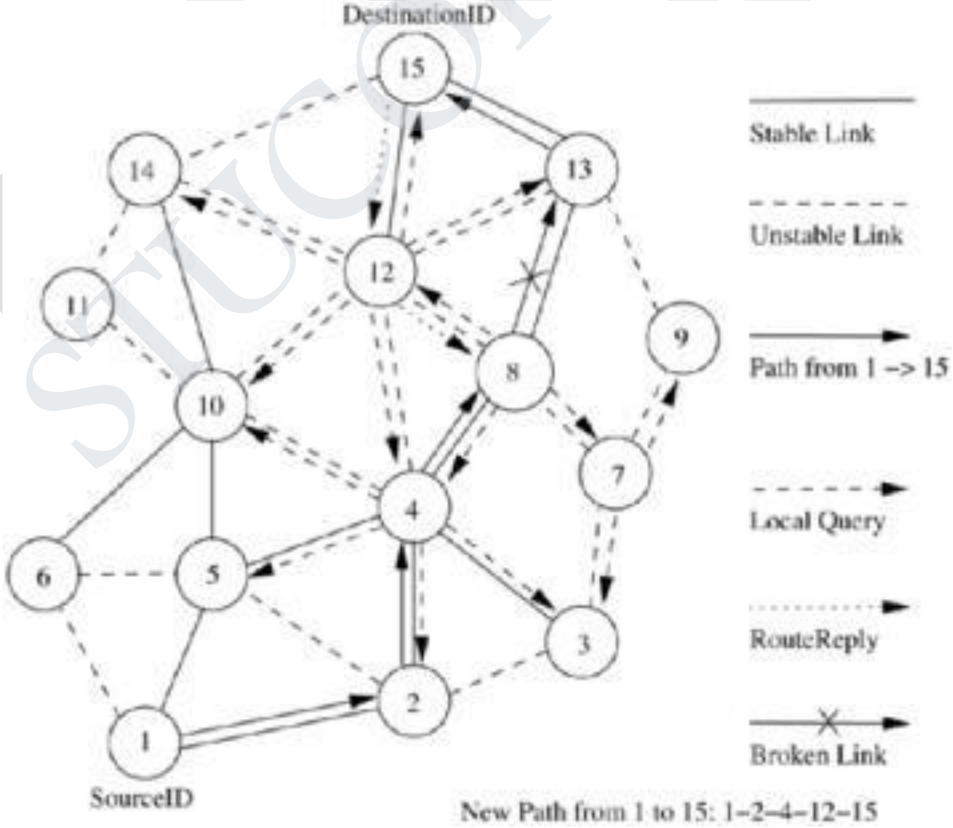


Figure 3.13(b): Route maintenance in ABR.

If a link break occurs at an intermediate node, the node closer to the source, which detects the break, initiates a local route repair process.In this process, the node locally broadcasts a route repair packet, termed the local query (LQ) broadcast, with a limited time to live (TTL), as shown in figure 3.13(b)

This way a broken link is bypassed locally without flooding a new RouteRequest packet in the whole network.

Advantage:

Stable routes have a higher preference compared to shorter routes

They result in fewer path breaks which, in turn, reduces the extent of flooding due to reconfiguration of paths in the network.

Disadvantage:

Chosen path may be longer than the shortest path between the source and destination because of the preference given to stable paths

Repetitive LQ broadcasts may result in high delays during route repairs.

6. Signal Stability-Based Adaptive Routing Protocol (SSA):

Uses signal stability as the prime factor for finding stable routes

This protocol is beacon-based, in which signal strength of the beacon is measured for determining link stability

The signal strength is used to classify a link as stable or unstable

This protocol consists of two parts: forwarding protocol (FP) and dynamic routing protocol (DRP)

These protocols use an extended radio interface that measures the signal strength from beacons

DRP maintains the routing table by interacting with the DRP processes on other hosts

FP performs the actual routing to forward a packet on its way to the destination

Every node maintains a table that contains the beacon count and the signal strength of each of its neighbors

If a node receives strong beacons, then link is classified as strong/stable link

The link is otherwise classified as weak/unstable link

Each node maintains a table called the signal stability table (SST) which is based on the signal strengths of its neighbors' beacons

This table is used by the nodes in the path to the destination to forward the incoming RouteRequest over strong links for finding the most stable end-to-end path

A source node which does not have a route to the destination floods the network with RouteRequest packets

SSA protocol process a RouteRequest only if it is received over a strong link

A RouteRequest received through a weak link is dropped without being processed

The destination selects the first RouteRequest packet received over strong links

The destination initiates a RouteReply packet to notify the selected route to the source

In figure 3.14(a), source node broadcasts a RouteRequest for finding the route to the destination node

Solid lines represent the stable links

Dotted lines represent the weak links

SSA restricts intermediate nodes from forwarding a RouteRequest packet if the packet has been received over a weak link

When a link breaks, the end nodes of the broken link notify the corresponding end nodes of the path

A source node, after receiving a route break notification packet, rebroadcasts the RouteRequest to find another stable path to the destination

Stale entries are removed only if data packets that use the stale route information fail to reach the next node

If no strong path is available when a link gets broken, then the new route is established by considering weak links also

This is done when multiple RouteRequest attempts fail to obtain a path to the destination using only the stable links

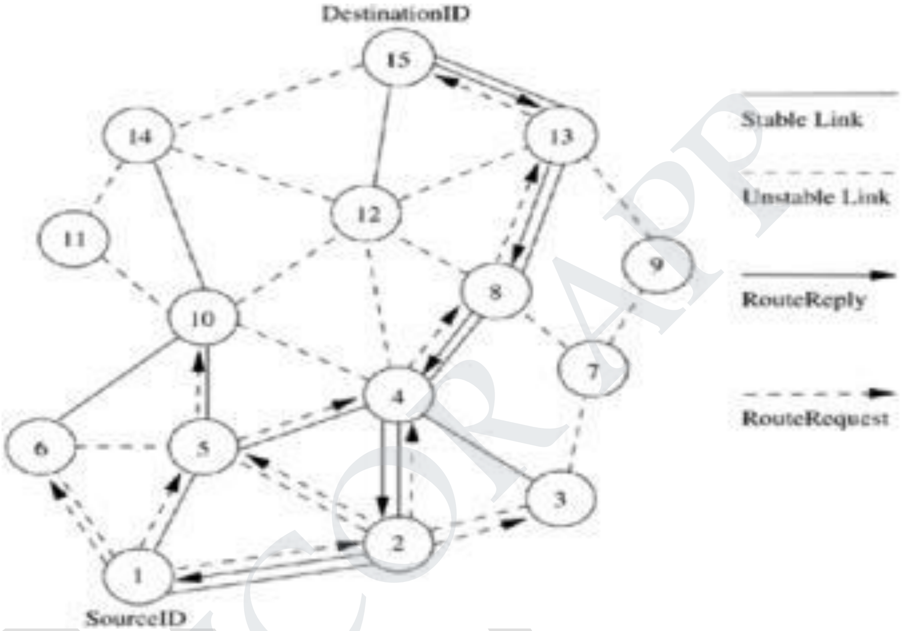


Figure 3.14 (a) : Route establishment in SSA.

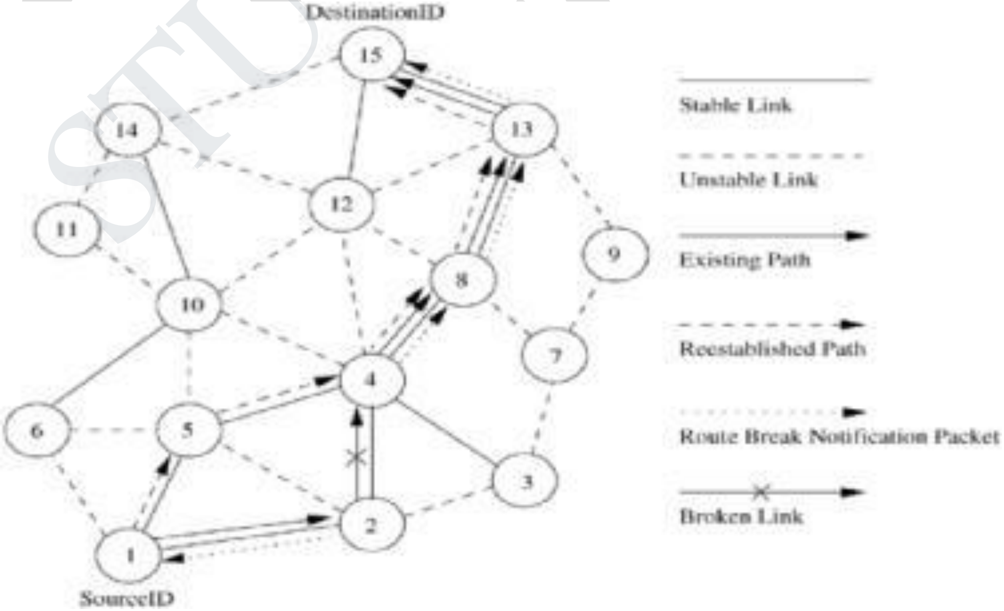


Figure 3.14 (b): Route maintenance in SSA.

Advantage:

Finds more stable routes when compared to the shortest path route selection protocols

Accommodates temporal stability by using beacon counts to classify a link as stable or weak

Disadvantage:

It puts a strong RouteRequest forwarding condition which results in RouteRequest failures

Multiple flooding of RouteRequest packets consumes significant amount of bandwidth

Increases the path setup time

Strong link criterion increases the path length

Flow-Oriented Routing Protocol (FORP)

Employs a prediction-based multi-hop-handoff mechanism for supporting time-sensitive traffic in adhoc wireless networks

Proposed for IPv6-based ad hoc wireless networks where QoS needs to be provided

The multi-hop-handoff is aimed at alleviating the effects of path breaks on the real time packet flows

A sender or an intermediate node initiates the route maintenance process only after detecting a link break

It may result in high packet loss leading to a low QoS provided to the user

FORP utilizes the mobility and location information of nodes to estimate the link expiration time (LET)

LET is the approximate lifetime of a given wireless link

The minimum of the LET values of all wireless links on a path is termed as the route expiry time (RET)

Every node is assumed to be able to predict the LET of each of its links with its neighbors

The LET between two nodes can be estimated using information such as current position of the nodes, their direction of movement, and their transmission ranges

FORP requires the availability of GPS information in order to identify the location of nodes

When a sender node needs to setup a real time flow to a particular destination, it checks its routing table for the availability of a route to that destination

If a route is available, then that is used to send packets to the destination

Otherwise sender broadcasts a flow-REQ packet carrying information regarding the source and destination nodes

The Flow-REQ packet also carries a flow identification number/sequence number which is unique for every session

A neighbor node, on receiving this packet, first checks if the sequence number of the received Flow –REQ is higher than the sequence number corresponding to previous packet

If the sequence number on the packet is less than that of the previous packet, then the packet is discarded

This is done to avoid looping of flow-REQ packets

The Flow-REQ packet, when received at the destination node, contains the list of nodes on the path it had traversed, along with the LET values of every wireless link on that path

FORP assumes all the nodes in the network to be synchronized to a common time by means of GPS information

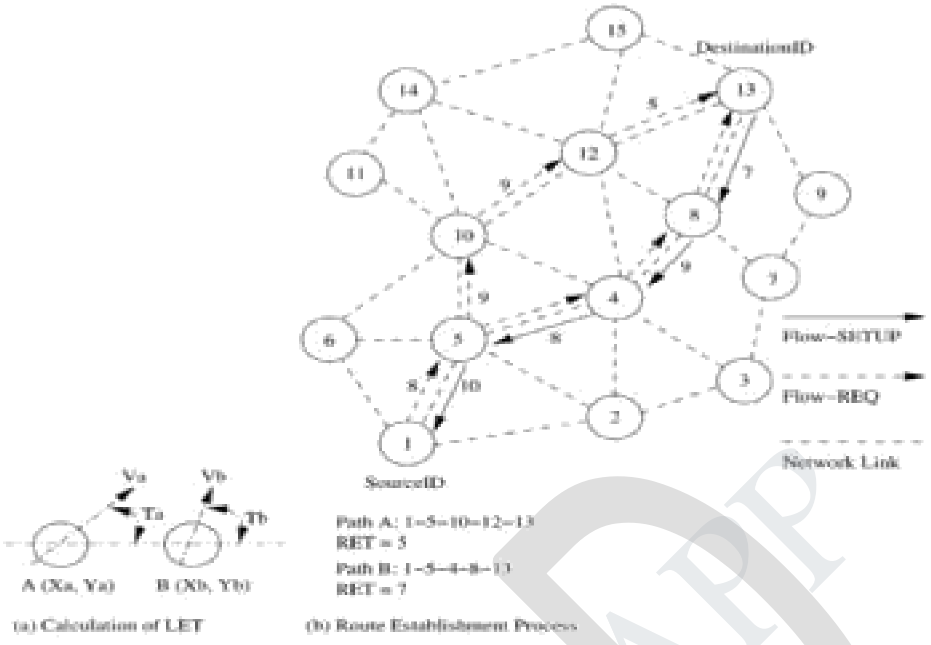


Figure 3.15(a): Route establishment in FORP.

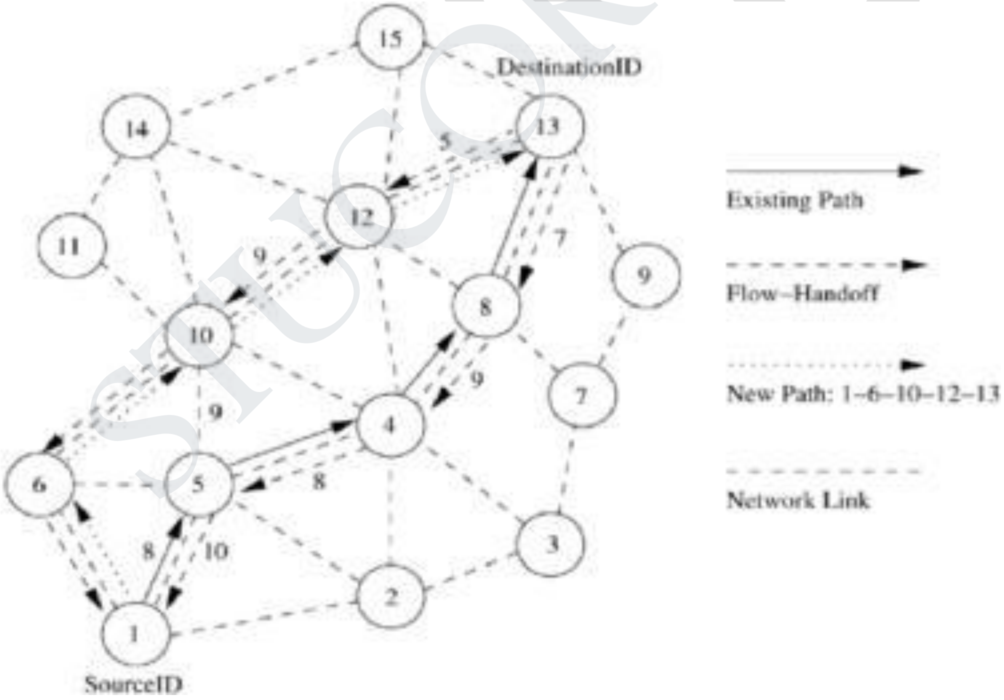


Figure 3.15 (b): Route maintenance in FORP.

Advantage:

Use of LET and RET estimates reduces path breaks

Reduces the reduction in packet delivery

Reduces number of out-of-order packets

Reduces non-optimal paths

Disadvantage:

Works well when topology is highly dynamic

Requirements of time synchronization increases the control overhead

Dependency on GPS infrastructure affects the operability of this protocol wherever it is not available.

