UNIT 3

Wireless medium access issues and MAC protocols

- Wireless medium access in the Internet of Things (IoT) refers to the methods and protocols used to manage
- how multiple IoT devices communicate over shared wireless communication channels.
- Efficient medium access control (MAC) is critical in IoT networks to ensure reliable data transmission,
- minimize collisions and interference, and optimize the use of limited wireless spectrum.
- Given the often dense and heterogeneous nature of IoT environments,
- effective MAC mechanisms are essential to maintaining network performance.

When it comes to communication using a wireless medium there is always a concern about the interference due to other present wireless communication technologies. Wireless means communication and message transfer without the use of physical medium i.e., wires.

b) Different Mobile stations (MS) are attached to a transmitter/receiver which communicates via a shared channel by other nodes. In this type of communication, it makes it difficult for the MAC design rather than the wire line networks.

The very important issues which are observed and are explained as following below.

1. Half Duplex operation:
Half-duplex transmission means when the sender and receiver both are capable of sharing data but one at a time. In wireless transmission, it is difficult to receive data when the transmitter is

sending the data because during transmission a large amount or a large fraction of signal energy is leaked while broadcasting. The magnitude of the transferred signal and received signal differs a lot. Due to which collision detection is even not possible by the sender as the intensity of the transferred signal is large than the received one. Hence this causes the problem of collision and the prime focus should be to minimize the collision.

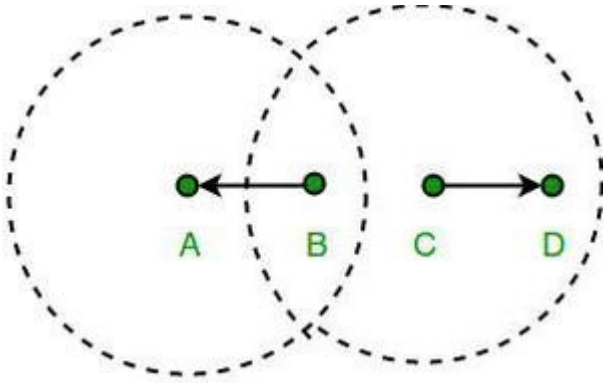
2. Time-varying channel :
Time-varying channels include the three mechanisms for radio signal propagations they are Reflection, Diffraction, and Scattering.

- **Reflection** –
  This occurs when a propagating wave carrying information intrudes on an object that has very large dimensions than the wavelength of the wave.
- **Diffraction** –
  This occurs when the radio path between the transmitter and the receiver is collided by the surface with sharp edges. This is a phenomenon which causes the diffraction of the wave from the targeted position.
- **Scattering** –
  This occurs when the medium through from the wave is traveling consists of some objects which have dimensions smaller than the wavelength of the wave.

3. Exposed Terminal Problem

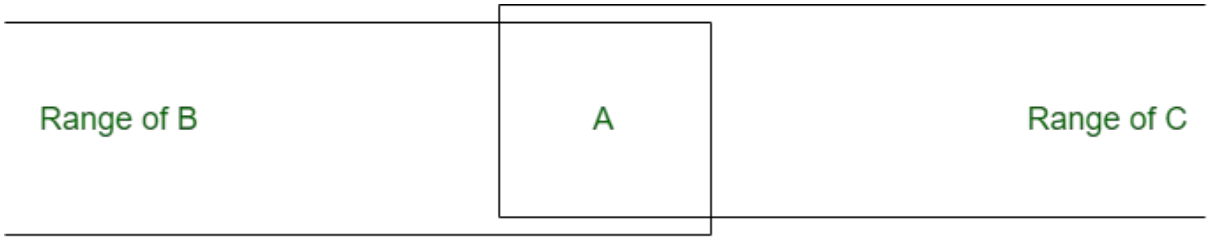
In wireless LAN (local area network) communication, the exposed terminal problem is a frequent difficulty. It happens when a wireless node cannot transfer data because another node that is outside its communication range is sending data to another node that is inside it. Throughput and network performance may suffer as a consequence. This happens when a station can be seen by a

wireless access point but not by other stations that are connected to the access point.



Let's assume there are four stations with the names A, B, C, and D, where B and C are transmitters and A and D are receivers. The stations are set up so that the two emitters B and C can hear each other but the two receivers A and D cannot hear each other over radio waves. Transmission from B to A is happening. As a result, C ceases attempting to transmit to D after mistakenly assuming that the above transmission will cause interference. However, since the communication from C to D is outside of B's range, interference would not have happened. Known as the exposed terminal issue.

4. **Hidden Station Problem (HSP) :**
When two stations hidden from each other i.e., not in range of each other send signals to third station at the same considering third station is free. It causes collision at third station and is known as Hidden Station Problem. It reduces capacity of network due to possibility of collision. Following is diagrammatically representation of Hidden Station Problem (HSP) in wireless LAN.

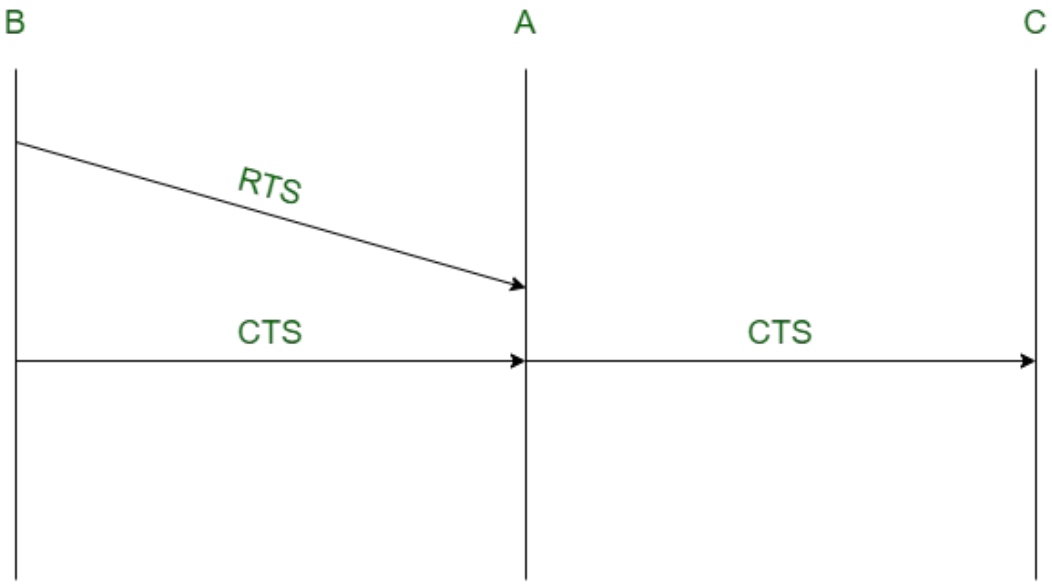


Hidden Station Problem

How HSP is created?
In the above shown diagram, station B and C both covers station A in their own range. Each station B and C can send data to station A separately. Both stations B and C are outside of range of each other. Suppose station B is sending data to station A and in middle of transmission station C also has to send data to station A. Since station B and station C are out of each other range therefore station C thinks that station A is free. Station C send data to station A and collision occurs at station A.

