



ST. ANNE'S COLLEGE OF ENGINEERING AND TECHNOLOGY
(Approved by AICTE, New Delhi. Affiliated to Anna University, Chennai)
ANGUCHETTYPALAYAM, PANRUTI – 607 106.

Unit 2

1. What is sensor network?

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

2. List the three subsystems of the sensor networks.

Sensor subsystem: senses the environment

Processing subsystem: performs local computations on the sensed data

Communication subsystem: responsible for message exchange with neighbouring sensor nodes

3. What are the components of WSN? (Dec 2019)

Communication device

Memory

Controller

Power supply

4. Write short notes on memory devices in WSN.

There is a need for Random Access Memory (RAM) to store intermediate sensor readings, packets from other nodes, and so on. While RAM is fast, its main disadvantage is that it loses its

content if power supply is interrupted. ROM, PROM, EPROM, EEPROM can be used to store the data.

5. Define transceivers in WSN.

The essential task is to convert a bit stream coming from a microcontroller (or a sequence of bytes or frames) and convert them to and from radio waves.

It is usually convenient to use a device that combines these two tasks in a single entity. Such combined devices are called transceivers.

6. Define noise figure.

The noise figure NF of an element is defined as the ratio of the Signal-to-Noise Ratio (SNR) ratio SNRI at the input of the element to the SNR ratio SNRO at the element's output. $NF = SNRI/SNRO$

7. What is Receiver sensitivity?

The receiver sensitivity (given in dBm) specifies the minimum signal power at the receiver needed to achieve a prescribed E_b/N_0 or a prescribed bit/packet error rate.

8. What is meant by Frequency stability?

The frequency stability denotes the degree of variation from nominal center frequencies when environmental conditions of oscillators like temperature or pressure change.

9. Write short note on different operational states of transceiver in WSN.

Many transceivers can distinguish four operational states

Transmit -In the transmit state, the transmit part of the transceiver is active and the antenna radiates energy.

Receive -In the receive state the receive part is active.

Idle

A transceiver that is ready to receive but is not currently receiving anything is said to be in an idle state.

Sleep

In the sleep state, significant parts of the transceiver are switched off.

10. What are wakeup receivers?

To keep this specialized receiver simple, it suffices for it to raise an event to notify other components of an incoming packet; upon such an event, the main receiver can be turned on and perform the actual reception of the packet. Such receiver concepts are called wakeup receivers.

11. List the issues and challenges in designing a sensor networks (April/May 2018)

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.

Sensor networks are infrastructure-less.

Power constraints.

A sensor network should also be capable of adapting to changing connectivity due to the failure of nodes, or new nodes powering up.

12. List the two kinds of sensor network architecture

The two basic kinds of sensor network architecture are

Layered

Clustered.

13. List the advantages of layered architecture.

Each node is involved only in short-distance.

Low-power transmissions to nodes of the neighboring layers.

14. What is 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 clusterheads, and these heads send message to a BS.

Figure: Clustered architecture.

15. What is event & Sink?

The node that generates data is called source and the information to be reported is called an event. A node which interested in an event is called sink.

16. What is QoS in WSN?

QoS can be regarded as a low-level, networking-device-observable attribute – bandwidth, delay,

jitter, packet loss rate – or as a high-level, user-observable, so-called subjective attribute like the

perceived quality of a voice communication or a video transmission.

17. Define Scalability.

The ability to maintain performance characteristics irrespective of the size of the network is referred to as scalability.

8. What is address and data centric in WSN?

In traditional communication networks the transfer of data between two specific devices, each equipped with (at least) one network address – the operation of such networks is thus addresscentric.

In data-centric routing, the sink which is responsible for gathering data and sending to the base station, issues a query for finding target data stored in the other nodes of WSN.

19. List the three main categories of sensors.

Passive, omnidirectional sensors -Thermometer, light sensors, vibration, microphones, humidity, mechanical stress or tension in materials

Passive, narrow-beam sensors - Camera, which can “take measurements” in a given direction, but has to be rotated if need be.

