QUESTION BANK

Name of the Department : **Electronics and Communication Engineering**

Subject Code & Name : **EC8702 & Ad Hoc and Wireless Sensor Networks**

Year & Semester : **IV & VII**

UNIT I AD HOC NETWORKS – INTRODUCTION AND ROUTING PROTOCOLS

PART-A

1. Define Computer Networks.

A computer network is the interconnection of multiple nodes through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels.

2. List the Advantages of Distributed processing.

Security
Faster problem solving
Security through redundancy

3. What are the Applications of Distributed Systems?

E-mail
Online Ticket Reservation
Banking

4. Define communications. Its types.

Communication medium refers to the physical channel through which data is sent and received. Data is sent in the form of voltage levels which make up the digital signal. A digital signal consists of 0s and 1s. There are basically two types of networks:

Wired network
Wireless network

5. Define Wired Network.

➢ In a wired network, data is transmitted over a physical medium. ➢ There are three types of physical cables used in a wired network.

Twisted Pair
Coaxial Cable
Fiber Optic

Examples: Cable TV, Broadband Telephone Communication.

6. Define Wireless Network.

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

7. List Types of Wireless Ad Hoc Networks.

Mobile ad hoc network (MANET)
Vehicular ad hoc network (VANET)
Smartphone ad hoc network (SPAN)
Wireless mesh network**:**
Army tactical MENT
Wireless sensor network
Disaster rescue ad hoc network

8. What are the Advantages of Ad Hoc Networks.

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

9. What are the Disadvantages of Ad Hoc Networks.

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

10. List out the issues in Ad hoc wireless networks.

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

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

11. List the major issues in MAC.

Distributed Operation
Synchronization
Hidden Terminals Problem
Exposed Terminals Problem
Throughput
Access delay
Fairness
Real-time Traffic support
Resource reservation

12. What is Hidden Terminals Problem?

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

13. Define Exposed Terminals Problem.

The nodes that are in the transmission range of the sender of an on-going session, are prevented from making a transmission. The exposed nodes should be allowed to transmit in a controlled fashion without causing collision to the on-going data transfer.

14. Define throughput.

The MAC protocol employed in ad hoc wireless networks should attempt to maximize the throughput of the system. The important considerations for throughput enhancement are,

Minimizing the occurrence of collisions.
Maximizing channel utilization.
Minimizing control overhead.

15. Define 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.

16. What is 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.

17. List the major challenges faces a routing protocol faces.

Mobility
Bandwidth constraint
Error-prone and shared channel
Location-dependent contention

18. What are the major requirements of a routing protocol in ad hoc wireless network?

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

19. What is Multicasting?

Multicasting 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.

20. What are the major issues in designing multicast routing protocols?

Robustness
Efficiency
Control overhead
Quality of Service
Efficient group management
Scalability
Security

21. What are the major objectives of Transport Layer Protocol?

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

22. Define Quality of Service (QoS).

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

QoS provisioning often requires,

Negotiation between host & the network.
Resource reservation schemes.
Priority scheduling.
Call admission control.

23. Define Self-Organization in ad hoc wireless network.

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)

24. Differentiate Passive attack and Active attack.

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.

25. What are the types of active attacks?

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.

26. Define Denial of service.

The attack affected by making the network resource unavailable for service to other nodes, either by consuming the bandwidth or by overloading the system.

27. What is Resource consumption?

The scarce availability of resources in ad hoc wireless network makes it an easy target for internal attacks, particularly aiming at consuming resources available in the network. The major types of resource consumption attacks are,

Energy depletion
Buffer overflow

28. What is 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.

29. List the Features of energy management.

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

30. What are the classifications of Energy management?

Transmission power management
Battery energy management
Processor power management
Devices power management

31. What is Transmission power management?

The power consumed by the Radio Frequency (RF) module of a mobile node is determined by several factors such as

The state of operation.
The transmission power and
The technology used for the RF circuitry.

