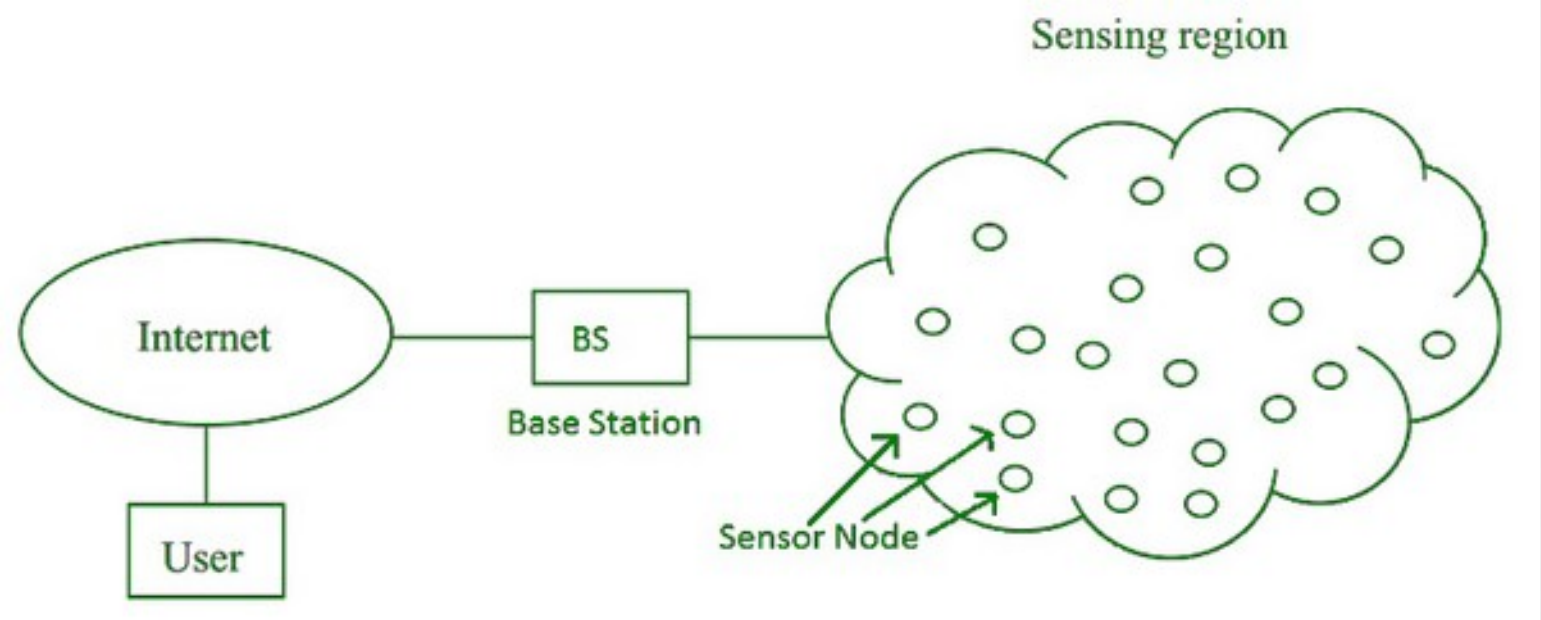
Wireless Sensor Network (WSN)

- 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.

- 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.

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

Architecture of Wireless Sensor Network (WSN)



Architecture of Wireless Sensor Network (WSN)

- As shown in the WSN architecture, WSN will have three main components as mentioned above viz. distributed sensor nodes, sink nodes (Base station or Gateway) and Software. Each sensor node usually will have single omnidirectional antenna and tranceiver, power supply and DSP embedded. Gateway is located at the boundary of the monitoring coverage area. The gateway helps connect micro-sensor network with the outside world such as internet or similar other WSN.

- Sensor network will have thousands of sensors distributed randomly and densely about 10-20 per square meter. Availability of flash memories and energy efficient batteries provide better wireless sensor networks.

- The algorithms based on wireless standards take care of collision and congestion situations in the wireless sensor networks(WSNs).

- WSNs have been classified based on network type, clustering type, communication method, protocol, application and coverage.

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

MANET

- MANET stands for Mobile Adhoc Network also called a wireless Adhoc network or Adhoc wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network.
- They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure.
- MANET nodes are free to move randomly as the network topology changes frequently.
- Each node behaves as a router as they forward traffic to other specified nodes in the network.