Active sensors - a sonar or radar sensor or some types of seismic sensors.

20. List the types of Mobility.

Node mobility

Event Mobility

Sink Mobility

21. What is Network half-life

When have 50% of the nodes run out of energy and stopped operating in sensor networks.

22. List the applications of sensor networks.

Disaster relief applications

Environment control and biodiversity mapping

Intelligent buildings

Facility management

Machine surveillance and preventive maintenance

Precision agriculture

Medicine and health care

23. How to reduce consumption in sensor node level?

To reduce power consumption of these components comes from chip-level and lower technologies:

Designing low-power chips is the best starting point for an energy-efficient sensor node.

24. What is Dynamic Voltage Scaling(DVS)?

The controller running at lower speed, that is, lower clock rates, consumes less power than at full

speed. This is due to the fact that the supply voltage can be reduced at lower clock rates while still

guaranteeing correct operation. This technique is called Dynamic Voltage Scaling (DVS).

25. What are the types of sink available in WSN?

There are essentially three options for a sink: it could belong to the sensor network as such and be just another sensor/actuator node or it could be an entity outside this network.

Part B

1. Explain the challenges for WSN.
2. Explain the technologies used in WSN.
3. Explain the applications of WSN in detail.
4. Explain about the hardware components of sensor nodes (Nov/Dec 2018) (April/May 2018)
5. Explain the issues and Challenges in designing a sensor networks
6. Explain the architecture of wireless sensor networks. (May 2019)
7. Explain the Operation States With Different Power Consumption. (April/May 2021)
8. Explain the Sensor Network Scenarios with neat diagram. (Nov/Dec 2020)
9. Explain the physical layer and transceiver design considerations in WSNs
10. . Explain the optimization goals and figure of merit (Nov/Dec 2022)

Unit 3

1. List the features of 802.15 standards. (Dec 2019)

Data rates of 250 kbps, 40 kbps, and 20 kbps.

Two addressing modes; 16-bit short and 64-bit IEEE addressing.

Support for critical latency devices, such as joysticks.

CSMA-CA channel access.

Automatic network establishment by the coordinator.

Fully handshaked protocol for transfer reliability.

Power management to ensure low power consumption.
channels in the 2.4GHz ISM band, 10 channels in the 915MHz I and one channel in the 868MHz band.

2. What is Low-rate WPANs?

IEEE 802.15.4 – Low-rate WPANs The reason for having low data rates is the focus of the working group on extremely low power consumption enabling multi-year battery life.

3. List the type of nodes that distinguish on the MAC layer.

The standard distinguishes on the MAC layer two types of nodes:

A Full Function Device (FFD) can operate in three different roles: it can be a PAN coordinator (PAN = Personal Area Network), a simple coordinator or a device.

A Reduced Function Device (RFD) can operate only as a device.

4. Draw the Super frame structure of IEEE 802.15.4.

5. List the challenges of MAC Protocols for Sensor Networks.

No single controlling authority, so global synchronization is difficult

Power efficiency issue

Frequent topology changes due to mobility and failure

6. Write the challenges posed by sensor network MAC protocol

No single controlling authority, so global synchronization is difficult

Power efficiency issue

Frequent topology changes due to mobility and failure

7. List the three 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

8. What are the mechanisms used in MAC layer? (Dec 2019)

The MAC protocol provides a channel of access and an addressing mechanism, so that each available node on the network may communicate with other nodes which are available – either on the same network, or on others.

9. What is hidden terminal problem?

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

10. What is exposed terminal problem?

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

11. Mention the design considerations for MAC protocols in wireless sensor networks.

Balance of requirements

Energy problems on the MAC layer

Collisions

Overhearing

Protocol overhead

Idle listening

12. What is the purpose of Low duty cycle protocols?

It tries to avoid spending time in the idle state and to reduce the communication activities of a sensor node to a minimum.

13. What is duty cycle?

The ratio of the listen period length to the wakeup period length is also called the node's duty cycle.