(a) Discuss in detail feedback based TCP and TCP BUS.

Feedback-Based TCP:

TCP-F is a feedback-based approach. It requires the support of a reliable link layer and routing protocol that can provide FB to the TCP sender about the path break.

The routing protocol is expected to repair the broken link within a reasonable period.

TCP-F aims to minimize the throughput degradation resulting from the frequent path breaks that occur in ad hoc wireless networks.

During a TCP session, there could be several path breaks resulting in considerable packet loss and path reestablishment delay.

Upon detection of packet loss, the sender in a TCP session invokes the congestion control algorithm leading to the exponential back-off of retransmission timers and a decrease in congestion window size.

In TCP-F, an intermediate node, upon detection of a path break, originates a route failure notification (RFN) packet.

This RFN packet is routed toward the sender of the TCP session.

The TCP sender's information is expected to be obtained from the TCP packets being forwarded by the node.

The intermediate node that originates the RFN packet is called the failure point (FP).

The FP maintains information about all the RFNs. Every intermediate node that forwards the RFNpacket understands the route failure, updates its routing table and avoids forwarding any more packets on that route.

If any of the intermediate nodes that receive RFN has an alternate route to the same destination, then it discards the RFN packet and uses the alternate path for forwarding further data packets, thus reducing the control overhead involved in the route reconfiguration process.

Otherwise, it forwards the RFN toward the source node. When a TCP sender receives an RFN packet, it goes into a state called snooze.

In the snooze state, a sender stops sending any more packets to the destination, cancels all the timers, freezes its congestion window, freezes the retransmission timer, and sets up a route failure timer.

This route failure timer is dependent on the routing protocol, network size, and the network dynamics.

When the route failure timer expires, the TCP sender changes from the snooze state to the connected state.

A TCP session is setup b/n node A and D over the path A-B-C-D(figure 3.16(a))

When the intermediate link b/n node C and node D fails, node C originates the RFN packet and forwards it on the reverse path to the source node.(figure 3.16(b))

The sender's TCP state is changed to the snooze state upon receipt of an RFN packet. If the link CD rejoins, or if any of the intermediate nodes obtains a path to destination node D, a route reestablishment notification (RRN) packet is sent to node A and the TCP state is updated back to the connected state. (figure 3.16 (c))

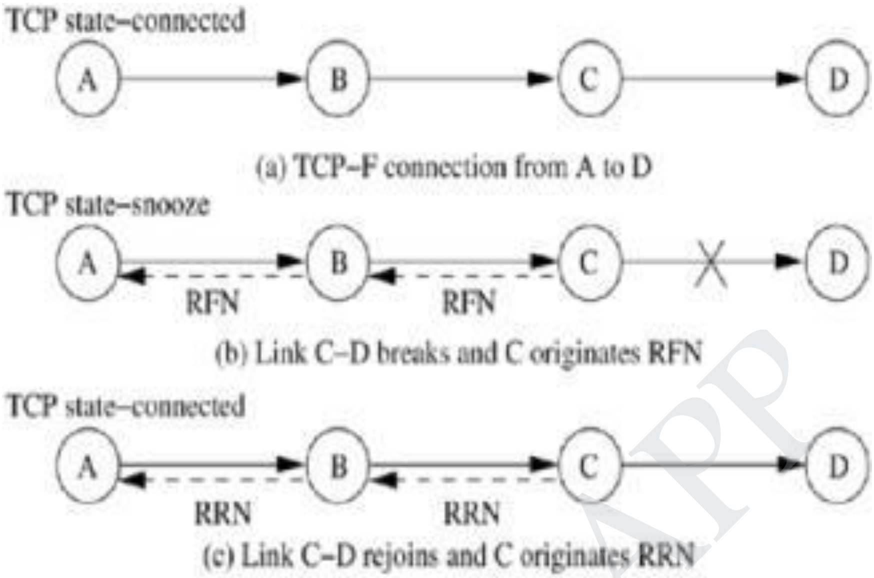

TCP state–connected
A
B
C
D
(a) TCP–F connection from A to D
TCP state–snooze
RFN
RFN
(b) Link C–D breaks and C originates RFN
TCP state–connected
RRN
RRN
(c) Link C–D rejoins and C originates RRN

Figure 3.16 (a) TCP-F connection from A to D
Figure 3.16 (b) Link C-D breaks and C originates RFN
Figure 3.16 (c) Link C-D rejoins and C originates RRN

Advantages:

TCP-F provides a simple FB based solution to minimize the problem arising out of frequent path breaks in ad hoc wireless networks.

At the same time, it also permits the TCP congestion control mechanism to respond to congestion in the n/w.

Disadvantages:

If the route to the sender is not available at the FP then additional control packets may need to be generated for routing the RFN packet.

TCP-F has an additional state compared to the traditional TCP state m/c, and hence its implementation requires modifications to the existing TCP libraries.

Congestion window used after a new route is obtained may not reflect the achievable transmission rate to the n/w and the TCP-F receiver.

TCP BUS:

TCP with buffering capacity and sequence information (TCP-Bus) is similar to TCP-F and TCP-ELFN in its use of feedback information from an intermediate node on detection of a path break. TCP-Bus was proposed with Associativity bared routing (ABR) scheme. TCP-Bus works as follows.

Upon detection of a path break an upstream intermediate node (called pivot node PN) originates explicit route disconnection notification (ERDN) message.

This ERDN is propagated to the TCP-Bus sender Upon reception of ERDN, the TCP-Bus sender stops transmissions and freezes all times and windows.

The packets in transit at the intermediate nodes from TCP-Bus sender to PN are buffered until a new partial path from the PN to the TCP-Bus receiver is obtained by PN.

Upon detection of a path break, the downstream node originates the route notification (RN) packet to the TCP bus receiver.

The PN includes the sequence number of the TCP segment belonging to the flow that is currently at the head of its queue in the ERDN packet.

A PN attempt to final an alternate route to the TCP-Bus receiver and availability of such partial route is to destination is intimated to the TCP-Bus sender through an explicit route successful notification (ERSN) packet.

The Local Query (LQ) packet carries the sequence number of the segment at the head of the queue buffered at the PN and REPLY carries the sequence number of the last successful segment the TC-Bus receiver received.

This enable the TCP-Bus receiver to understand the packets lost in transition and those buffered at the intermediate nodes.

This is used to avoid fast retransmission requests generated by the TCP-BuS receiver when it notices an out-of-order packet delivery.

When the TCP-BuS sender receives an ERSN packet, it resumes the data transmission

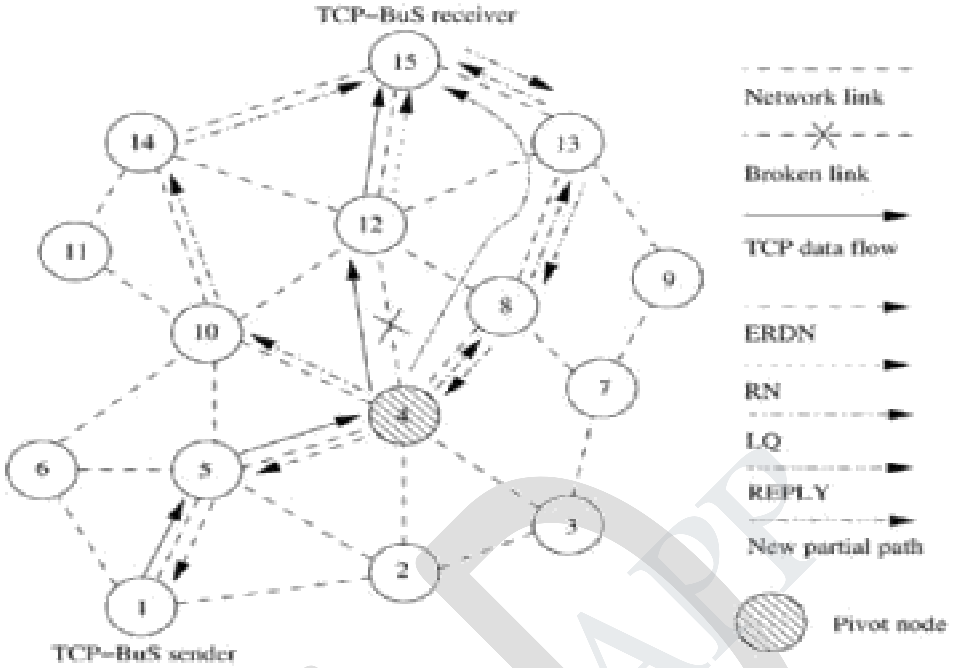


Figure 3.17: Operation of TCP-BUS

The TCP-BuS sender also periodically originates probe packets to check the availability of a path to the destination.

Fig shows the propagation of ERDN and RN messages when a link between nodes 4 and 12 fails.

When a TCP-BuS sender receives the ERSN message, it understands, from the sequence number of the last successfully received packet at the destination and the sequence number of the packet at the head of the queue at PN, the packets lost in transition.

The TCP-BuS receiver understands that the lost packets will be delayed.

The Lost packets are retransmitted by the TCP-Bus sender.

Advantages:

Performance improvement and avoidance of fast retransmission due to the use of buffering, seq numbering and selective acknowledgement.

It takes advantage of ABR

Disadvantages:

Increased dependency on the routing protocol and buffering at intermediate nodes

The failure of intermediate nodes that buffer the packets may lead to loss of packets and performance degradation.

5 .(b) With a neat diagram, explain the operation of ad hoc TCP(ATCP) protocol.

Ad hoc TCP (ATCP) (nov/Dec 2016)

ATCP also uses the feedback mechanism to make the sender aware of the status of the network path. Based on the feedback information retrieved from the intermediate nodes, the TCP sender changes its state to the persist state, congestion control state, or the retransmit state.

When an intermediate node finds that the network is partitioned, then the TCP sender state is changed to the persist state where it avoids unnecessary retransmissions.

When ATCP puts TCP in the persist state, it sets TCP's congestion window size to one in order to ensure that TCP does not continue using the old congestion window value.

This forces TCP to probe the correct value of the congestion window to be used for the new route. If an intermediate node loses a packet due to error, then the ATCP at the TCP sender immediately retransmits it without invoking the congestion control algorithm. In order to be compatible with widely deployed TCP-based networks, ATCP provides this feature without modifying the traditional TCP.

ATCP is implemented as a thin layer residing between the IP and TCP protocols. The ATCP layer essentially makes use of the explicit congestion notification (ECN) for maintenance of the states.

Fig (a) shows the thin layer implementation of ATCP between the traditional TCP layer and the IP layer. This does not require changes in the existing TCP protocol. This layer is active only at the TCP sender.The major function of the ATCP layer is to monitor the packets sent and received by the TCP sender, the state of the TCP sender, and the state of the network.

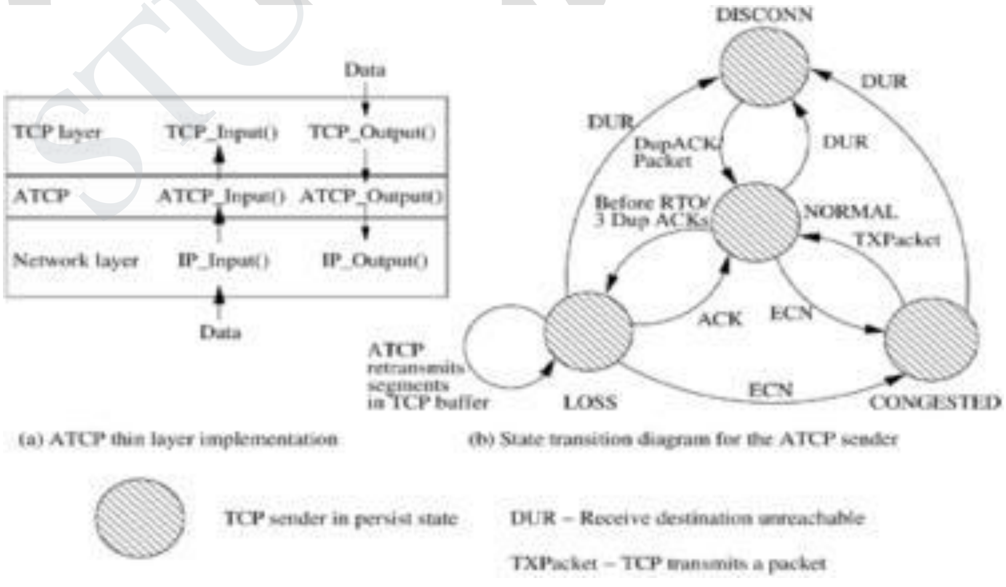
Fig (b) shows the state transition diagram for the ATCP at the TCP sender. The four states in the ATCP are (I) NORMAL (II) CONGESTED (III) LOSS(IV) DISCONN

TCP and the TCP sender is removed from the persist state and then the ATCP sender changes to the NORMAL state.

When a TCP connection is established, the ATCP sender is in NORMAL State. In this state, ATCP does not interfere with the operation of TCP

When packets are lost or arrive out-of-order at the destination, it generates duplicate ACKs. In traditional TCP, upon reception of duplicate ACKs, the TCP sender invokes the congestion control. But the ATCP sender counts the number of duplicate ACKs received, if it reaches three, of it puts TCP in persists state and ATCP in loss state

.



(a) ATCP thin layer implementation

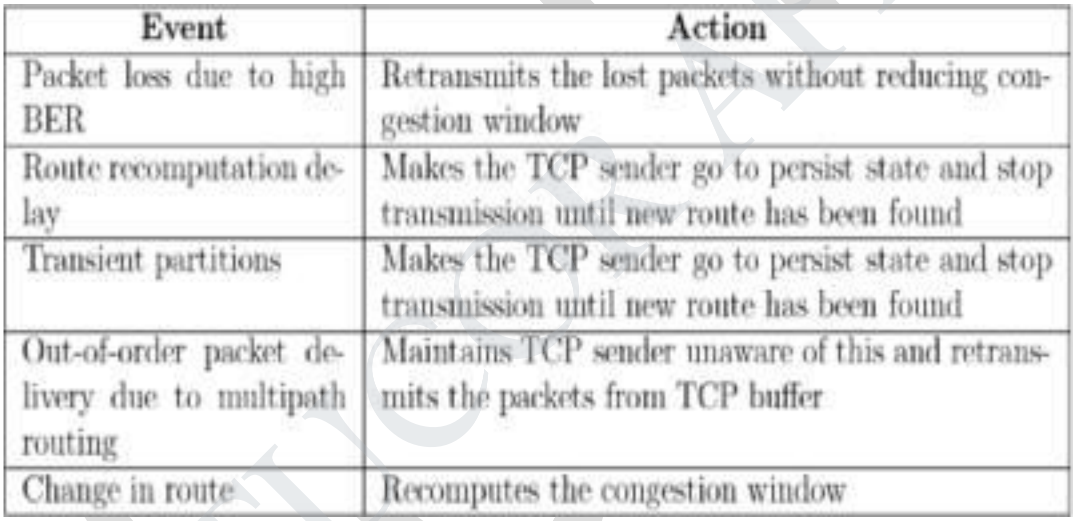
(b) State transition diagram for the ATCP sender

Figure 3.18: An illustration of ATCP thin layer and ATCP state diagram.

When a new ACK comes from TCP receiver. It is forwarded to TCP and the TCP sender is removed from the persists state and then the ATCP sender change to the NORMAL state.

When ATCP sender is in loss state, the receipt of an ECN message charges it to the CONGESTED State. Along with this transition, ATCP sender removes the TCP from the persists state.

When the n/w gets congested, the ECN flag is set in the data and the ACK packets.



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

Figure 3.19: The actions taken by ATCP

Advantages

It maintains the end to end semantics of TCP

It is compatible with traditional TCP

Disadvantages

The dependency on the networks layers protocol to detect the route changes and partitions, which not all-routing protocols may implement.