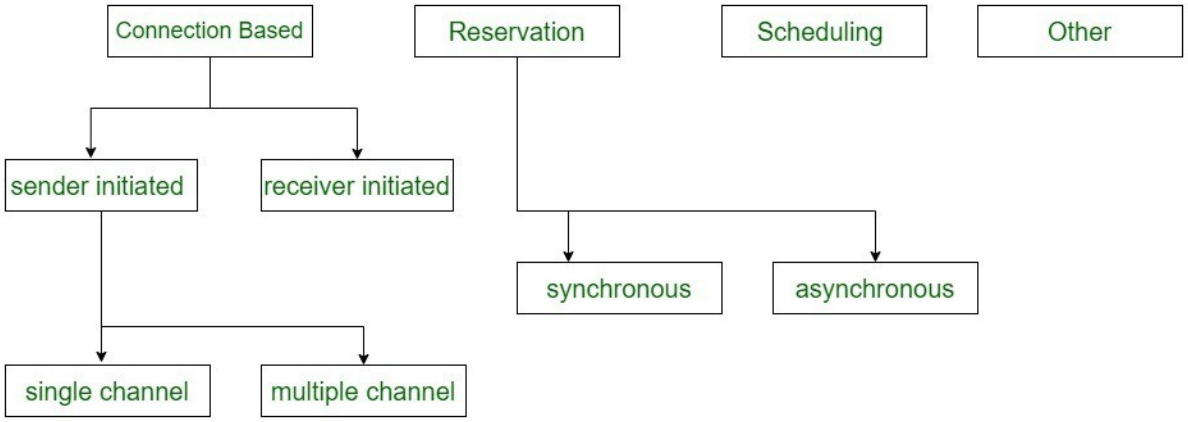
How to prevent HSP?
Hidden Station Problem (HSP) can be prevented by using handshake frames.

In the below shown diagram, RTS message from B reaches A but not C. However, both B and C are within range of A. CTS message containing duration of data transmission from B to A, reaches C. Thus C knows some hidden station is using channel and does not transmit until that duration is over.



Use of handshaking to prevent hidden station problem

Classification of MAC protocols



MAC (Medium Access Control) Layer

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels

The **Media Access Control (MAC) layer** is an important sublayer within the Data Link Layer of the OSI model. It's responsible for controlling how devices on a shared network gain access to and utilize the communication medium. Coordinating access to the shared medium and preventing collisions enables multiple devices to share the network bandwidth effectively.

Contention-Based Protocols Without Reservation/Scheduling

Multiple devices attempt to access the channel simultaneously without coordination. When collisions occur, devices back off and try again. Devices transmit when they have data, relying on techniques like carrier sensing or random backoffs to reduce collisions. It is simple to implement, and adaptive to changing network conditions.

Key Points:

- Bandwidth is not reserved.
- No guarantees.

- Sender-initiated protocols: The transmission of packets are initiated by the sender node.
- Single-channel sender initiated
- Multiple-channel sender initiated protocols.
- Receiver-initiated protocols: The connection is initiated by the receiver node.

2. Contention-Based Protocols With Reservation Mechanisms

A central controller periodically polls devices to grant them exclusive access to the channel, ensuring each one of them gets a turn. A master or base station queries each device in turn and only the polled device is allowed to transmit.

Key Points:

- Bandwidth is reserved for transmission.
- Guarantees can be given.
- Synchronous protocols: In synchronous transmission, data is sent in continuous streams or blocks without start/stop bits for each character. Sender and receiver must be synchronized with a common clock signal. It is more complex to implement compared to asynchronous transmission.
- Asynchronous protocols: In asynchronous transmission, data is sent character-by-character, with start and stop bits added to each character for synchronization. Easier and less expensive to implement. It is less efficient due to the overhead of start/stop bits. Relative time information is used to achieve effecting reservations.

3. Contention-Based Protocols with Scheduling Mechanisms

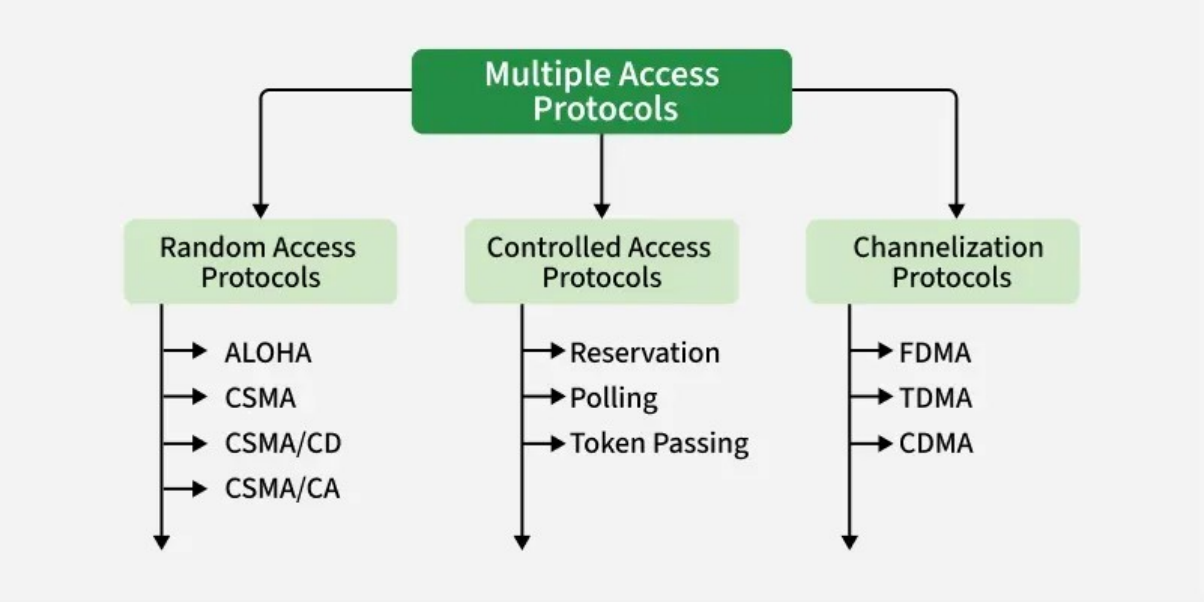
The network allocates specific time/frequency/code resources to each device, so transmissions do not overlap. Each station is assigned a unique time slot, frequency band, or spreading code, ensuring non-interfering transmissions. It provides deterministic access, predictable QoS, and efficient utilization under steady traffic conditions.