14. What is SMAC protocol?

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

S-MAC adopts a periodic wakeup scheme, that is, each node alternates between a fixed-length listen period and a fixed-length sleep period according to its schedule.

15. What is the drawback of SMAC protocol?

It is hard to adapt the length of the wakeup period to changing load situations, since this length is essentially fixed, as is the length of the listen period.

16. When mediation device can be used in WSN?

When a node wants to transmit a packet to a neighbor, it has to synchronize with it.

The dynamic synchronization approach achieves this synchronization without requiring the transmitter to be awake permanently to detect the destinations query beacon. To achieve this, a mediation device (MD) is used.

17. What is wakeup radio concept?

The wakeup radio concept strives to achieve this goal by a simple, “powerless” receiver that can trigger a main receiver if necessary. One proposed wakeup MAC protocol assumes the presence of several parallel data channels, separated either

18. What is a contention protocol?

In contention-based protocols, a given transmit opportunity toward a receiver node

Can in principle be taken by any of its neighbours?

If only one neighbour tries its luck, the packet goes through the channel.

19. List the Features of PAMAS.

It uses two channels: a data channel and a control channel.

All the signalling packets (RTS, CTS, busy tones) are transmitted on the control Channel, while the data channel is reserved for data packets.

20. What is scheduling based protocols?

Schedule-based protocols that do not explicitly address idle listening avoidance but do so implicitly, for example, by employing TDMA schemes, which explicitly assign transmission and reception opportunities to nodes and let them sleep at all other times.

21. What is LEACH protocol?

The LEACH protocol (Low-energy Adaptive Clustering Hierarchy) assumes a dense sensor network of homogeneous, energy-constrained nodes, which shall report their data to a sink node. In LEACH, a TDMA based MAC protocol is integrated with clustering and a simple “routing” protocol.

22. List the issues in designing a transport layer protocol for adhoc wireless networks.

Induced Traffic:

Induced throughput unfairness:

Separation of congestion control, reliability and flow control:

Power and Band width constraints:

Interpretation of congestion:

Completely decoupled transport layer:

Dynamic topology:

23. List the design goals of transport layer protocol for adhoc network.

The protocol should maximize the throughput per connection.

It should provide throughput fairness across contending flows.

It should incur minimum connection set up and connection maintenance to overheads.

It should have mechanisms for congestion control and flow control in the network.

It should be able to provide both reliable and unreliable connections as per the requirements of the application layer.

24. Draw the frame structure of LEACH.

25. Draw the frame structure of SMAC.

Part B

1. Explain the design considerations for MAC protocols in wireless sensor networks.
2. Explain about Low duty protocols in WSN with neat diagram.
3. Explain about S-MAC protocol in WSN with neat diagram. (NOV/DEC 2021))
4. Explain the mediation device protocol with neat diagram.
5. Explain the wakeup radio concepts in WSN
6. Explain the contention based protocol PAMAS with neat diagram. (NOV/DEC 2022))
7. Write short notes on advantages and disadvantages of scheduled based protocols.
8. Explain the operation of LEACH protocol.
9. Explain about the MAC protocol in WSN (April/May 2018)(Dec 2019)
10. Explain the Energy efficient unicast routing protocol with an example. 2013 (NOV/DEC 2020))
11. . Explain the issues in designing a transport layer protocol for adhoc wireless networks.(May/ June 2013 (NOV/DEC 2018)) 2013 (NOV/DEC 2022))
12. Explain the significance and design goals of transport layer protocol for adhoc network

Unit4

Part A

1. What are the requirements of network security?

Confidentiality

Integrity

Availability

Non-repudiation

2. List the issues and challenges in security provisioning:-

Shared broadcast radio channel

Insecure operational environment

Lack of central authority

Lack of association

Limited resource availability

Physical vulnerability

3. What are the two types of security attacks?

Active attack

Passive attack

4. List the types of attacks are included in active attacks:-

MAC layer attacks

Network layer attacks

Transport layer attacks

Application layer attacks

Other attacks

5. What is an active and passive attack of network security?

Passive attacks:

Advisory snoops the data exchanged the network without altering it.