The addition of thin TCP layer to the protocol stack that requires changes in the interface functions currently used.

6.a) Illustrate the working of split TCP with a neat diagram.
Discuss briefly why the TCP does not perform well in ad hoc wireless Networks.

Working of split TCP with a neat diagram.

In networks, the short connections generally obtain much higher throughput than long connections. This can also lead to unfairness among TCP session, where one session may obtain a much higher throughput than the other sessions.

This unfairness problem is worsened by the use of MAC protocols such as IEEE 802.11, which are found to give a higher throughput for certain link-level sessions, leading to an effect known as **channel capture effect.**

This effect leads to certain flows capturing the channel for longer time durations. The channel capture effect can lead to low overall system throughput.

Split TCP provides the solution to the throughput unfairness problem by splitting the transport layers objectives into congestion control and end to end reliability. The congestion control is mostly a local solution.

At the same time, reliability is an end to end requirement and needs end to end acknowledgements.

Split-TCP splits a long TCP connection into a set of short concatenated TCP connections (called segments or zones) with a number of selected intermediate nodes (known as proxy nodes) as terminating points of these short connections.

The operation of the split TCP is shown in fig where a three stage split connection exists b/n node 1 and node 15.

A proxy node receive the TC packet, reads it, store it in its local buffer and sends LACK to the source (or the previous proxy). This acknowledgment called local acknowledgment (LACK) does not guarantee end-to-end delivery.

The responsibility of further delivery of packets is assigned to proxy node.

A proxy node clears a buffered packet once it receives LACK from the immediate success or proxy for that packet the split TCP maintains the end to end ACK mechanism in addition to zone wise LACK.

The source node clears the buffered packets only after receiving the end to end acknowledgements.

The below fig shows that the node 1 initiates a TCP session to node 15. Node 4 and node 13 are chosen as proxy nodes.

The number of proxy nodes in a TCP session is determined by the length of the path between source and destination nodes.

Based on a distributed algorithm, the intermediate nodes that receive TCPpackets determine whether to act as a proxy node or just as a simple forwarding node.

The simplest algorithm makes the decision for acting as proxy node if the packet has already traversed more than a predetermined number of hops from the last proxy node or the sender of the TCP session.

In fig, the path between node 1 and node 4 is the first zone (segment), the path between nodes 4 and 13 is the second zone (segment), and the last zone is between node 13 and 15.

The transmission control window at the TCP sender is also split into two windows

The congestion window and the end-to-end window.

The congestion window changes the rate of arrival of LACKs from the next proxy node and the end-to-end window is updated based on the arrival of end-to-end ACKs.

In addition to these transmission windows at the TCP sender, every proxy node maintains a congestion window that governs the segment level transmission rate.

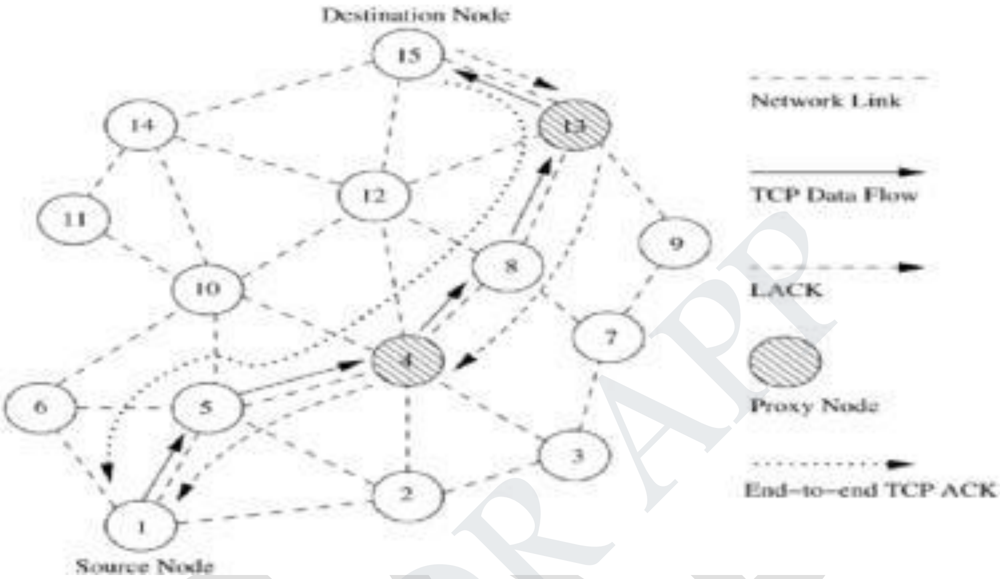


Figure 3.20: An illustration of Split-TCP.

Advantages:

Improved throughput fairness

Lessened impact of mobility. Since in split TCP the path length can be shorter than the end to end path length, the effect of

Mobility on throughput is lessened.

Disadvantages:

It require modifications to TCP protocol

The end to end connection handling of traditional TCP is violated

The failure of proxy nodes can lead to the throughput degradation.

6.b) Discuss briefly why the TCP does not perform well in ad hoc wireless networks.

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

i) Misinterpretation of Packet Loss

In traditional TCP design, packet-loss is mainly attributed to network congestion.

Ad hoc-network experience a much higher packets loss due to

High bit rate in the wireless channel.

Increased Collisions due to the presence of hidden terminals.

Presence of interference

location-dependent contention,

uni-directional links,

Frequent path breaks due to mobility of nodes and

The inherent fading properties of the wireless channel.

Frequent Path Breaks

The responsibility of finding a route and reestablishing it once it gets broken is attached to the network layer.

Once a path is broken, the routing protocol initiates a route reestablishment process. This route reestablishment process takes a significant amount of time to obtain a new route to the destination.

The route reestablishment time is a function of the number of nodes in the network, transmission ranges of nodes, current topology of the network, bandwidth of the channel, traffic load in the network, and the nature of the routing protocol.

If the route re-establishment time is greater than the RTO period of sender, then the sender

Assumes congestion in the network

Retransmits lost packets and

Initiates congestion-control algorithm.

This leads to wastage of: 1) Bandwidth and 2) Battery-power.

iii) Effect of Path Length

The TCP throughput degrades rapidly with an increase in path length in string (linear chain) topology ad hoc wireless networks.

As path length increases, the throughput decreases the possibility of a path break increases with path length. Given that the probability of a link break is pl , the probability of a path break (pb) for a path of length k can be obtained as pb = 1 - (1 -pl)k.

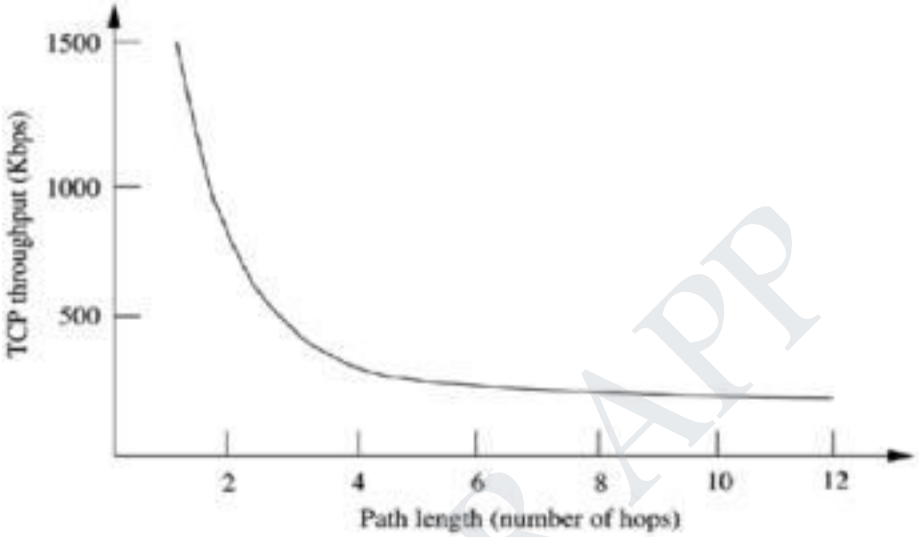


Figure 3.21 (a): Variation of TCP throughput with path length.

- The variation of pb with path length for pl = 0.1. Hence as the path length increases, the probability of a path break increases, resulting in the degradation of the throughput in the network.

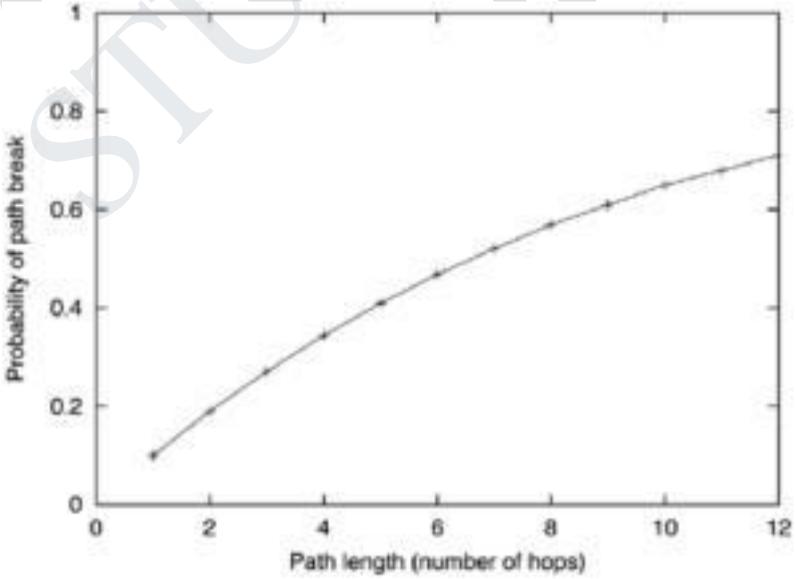


Figure 3.21 (b): Variation of pb with path length (pl = 0.1).

iv)Misinterpretation of Congestion Window

In ad hoc wireless networks, the congestion control mechanism is invoked when the network gets partitioned or when a path break occurs.

This reduces the congestion window and increases the RTO period.

When the route is reconfigured, the congestion window may not reflect the transmission rate acceptable to the new route, as the new route may actually accept a much higher transmission rate.

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

Asymmetric Link Behavior

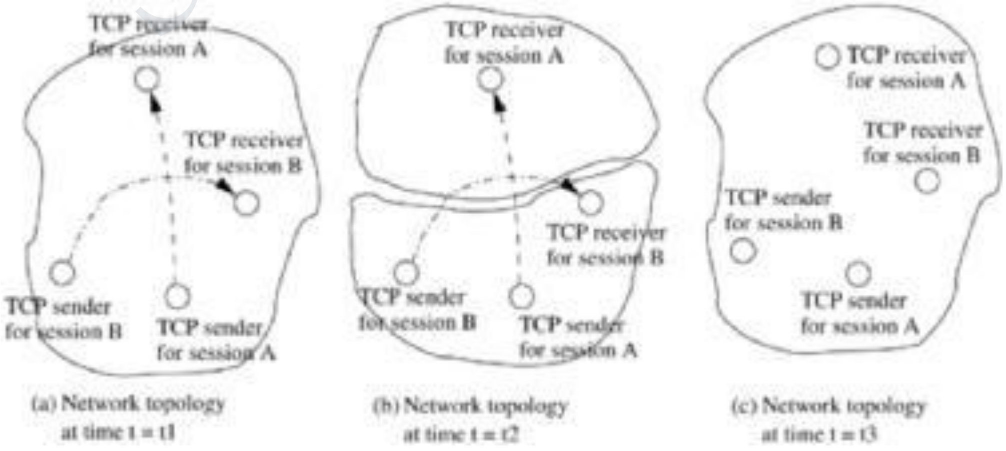
Radio-channel has different properties such as location dependent contention, directional properties etc leading to asymmetric links.

The directional links can result in delivery of a packet to a node, but failure in the delivery of the acknowledgment back to the sender. It is possible for a bidirectional link to become uni-directional for a while.

This can lead to TCP invoking the congestion-control algorithm and several retransmissions.

Network Partitioning & Remerging

The randomly moving nodes in an ad hoc wireless network can lead to network partitions.



(a) Network topology at time t = t1

(b) Network topology at time t = t2

(c) Network topology at time t = t3

Figure 3.22: Effect of partitioning and merging of network.

A network with two TCP sessions A and B is shown in Figure 3.22(a) at time instant t1.

Due to dynamic topological changes, the network gets partitioned into two as in Figure 3.22(b) at time t2.

The TCP session A's sender and receiver belong to two different partitions and the TCP session B experiences a path break. These partitions could merge back into a single network at time t3.

Uni-directional Path

TCP relies on end-to-end ACK for ensuring reliability.

Path-break on an entirely different reverse path can affect the performance of the network as much as a path-breaks in the forward path.

Multipath Routing

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

UNIT -IV

WIRELESS SENSOR NETWORKS & MAC PROTOCOLS

Single node architecture: hardware and software components of a sensor node - WSN Network architecture: typical network architectures-data relaying and aggregation strategies -MAC layer protocols: self-organizing, Hybrid TDMA/FDMA and CSMA based MAC- IEEE 802.15.4.

PART - A

1. Define Sensor Networks. (April/May 2017)

Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system.

2. What are the features of sensor nodes?

Limited sensing region, processing power, energy

3.What are the advantages of sensor networks?

Robust : a large number of sensors

Reliable :

Accurate : sensor networks covering a wider region

Fault-tolerant : many nodes are sensing the same event

4. Write the subsystem of sensor networks node? (April/May 2017)

Each node of the sensor networks consist of three subsystem:

Sensor subsystem: senses the environment

Processing subsystem: performs local computations on the sensed data

Communication subsystem: responsible for message exchange with neighboring sensor node.

5. What are the goals of data fusion?

The main goals of data fusion are to reduce bandwidth consumption, media access delay, and power consumption for communication.

6. What is UNPF?

It is a set of protocols for complete implementation of a layered architecture for sensor networks. UNPF integrates three operations in its protocol structure: network initialization and maintenance, MAC, and routing protocols.

7. Why using LEACH protocol in sensor networks?

Sensor networks should be self-organizing, hence the cluster formation and election of cluster-heads must be an autonomous, distributed process. This is achieved through network layer protocols such as the low-energy adaptive clustering hierarchy (LEACH) .

8.What are the challenges posed by MAC protocol in sensor network?

No single controlling authority, so global synchronization is difficult

Power efficiency issue ,Frequent topology changes due to mobility and failure.

9.List the different kinds of MAC protocols used in sensor network?

There are three kinds of MAC protocols used in sensor network:

Fixed-allocation

Demand-based

Contention-based.

10. Write the use of SMACS and EAR protocol.

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

11.What are the application areas of IEEE 802.15.4?

Application areas include industrial control, agricultural, vehicular and medical sensors and actuators that have relaxed data rate requirements.

Inside the home, there are several areas where such technology can be applied effectively:

PC-peripherals including keyboards, wireless mice, low end PDAs, joysticks; consumer electronics including radios, TVs, DVD players, remote controls;

Home automation including heating, ventilation, air conditioning, security, lighting, control of windows, curtains, doors, locks; health monitors and diagnostics.

12. What is GTS ?

Channel access is usually contention based though the PAN may assign time slots to a single device. This is known as a guaranteed time slot (GTS)

PART-B

1.a. Compare Adhoc-wireless and Wireless sensor networks.

The number of nodes in sensor network can be several orders of magnitude large than the number of nodes in an ad hoc network.

Sensor nodes are more easy to failure and energy drain, and their battery sources are usually not replaceable or rechargeable.

Sensor nodes may not have unique global identifiers (ID), so unique addressing is not always feasible in sensor networks.

Sensor networks are data-centric, the queries in sensor networks are addressed to nodes which have data satisfying some conditions. Ad Hoc networks are address-centric, with queries addressed to particular nodes specified by their unique address.