32. Define Battery energy management.

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

33. What is Processor power management?

The clock speed and the number of instructions executed per unit time are some of the processor parameters that affect power consumption. The CPU can be put into different power saving modes during low processing load conditions. The CPU power can be completely turned off if the machines is idle for a long time.

34. Define Devices power management.

Intelligent device management can reduce power consumption of a mobile node significantly. This can be done by the operating system (OS) by selectively powering down interface devices that are not used or by putting devices into different power saving modes, depending on their usage.

35. Define 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.

36. List out the Commercial Applications of Ad Hoc Networking.

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

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

37. What is Wireless Sensor Networks?

The Wireless Sensor Networks (WSN) are special category of Adhoc wireless network that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.

38. What are the issues in Designing a Routing Protocol for Ad Hoc Wireless Networks?

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

Mobility of nodes

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

39. List any two Characteristics of an Ideal Routing Protocol for Ad Hoc Wireless Networks.

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.

40. What are the Classifications of Routing Protocols?

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

41. What is Table Driven Routing Protocols?

These protocols are extensions of the wired network routing protocols.
They maintain the global topology information in the form of tables at every node.
Tables are updated frequently in order to maintain consistent and accurate network state information.

42. List some examples of Table Driven Routing Protocols?

Destination Sequenced Distance Vector Routing Protocol (DSDV)
Wireless Routing Protocol (WRP)
Source-Tree Adaptive Routing Protocol (STAR)
Cluster-head Gateway Switch Routing Protocol (CGSR)

43. What is On–Demand Routing protocols?

In table-driven protocols, each node maintain up-to-date routing information to all the nodes in the network where in on-demand protocols a node finds the route to a destination when it desires to send packets to the destination.

PART-B

1. Explain the elements of Ad hoc Wireless Networks in detail.
2. Discuss the issues in Ad hoc wireless networks in detail.
3. Summarize some commercial applications of Ad hoc networking in detail.
4. Explain in detail about the importance of Ad hoc wireless Internet.
5. Discuss in detail about issues in designing a Routing Protocol for Ad Hoc Wireless Networks.
6. Describe the Classification of Routing Protocols in detail.
7. Explain about Table Driven Routing Protocols in detail.
8. Discuss Destination Sequenced Distance Vector in detail.
9. Explain in detail about On–Demand Routing protocols.
10. Explain in detail about Ad hoc On–Demand Distance Vector Routing.

UNIT II SENSOR NETWORKS – INTRODUCTION & ARCHITECTURES

PART-A

1. Define Sensor.

A Sensor is a device that responds and detects some type of input from both the physical or environmental conditions, such as pressure, heat, light, etc.

The output of the sensor is generally an electrical signal that is transmitted to a controller for further processing.

2. What is Wireless Sensor Networks?

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

3. Define sink or base station.

A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically a wireless sensor network contains hundreds of thousands of sensor nodes.

4. List the Components of WSN.

Sensors
Radio Nodes
WLAN Access Point
Evaluation Software

5. What are the Characteristic of Wireless Sensor Network?

Chance to cope with node failures (resilience)
Mobility of nodes
Heterogeneity of nodes
Scalability to large scale of deployment
Capability to withstand harsh environmental conditions
Simplicity of use
Cross layer design

6. List any two Advantages WSN.

Network setups can be carried out without fixed infrastructure.
Suitable for the non-reachable places such as over the sea, or deep forests.