- Polling schemes in Bluetooth piconets (master polls slaves), industrial networks using a central controller.
- Ideal for networks needing strict timing guarantees, such as industrial control systems or sensor networks requiring reliable data collection.
- Cellular networks, satellite communications, and environments where guaranteed bandwidth and predictable latency are critical.

4. Other Hybrid Protocols

Combine features of contention-based and scheduled approaches (or other methods) to balance flexibility, efficiency, and reliability. The part of the bandwidth or time is allocated deterministically (scheduled slots), while the remainder is accessed using contention or polling. It is adaptable to varying traffic conditions, can provide QoS guarantees and handle heavy traffic efficiently.

Multiple access protocols can be subdivided further as



1. Random Access Protocol

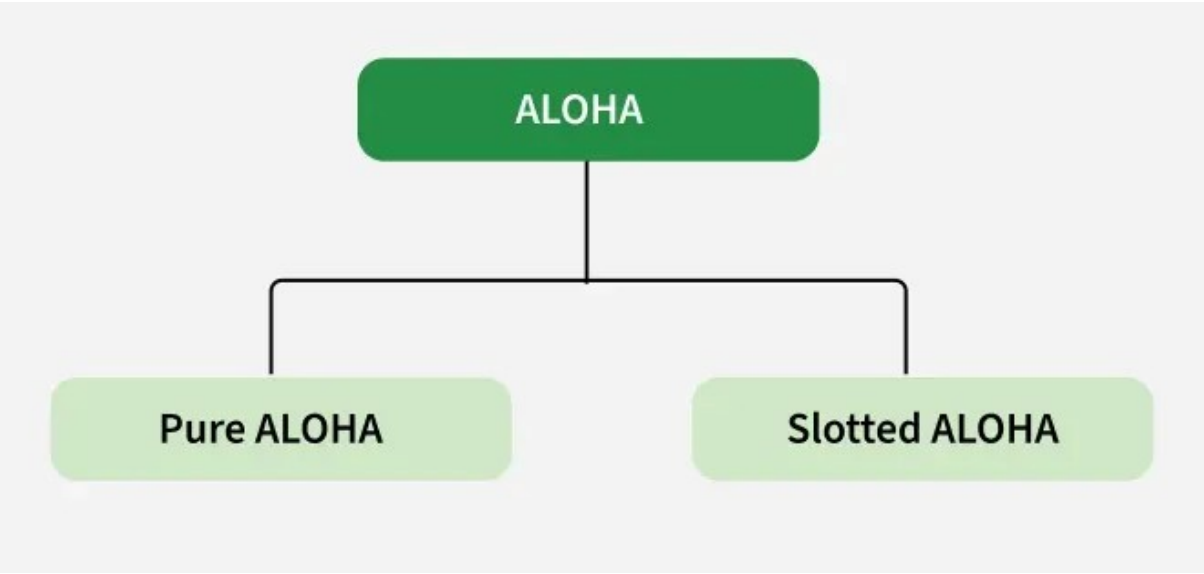
In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

- There is no fixed time for sending data
- There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

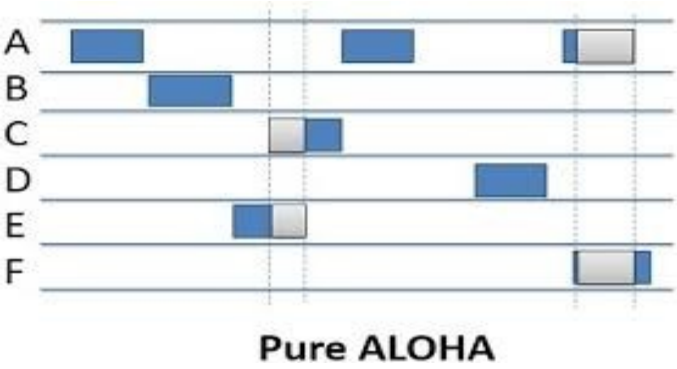
ALOHA

It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.



Pure ALOHA

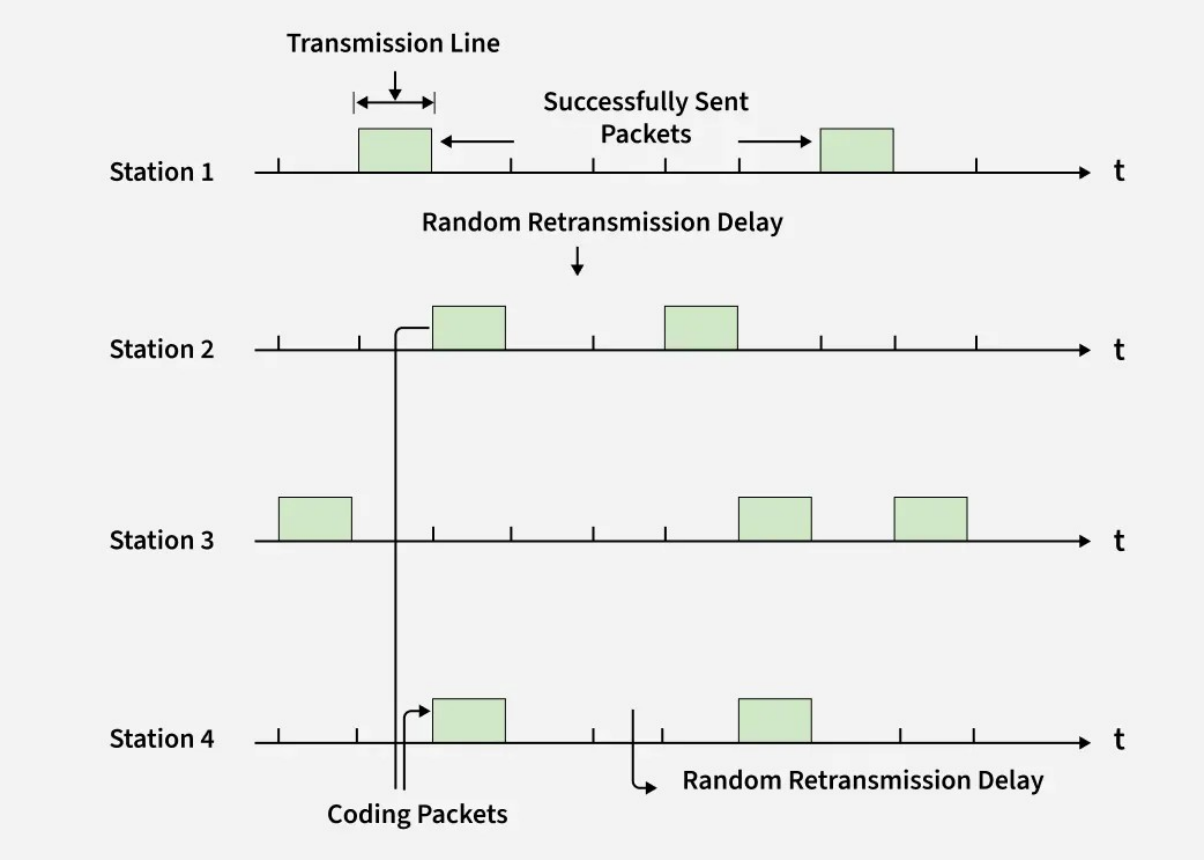
When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.