MANET

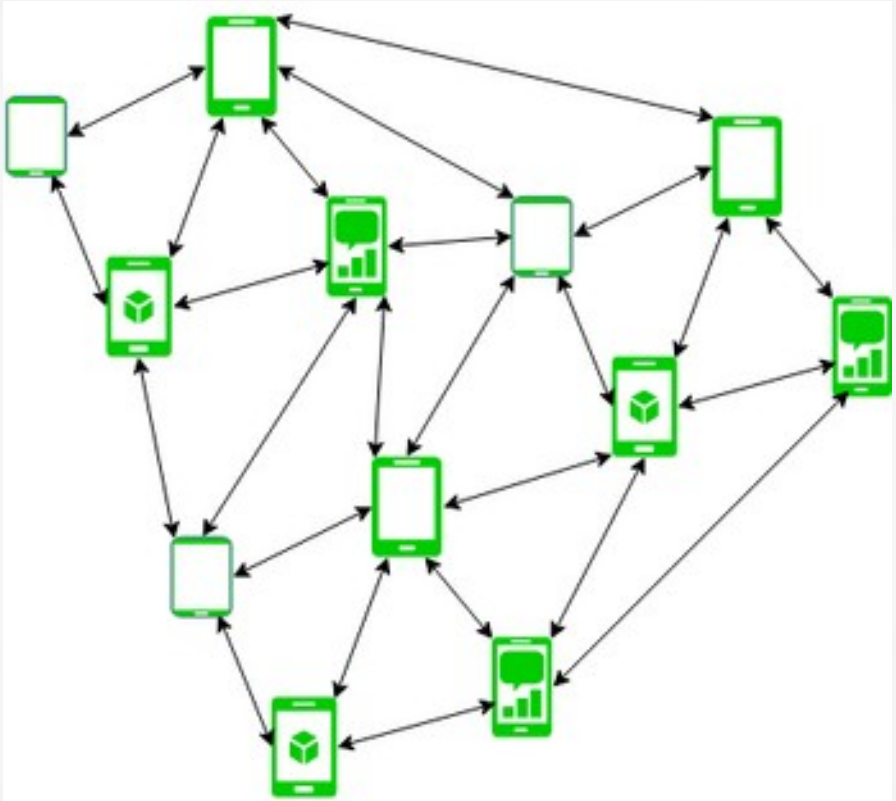


Figure - Mobile Ad Hoc Network

Similarities between MANET and WSN

- Both are infrastructure-less, distributed wireless networks
- Routing Techniques are more or less the same
- Both are Ad-hoc networks
- Topology can change over a period
- Nodes can be operated on a battery
- Both wireless channels use unlicensed spectrum (cause of interference)

Difference between MANET and WSN

- The data rate of MANETs is more than WSN
- The number of nodes in the WSN is more than MANETs
- Mobility is very high in MANETs(since nodes are less) than WSN
- Sensor nodes of WSN are generally static and cooperate together to transfer the sensed data
- Sensor nodes usually consume less energy than MANET’s nodes
- MANETs are usually close to civilization
- Public-key cryptography is used in MANETs whereas symmetric key cryptography used in WSNs for security purposes
- Compared to MANETs, WSNs are smaller, more powerful, and more memory-constrained
- Mostly, MANETs are used for distributed computing whereas WSNs are used for information gathering from the environment
- WSNs are more prone to failures than MANETs

Characteristics of WSN

- Power consumption limitations for sensor nodes.
- Ability to cope with failures of nodes.
- Mobility of nodes.
- Heterogeneity of nodes.
- Homogeneity of nodes.
- Ability to deploy on a large scale.
- Capability to survive harsh environmental conditions.
- Helps to use easily.

Design Issues in WSN

- Fault Tolerance: Possibility of node failure and change of topology of network is quite high in case of WSN. Hence the designer of network should make the network robust and reliable even in case of node failures and topology changes. The network should function smoothly and normally irrespective of node failures and topology changes.

- Life Time: WSN are supposed to work for a quite long time with low power consumption. They are supposed to last at-least for 6 months to 1 year. We need to keep in mind that every node in WSN may be powered using just a 3 V battery and this should be sufficient for the entire life time of the node . The design of protocols of WSN should be such that the node consumes as less energy as possible. This will help in making the WSN last longer.

- Scalability: The design of WSN should support addition of new nodes any time and also the design should support large number of nodes because some applications in WSN may require quite a huge number of sensor nodes.

Design Issues in WSN

- Date Aggregation: The sensor nodes in WSN are located close to each other hence the possibility of similar data being generated by the nodes next to each other is quite high. So the data needs to be aggregated and the duplicate data needs to be avoided because the transmission and reception data is the most costly affair in WSN.The data needs to be aggregated at different levels in WSN so that only the necessary data is transmitted and recevied and the redundant data is not communicated.