7. What are the Disadvantages of WSN?

WSN is it is not fully secure. Hackers hack the network easily. It is easy for hackers to hack it we couldn't control propagation of waves.
Works in short communication range – consumes a lot of power
Short battery life. Sensor nodes need to be charged at after few times at intervals.
Communication speed is very poor, on the other hand, wired networks have good speed of communication.
More complicated to configure compared to a wired network

8. List the applications of WSN.

Internet of Things (IOT)
Surveillance and Monitoring for security, threat detection
Environmental temperature, humidity, and air pressure
Noise Level of the surrounding
Medical applications like patient monitoring
Agriculture
Landslide Detection

9. List the major issues and challenges that affect the design and performance of a wireless sensor networks.

Energy Efficiency
Quality of Service
Security Issue
Deployment
Node Costs
Limited Bandwidth

10. Define Fault-Tolerance.

In a hostile environment, a sensor node may fail due to physical damage or lack of energy (power). If some nodes fail, the protocols that are working upon must accommodate these changes in the network. As an example, for routing or aggregation protocol, they must find suitable paths or aggregation point in case of these kinds of failures.

11. What are the Enabling Technologies for Wireless Sensor Networks.

Hardware Design
Energy Consumption
Software
Routing protocols
Operating systems

12. What are the numerous applications of WSNs?

Military or Border Surveillance Applications
Environmental Applications
Health Care Applications
Home Intelligence
Industrial Process Control
Agriculture
Structural Monitoring

13. What are the five main components of sensors?

Controller
Memory
Sensors and Actuators
Communication Devices

Power Supply Unit

14. List some of the characteristics Transceiver.

Service to upper layer
Power consumption and energy efficiency
Carrier frequency and multiple channels
State change times and energy

15. What are the various aspects of Power Supply Unit?

- Storing Energy
- Energy Scavenging

16. What are the various Sensor Network Scenarios?

Single-Hop versus Multi-Hop Networks
Multiple Sinks and Sources

17. What are the three types of mobility?

In wireless sensor networks, mobility can appear in three main forms
Node mobility
Sink mobility
Event mobility

18. How the sensors used in Agriculture.

Sensors used in smart farming are known as agriculture sensors. These sensors provide data which assist farmers to monitor and optimize crops by adapting to changes in the environmental conditions. These sensors are installed on weather stations, drones and robots used in the agriculture industry.

19. What is the use of Controller?

A controller to process all the relevant data, capable of executing arbitrary code. The controller is the core of a wireless sensor node. It collects data from the sensors, processes this data, decides when and where to send it, receives data from other sensor nodes, and decides on the actuator's behaviour.

20. What are the three categories of sensors?

Passive, omnidirectional sensors
Passive, narrow-beam sensors
Active sensor

PART-B

1. Explain in detail about the components, characteristics and applications of WSN.
2. Describe in detail about Challenges for Wireless Sensor Networks.
3. Summarize the Enabling Technologies for Wireless Sensor Networks.
4. Explain Wireless Sensor Networks application with examples.
5. Describe in detail about network requires a device for sending and receiving information over a wireless channel.
6. Summarize the Transceiver tasks and characteristics in detail.
7. Explain about Single-Node Architecture in detail with a neat diagram.
8. Describe the Hardware Components in detail.
9. Explain in detail about Energy Consumption of Sensor Nodes.
10. Describe about Network Architecture in detail.
11. Summarize various sensor network scenarios detail.
12. Explain Single-Hop versus Multi-Hop Networks.
13. Explain about different kinds of mobility in detail.
14. Explain about Consideration of Transceiver Design in detail.
15. Explain various Optimization Goals of WSN and Figures of Merit in detail.
16. Explain the most commonly considered aspects of energy efficiency in detail.

UNIT III WSN NETWORKING CONCEPTS AND PROTOCOLS

PART-A

1. Define MAC Protocols.

The MAC sub-layer is a part of the data link layer protocol.
It provides the channel access mechanism to several medium sharing devices.
On a wireless medium, which is shared by multiple devices and is broadcast in nature, when one device transmits, every other device in the transmission range receives its transmission.