Pure ALOHA

Slotted ALOHA

It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.



CSMA

Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA/CD

Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected. For more details refer – Efficiency of CSMA/CD.

CSMA/CA

Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA Avoids Collision

- **Interframe Space:** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
- **Contention Window:** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
- **Acknowledgement:** The sender re-transmits the data if acknowledgement is not received before time-out.

What is the Controlled Access?

In controlled access, the stations seek data from one another to find which station has the right to send. It allows only one node to send at a time, to avoid the collision of messages on a shared medium. The three controlled-access methods are:

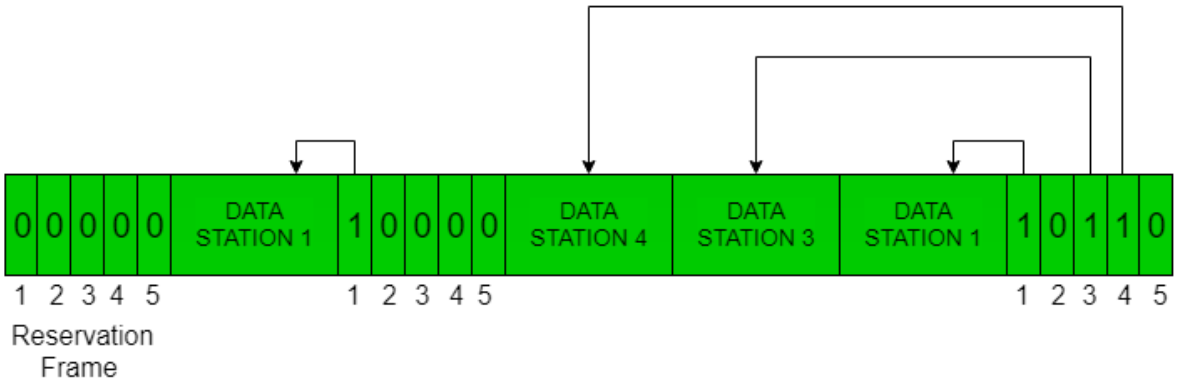
- Reservation

- Polling
- Token Passing

I. Reservation

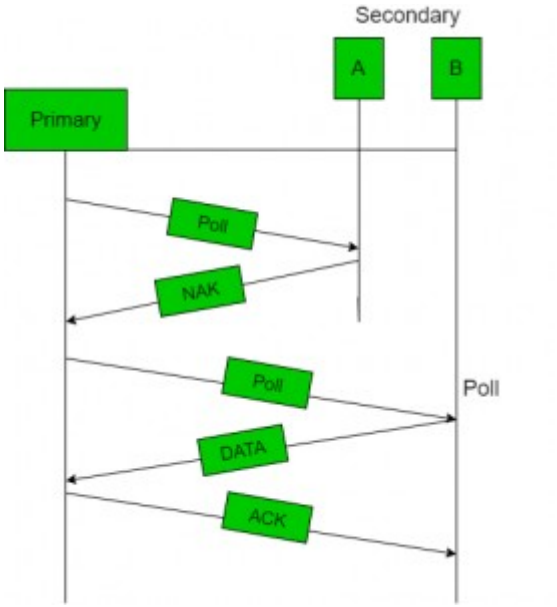
- In the reservation method, a station needs to make a reservation before sending data.
- The timeline has two kinds of periods:
    - Reservation interval of fixed time length
    - Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.

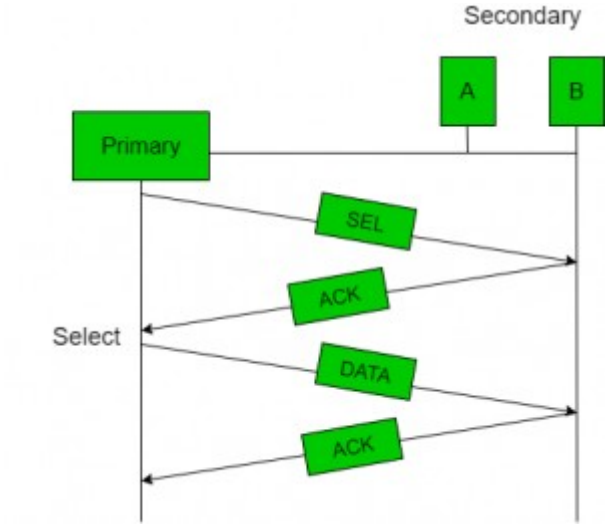
The following figure shows a situation with five stations and a five-slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.



II. Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.
- Although all nodes receive the message the addressed one responds to it and sends data if any. If there is no data, usually a “poll reject”(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.