Active attacks:

It alters or destroys the data being exchanged in the network thereby disrupting the normal functions of the network.

6. What is difference between wormhole and black hole attacks?

Wormhole attacks Blackhole attacks

An attacker receives packet at one location in the network tunnels them to another location in the network. This tunneling between two colliding attackers is referred as wormhole attacks A malicious node falsely advertises good paths to the destination node during the path finding process (or)in the route update messages.

7. What is resource consumption attack?

A malicious node tries to consume waste away resource of other nodes present in the network.

The resources that are targeted are battery power, bandwidth and computational power which are only limitedly available in adhoc wireless networks.

8. What is the term of session hijacking?

An adversary takes control over a session between two nodes. Since most authentication process are carried out only at the start of the session, once the session between two nodes gets established, the adversary node masquerades as one of the end nodes of the session and hijacks the session.

9. What is repudiation in application layer attacks in network security?

Repudiation refers to the denial (or) attempted denial by a node involved in a communication of having participated in all parts of the communication.

10. What are the various attacks are involved in the routing attacks?

- Routing table overflow
- Routing table poisoning
- Packet replication
- Route cache poisoning
- Rushing attacks

11. What is denial of service attacks?

An adversary attempts to prevent legitimate and authorized users of services offered by the network from processing those services.

12. Some of the DOS attacks are included in the network security.

- Jamming
- SYN flooding
- Distributed DOS attacks.

13. What are the requirements of a secure routing protocol for adhoc wireless networks?

- Detection of malicious nodes
- Guarantee of correct route discovery
- Confidentiality of network topology
- Stability against attacks.

14. What is blackhole attacks and how to overcome it?

A malicious intermediate node could advertise that enhance the shortest path to the destination, thereby redirecting all the packets through itself. This is called blackhole attacks.

15. How to overcome blackhole attacks?

To restrict the intermediate nodes from originating route reply packets. Only the destination node would be permitted to initiate route reply packets. Security is still not completely assured, since the malicious node may lie in the path chosen by the destination node.

16. What is Byzantine attack? (May/June 2012)

A compromised intermediate node could create routing loops and leads to wastage of power and bandwidth.

17. What is Distributed DoS attack?

Several adversaries that are distributed throughout the network collide and prevent legitimate users from accessing the services offered by the network.

18. What is SYN flooding?

An adversary sends a large number of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The victim node builds up a table/data structure for holding information regarding all pending connections.

19. What is jamming? How to overcome it?

The adversary initially keeps monitoring the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender. Frequency hopping spread spectrum(FHSS) and direct sequence spread spectrum (DSSS) are two commonly used techniques that overcome jamming attacks

20. What is Routing table poisoning attack?

The compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes.

21. What is wormhole attack?

An attacker receives packets at one location in the network & tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network. This tunnel between 2 colliding attackers is referred to as a wormhole.

22. What are the different attacks possible over adhoc networks?

23. What is Symmetric and Asymmetric key algorithms?

1. Symmetric key algorithms, which use the same key for encryption & decryption.
2. Asymmetric key algorithms, which use two different keys for encryption & decryption.

24. What is key management?

The secure administration of cryptographic keys[private,public] is called as key management.

25. What are the two major kinds of cryptographic algorithms?

symmetric key algorithms

asymmetric key algorithms.

26. what are various approaches in key management?

Key predistribution

Key transport

Key arbitration

Key agreement

27. What are the requirements of a secure routing protocol for adhoc wireless networks?

Detection of malicious nodes

Guarantee of correct route discovery

Confidentiality of network topology

Stability against attacks.

28. What are the modules in SPINS protocol?

SPINS consists of two main modules:

Sensor Network Encryption Protocol (SNEP)

a micro version of timed, efficient, streaming , loss- tolerant authentication protocol

(μ TESLA).