Data fusion/aggregation: the sensor nodes aggregate the local information before relaying. The goals are reduce bandwidth consumption, media access delay, and power consumption for communication.

1. b. What are the applications of Sensor Networks?

1.Using in military

– Battlefield surveillance and monitoring, guidance systems of intelligent missiles, detection of attack by weapons of mass destruction such as chemical, biological, or nuclear

2.Using in nature

– Forest fire, flood detection, habitat exploration of animals

3.Using in health

– Monitor the patient's heart rate or blood pressure, and sent regularly to alert the concerned doctor, provide patients a greater freedom of movement.

4.Using in home (smart home)

– Sensor node can built into appliances at home, such as ovens, refrigerators, and vacuum cleaners, which enable them to interact with each other and be remote-controlled

5.Using in office building

– Airflow and temperature of different parts of the building can be automatically controlled

6.Using in warehouse

– Improve their inventory control system by installing sensors on the products to track their movement

2. Draw and explain the architecture of Sensor Networks. (April/May 2017) (nov/Dec 2016)

The design of sensor networks is influenced by factors such as scalability, fault tolerance, and power consumption .

The two basic kinds of sensor network architecture are

Layered architecture

Clustered. architecture

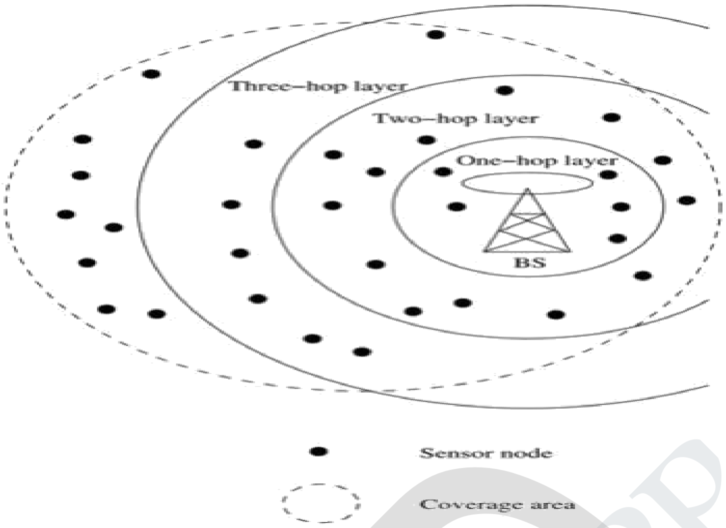


Figure 4.1.Clustered. architecture

Layered architecture has a single powerful base station (BS), and the layers of sensor nodes around it correspond to the nodes that have the same hop-count to the BS. Layered architectures have been used with in-building wireless backbones, and in military sensor-based infrastructure, such as the multi-hop infrastructure network architecture (MINA) . In the in-building scenario, the BS acts an access point to a wired network, and small nodes form a wireless backbone to provide wireless connectivity. The users of the network have hand-held devices such as PDAs which communicate via the small nodes to the BS.

Similarly, in a military operation, the BS is a data-gathering and processing entity with a communication link to a larger network. A set of wireless sensor nodes is accessed by the hand-held devices of the soldiers.

The advantage of a layered architecture is

1.Each node is involved only in short-distance,

2.Low-power transmissions to nodes of the neighboring layers.

Unified Network Protocol Framework (UNPF) is a set of protocols for complete implementation of a layered architecture for sensor networks. UNPF integrates three operations in its protocol structure:

Network initialization and maintenance,

MAC, and

3.Routing protocols.

• Network Initialization and Maintenance Protocol: The network initialization protocol organizes the sensor nodes into different layers, using the broadcast capability of the BS. The BS can reach all nodes in a one-hop communication over a common control channel. The BS broadcasts its identifier (ID) using a known CDMA code on the common control channel. All nodes which hear this broadcast then record the BS ID. They send a beacon signal with their own IDs at their low default power levels. Those nodes which the BS can hear form layer one since they are at a single-hop distance from the BS. The BS now broadcasts a control packet with all layer one node IDs. All nodes send a beacon signal again. The layer one nodes record the IDs which they hear, and these form layer two, since they are one hop away from layer one nodes. In the next round of beacons, the layer one nodes inform the BS of the layer two nodes, which is then broadcast to the entire network. In this way, the layered structure is built by successive rounds of beacons and BS broadcasts. Periodic beaconing updates neighbor information and alters the layer structure if nodes die out or move out of range.

• **MAC Protocol** Network initialization is carried out on a common control channel. During the data transmission phase, the distributed TDMA receiver oriented channel (DTROC) assignment MAC protocol is used. Each node is assigned a reception channel by the BS, and channel reuse is such that collisions are avoided. The node schedules transmission slots for all its neighbors and broadcasts the schedule. This enables collision-free transmission and saves energy, as nodes can turn off when they are not involved in a send/receive operation. The two steps of DTROC are channel allocation (the assignment of reception channels to the nodes) and channel scheduling (the sharing of the reception channel among the neighbors). DTROC avoids hidden terminal and exposed terminal problems by suitable channel allocation algorithms.

• **Routing Protocol** Downlink from the BS is by direct broadcast on the control channel. The layered architecture enables multi-hop data forwarding from the sensor nodes to the BS. The node to which a packet is to be forwarded is selected considering the remaining energy of the nodes. This achieves a higher network lifetime. Existing ad hoc routing protocols can be simplified for the layered architecture, since only nodes of the **next layer need to be maintained** in the routing table. A modification to the UNPF protocol set termed the UNPF-R has been proposed. It makes the sensor nodes adaptively vary their transmission range so that network performance can be optimized. While a very small transmission range could cause network partitioning, a very large transmission range will reduce the spatial reuse of frequencies. The optimal range is determined through an algorithm similar to simulated annealing. This is a centralized control algorithm in which the BS evaluates an objective function periodically.

For a transmission range R, the objective function is, where N is the total number of sensors in the system; n is the number of nodes in layer one; is the energy consumption per packet; and d is the average packet delay. The BS selects a new transmission range R' as follows. If no packet is received by the BS from any sensor node for some interval of time, the transmission range is increased by Δr, a predefined increment. Otherwise, the transmission range is either decreased by Δr with probability 0.5 × (n/N), or increased by Δr with probability [1 - 0.5 × (n/N)].

The objective function is reevaluated with the new transmission range. If , then the transmission range R' is adopted. Otherwise, R is modified to R' with probability, where T is the temperature parameter, as in simulated annealing. The advantage of the UNPF-R is that it minimizes the energy × delay metric, and maximizes the number of nodes which can connect to the BS. The minimization of the energy × delay metric ensures that transmission should occur with minimum delay and with minimum energy consumption. The two conflicting objectives are together optimized by minimizing their product.

Simulated annealing algorithm is an optimization heuristic in which an objective function is evaluated for different values of the independent variable. A value which provides an inferior objective value is also accepted with a probability, which is reduced as the algorithm progresses. This is to escape local minima of the objective function. The progress of the heuristic is indicated by the decreasing temperature parameter.

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

Figure represents a clustered architecture where any message can reach the BS in at most two hops. Clustering can be extended to greater depths hierarchically.

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

Sensor networks should be self-organizing, hence the cluster formation and election of cluster-heads must be an autonomous, distributed process. This is achieved through network layer protocols such as the low-energy adaptive clustering hierarchy (LEACH) .

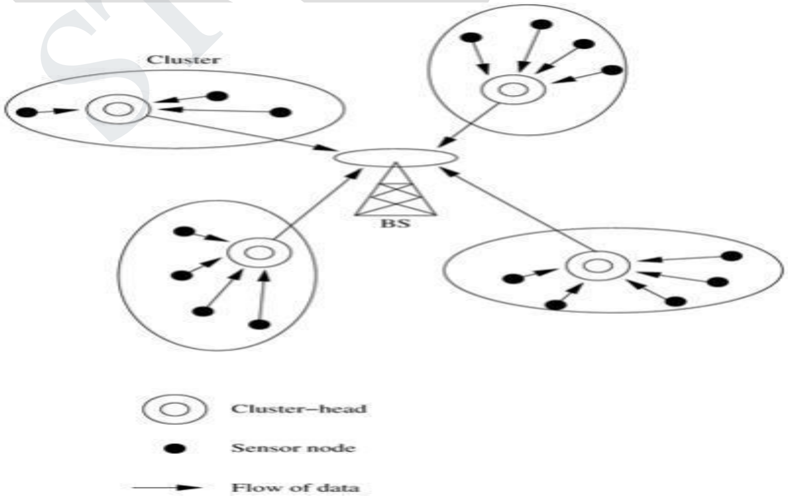


Figure 4.2. Clustered architecture

Low-Energy Adaptive Clustering Hierarchy (LEACH) LEACH is a clustering-based protocol that minimizes energy dissipation in sensor networks.

LEACH randomly selects nodes as cluster-heads and performs periodic reelection, so that the high-energy dissipation experienced by the cluster-heads in communicating with the BS is spread across all nodes of the network.

If this is lower than the threshold for node n, T(n), the sensor node becomes a cluster-head. The threshold T(n) is calculated as where P is the desired percentage of nodes which are cluster-heads, r is the current round, and G is the set of nodes that has not been cluster-heads in the past 1/P rounds.

This ensures that all sensor nodes eventually spend equal energy. After selection, the cluster-heads advertise their selection to all nodes.

All nodes choose their nearest cluster-head when they receive advertisements based on the received signal strength.

The cluster-heads then assign a TDMA schedule for their cluster members.

The steady phase is of longer duration in order to minimize the overhead of cluster formation. During the steady phase, data transmission takes place based on the TDMA schedule, and the cluster-heads perform data aggregation/fusion through local computation.

The BS receives only aggregated data from cluster heads, leading to energy conservation. After a certain period of time in the steady phase, cluster-heads are selected again through the set-up phase.

3.What are the issues and challenges in designing a Sensor Network?

A sensor network has some design challenges due to the following reasons:

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

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

The operation of sensor nodes is the available energy. Sensors usually rely only on their battery for power, which in many cases cannot be recharged or replaced. Energy problem

Hardware and software should be designed to conserve power.

Sensor nodes should be able to synchronize with each other in a completely distributed manner, so that TDMA schedules can be imposed

A sensor network should also be capable of adapting to changing connectivity due to the failure of nodes, or new nodes powering up. The routing protocols should be able to dynamically include or avoid sensor nodes in their paths.

Real-time communication over sensor networks must be supported through provision of guarantees on maximum delay, minimum bandwidth, or other QoS parameters.

Provisions must be made for secure communication over sensor networks, especially for military applications which carry sensitive data.

4. Explain Mac Layer protocols in sensor Networks. (April/May 2017)

The challenges posed by sensor network MAC protocol has no single controlling authority, so global synchronization is difficult

Efficiency issue

Frequent topology changes due to mobility and failure

There are three kinds of MAC protocols used in sensor network:

Fixed-allocation

Demand-based

Contention-based

Fixed allocation MAC protocols share the common medium through a predetermined assignment. It is suitable for sensor network that continuously monitor and generate deterministic data traffic.

It provides a bounded delay for each node.However, in the case of bursty traffic, where the channel requirements of each node may vary over time; it may lead to inefficient usage of the channel.

Demand based MAC protocols are used in such cases, where the channel is allocated according to the demand of the node. Though they require the additional overhead of a reservation process, variable rate traffic can be efficiently transmitted using demand-based MAC protocols.

Contention based MAC protocols involve random-access-based contention for the channel when packets need to be transmitted. They are again suitable for bursty traffic, but there is a possibility of collisions and no delay guarantees can be provided. Hence, they are not suitable for delay-sensitive or real-time traffic.

Self-Organizing MAC for Sensor Networks (SMACS) and Eavesdrop and Register (EAR)

SMACS and EAR protocols which handle network initialization and mobility support, respectively. **SMACS** is a distributed protocol for network initialization and link-layer organization.

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

A communication link between two nodes consists of a pair of time slots, at a fixed frequency, which is randomly chosen at the time of establishing the link. Such an assignment is possible in sensor networks without interference from neighboring nodes because the available bandwidth is much larger than the data rate required for a message transmission between two nodes.

This scheme requires synchronization only between communicating neighbors, in order to precisely define the slots to be used for their communication.

Power is conserved by turning off the transceiver during idle slots, and using a random wake-up schedule during the network start-up phase.

EAR protocol:

The **EAR** protocol enables seamless connection of nodes under mobile and stationary conditions. This protocol makes use of certain mobile nodes, besides the existing stationary sensor nodes, to offer service to maintain connections. Mobile nodes eavesdrop on the control signals and maintain neighbor information.

Hybrid TDMA/FDMA

This is a centrally controlled scheme which assumes that nodes communicate directly to a nearby BS.

A pure TDMA scheme minimizes the time for which a node has to be kept on, but the associated time synchronization costs are very high. A pure FDMA scheme allots the minimum required bandwidth for each connection.

The hybrid TDMA/FDMA scheme, proposed in , uses an optimum number of channels, which gives minimum overall power consumption. This is found to depend on the ratio of power consumption of transmitter to receiver.

If the transmitter consumes more power, a TDMA scheme is favored, since it can be switched off in idle slots to save power.

On the other hand, the scheme favors FDMA when the receiver consumes greater power. This is because, in FDMA, the receiver need not expend power for time synchronization by receiving during the guard band between slots, which becomes essential in a TDMA scheme.

CSMA-Based MAC Protocols

CSMA-based schemes are suitable for point-to-point randomly distributed traffic flows. The sensing periods of CSMA are constant for energy efficiency, while the back-off is random to avoid repeated collisions.

Binary exponential back-off is used to maintain fairness in the network. Use an adaptive transmission rate control (ARC) to balance originating traffic and route-through traffic in nodes. This ensures that nodes closer to the BS are not favored over farther nodes.CSMA-based MAC protocol are contention-based and are designed mainly to increase energy efficiency and maintain fairness.

5. Draw the protocol stack of IEEE 802.15.4 and explain its functions.

IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low rate, low-speed ubiquitous communication between devices. It can be contrasted with other approaches, such as Wi-Fi, which offer more bandwidth and require more power.

It is used in home networking applications where the key motivations are reduced installation cost and low power consumption.

The basic framework conceives a 10-meter communications range with a transfer rate of 250 kbit/s.

Lower transfer rates of 20 and 40 kbit/s were initially defined, with the 100 kbit/s rate being added in the current revision.

Even lower rates can be considered with the resulting effect on power consumption.

Features:

Reservation of guaranteed time slots, Collision avoidance through CSMA/CA

Integrated support for secure communications.

Devices also include power management functions such as link quality and energy detection.

IEEE 802.15.4 protocol stack:

Physical layer has 2 parts

IEEE 802.15.4 868/915 MHz

IEEE 802.15.4 2400 MHz

The network layers is based on the OSI model, although only the lower layers are defined in the standard, interaction with upper layers is intended, possibly using an IEEE 802.2 logical link control sub layer accessing the MAC through a convergence sub layer.

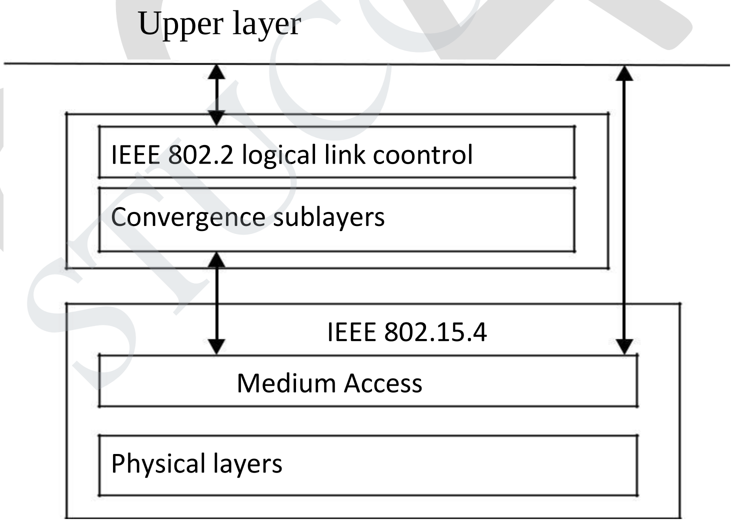


Figure 4.4 IEEE 802.15.4 protocol stack**:**

The physical layer

The physical layer is the initial layer in the OSI reference model.