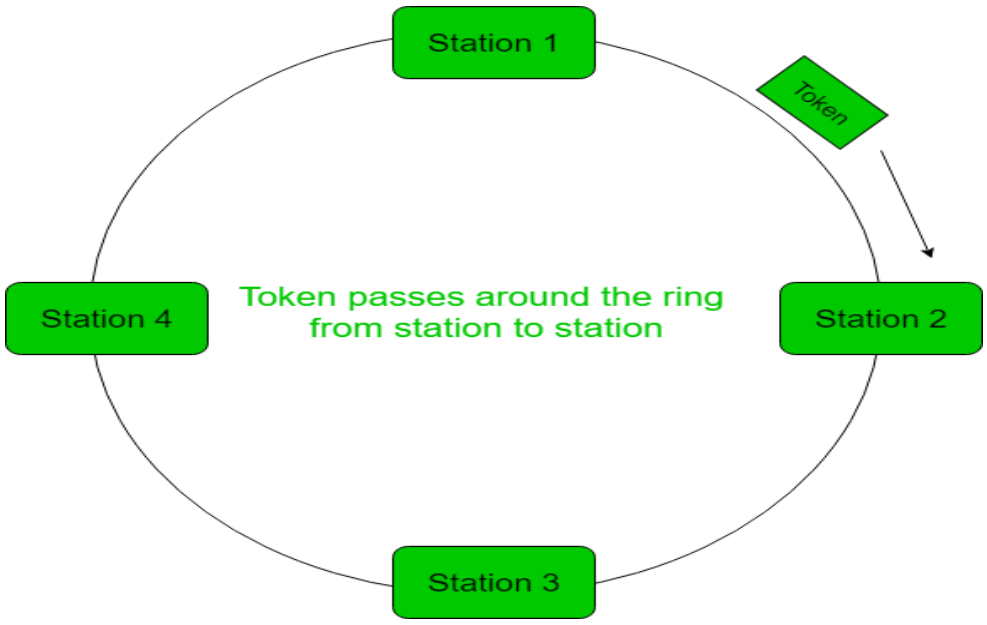


III. Token Passing

- In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each

station uses the bus to send the token to the next station in some predefined order.

- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbours and the other N – 1 stations to send a frame, if they have one.
- There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.



3. Channelization

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA)** – The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA)** – In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.

WIRELESS SENSOR NETWORK (WSN)

a) 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.

b) Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.

Base Station in a WSN System is connected through the Internet to share data.

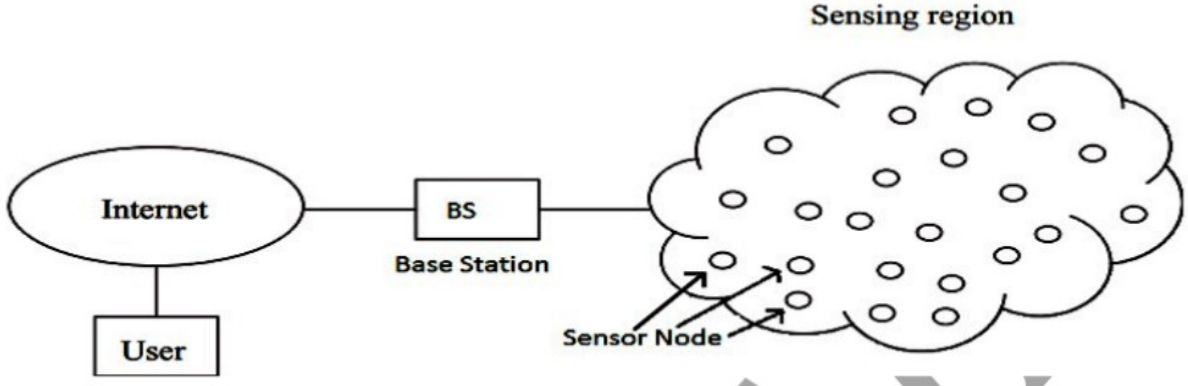


Fig. 3.1 Base Station in a WSN System

COMPONENTS OF WSN

1. **SENSORS**

   Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.

2. **RADIO NODES**

   It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.

3. **WLAN ACCESS POINT**

   It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.

4. **EVALUATION SOFTWARE**

   The data received by the WLAN Access Point is processed by software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

WSN can be used for processing, analysis, storage, and mining of the data.

APPLICATIONS OF WSN

1. Internet of Things (IoT)
2. Surveillance and Monitoring for security, threat detection
3. Environmental temperature, humidity, and air pressure
4. Noise Level of the surrounding
5. Medical applications like patient monitoring
6. Agriculture
7. Landslide Detection

A MODERN WIRELESS SENSOR NETWORK (WSN) CHALLENGES

a) **Limited power and energy**

WSNs are typically composed of battery-powered sensors that have limited energy resources. This makes it challenging to ensure that the network can function for long periods of time without the need for frequent battery replacements.

b) **Limited processing and storage capabilities**

Sensor nodes in a WSN are typically small and have limited processing and storage capabilities. This makes it difficult to perform complex tasks or store large amounts of data.

c) **Heterogeneity**

WSNs often consist of a variety of different sensor types and nodes with different capabilities. This makes it challenging to ensure that the network can function effectively and efficiently.

d) **Security**

WSNs are vulnerable to various types of attacks, such as eavesdropping, jamming, and spoofing. Ensuring the security of the network and the data it collects is a major challenge.

e) **Scalability**

WSNs often need to be able to support a large number of sensor nodes and handle large amounts of data. Ensuring that the network can scale to meet these demands is a significant challenge.

f) **Interference**

WSNs are often deployed in environments where there is a lot of interference from other wireless devices. This can make it difficult to ensure reliable communication between sensor nodes.

g) **Reliability**

WSNs are often used in critical applications, such as monitoring the environment or controlling industrial processes. Ensuring that the network is reliable and able to function correctly in all conditions is a major challenge.

ADVANTAGES OF WIRELESS SENSOR NETWORKS (WSN)

a) **Low cost:** WSNs consist of small, low-cost sensors that are easy to deploy, making them a cost-effective solution for many applications.

b) **Wireless communication:** WSNs eliminate the need for wired connections, which can be costly and difficult to install. Wireless communication also enables flexible deployment and reconfiguration of the network.

c) **Energy efficiency:** WSNs use low-power devices and protocols to conserve energy, enabling long-term operation without the need for frequent battery replacements.

d) **Scalability:** WSNs can be scaled up or down easily by adding or removing sensors, making them suitable for a range of applications and **environments.**

e) **Real-time monitoring:** WSNs enable real-time monitoring of physical phenomena in the environment, providing timely information for decision making and control.