2. List out some of the characteristics of MAC Protocols.

Transmission delay
Throughput
Fairness
Scalability
Robustness
Stability

3. What are the goals of MAC Protocols?

Minimize Energy Consumption
Overhearing: unnecessarily receive a packet destined to another node
Idle listening: staying active to receive even if there is no sender
Minimize the active time
Eliminate packet collisions
Minimize control packet overhead
Prevent buffer overflow

4. Define low duty cycle protocol.

The concept of a low duty cycle is represented as a periodic wake-up scheme. A node wakes up periodically to transmit or receive packets from other nodes. Usually after a node wakes up, it listens to the channel for any activity before transmitting or receiving packets.

5. What is sleep / wake-up period?

If no packet is to be transmitted or received, the node returns to the sleep state. A whole cycle consisting of a sleep period and a listening period is called a sleep / wake-up period.

6. Define duty cycle.

Duty cycle is measured as the ratio of the listening period length to the wake-up period length which gives an indicator of how long a node spends in the listening period.

7. Define S-MAC.

The S-MAC (Sensor-MAC) protocol provides mechanisms to avoid idle listening, collisions, and overhearing.

8. What are the listen period phases?

SYNCH Phase
RTS Phase
CTS Phase

9. What is Mediation Device Protocol?

The Mediation Device Protocol is compatible with the peer-to-peer communication mode of the IEEE 802.15.4. It allows each node in a WSN to go into sleep mode periodically and to wake up only for short times to receive packets from neighbour nodes.

10. Define Contention Based Protocols.

A Contention based protocol is a communication protocol for operating wireless telecommunication equipment that allows many users to use the same radio channel without pre coordination.

11. What is Schedule Based Protocols?

The scheduled Based MAC Protocol is a communication protocol, it is used for access nodes in the shared medium is divided with respect to time (Time Division Multiple Access), frequency (Frequency Division Multiple Access) and pseudo codes (Code Division Multiple Access).

12. Define IEEE 802.15.4 MAC.

The Institute of Electrical and Electronics Engineers (IEEE) released the 802.15.4 MAC standard for wireless personal area networks (WPANs) equipped with a duty cycle mechanism where the size of active and inactive parts can be adjustable during the PAN formation.

13. List the Applications of IEEE 802.15.4.

Wireless sensor networks
Home Automation
Home Networking
Connecting Devices to a PC
Home security, etc.

14. Define Flooding.

Flooding is a common technique frequently used for path discovery and information dissemination in wired and wireless ad hoc networks. Flooding uses a reactive approach whereby each node receiving a data or control packet sends the packet to all its neighbours. After transmission, a packet follows all possible paths. Unless the network is disconnected, the packet will eventually reach its destination.

15. List the Design challenges in WSNs.

Energy efficiency
Complexity
Scalability
Delay
Robustness
Data transmission and transmission models
Sensor location

16. What is Unicast routing?

Unicast routing is used to send a message generated by a sensor node to a single destination or sink.

17. What is broadcasting?

Broadcasting is used to send a message from a sensor node to every other node in the network.

18. What is Multicasting?

Multicasting is used to deliver messages from a single source to a set of destinations. Multicasting protocols try to minimize the consumption of network resources. For instance, sending one copy of the data to each destination using unicast is not considered as multicast routing.

19. What is Transport Layer Protocol?

The transport layer provides end-to-end segment transportation, where messages are segmented into a chain of segments at the source and are reassembled back into the original message at the destination nodes.

20. What are the uses of Transport protocols?

Mitigate congestion
Reduce packet loss
Provide fairness in bandwidth allocation
Guarantee end-to-end reliability

21. List some Examples of Traditional transport Layer Protocol.

Transport Control Protocol (TCP)
User Datagram Protocol(UDP)
Sequenced Packet Exchange Protocol (SPX)
NWLink (Microsoft's approach to implementing IPX/SPX)