It operates on one of 2 possible unlicensed frequency bands.

2.4 GHz ISM band (250 kbps) and

868/915 MHz (20-40 kbps).

They also differ with respect to the data rates supported.

The ISM band PHY layer offers a transmission rate of 250 kbps while the 868/915 MHz offers 20 and 40 kbps.

The lower rate can be translated into better sensitivity and larger coverage area, while the higher rate of the 2.4 GHz band can be used to attain lower duty cycle, higher throughput and lower latencies.

Each device should be able to transmit at least 1 mW.

It uses a simple DSSS in which each bit is represented by a 15-chip maximal length sequence (m-sequence).

Encoding is done by multiplying the msequence with +1 or -1 , and the resulting sequence is modulated by the carrier signal using BPSK.

The 2.4 GHz PHY supports 16 channels between 2.4 GHz and 2.4835 GHz with 5 MHz channel spacing for easy transmit and receive filter requirements. It employs a 16-ary quasi-orthogonal modulation technique based on DSSS.

The two PHY layers though different, maintain a common interface to the MAC layer, i.e., they share a single packet structure as shown in Figure 4.5.

Frame Format :

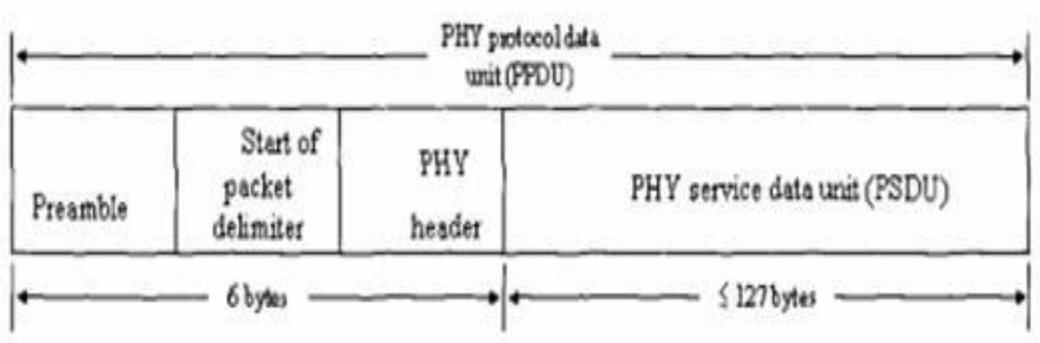

PHY protocol data unit (PPDU)
Preamble
Start of packet delimiter
PHY header
PHY service data unit (PSDU)
6 bytes
≤ 127 bytes

Figure 4.5 frame format

Preamble 32 bits - synchronization

Start of packet delimiter (8 bits) – signify end of preamble

PHY header (8 bits) – specify PSDU

PSDU (<=127 bits) – PHY layer payload

PHY protocol data unit(PPDU) Preamble Start of packet delimiter PHY header PHY service data unit (PSDU) 6 bytes i 127 bytes PHY packet fields.

The packet or PHY protocol data unit (PPDU) consists of the synchronization header, a PHY header for the packet length, and the payload itself which is also referred to as the PHY service data unit (PSDU).

preamble – used for synchronization 8-bit start of packet delimiter, signifying the end of the preamble. Out of the 8 bits in the PHY header, seven are used to specify the length of the PSD which can range from 0-127 bytes.

Beyond these three bands, the IEEE 802.15.4c study group considered the newly opened 314–316 MHz, 430–434 MHz, and 779–787 MHz bands in China.

In August 2007, IEEE 802.15.4a was released expanding the four PHYs available in the earlier 2006 version to six, including one PHY using Direct Sequence ultra-wide band(UWB) and another using chirp spread spectrum (CSS).

The MAC layer

The Medium Access Control (MAC) enables the transmission of MAC frames through the use of the physical channel. Besides the data service, it offers a management interface and itself manages access to the physical channel and network beaconing.

It also controls frame validation, guarantees time slots and handles node associations. Finally, it offers hook points for secure services.

The MAC protocol data unit (MPDU), or the MAC frame, consists of

1.The MAC header (MHR),

MAC service data unit (MSDU) and

MAC footer (MFR).

The MHR consists of a 2 byte frame control field that specifies the frame type, the address format and controls the acknowledgement, 1 byte sequence number which matches the acknowledgement frame with the previous transmission, and a variable sized address field (0-20 bytes).

The payload field is variable in length but the maximum possible size of an MPDU is 127 bytes.

The MFR completes the MPDU and consists of a frame check sequence (FCS) field which is basically a 16-bit CRC code.

IEEE 802.15.4 under certain conditions provides dedicated bandwidth and low latencies to certain types of applications, by operating in a super frame mode.

Channel access is usually contention based though the PAN may assign time slots to a single device. This is known as a guaranteed time slot (GTS) .

An important function of MAC is to confirm successful reception of frames. Valid data and command frames are acknowledged; otherwise it is simply ignored.

The frame control field indicates whether a particular frame has to be acknowledged or not.

IEEE 802.15.4 provides three levels of security:

No security,
Access control lists and
Symmetric key security using AES-128.

IEEE 802.15.4 PHYs only support frames of up to 127 bytes .

Higher layers

Other higher-level layers and interoperability sub layers are not defined in the standard. Specifications, such as6l0WPNand ZigBee build on this standard. The standard defines two types of network node.

The first one is the **full-function device** (FFD). It can serve as the coordinator of a personal area network just as it may function as a common node.

On the other hand, there are **reduced-function devices** (RFD). These are meant to be extremely simple devices with very modest resource and communication requirements; due to this, they can only communicate with FFDs and can never act as coordinators.

3. Explain the main components of the wireless sensor node.

Main components of a WSN node

Controller
Communication device(s)
Sensors/actuators
Memory
Power supply

Microcontrollers:

The processor for general purposes

It is used in Optimized for embedded applications

Low energy consumption.

The communication module of a sensor node is called "Radio Transceiver"

The essentially tasks of transceiver is to "transmit" and "receive" data between a pair of nodes.

The following characteristics of the transceiver should be consider for sensor nodes

Capabilities

Energy characteristics

Radio performance

Transceivers typically has several different states/modes

Transmit mode

Transmitting data

Receive mode

Receiving data

Idle mode

Ready to receive, but not doing so some functions in hardware can be switched off.

Reducing energy consumption a little

Sleep mode

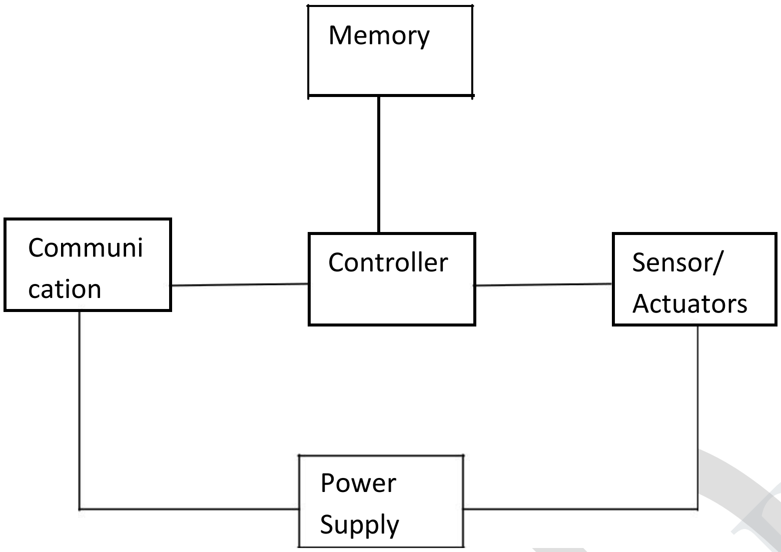


Figure 4.6.Sensor node architecture

- Significant parts of the transceiver are switched off
- Not able to immediately receive something
- Recovery time and startup energy in sleep state can be significant

Sensor main category

Passive and active

Directional Vs omni directional

Power supply module

provides as much energy as possible includes following requirements

Longevity

Low self

discharge

Voltage stability

Smallest cost

High capacity/volume

Efficient recharging at low current

Shorter recharge time

Options of power supply module

Primary batteries -not rechargeable

Secondary batteries -rechargeable

In WSN, recharging may or may not be an option.

The memory module of a sensor node has two major tasks

To store intermediate sensor readings, packets from other nodes, and so on.

To store program code.

UNIT V

WSN ROUTING, LOCALIZATION & Qos

Issues in WSN routing – OLSR- Localization – Indoor and Sensor Network Localization-absolute and relative localization, triangulation-QOS in WSN-Energy Efficient Design-Synchronization-Transport Layer issues.

PART – A

1.What are the design challenges in sensor networks?(april/May 2017)

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

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

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

Sensor nodes should be able to synchronize with each other in a completely distributed manner, so that TDMA schedules can be imposed and temporal ordering of detected events can be performed without ambiguity.

2.Define Localization.

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

Atomic multi-lateration.

Iterative multi-lateration.

Collaborative multi-lateration.

3.Define worst-case and best-case coverage.

The worst-case coverage defines areas of breach, that is, where coverage is the poorest. This can be used to determine if additional sensors need to be deployed to improve the network.

The best-case coverage, on the other hand, defines the areas of best coverage. A path along the areas of best coverage is called a maximum support path or maximum exposure path.

4.What is meant by Resynchronization?

Resynchronization is the process of synchronizing different network partitions that are independently synchronized to different clocks to a common clock. In dynamic networks such as sensor networks, frequent changes in topology make resynchronization an important issue.

5. What is Localized encryption and authentication protocol?

Localized encryption and authentication protocol (LEAP) is a key management protocol (a protocol to distribute cryptographic keys) for sensor networks based on symmetric key algorithms, that is, the same key is used by sender and receiver.

In a network, requiring every pair of nodes to have a shared key to be used for communication between them is ideal for security, because an attack on any one node does not compromise the security of other nodes.

6. Define OLSR protocol.

The optimized link state routing (OLSR) protocol is a proactive routing protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying.

This protocol optimizes the pure link state routing protocol. Optimizations are done in two ways: by reducing the size of the control packets and by reducing the number of links that are used for forwarding the link state packets.

7. Difference between WSN and Ad-hoc sensor network.

Difference between WSN and Ad hoc

Sensor nodes are densely deployed

Sensor nodes are prone to failures

The topology of a sensor network changes very frequently

WSN broadcast but ad hoc point-to point

Sensor node are limited in power computation capacities and memory

Sensor nodes may not have global identification

8. What is meant by WSN?

Consist of large amount of sensor nodes

Multi-hop, self-organize

Wireless communication

Cooperative sensing, collection, process

Send to observe.

9. Define hierarchical state routing protocol.

The hierarchical state routing (HSR) protocol is a distributed multi-level hierarchical routing protocol that employs clustering at different levels with efficient membership management at every level of clustering. The use of clustering enhances resource allocation and management.

10. Which two protocols support real-time communication in sensor networks?

SPEED

A stateless protocol, SPEED, which supports real-time communication in sensor networks. SPEED is a localized algorithm which provides real-time unicast, real-time area-multicast (multicast to all nodes in a particular region), and real-time anycast support for packet transmission. SPEED has minimal overheads, as it does not require routing tables.

RAP

It provides APIs for applications to address their queries. An application layer program in the BS can specify the kind of event information required, the area to which the query is addressed, and the deadline within which information is required.

PART – B

1. Explain in detail about OLSR protocol with neat diagram?

- The optimized link state routing (OLSR) protocol is a proactive routing protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying. This protocol optimizes the pure link state routing protocol.

Optimizations are done in two ways:

by reducing the size of the control packets and

by reducing the number of links that are used for forwarding the link state packets.

The reduction in the size of link state packets is made by declaring only a subset of the links in the link state updates.

This subset of links or neighbors that are designated for link state updates and are assigned the responsibility of packet forwarding are called multipoint relays.

The optimization by the use of multipoint relaying facilitates periodic link state updates.

The link state update mechanism does not generate any other control packet when a link breaks or when a link is newly added.

The link state update optimization achieves higher efficiency when operating in highly dense networks.

Figure 5.1(a) shows the number of message transmissions required when the typical flooding-based approach is employed. In this case, the number of message transmissions is approximately equal to the number of nodes that constitute the network.

The set consisting of nodes that are multipoint relays is referred to as MPRset. Each node (say, P) in the network selects an MPRset that processes and forwards every link state packet that node P originates.

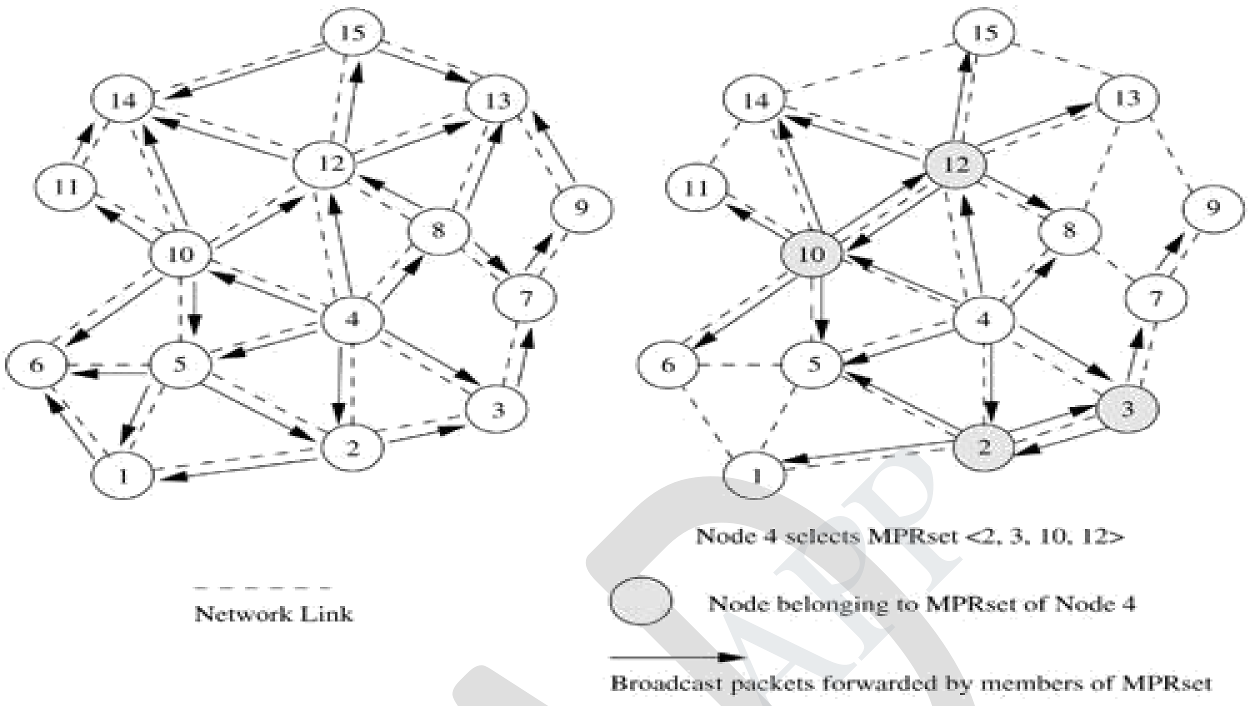
The neighbor nodes that do not belong to the MPRset process the link state packets originated by node P but do not forward them.