Part B

1. Explain the requirements of security in Adhoc networks.
2. Explain how the security provisioning in adhoc network differs from that in infrastructure based network.
3. Explain various network and application layer security attacks in detail.
4. Explain in detail about Key Management approaches which includes symmetric and Asymmetric algorithms.
5. What are the different Key Management techniques used for Ad Hoc Networks?
6. Explain the Requirements of A Secure Routing Protocol For Adhoc Wireless Networks or WSN.
7. Explain about secure routing- SPINS

Unit 5

Part A

1. How sensor node hardware is categorized?

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

2. Give some examples of dedicated embedded sensor node.

- Berkeley mote family,
- UCLA Medusa family,
- Ember nodes,
- MIT μ AMP.

3. What are the features of SoC nodes?

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.

4. Give some examples of SoC nodes.

- Smart dust,
- BWRC picoradio node,
- PASTA node.

5. List the types of Berkeley motes.

- WeC

- Rene
- Mica
- Mica2
- Mica2 Dot

6. List the Features of MICA mote

- The MICA motes have a two-CPU design.
- The main microcontroller (MCU), an Atmel ATmega103L, takes care of regular processing.
- The ATmega103L MCU has integrated 512 KB flash memory and 4 KB of data memory.

7 List the power consumption of MICA motes.

FIGURE - Power consumption of MICA motes.

8. What is mote?

A sensor node, also known as a mote , that is capable of performing some processing ,gathering sensory information and communicating with other connected nodes in the network.

9. Draw the mica mote architecture.

10. What are the challenges in Sensor network programming?

When applying such a model to programming networked embedded systems, such as sensor networks, the application programmers need to explicitly deal with message passing, event synchronization, interrupt handing, and sensor reading.

11. What is Cooja simulator?

A system that typically enables the host system to run software or use peripheral devices designed for the guest system: e.g. Cooja enabling your laptop to run the RPL protocol, LIBP and/or other IoT protocols of interest.

12. What are the properties used for changing states by programming nodes?

A distinctive property of physical states, such as location, shape, and motion of objects, is their continuity in space and time. Their sensing and control is typically done through sequential state updates.

13. What is TinyViZ?

TOSSIM has a visualization package called TinyViz, which is a Java application that can connect to TOSSIM simulations.

TinyViz also provides mechanisms to control a running simulation by, e.g., modifying ADC readings, changing channel properties, and injecting packets.

14. What is TOSSIM simulator?

TOSSIM is a dedicated simulator for TinyOS applications running on one or more Berkeley motes.

The key design decisions on building TOSSIM were to make it scalable to a network of potentially thousands of nodes, and to be able to use the actual software code in the simulation.

15. What is the aim of SensorSim?

SensorSim aims at providing an energy model for sensor nodes and communication, so that power properties can be simulated.

SensorSim also supports hybrid simulation, where some real sensor nodes, running real applications, can be executed together with a simulation.

16. List the various commercial simulators used in WSN.

There are several open-source or commercial simulators available such as ns-2, J-Sim (previously known as JavaSim), and GloMoSim/QualNet.

17. List the types of simulation depends on time.

Depending on how the time is advanced in the simulation, there are two types of execution models: cycle-driven (CD) simulation and discrete-event (DE) simulation.

18. List the types of codes used in nesC.

In nesC, code can be classified into two types:

- Asynchronous code (AC): Code that is reachable from at least one interrupt handler.
- Synchronous code (SC): Code that is only reachable from tasks.

19. What is TinyOS?

TinyOS is an embedded, component-based operating system and platform for low-power

wireless devices, such as those used in wireless sensor networks (WSNs), smartdust, ubiquitous computing, personal area networks, building automation

20. List the components used in nesC.

There are two types of components in nesC depending on how they are implemented: modules and configurations.

Modules are implemented by application code (written in a C-like syntax).

Configurations are implemented by connecting interfaces of existing components.

21. List the examples of node level programming tools.

TinyOS and TinyGALS are two representative examples of node-level programming tools.

22. What is timer component in TinyOS?

The Timer has an `init()` method that initializes its internal flag, and it can be enabled and disabled via the `start` and `stop` calls.

FIGURE :The Timer component and its interfaces