22. What are the main functions of transport control protocols?

Congestion control
Loss recovery

PART-B

1. Explain the basics of MAC Protocols also explain its characteristics and goals.
2. Describe the specific requirements and design considerations for MAC protocols in wireless sensor networks.
3. Explain the basic idea of low duty cycle protocols in detail. Also explain the wakeup concepts.
4. Explain about S-MAC schemes in detail.
5. Summarize the Network Allocation Vector (NAV) Approach in detail.
6. Explain about The Mediation Device Protocol in detail.
7. Describe about Power Aware Multi-Access with Signaling in detail.
8. Explain in detail about schedule Based Protocols.
9. Describe about Low Energy Adaptive Clustering Hierarchy in detail.
10. Explain the Network Architecture and Types of IEEE 802.15.4 MAC.
11. Explain in detail about Routing Protocols.
12. Explain the design challenges in WSNs in detail.
13. Describe in detail about Energy Efficient Routing.
14. Explain the challenges and issues of Transport Layer Protocol in detail.

UNIT IV SENSOR NETWORK SECURITY

PART-A

1. Why Security needed in Wireless Sensor Networks?

WSN is a special type of network. The sensor networks, based on an inherently broadcast wireless medium, are vulnerable to a variety of attacks. Security is of prime importance in sensor networks because the absence of central authority, random deployment of nodes in the network and nodes assume a large amount of trust among themselves during data aggregation and event detection.

2. List the most important security requirements in WSN.

Data Confidentiality
Authentication
Data Integrity
Data Freshness

Availability
Self-Organization
Time synchronization
Source Localization
Scalability

3. List some issues of designing a new routing protocol for WSN security and privacy.

- Node Mobility
- Coverage Problem
- Shared Broadcast Radio Channel
- Insecure Operational Environment
- Lack of Central Authority

4. What is meant by Network Security Attacks?

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, WSNs have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

For a large-scale sensor network, it is impractical to monitor and protect each individual sensor from physical or logical attack. Attackers may device different types of security attacks to make the WSN system unstable.

5. Differentiate Passive versus Active attacks.

Passive attacks include eavesdropping on or monitoring packets exchanged within a WSN; active attacks involve some modifications of the data steam or the creation of a false stream.

6. What is replaying existing messages?

This operation threatens message freshness. The main purpose of this operation is to confuse or mislead the parties involved in the communication protocol that is not time-aware.

7. What are the Physical Layer Attacks?

Jamming
Radio Interference
Tampering or Destruction

8. Define Tampering or Destruction.

Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node.
One defense to this attack involves tamper-proofing the node's physical package.
Self-Destruction (tamper-proofing packages) – whenever somebody accesses the sensor nodes physically the nodes vaporize their memory contents and this prevents any leakage of information.

9.List the Data Link Layer Attacks.

Continuous Channel Access (Exhaustion)
Collision

Unfairness
Interrogation
Sybil Attack

10. Define Sybil Attack.
In this attack, a single node presents multiple identities to all other nodes in the WSN. This may mislead other nodes, and hence routes believed to be disjoint with respect to node can have the same adversary node.
A countermeasure to Sybil Attack is by using a unique shared symmetric key for each node with the base station.

11. List the various Network Layer Attacks.
Sinkhole Attack
Hello Flood
Node Capture
Selective Forwarding/ Black Hole Attack
Wormhole Attacks
Replayed Routing Information
Misdirection
Homing

12. List the Transport layer Attacks.
Flooding
De-synchronization Attacks

13. List the various Application layer Attacks.
Overwhelm Attack
Path-based DOS Attack
Deluge (reprogram) Attack

14. What is Overwhelm Attack?
An attacker might attempt to overwhelm network nodes with sensor stimuli, causing the network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy.

15. Define Jamming Attack.
Jamming in wireless networks is defined as the disruption of existing wireless communications by decreasing the signal-to-noise ratio at receiver sides through the transmission of interfering wireless signals. Jamming can be done at different levels, from hindering transmission to distorting packets in legitimate communications.

16. What are the Types of Jammers?
Proactive jammer
Constant jammer
Deceptive jammer
Random jammer

Reactive Jammer
Reactive RTS/CTS jammer
Reactive Data/ACK jammer

17. What is Block Hole Attack and it's Counter measures?

Black Hole attack occurs under Dos (Denial of service) attack in the network layer of OSI Model. In this kind of attacks the malicious node forgery other nodes by announcing a shortest false route to the destination then attracts additional traffic and drops continually the packets.