Similarly, each node maintains a subset of neighbors called MPR selectors, which is nothing but the set of neighbors that have selected the node as a multipoint relay.

A node forwards packets that are received from nodes belonging to its MPRSelector set. The members of both MPRset and MPRSelectors keep changing over time.

The members of the MPRset of a node are selected in such a manner that every node in the node's two-hop neighborhood has a bidirectional link with the node.

The selection of nodes that constitute the MPRsetsignificantly affects the performance of OLSR because a node calculates routes to all destinations only through the members of its MPRset.


Node 4 selects MPRset <2, 3, 10, 12>
Network Link
Node belonging to MPRset of Node 4
Broadcast packets forwarded by members of MPRset

(a) Flooding the network takes as many transmissions as the number of nodes

(b) Flooding the entire network with six transmissions using MPR scheme

Figure 5.1.Example selection of MPR set in OLSR

Every node periodically broadcasts its MPR Selector set to nodes in its immediate neighborhood. In order to decide on the membership of the nodes in the MPRset, a node periodically sends Hello messages that contain the list of neighbors with which the node has bidirectional links and the list of neighbors whose transmissions were received in the recent past but with whom bidirectional links have not yet been confirmed.

The nodes that receive this Hello packet update their own two-hop topology tables. The selection of multipoint relays is also indicated in theHello packet. A data structure called neighbor table is used to store the list of neighbors, the two-hop neighbors, and the status of neighbor nodes.

The neighbor nodes can be in one of the three possible link status states, that is, uni- directional, bidirectional, and multipoint relay. In order to remove the stale entries from the neighbor table, every entry has an associated timeout value, which, when expired, removes the table entry.

Similarly a sequence number is attached with the MPRset which gets incremented with every new MPRset.

The MPR set need not be optimal, and during initialization of the network it may be same as the neighbor set.

The smaller the number of nodes in the MPRset, the higher the efficiency of protocol compared to link state routing.

Every node periodically originates topology control (TC) packets that contain topology information with which the routing table is updated.

These TC packets contain theMPRSelector set of every node and are flooded throughout the network using the multipoint relaying mechanism.

Every node in the network receives several such TC packets from different nodes, and by using the information contained in the TC packets, the topology table is built.

A TC message may be originated by a node earlier than its regular period if there is a change in the MPR Selector set after the previous transmission and a minimal time has elapsed after that.

An entry in the topology table contains a destination node which is the MPRSelector and a last-hop node to that destination, which is the node that originates the TC packet.

Hence, the routing table maintains routes for all other nodes in the network.

Selection of Multipoint Relay Nodes

Figure 5.1 (b) shows the forwarding of TC packets using the MPRset of node 4. In this example, node 4 selects the nodes 2, 3, 10, and 12 as members of its MPRset. Forwarding by these nodes makes the TCpackets reach all nodes within the transmitting node’s two-hop local topology. The selection of the optimal MPRset is NP-complete. In a heuristic has been proposed for selecting the MPRset.The notations used in this heuristic are as follows: N i (x) refers to the ith hop neighbor set of node x andMPR(x) refers to the MPRset of node x.

```
MPR(x) ← Ø/* Initializing empty MPRset */
MPR(x) ← {Those nodes that belong to N 1 (x) and which are the only neighbors of nodes in N 2 (x)}
While there exists some node in N 2 (x) which is not covered by MPR(x)
    For each node in N 1 (x), which is not in MPR(x), compute the maximum number of nodes that it covers among the uncovered nodes in the set N 2 (x).
    Add to MPR(x) the node belonging to N 1 (x), for which this number is maximum.
```

A node updates its MPRset whenever it detects a new bidirectional link in its neighborhood or in its two-hop topology, or a bidirectional link gets broken in its neighborhood.

Advantages and Disadvantages

OLSR has several advantages that make it a better choice over other table-driven protocols.

It reduces the routing overhead associated with table-driven routing, in addition to reducing the number of broadcasts done.

Hence OLSR has the advantages of low connection setup time and reduced control overhead.

2.Explain the two basic localization mechanisms of WSN in detail?(April 2017) (Nov 2016)

The location information of sensors has to be considered during aggregation of sensed data.

This implies each node should know its location and couple its location information with the data in the messages it sends.

A low-power, inexpensive, and reasonably accurate mechanism is needed for location discovery.

A global positioning system (GPS) is not always feasible because it cannot reach nodes in dense foliage or indoors.

It also consumes high power and makes sensor nodes bulkier. Two basic mechanisms of location discovery are

Indoor Localization

Sensor Network Localization

Indoor Localization

Indoor localization techniques use a fixed infrastructure to estimate the location of sensor nodes.

Fixed beacon nodes are strategically placed in the field of observation, typically indoors, such as within a building.

The randomly distributed sensors receive beacon signals from the beacon nodes and measure the signal strength, angle of arrival, and time difference between the arrivals of different beacon signals.

Using the measurements from multiple beacons, the nodes estimate their location. Some approaches use simple triangulation methods, while others require a priori database creation of signal measurements.

The nodes estimate distances by looking up the database instead of performing computations.

However, storage of the database may not be possible in each node, so only the BS may carry the database.

Sensor Network Localization

In situations where there is no fixed infrastructure available and prior measurements are not possible, some of the sensor nodes themselves act as beacons.

They have their location information, using GPS, and these send periodic beacons to other nodes. In the case of communication using RF signals, the received signal strength indicator (RSSI) can be used to estimate the distance, but this is very sensitive to obstacles and environmental conditions.

Alternatively, the time difference between beacon arrivals from different nodes can be used to estimate location, if RF or ultrasound signals are used for communication. This offers a lower range of estimation than RSSI, but is of greater accuracy.

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

Multi-lateration techniques

Atomic ML: If a node receives three beacons, it can determine its position by a mechanism similar to GPS. This is illustrated in Figure 5.2.

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

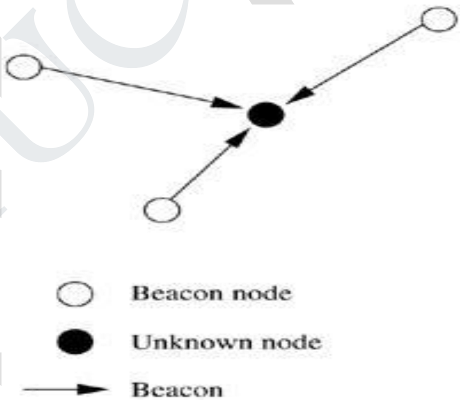


Figure 5.2. Atomic multi-lateration

- Iteratively, all nodes in the network can estimate their location. This is shown in Figure 5.3. The drawback of this multi-hop method is that errors are propagated; hence estimation of location may not be accurate.

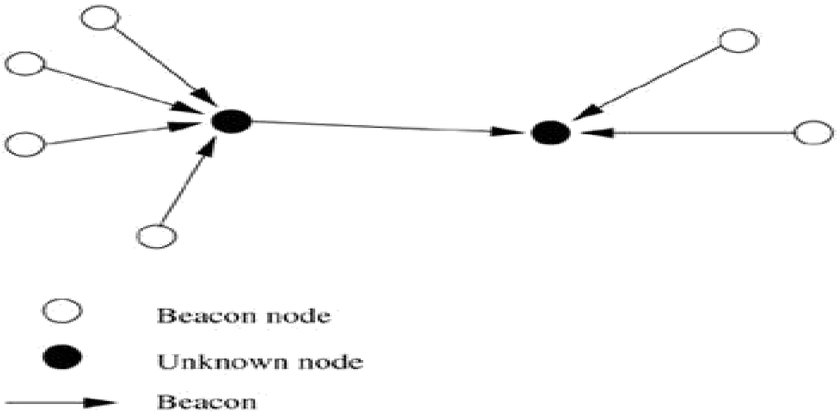


Figure 5.3 Iterative multi-lateration.

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

As shown in Figure 5.4, node A and node B have three neighbors each. Of the six participating nodes, four are beacons, whose positions are known. Hence, by solving a set of simultaneous quadratic equations, the positions of A and B can be determined.

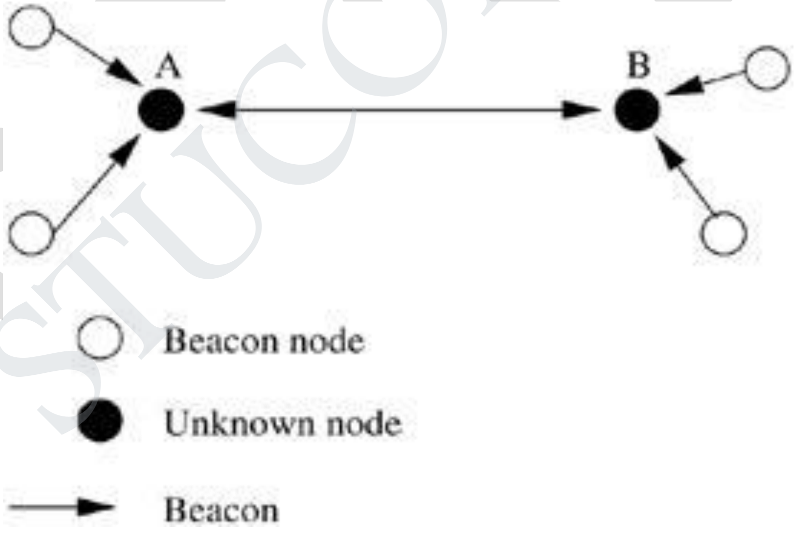


Figure 5.4. Collaborative multi-lateration.

This assumes that beacon nodes have broadcast capability to reach all nodes of the network, and a central controller rotates the beacons with a constant angular velocity ω radians/s. A constant angular separation is maintained between the beacon nodes.

Nodes in the network measure the angles of arrival of beacon signals to estimate their location. The errors in this technique occur due to non- zero beam-width from the beacons.

The beam is not a straight line as theoretically imagined, but it has a finite width. Hence, the measurement of the angle of the beacon signal will be inaccurate.

3. Explain the parameters of QOS in wireless senor networks in detail? (April 2017)(Nov 2016)

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

Coverage

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

- The worst- case coverage defines areas of breach, that is, where coverage is the poorest. This can be used to determine if additional sensors need to be deployed to improve the network.
- The best-case coverage, on the other hand, defines the areas of best coverage. A path along the areas of best coverage is called a maximum support path or maximum exposure path.
- The coverage problem is formally defined as follows: Given a field A with a set of sensors S = {s1 , s2 , ...,sn }, where for each sensor si in S, its location coordinates (xi , yi) are known, based on localization techniques.
- Areas I and F are the initial and final locations of an intruder traversing the field. The problem is to identify P B, the maximal breach path starting in I and ending in F. P B is defined as the locus of point’s p in the region A, where p is in P B if the distance from p to the closest sensor is maximized.

- A mathematic al technique to solve the coverage problem is the Voronoi diagram. It can be proved that the path P B will be composed of line segments that belong to the Voronoi diagram corresponding to the sensor graph.
- In two dimensions, the Voronoi diagram of a set of sites is a partitioning of the plane into a set of convex polygons such that all points inside a polygon are closest to the site enclosed by the polygon, and the polygons have edges equidistant from the nearby sites.
- A Voronoi diagram for a sensor network, and a breach path from I to F, are shown in Figure 5.5.

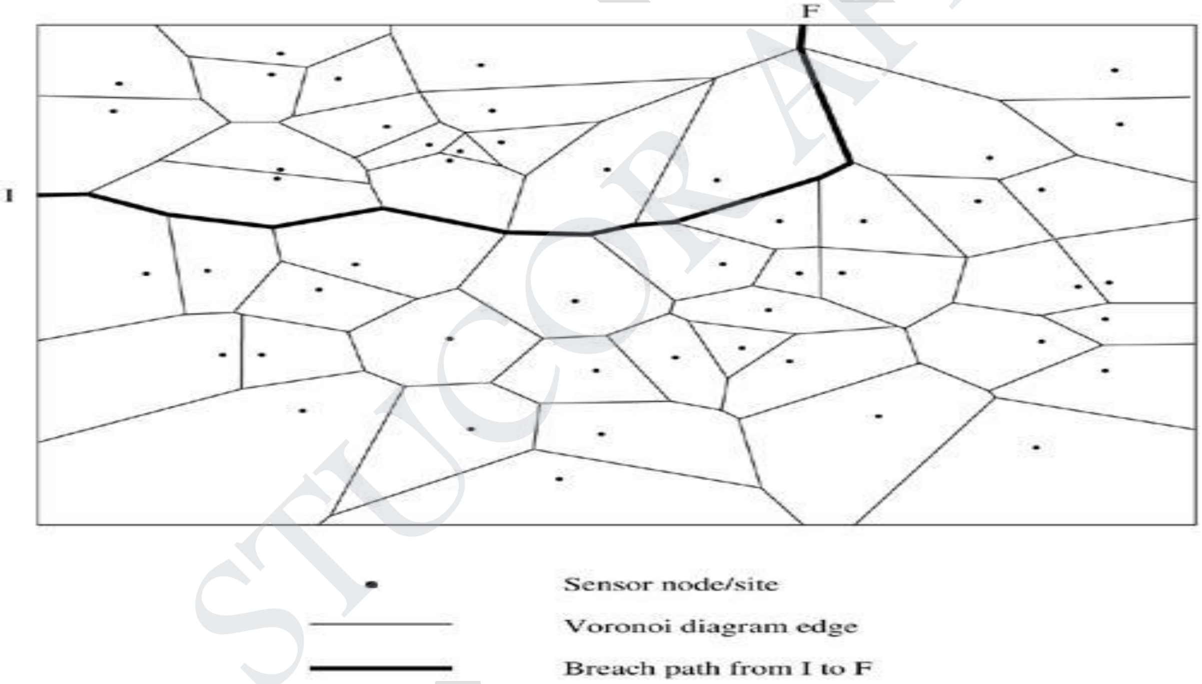


Figure 5.5. Voronoi diagram.

The algorithm to find the breach path P B is:

- Generate the Voronoi diagram, with the set of vertices V and the set of edges E. This is done by drawing the perpendicular bisectors of every line segment joining two sites, and using their points of intersection as the vertices of the convex polygons.

Create a weighted graph with vertices from V and edges from E, such that the weight of each edge in the graph is the minimum distance from all sensors in S. The edge weights represent the distance from the nearest sensor. Smaller edge weights imply better coverage along the edge.

Determine the maximum cost path from I to F, using breadth-first search. The maximum cost implies least coverage. Hence, the required breach path is along this maximum-cost path determined from the Voronoi diagram.
The breach path shows the region of maximum vulnerability in a sensor network,

where the coverage provided by the sensors is the weakest.

A related problem is that of finding the best-case coverage. The problem is formally stated as finding the path which offers the maximum coverage, that is, the maximum support path P S in S, from I to F. The solution is obtained by a mathematical technique called Delaunay triangulation, shown in Figure 5.6

This is obtained from the Voronoi diagram by connecting the sites whose polygons share a common edge. The best path P S will be a set of line segments from the Delaunay triangulation, connecting some of the sensor nodes.

The algorithm is again similar to that used to find the maximum breach path, replacing the Voronoi diagram by the Delaunay triangulation, and defining the edge costs proportional to the line segment lengths. The maximum support path is hence formed by a set of line segments connecting some of the sensor nodes.