DISADVANTAGES OF WIRELESS SENSOR NETWORKS (WSN):

a) **Limited range:** The range of wireless communication in WSNs is limited, which can be a challenge for large-scale deployments or in environments with obstacles that obstruct radio signals.
b) **Limited processing power:** WSNs use low-power devices, which may have limited processing power and memory, making it difficult to perform complex computations or support advanced applications.
c) **Data security:** WSNs are vulnerable to security threats, such as eavesdropping, tampering, and denial of service attacks, which can compromise the confidentiality, integrity, and availability of data.
d) **Interference:** Wireless communication in WSNs can be susceptible to interference from other wireless devices or radio signals, which can degrade the quality of data transmission.
e) **Deployment challenges:** Deploying WSNs can be challenging due to the need for proper sensor placement, power management, and network configuration, which can require significant time and resources.

Survey routing protocols

The routing protocol is a process to select suitable path for the data to travel from source to destination. The process encounters several difficulties while selecting the route, which depends upon, type of network, channel characteristics and the performance metrics.

The data sensed by the sensor nodes in a wireless sensor network (WSN) is typically forwarded to the base station that connects the sensor network with the other networks (may be internet) where the data is collected, analyzed and some action is taken accordingly.

Routing challenges in WSNs

The design task of routing protocols for WSN is quite challenging because of multiple characteristics, which differentiate them, from wireless infrastructure-less networks. Several types of routing challenges involved in wireless sensor networks. Some of important challenges are mentioned below:

- It is almost difficult to allocate a universal identifiers scheme for a big quantity of sensor nodes. So, wireless sensor motes are not proficient of using classical IP-based protocols.
- The flow of detected data is compulsory from a number of sources to a specific base station.
- The created data traffic has significant redundancy in most of cases. Because many sensing nodes can generate same data while sensing. So, it

is essential to exploit such redundancy by the routing protocols and utilize the available bandwidth and energy as efficiently as possible.

Classification of routing protocols

A classification tree is shown below: The routing protocol for adhoc 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 pathfinding 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

Survey routing protocols

Hierarchical Routing Protocols

- **Description**: In hierarchical routing, nodes are organized into groups, often with a hierarchy of nodes that handle different tasks. Some nodes, such as gateways or cluster heads, perform more complex routing tasks, while others act as simple sensors or data producers.
- Divides the network into clusters or hierarchies to facilitate efficient data aggregation and routing.
- **Examples**:
    - **LEACH (Low Energy Adaptive Clustering Hierarchy)**: A widely used protocol where nodes are divided into clusters. Cluster heads aggregate data from nodes in their cluster and communicate with the sink or base station.

Geographical Routing Protocols

- **Description**: These protocols use the physical location of nodes (often provided by GPS) to make routing decisions, reducing overhead caused by maintaining a global network topology.
- **Examples**:
    - **Greedy Routing**: Nodes forward data packets to the neighbor closest to the destination based on geographical position.

Dynamic Routing:

Adapts routing paths based on real-time network conditions, such as traffic load or topology changes.

- **Examples:** Protocols that dynamically adjust routes to avoid congested or unreliable links.

Flat Routing Protocols

- **Description**: In flat routing, all nodes are treated equally, and each node may participate in routing decisions.
- **Examples**:
    - **Flooding**: A simple technique where each node broadcasts the packet to all of its neighbors. However, this can cause redundancy and network congestion.

Other Notable Protocols:

- **AODV (Ad-hoc On-Demand Distance Vector):** A reactive routing protocol used in mobile ad-hoc networks.
- **DSR (Dynamic Source Routing):** Another reactive routing protocol that uses source routing to find paths in mobile ad-hoc networks.
- **EPR (Energy-Aware Peering Routing):** Designed to reduce network traffic and energy consumption in wireless body sensor networks.

Sensor deployment & Node discovery

SENSOR DEPLOYMENT IN WSN : ⇒

In WSN, the nodes are deployed in different ways based on their applications. The deployment methods are nearly based applications of the wireless sensor networks. The two main classification of the deployment methods in the wireless sensor networks are:

1. Deterministic-based deployment
2. Random deployment.

In deterministic-based deployment method where the application status of the environment known, the sensor node can be fixed at the selected area of the application and the operation status can be fixed in the selection area of WSN.

In random deployment method, the full coverage of particular environment is difficult. The random deployment is also known as the economical deployment. In order to achieve the full coverage of the selected environment by the random deployment method, numerous amounts of the nodes should be deployed in the sensor network.

Random Deployment: ⇒

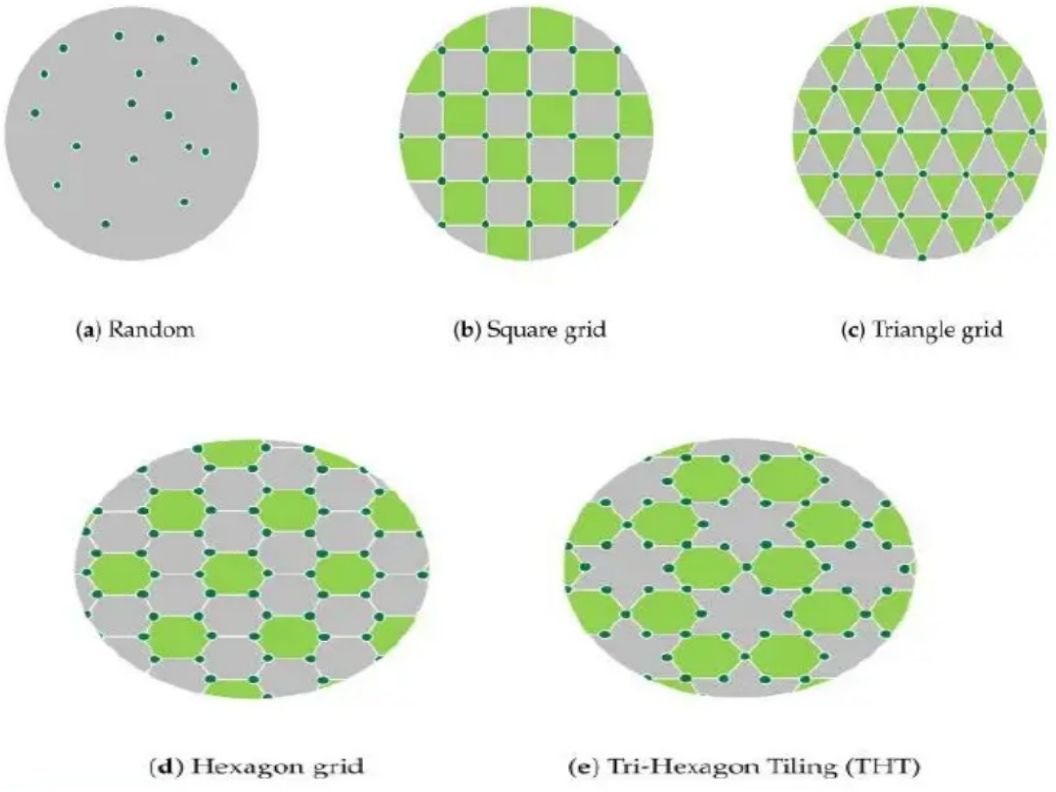
In random deployment, sensors are randomly scattered over the region of interest to gather the target information. Figure 2a shows an example of random placement. It is suitable for regions where human existence is difficult (e.g., disaster areas, battlefields, air pollution, and forest fires). Random sensor deployment is preferred in many WSN applications due to the simplicity of the sensor distribution. As a drawback, however, this method leads to uneven connectivity with critical sensors, which results in a network which is non-robust to sensor failure.