18. Define Cryptography.

Cryptography is one of the most common and reliable means to ensure security. It is the study of the principles, techniques, and algorithms by which information is transformed into a disguised version which no unauthorized person can read, but which can be recovered in its original form by an intended recipient. In cryptography, the original information to be sent from one person to another is called plaintext. This plaintext is converted into ciphertext by the process of encryption, that is, the application of certain algorithms or functions.

19. Define Key.

An authentic receiver can decrypt/decode the ciphertext back into plaintext by the process of decryption. The processes of encryption and decryption are governed by keys, which are small amounts of information used by the cryptographic algorithms. When the key is to be kept secret to ensure the security of the system, it is called a secret key. The secure administration of cryptographic keys is called key management.

20. What are the main approaches of Key Distribution?

Key Pre-distribution
Pairwise Key Generation
Key Transport
Key Agreement

21. What is Security Protocols for Sensor Networks?

Security protocols for sensor networks (SPINS) consists of a suite of security protocols that are optimized for highly resource-constrained sensor networks. SPINS consists of two main modules:

- Sensor Network Encryption Protocol (SNEP)
- Micro-version of Timed Efficient Stream Loss-TolerantAuthentication protocol (μTESLA)

22. List the properties of the SNEP protocol.

Semantic security
Data authentication
Replay protection
Weak freshness
Low communication overhead

PART-B

1. Explain about various Network Security Requirements in detail.
2. Summarize the issues and Challenges in Security Provisioning.
3. Describe about Network Security Attacks in detail.
4. Write notes on Host Based Vs Network Based attacks.
5. Explain the various Layer wise Attacks in Wireless Sensor Networks.
6. Write Short notes on Physical Layer Attacks.
7. Explain Data Link Layer Attacks in detail.
8. Explain about Network Layer Attacks in detail.
9. Write notes on Application layer Attacks.
10. Explain in detail about Jamming Attack and its Countermeasures.
11. Summarize the types of jammer in detail.
12. Explain about Tampering Attack and its Countermeasures.
13. Explain about Block Hole Attack and its Countermeasures.
14. Describe in detail about Flooding Attack and its Countermeasures.
15. Explain Key Distribution and Management in detail.
16. Explain about Symmetric key algorithms and asymmetric key algorithms.
17. Explain various Key Distribution (Management) Approaches in detail.
18. Describe about Secure Routing in Wireless Sensor Networks.
19. Explain the Requirements of a Secure Routing Protocol for Wireless Sensor Networks.
20. Explain in detail about Security Protocols for Sensor Networks.
21. Explain about Reliability Requirements in Sensor Networks.

UNIT V SENSOR NETWORK PLATFORMS AND TOOLS

PART-A

1. What are the categories Sensor Node Hardware?

Augmented general-purpose computers
Dedicated embedded sensor nodes
System on-chip (SoC) nodes

2. What is augmented general-purpose computers?

These nodes typically run off-the-shelf operating systems such as WinCE, Linux, or real-time operating systems and use standard wireless communication protocols such as IEEE 802.11, Bluetooth, Zigbee etc.

3. What is dedicated embedded sensor nodes?

These platforms typically use commercial off-the-shelf (COTS) chip sets with emphasis on small form factor, low power processing and communication, and simple sensor interfaces.

4. What is System on-chip (SoC) nodes?

These platforms try to push the hardware limits by fundamentally rethinking the hardware architecture trade-offs for a sensor node at the chip design level.
The goal is to find new ways of integrating CMOS, MEMS, and RF technologies to build extremely low power and small footprint sensor nodes that still provide certain sensing, computation, and communication capabilities.

Examples of SoC hardware include smart dust the BWRC picoradio node, and the PASTA node.