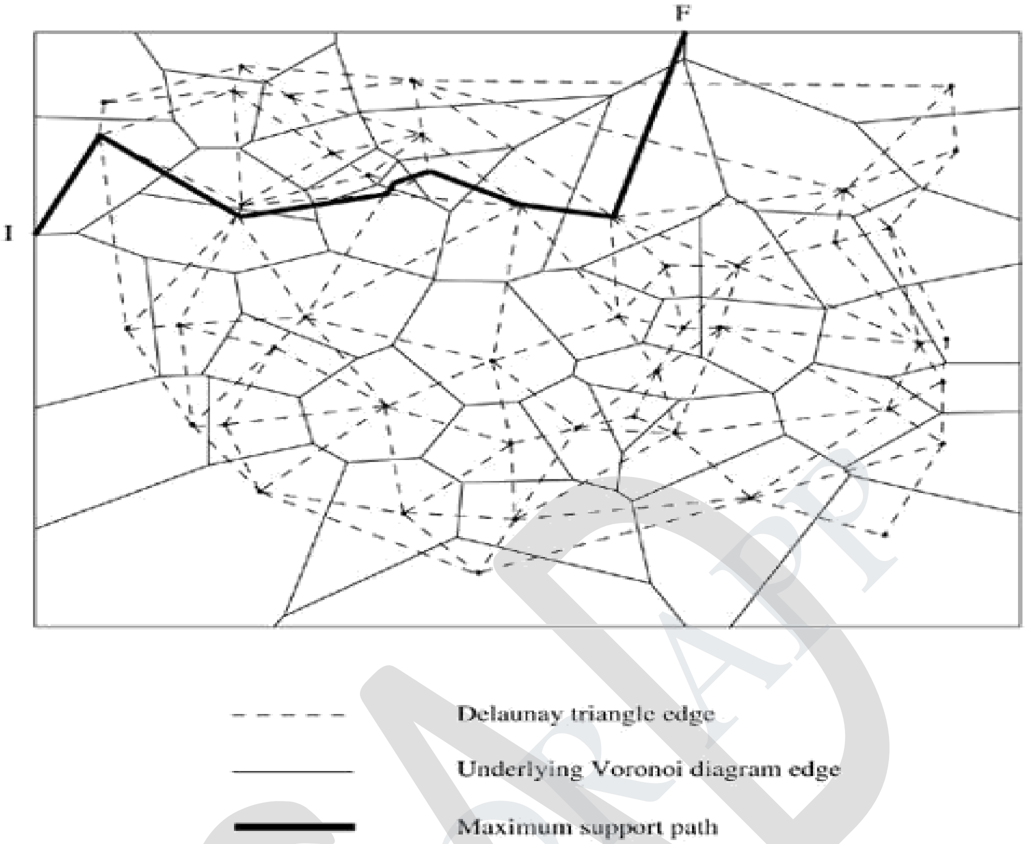


Figure 5.6. Delaunay triangulation.

Exposure

Exposure is defined as the expected ability of observing a target in the sensor field. It is formally defined as the integral of the sensing function on a path from source node P s to destination node P d. The sensing power of a node s at point p is usually modeled as

$$S(s,p) = \frac{\lambda}{[d(s,p)]^k}$$

Where λ and k are constants, and d(s, p) is the distance of p from s. Consider a network with sensors s1, s2... sn . The total intensity at point p, called the all- sensor field intensity, is given by

$$I_A(F,p) = \sum_{i=1}^{n} S(s_i,p)$$

- The closest-sensor field intensity at p is

$$I_C(F,p) = S(s_{min},p)$$

where smin is the closest sensor to p. The exposure during travel of an event along a path p(t) is defined by the exposure function

$$E[p(t), t_1, t_2] = \int_{t_1}^{t_2} I_{AorC}(F, p(t)) \left| \frac{dp(t)}{dt} \right| dt$$

where $\frac{dp(t)}{dt}$ is the elemental arc length, and t1 , t2 are the time instances between which the path is traversed. For conversion from Cartesian coordinates (x(t), y(t)),

$$\frac{dp(t)}{dt} = \sqrt{\left(\frac{dx(t)}{dt}\right)^2 + \left(\frac{dy(t)}{dt}\right)^2}$$

In the simplest case of having one sensor node at (0, 0) in a unit field, the breach path or minimum exposure path (MEP) from (-1, -1) to (1, 1) is shown in Figure 5.7

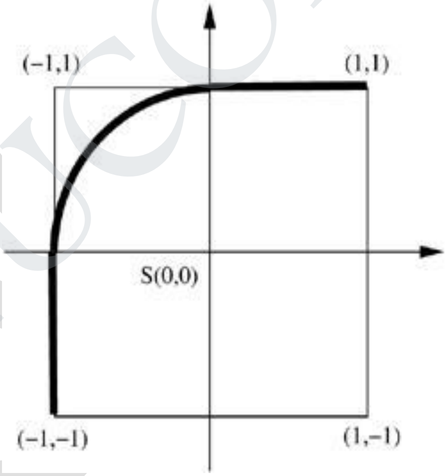


Figure 5.7. Unit field minimum exposure path**.**

It can also be proved that for a single sensor s in a polygonal field, with vertices v1, v2 , ..., vn , the MEP between two vertices vi and vj can be determined as follows. The edge (vi , vi+ 1) is tangent to the inscribed circle at u i . Then the MEP consists of the line segment from vi to u i , part of the inscribed circle from u i to u j , and the line segment from u j to vj . This is shown in Figure 5.8

The exposure problem is still unsolved for two points in the same corner, or for points within the inscribed circle. For the generic exposure problem of determining the MEP for randomly placed sensor nodes in the network, the network is tessellated with grid points. An example is shown in Figure 5.9.

To construct an n × n grid of order m, each side of a square is divided into m equal parts, creating (m + 1) vertices on the edge. Within each square, all vertices are connected to obtain a grid. Higher order grids have greater accuracy.

For each edge in the grid network, the exposure function is used to determine the edge weights, and the MEP is defined as the shortest path, determined by Dijkstra's algorithm.

.

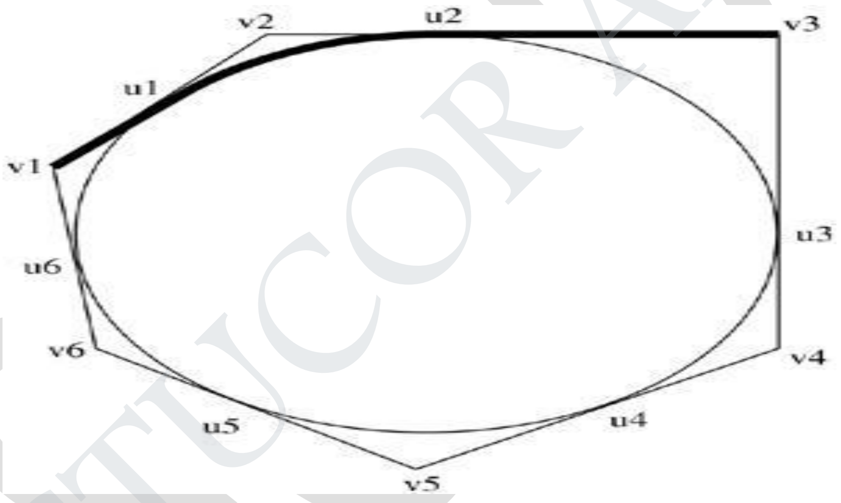


Figure 5.8 Polygon field minimum exposure path

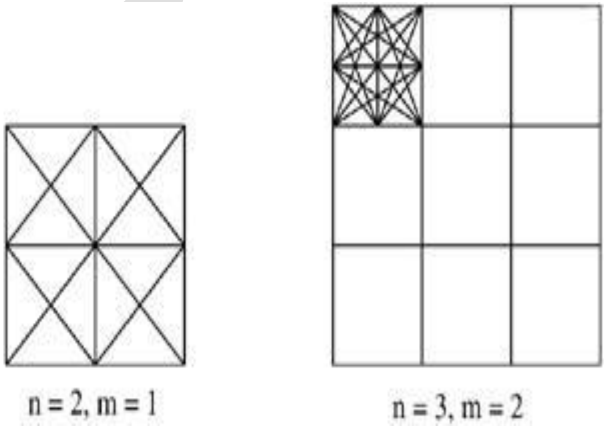


Figure 5.9. Generic minimum exposure path**.**

The mathematical concept of exposure is important for evaluating the target detection capability of a sensor network. Sensors are deployed in a given area to detect events occurring in the field of interest.

The nodes collaborate among themselves (perform data fusion) through the exchange of localized information, and reach a decision about the location and movement of a given event or target.

4. Explain the concept of synchronization and resynchronization in WSN.

Synchronization among nodes is essential to support TDMA schemes on multi-hop wireless networks.

Also, time synchronization is useful for determining the temporal ordering of messages sent from sensors and the proximity of the sensors.

Usually, sensor nodes are dropped into the environment from which data has to be collected, and their exact positions are not fixed before deployment.

Hence, synchronization is the only way by which the nodes can determine their relative positions.

Further, in order to furnish aggregate data to the monitor node, the sensors must evolve a common timescale using their synchronized clocks, to judge the speed of a moving target or phenomenon.
Sensors must be able to recognize duplicate reports of the same event by different nodes and discard them, which means that the node must be able to precisely determine the instant of time at which the event occurred.

There are two major kinds of synchronization algorithms: one which achieves long-lasting global synchronization, that is,lasts throughout the network for its entire lifetime, and one which achieves a short-lived or pulse synchronization where the nodes are synchronized only for an instant.

Synchronization protocols typically involve delay measurements of control packets. The delays experienced during a packet transmission can be split into four major components,

send time,
access time,
propagation time, and
receive time.

The send time is the time spent at the sender to construct the message.

The access time is the time taken by the MAC layer to access the medium, which is appreciable in a contention-based MAC protocol.

The propagation time reflects the time taken by the bits to be physically transmitted through the medium over the distance separating the sender and receiver.

The receive time is the time for processing required in the receiver's network interface to receive the message from the channel and notify the host of its arrival.

If the arrival time is time-stamped at a low layer, overheads of context switches and system calls are avoided, and the arrival time-stamp closely reflects the actual arrival time, with the only non-determinism introduced being due to reception of the first bit.

Many existing synchronization algorithms for sensor networks rely on the time information obtained through the GPS to provide coarse time synchronization. The accuracy of time synchronization provided by GPS depends on the number of satellites observed by the GPS receiver.

In the worst case, with only one observed satellite, GPS offers an accuracy of 1 μs. However, GPS is not a suitable choice for sensor networks because GPS receivers cannot be used inside large buildings and basements, or underwater, or in other satellite-unreachable environments where sensor networks may have to be deployed.

A low-power synchronization scheme called post facto synchronization has been proposed by Elson and Estrin in for wireless sensor networks. In this scheme, the clocks of the nodes are normally unsynchronized.

When an event is observed, a synchronization pulse is broadcast by a beacon node, with respect to which all nodes normalize their time-stamps for the observation of the event. This scheme offers short-lived synchronization, creating only an "instant" of synchronization among the nodes which are within transmission range of the beacon node. The propagation delay of the synchronization pulse is assumed to be the same for all nodes.

Yoram Ofek proposed a global synchronization protocol based on exchange of control signals between neighboring nodes.

A node becomes a leader when elected by a majority of nodes in the network. A distributed election protocol is used which ensures the presence of a unique leader for the network. The leader then periodically sends synchronization messages to its neighbors. These messages are broadcast in turn to all nodes of the network. The time-difference bounds have been theoretically analyzed, and fault- tolerance techniques have been added to account for errors in the synchronization messages.

A long-lasting synchronization protocol is proposed in, which ensures global synchronization of a connected network, or synchronization within connected partitions of a network. Each node in the network maintains its own local clock (real clock) and a virtual clock to keep track of its leader's clock.

A unique leader is elected for each partition in the network, and virtual clocks are updated to match the leader's real clock. The leader election process occurs as follows. On power-up, every node makes an attempt to either locate a leader in its partition or claims to be a leader itself. A node decides, with a small probability, to stake a claim for leadership and announces its claim with a random number sent on the claim packet. This LeaderAnnouncement packet also contains the transmission power used by the node.

A node which receives this claim applies a correction for the propagation delay experienced by the claim packet (calculated based on received power), and updates its virtual clock to the expected value of the leader's real clock at that instant. Time-stamping of claims is performed at the physical layer, to avoid the variable queuing and medium access delays introduced by the MAC layer.

The claim is flooded throughout the partition, bounded by a TTL field. In case two nodes within a partition stake a leadership claim, the one whose LeaderAnnouncement has a higher random number resynchronizes to the leader whose LeaderAnnouncement has the lower random number, and then rebroadcasts theLeaderAnnouncement of the node that generated the lower random number.

In the highly unlikely case of two leaders generating the same random number, node ID is used for resolution. Periodic beaconing ensures that synchronization is maintained throughout the partition, and nodes which join it later also synchronize their clocks.

Resynchronization

Resynchronization is the process of synchronizing different network partitions that are independently synchronized to different clocks to a common clock. In dynamic networks such as sensor networks, frequent changes in topology make resynchronization an important issue. Resynchronization takes place in situations such as the merging of two partitions due to mobility, where all clocks in a partition may need to be updated to match the leader of the other partition, as shown in Figure 5.10

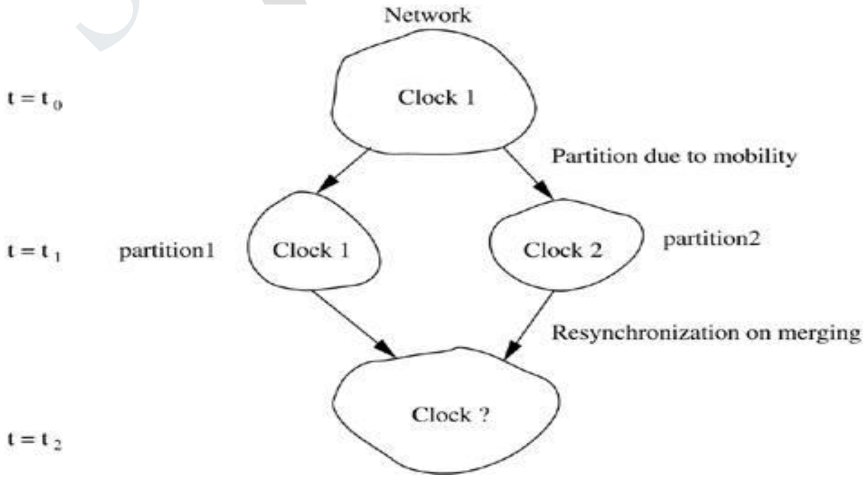


Figure 5.10. Resynchronization

The typical TDMA superframe structure is shown in Figure 5.11(a). Presynch frames define the start and end of a superframe, control frames transmit control information, and data frames are the TDMA time slots allotted to the nodes involved in data transfer.

A positive shift in resynchronization is defined as the transmission of a data packet at an absolute time later than the slot in the current frame structure.

Negative shift is defined as advancing the start of a superframe to transmit the data packets earlier than the start of transmission in the current frame structure.

Resynchronization maintains slot assignment to routes through the node, but shifts the start of the superframe. If the clocks of nodes of partition 1 have to be updated, the superframe can be shifted without loss of data or reconfiguration. However, if the clocks of partition 2 have to be shifted, as shown in Figure 5.11 (b), some data frames are lost due to the negative shift.

If the policy of positive shift is followed uniformly, the nodes must have the capacity to buffer up to an entire superframe's data packets to start afresh with the new timing, as shown in Figure 5.11 (c).

Buffering alleviates the problem of data loss on the link whose end-points are being resynchronized, but neighboring links may suffer collisions when they follow different clocks.

Hence, as the resynchronization proceeds radially from the new leader, there is data loss along the head of the resynchronization wave. This remains for a time period proportional to the time taken for the LeaderAnnouncement packet to propagate from the leader to the farthest node, which in turn depends on the diameter of the network, until the entire network is resynchronized.

Also, different methods for transmitting the synchronization information have been studied. Out-of-band synchronization uses a separate control channel for sending claim and beacon packets.

Collisions are reduced to a great extent for the control packets. However, the available bandwidth for data transmission is reduced, and the cost of the mobile nodes increases because of the need for an additional radio interface.