Deterministic Deployment: ⇒

In deterministic deployment, sensors are placed on the region of interest based on a certain geometrical structure. Examples of this type of deployment are square, triangle, and hexagon grids, and tri-hexagon tiling (THT), as shown in Figure 2 b–e, respectively.

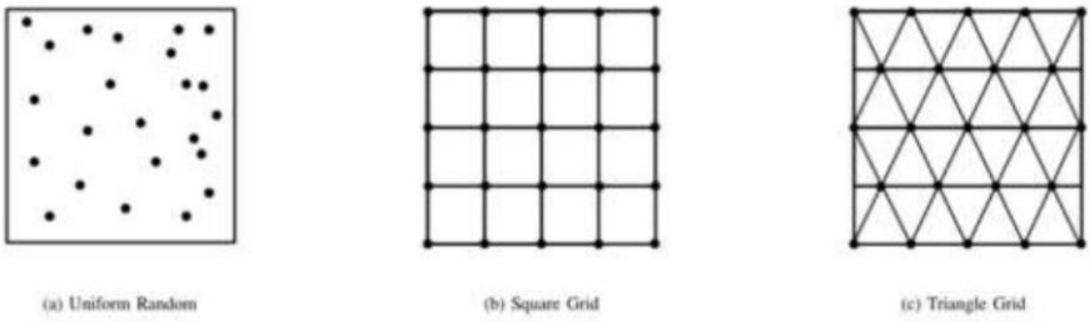
A theoretical analysis in proved that a hexagonal structure can provide a high coverage area with low energy consumption using a minimum number of sensors. Tri-hexagon tiling deployment was proposed to combine the advantages of the triangle and hexagon deployment methods. In terms of energy consumption, the THT deployment outperforms the square and hexagon deployments

Figure 2:

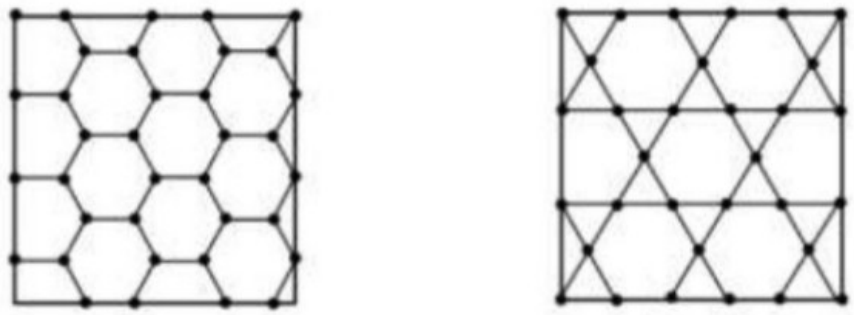


Sensor Deployment & Node Discovery

Five static sensor deployment strategies are introduced. The deployment strategies are one uniform random deployment and four regular deployments: square grid, triangle grid, hexagon grid, and THT. These strategies are shown in Figure 2.2. A square field is considered in this work.



(a) Uniform Random (b) Square Grid (c) Triangle Grid



(d) Hexagon Grid (e) Tri-Hexagon Tiling (THT)

- Uniform Random Deployment

- Regular Deployment
  1. Square Grid
  2. Triangle Grid
  3. Hexagon Grid
  4. Tri-Hexagon Tiling (THT)

a) Uniform Random Deployment:

In the random deployment scheme, sensors are deployed in a random way. Therefore, the exact locations of nodes are not known. Random deployment is usually suitable in the following cases:

- When the environment is harsh and therefore, deployment of nodes is exceedingly difficult.
- When wireless sensor network is large scale.
- When the cost of sensors is not an issue

In this method, sensors are dropped form a helicopter, an airplane or an unmanned vehicle. Uniform random deployment is random deployment where nodes are placed in a sensing area randomly with uniform distribution. Figure 2.2 (a) illustrates the uniform random deployment method.

Regular Deployment:
Regular deployment refers to placing sensors in a regular form in a sensing area. This type of deployment can usually be applied in non-harsh environment and non-large-scale regions. In this paper, four regular deployment strategies are introduced.

1) **Square Grid:** In the square grid deployment, a square sensing area is divided into small squares and the nodes are placed at the points of grid intersection as shown in Figure 2.2(b).
2) **Triangle Grid:** A square sensing area in this model is divided into small triangles and the sensors are located in the points of triangle heads as shown in Figure 2.2(c).
3) **Hexagon Grid:** In hexagon grid deployment scheme, a sensing area is divided into hexagons, as illustrated in Figure 2.2(d) and the sensors are placed at the vertices of hexagons.
4) **Tri-Hexagon Tiling (THT):** In this model, is a pattern of hexagonal stars that consist of triangles and hexagons. Tiling refers to covering the area without leaving any gaps and without any overlapping. Figure 2.2(e) displays the THT deployment strategy.

IoT Sensor Deployment Challenges:

The business benefits of IoT coupled with market trends are driving rapid IoT adoption in every industry vertical like smart cities, building automation, industrial, healthcare, etc. This growing demand for IoT connectivity is paving the way to a plethora of sensor types for various use cases such as traffic sensors, parking meters, pressure sensors, electricity sensors, and so on. Efficient sensor deployment is one of the key success factors in every IoT investment and that's where most enterprises struggle a lot today.

Challenge #1: Variety of sensors and chipsets
There is an increasing number of commercial launches of cellular technologies like NB-IoT, Cat-M1/M2, LTEM, LoRa, etc. Each of these technologies has specific electronics for sensing endpoints. Although the cost of mobile chipsets has been declining over time, currently there's no cost-effective solution that can work with the widespread in electronics of the cellular-connected IoT sensors to measure connectivity parameters.