5. Define Berkeley Motes.

Berkeley Mote platform as it is an open hardware/software, smart-sensing platform with a large user community. The Berkeley Mote platform was developed under the Networked Embedded Systems Technology (NEST) program with the quantitative target of building dependable, real-time, distributed, embedded applications comprising 100 to 100 000 simple computing nodes.

6. Define Node-Level Software Platforms.

A node level platform can be node-centric operating system, which provides hardware and networking abstractions of a sensor node to programmers, or it can be a language platform, which provides a library of components to programmers.

7. List the various design issues of Operating System.

Process management and scheduling
Memory management
Kernel model
Application program interface
Code upgrade and reprogramming
Sensor nodes generally have no external disk

8. What is TinyOS?

The design of TinyOS allows application software to access hardware directly when required. TinyOS is a tiny micro threaded OS that attempts to address two issues:

- How to guarantee concurrent data flows among hardware devices, and

How to provide modularized components with little processing and storage overhead.

9. Define nesC.

nesC is a component-based, event-driven programming language used to build applications for the TinyOS platform. TinyOS is an operating environment designed to run on embedded devices used in distributed wireless sensor networks. The name nesC is an abbreviation of “network embedded systems C”. nesC is an extension of C.

10. Define ContikiOS.

ContikiOS is open source operating system for resource constraint hardware devices with low power and less memory. It was developed by Adam Dunkels in 2002. This OS is fully GUI based system requires only 30 KB ROM and 10 KB RAM. It also provide multitasking feature and have the built in TCP/IP suit.

11. What is Node-Level Simulators?

Node-level design methodologies are usually associated with simulators that simulate the behavior of a sensor network on a per-node basis.

12. Define COOJA.
Cooja simulator is the efficient simulate wireless sensor networks. Cooja is the default simulator of Contiki operating system that helps to simulate the wireless sensor networks in addition it helps to do the performance evolution.

13. Define Contiki.
Contiki is a light weight operating system that is developed mainly for wireless nodes. The motes that are developed by the contiki offers many advantages. Contiki offers a java based simulator called as cooja which is used to simulate the wireless sensors. Cooja simulator is more flexible so that many parts of the simulator is replaceable and extendable. The parts of the simulator like simulated node hardware, plug-ins and radio medium can be replaceable.

14. What are the Characteristics of Cooja?
Scalability
Efficiency
Extensibility
Flexibility

15. What is Contiki Cooja WSN simulator?
Contiki cooja is the best simulator to simulate any wireless sensors with its own property. For example, if we are designing a wireless sensor network that detects the earth quake, the sensor has its own property like lifetime, withstand ability, capacity, etc.

16. Define TOSSIM.
TOSSIM (TinyOS Mote Simulator) is an open-source operating system specially developed for the wireless embedded sensor networks. There are few hardware platforms available for TinyOS, some commercial and some non-commercial.

17. What is the main aim of State-centric programming?
State-centric programming aims at providing design methodologies and frameworks that give meaningful abstractions for these issues, so that system designers can continue to write algorithms on top of an intuitive understanding of where and when the operations are performed.

PART-B

1. Explain in detail about Sensor Node Hardware.
2. Describe in detail about Berkeley Motes.
3. Explain the Challenges of Sensor Network Programming in detail.
4. Write notes on Node-Level Software Platforms.
5. Summarize the various design issues of Operating System.
6. Explain about the Operating System: TinyOS in detail with a neat architecture.
7. Explain in detail about nesC.
8. Describe in detail about ContikiOS.
9. Explain in detail about Node-Level Simulators.

10. Write notes on network simulator execution models.
11. Explain in detail about NS2 and its Extension to Sensor Networks.
12. Explain about COOJA in detail.
13.Explain about TOSSIM (TinyOS Mote Simulator) in detail with a neat architecture.
14. Explain about Programming beyond Individual Nodes in detail.
15. Explain in detail about State Centric Programming.