In in-band synchronization, control information for synchronization shares the same channel with the data packets, as shown in Figure 5.12 (a). This leads to a greater number of collisions, but avoids an additional channel or bandwidth reservation.

Piggy-backing can be used to reduce explicit control packets.

Control information is piggy-backed onto outgoing data packets, as in Figure 5.12

(b). This involves very low overhead with each packet and leads to considerable bandwidth saving.

A control packet carrying the synchronization information is originated only if there are no data packets to be sent from the node.

The scheme can also be applied with piggy- backing on the link-level acknowledgments. In sensor networks, data usually flows from all sensors to the monitor, which is a fixed node with greater computing and power resources than the sensors.

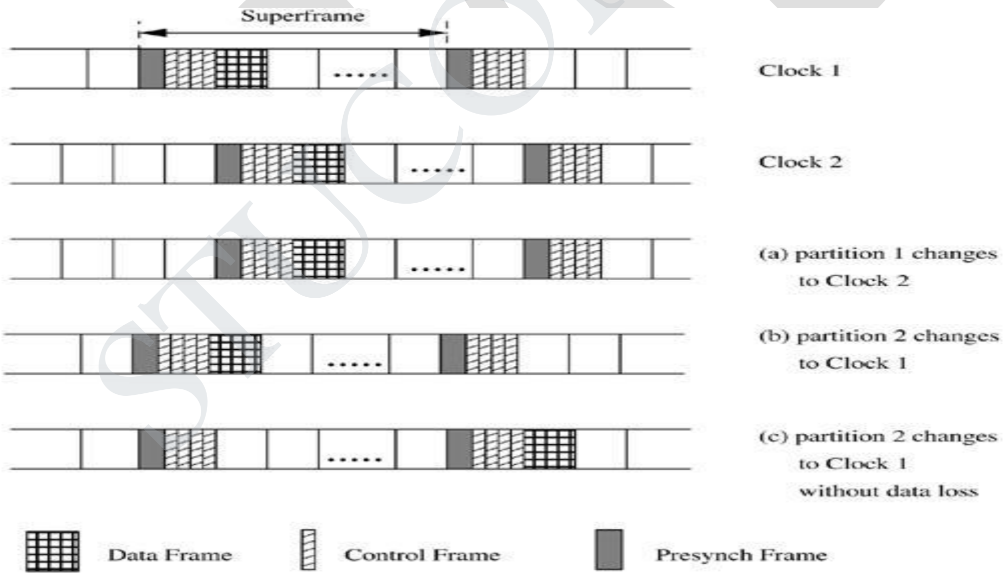
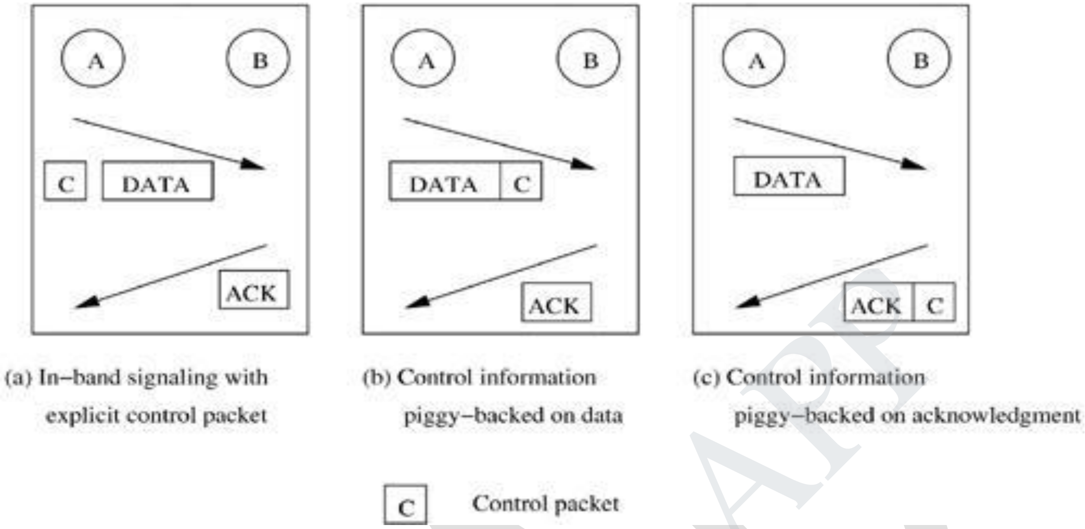

Superframe
Clock 1
Clock 2
(a) partition 1 changes to Clock 2
(b) partition 2 changes to Clock 1
(c) partition 2 changes to Clock 1 without data loss
Data Frame
Control Frame
Presynch Frame

Figure 5.11. Shifting of frames on resynchronization**.**

- If the monitor is forced to be the leader, the synchronization information moves in the reverse direction, that is, along the link-level acknowledgments sent by the nodes for each hop of the data packets, as shown in Figure 5.12 (c). Using simulation studies, this has been observed to be the most efficient mechanism.



(a) In–band signaling with explicit control packet

(b) Control information piggy–backed on data

(c) Control information piggy–backed on acknowledgment

Figure 5.12. In-band signaling.

5. Write short notes on

Energy-Efficient Design

Transport Layer Issues (April/May 2017)

Energy-Efficient Design

The sensor nodes have a very stringent energy constraint. Energy optimization in sensor networks must prolong the life of a single node as well as of the entire network.

Power saving in the micro-controller unit has been analyzed, where the power required by different processors has been compared.

The choice of the processor should be application-specific, such that performance requirements are met with the least power consumption.

Computation can be carried out in a power-aware manner using dynamic power management (DPM).

One of the basic DPM techniques is to shut down several components of the sensor node when no events take place.

The processor has a time-varying computational load; hence the voltage supplied to it can be scaled to meet only the instantaneous processing requirement. This is called dynamic voltage scaling (DVS).

The software used for sensor networks such as the operating system, application software, and network software can also be made energy-aware.

The real-time task scheduler should actively support DVS by predicting the computation and communication loads.

Sensor applications can use a trade-off between energy and accuracy by performing the most significant operations first, so that premature termination of the computation due to energy constraints does not affect the result by a large margin.

The communications subsystem should also perform energy-aware packet forwarding. The use of intelligent radio hardware enables packets to be forwarded directly from the communication subsystem, without processing it through the micro-controller.

Techniques similar to DVS are used for modulation, to transmit data using a simpler modulation scheme, thereby consuming less energy, when the required data transmission rate is lower. This is called modulation scaling.

Besides incorporating energy-efficient algorithms at the node level, there should be a network-wide cooperation among nodes to conserve energy and increase the overall network lifetime.

The computation-communication trade-off determines how much local computation is to be performed at each node and what level of aggregated data should be communicated to neighboring nodes or BSs.

Traffic distribution and topology management algorithms exploit the redundancy in the number of sensor nodes to use alternate routes so that energy consumption all over the network is nearly uniform.

Transport Layer Issues (April/May 2017)

- The major issue in transport layer protocols for sensor networks is the provision of reliable data delivery.

This assumes special significance in the design of general-purpose sensor networks, where groups of nodes may need to be reconfigured or reprogrammed to suit an evolving application.

This may require disseminating a code segment to some nodes, where loss of even a single line of code would render the retasking operation a failure.

A reliable, robust, scalable, and customizable transport protocol, pump slowly fetch quickly (PSFQ), is proposed.

The key concept behind the protocol is that a source node distributes data at a slow rate (pump slowly), and a receiver node which experiences data loss retrieves the missing data from immediate neighbors quickly (fetch quickly).

PSFQ assumes that data loss is due to poor link conditions rather than traffic congestion. It proposes a hop-by-hop error recovery scheme, rather than holding only the destination node responsible for error detection.

The overhead of requiring intermediate nodes to keep track of forwarded data is justified in sensor networks, because most transmissions are intended for groups of sensors, so intermediate nodes are also intended receivers.

PSFQ consists of three functions: message relaying (pump), error recovery (fetch), and selective status reporting (report).

The pump operation disseminates data to all target nodes, performs flow control, and localizes loss by ensuring caching at intermediate nodes.

Hence, the errors on one link are rectified locally without propagating them down the entire path. When a receiver detects gaps in the received sequence numbers, a loss is indicated, and it goes into fetch mode. It requests a retransmission from neighbor nodes.

An attempt is made to aggregate losses, that is, many message losses are batched into a single fetch operation, which is especially appropriate for bursty losses. PSFQ supports a report operation to provide feedback on data delivery status to the source.

The farthest target node initiates its report on the reverse path of data, and all intermediate nodes append their reports to the same.

Hence, PSFQ ensures that data segments are delivered to all intended receivers in a scalable and reliable manner, even in an environment where the radio link quality is poor. It has been observed that the ratio between the fetch and pump rates should be around 5 for maximum effectiveness.

A recent protocol, event-to-sink reliable transport (ESRT), studies a new perspective on reliability in sensor networks.

It defines event-to-sink reliability in place of the traditional end-to-end reliability provided by the transport layer, that is, data about the event is to be carried reliably to the sink, with minimum energy expenditure.

The sink is required to track reliably only the collective report about an event and not individual reports from each sensor. This enables a relaxation in stringent end-to-end reliability for each flow.

The salient features of ESRT are its self-configuring capability, energy awareness, and congestion control. ESRT defines the term observed reliability as the number of packets that are routed from event to sink, and required reliability as the desired number of such packets for the event to be successfully tracked. If the observed reliability of an event falls below the requirement, ESRT increases the reporting frequency.

On the other hand, if the reliability level required has been exceeded, ESRT decreases the reporting frequency in order to conserve energy.

The frequency at which sensors must send their reports is conveyed to them through broadcasts from the sink, after appropriate calculations, so that the required reliability is achieved. Congestion control is achieved by monitoring buffer levels at forwarding sensors.

Reliability in the reverse direction, from sink to sensors, is discussed. The different kinds of reliability required in this direction are listed. On one hand, small queries are sent in a single packet, whereas software that needs to be updated in the sensors may be sent across multiple packets.

Accordingly, reliability should be ensured for single or multiple packets, depending on the content. Further classification is based on the intended set of receivers.

A message may need to be sent to all sensors of the network, or to all within a sub-area (as in a location-based query), or maybe to a subset of sensors which, among themselves, covers a certain area.

In the last case, not all sensors in the area need to receive the message, but only a small subset, the union of whose coverage areas adds up to the required area, needs to reliably receive the message.

One of the ways to ensure any of these forms of reliability is to use some nodes as recovery servers, which retransmit the message to sensors which did not receive it.

Question Paper code: 80273

B.E/B.Tech DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016
Seventh Semester
Computer Science and Engineering
CS 6003- ADHOC AND SENSOR NETWORKS
(Common to Information Technology)
(Regulation 2013)

Time: Three hours Maximum:100

Answer ALL questions

Part A-(10*2=20 marks)

1. What is handoff?
2. Define multicasting.
3. How single- channel sender- initiated contention based MAC protocols for ad hoc wireless networks work?
4. Outline how node scheduling is done in contention based MAC protocols with scheduling mechanisms.
5. How table driven routing protocols for ad hoc network works?
6. List the major functions performed by TCP.
7. Outline the functions performed by a node in a wireless sensor networks.
8. How CSMA based MAC protocol for wireless sensor network work?
9. What is data dissemination in a wireless sensor network?
10. Why wireless sensor networks need localization protocols?

Part B-(5 x 16 = 80 marks)

11. (a) (i) Tabulate the difference between cellular networks and ad hoc wireless networks. (8)
(ii) Explain with an example and diagrammatic illustration reflection, diffraction and scattering. (8)

Or

(b) Outline the design challenges in mobile ad hoc networks and wireless sensor networks. (16)

12. (a) (i) Explain the hidden and exposed terminal problems with an example and diagrammatic illustration. (8)
(ii) How media access protocol for wireless LANs(MACAW) based on multiple access collision avoidance protocol (MACA) works? How MACA avoids the problem of hidden terminals? How MACA avoids the problem of exposed terminals? Give example. (8)

Or

(b) (i) How distributed packet reservation multiple access protocol works? Discuss with an example. (8)
(ii) How MACA protocol with piggy- backed reservation works? Discuss with an example.(8)

13. (a) Illustrate the working of destination sequenced distance vector routing protocol for wireless adhoc network with an example and diagrammatic illustrations. (16)

Or

(b) Present a comparison of TCP solutions for wireless ad hoc networks. (16)

14. (a) What is a wireless sensor network? Explain with diagrammatic illustration wireless sensor network architecture. (16)

Or

(b)How hybrid TDMA/FDMA medium access control protocol for wireless sensor network works? Explain with an example. (16)

15. (a) (i) Outline the issues related to routing in Wireless sensor networks. (8)

(ii) What is range based localization? Explain with an example how triangulation works. (8)

Or

(b) What is quality of Service (QoS)? Discuss QoS in wireless Sensor networks. (16)

Question Paper code: 71656

B.E/B.Tech DEGREE EXAMINATION, APRIL/MAY 2017
Seventh Semester
Computer Science and Engineering
CS 6003- ADHOC AND SENSOR NETWORKS
(Common to Information Technology)
(Regulation 2013)

Time: Three hours Maximum:100

Answer ALL questions
Part A-(10*2=20 marks)

1. Define a wireless sensor network.
2. State the difference between cellular network and Ad hoc wireless network.
3. Define packet dellivery ratio.
4. What is a contention based protocol?
5. How the table driven protocols work in Ad hoc network?
6. What is hybrid routing?
7. List the components of a sensor node.
8. Define data relaying in a wireless sensor network.
9. Outline the need for data dissemination in a wirelesss sensor network.
10. Define quality of service.

PART B – (5 X 16 = 80 marks)

11. (a) (i) Discuss the characteristics of wireless channel. (6)
(ii) Explain the radio propagation mechanisms. (10)

Or

(b) (i) What is multipath propagation? Explain with an example how it affects the signal quality. (6)
(ii) Explain the design issues in Ad Hoc networks. (10)

12. (a) Discuss the issues in designing of MAC protocol for Ad Hoc networks (16)

Or

(b) classify MAC protocols for Ad Hoc networks and present an overview of the same. (16)

13. (a) Discuss any four reactive routing protocols for Ad Hoc wireless sensosr networks. (16)

Or

(b) What is TCP? Discuss with an example TCP over Ad Hoc wireless sensor networks. (16)

14. (a) Discuss the architecture of wireless sensor network with diagtammatic illustration. (16)

(b) Present an overview of MAC protocols for Ad Hoc wireless sensor networks. (16)

15. (a) (i) Appraise the issues related to routing in Ad Hoc wireless sensosr networks. (8)

(ii) Present an overview of Localization in Ad Hoc wireless sensor networks. (8)

(b) (i) Appraise the QoS related measures in Ad Hoc wireless sensosr networks. (8)

(ii) Outline the issues related to the transport layer in Ad Hoc wireless sensor networks. (8)

INDUSTRIAL / PRACTICAL CONNECTIVITY OF THE SUBJECT:

Disaster relief operations:

•Drop sensor nodes from an aircraft over a wildfire

•Each node measures temperature

•Derive a "temperature map"

Biodiversity mapping

•Use sensor nodes to observe wildlife

Intelligent buildings (or bridges)

•Reduce energy wastage by proper humidity, ventilation, air conditioning (HVAC) control

•Needs measurements about room occupancy, temperature, air flow, …

•Monitor mechanical stress after earthquakes.

Facility management

•Intrusion detection into industrial sites

•Control of leakages in chemical plants, …

Machine surveillance and preventive maintenance

•Embed sensing/control functions into places no cable has gone before •E.g., tire pressure monitoring

Precision agriculture

•Bring out fertilizer/pesticides/irrigation only where needed

Medicine and health care

•Post-operative or intensive care

•Long-term surveillance of chronically ill patients or the elderly