Challenge #2:Identify an optimal location to deploy sensors

Whether it is a factory floor or a smart building, it is never easy to identify the perfect spot to deploy the IoT sensors. To successfully capture and transmit the ambient inputs over-the-air, the sensor must be located near the input-source and also where the network signal strength is reliable. To determine signal quality spread, today operators mostly rely on statistical modeling using terrain and clutter models. This results in statistical variabilities. Currently, there is no way to capture empirical network data, the lack of which often leads to installing sensors in sub optimal locations where the signal quality is poor and unreliable. Unreliable connectivity results in poor sensor performance which in turn affects the performance of the overall IoT solution and impacts the customer experience.

Challenge # 3: Not easy to remediate sensor performance issues

IoT sensors are typically installed in hard-to-access locations. When a sensor exhibits sub-optimal performance due to network connectivity, it is hard to root-cause the problem. Currently, there is no way to obtain real-time visibility into connectivity data to assess network health. The technicians may need to try a different location hoping for better wireless connectivity or replace the sensor itself. In such trial-and-error methodology, multiple truck rolls could be needed before the problem is identified and rectified. This impacts both OpEx and TCO and also skews up inventory management.

Challenge # 4 Network validations for connectivity SLAs

It is difficult to guarantee a satisfactory level of service if the IoT devices fail to deliver due to poor connectivity. Currently, RF and RAN design are done based on statistical models. Once the IoT network is deployed, due to the lack of network health data, it is not possible to validate your network design assumptions and performance in the context of the initial SLAs.

In a highly competitive digital marketplace, businesses can’t live with these challenges for too long.

NODE DISCOVERY:=>

Node discovery is the process of identifying and adding new devices to an IOT network. It is essential to ensure that new devices can join the network seamlessly and begin communicating with other devices without disrupting the existing network. Node discovery is also critical for maintain the scalability and flexibility of IOT networks.

- Sensor nodes are used to monitor environmental conditions like temperature, pressure, humidity, sound, vibration, position etc.
- Each and every node is capable to perform data gathering, sensing, processing and communicating with other nodes.
- The sensing unit senses the environment
- The processing unit computes the confined permutations of the sensed data
- The communication unit performs exchange of processed information among neighboring sensor nodes.

Data dissemination

Data Dissemination is a procedure where the server initiates and manages transfer of data as well as updates. It also helps in maintaining data consistency and cache management. It is defined as “Pushing data to mobile devices from a server or some other computer.” Mobile devices can select time and cache required data. In ad-hoc network, traffic is peer to peer. Multi-hop routing is used to communicate data. In wireless sensor network, other traffic models are possible which are as follows:

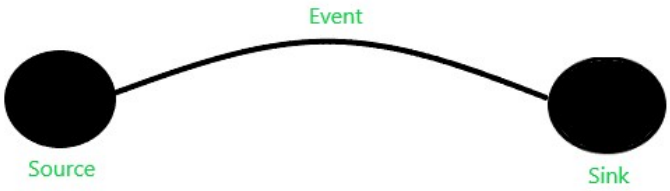
- Data Collection Model: The source sends data to a collection periodically on demand
- Data Diffusion Model: A sensor node that generates data based on its sensing mechanism’s observation.

Data dissemination has two different entities:

- Source: Generating data.

- Event: Something that needs to be reported for example, in target detection, some abnormal activity.
- Sink: A node randomly located in the field, that is interested in events and seeks such information.

Event in the below diagram indicates the information to be reported or sent. After source receives an interest from the sink, the event is transferred from the source to the sink. Data dissemination is a two step process. First, the node that is interested in some events, broadcasts its interests to its neighbors periodically. Interests are then propagated through the whole sensor network. In the second step, nodes that have requested data, send back data after receiving the request. Intermediate nodes in the sensor network also keep a cache of received interests and data.



There exists several data dissemination methods:

Flooding: It is the simplest design. In this method, each node receiving data repeats it by broadcasting the data to every neighbor unless the maximum hop lifetime of the data has been reached.

Data dissemination is a critical function in wireless sensor networks (WSNs) that involves the transmission of sensor data

from one or more nodes to a base station or other nodes in the network.

Gossiping: It is the enhancement of Flooding. In this, when a node receives data, it randomly chooses a neighbor and sends the data to it. Unlike Flooding, we does not need to bother about duplicate data packets being sent to the same location. It also contributes to the latency of network.

Advantages

- This protocol is easily scalable.
- It eliminates some of the shortcomings of Flooding.
- This protocol sends data in autonomous and decentralized manner

Disadvantages of Gossiping

- The destination is selected randomly so it may lead to starvation for some nodes as they may not be selected to send data at all.

SPIN: Sensor Protocols for Information via Negotiation (SPIN) has the required features which can overcome the shortcomings of flooding. When interested nodes send a request, SPIN will send the data to the corresponding node otherwise it will not on its own. SPIN messages can be distinguished into three types:

- ADV- ADV message is used to signal that the sensor has data to send and describes the data by the help of a sensor
- REQ- REQ message is used when a node is ready to receive data from neighboring node
- DATA- The information to be sent is contained here

Advantages

- SPIN is more efficient than flooding since the negotiation reduces the implosion and overlap.

Data Aggregation: ⇒

Data aggregation is the process of collecting and aggregating the useful data.

The data aggregation is a technique used to solve the implosion and overlap problems in data centric routing. Data coming from multiple sensor nodes are aggregated as if they are about the same attribute of the phenomenon when they reach the same routing node on the way back to the sink. Data aggregation is a widely used technique in wireless sensor networks. The security issues, data confidentiality and integrity, in data aggregation become vital when the sensor network is deployed in a hostile environment. Data aggregation is a process of aggregating the sensor data using aggregation approaches. The general data aggregation algorithm works as shown in the below figure1. Figure 1 illustrates that data aggregation is the process of aggregating the sensor data using aggregation approaches. Then the algorithm uses the sensor data from the sensor nodes and then aggregates the data by using some aggregation algorithms such as centralized approach, LEACH(Low Energy Adaptive Clustering Hierarchy), TAG(Tiny Aggregation) etc. This aggregated data is transfer to the sink node by selecting the efficient path.

•Data aggregation in IoT (Internet of Things) involves the process of combining and summarizing data from multiple sensors or devices into a more concise and meaningful form. The primary goal is to reduce the volume of transmitted data, minimize communication overhead, and improve the efficiency of data transfer within an IoT network. Aggregated data is often more manageable for storage, analysis, and transmission compared to raw data from individual sensors.