- Cost: The cost of each sensor node is supposed to be 1$, as WSN can have large number of sensor nodes the total cost of the network can become a quite expensive affair. So the designer of WSN needs to decide on the optimal number of nodes necessary for the application.

- Environment: The environment in which the WSN is deployed can be very demanding , so the design of WSN should be such that WSN should be able to survive regardless of the conditions in which WSN s deployed.

Design Issues in WSN

- Heterogeneity Support: The protocols designed for WSN should support different kinds of sensor nodes and also be able to support variety of applications.

- Autonomous Operations: The WSN should be able to organize , reorganize and operate autonomously because sometimes WSN deployed in places where human habitation is not possible.

- Limited Memory and Processing Capability : The sensor nodes have very limited memory, power and processing capabilities , so all designs of WSN should not be demanding in terms of processing requirements or memory requirements .

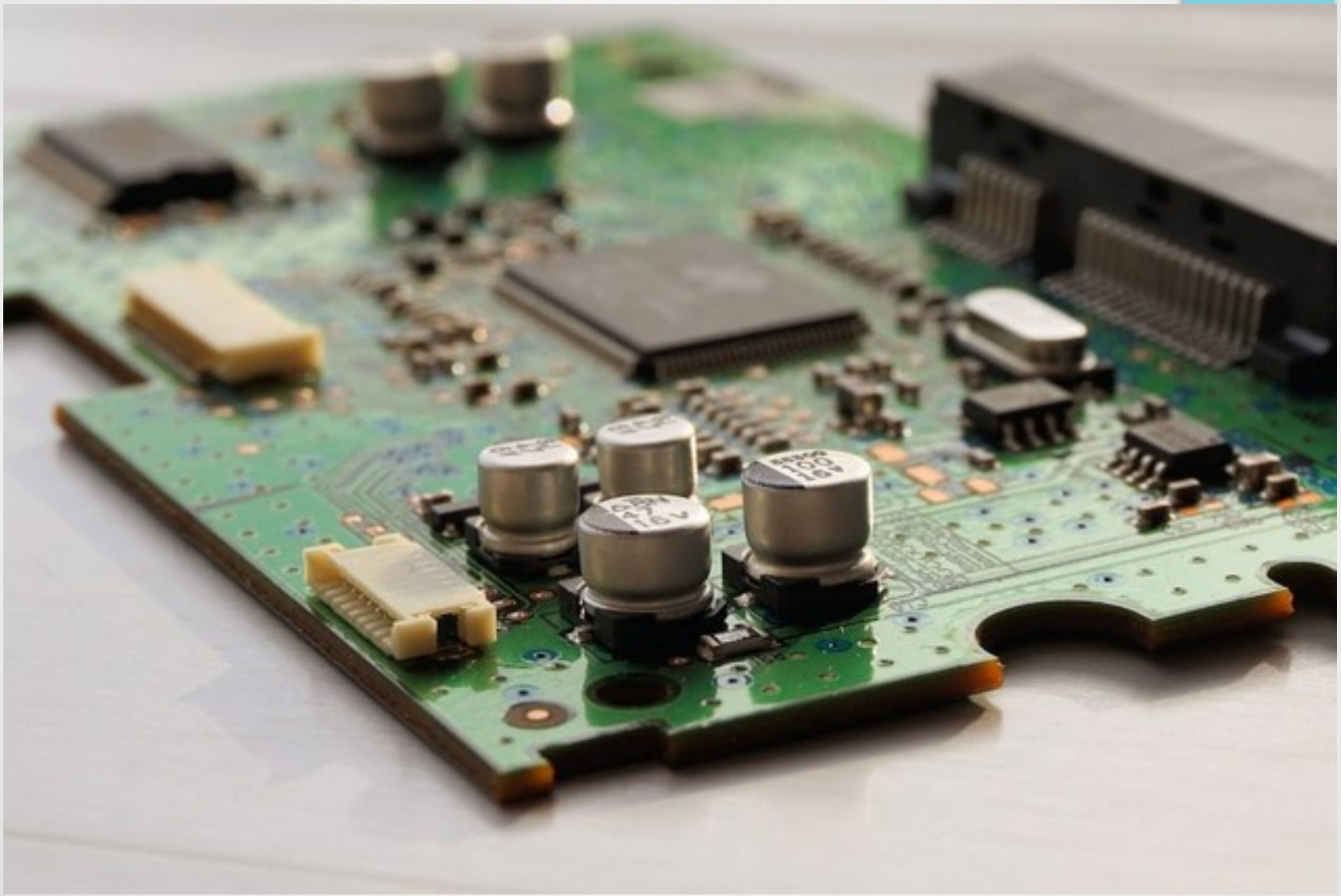
Advantages of WSN

- It is scalable and hence can accommodate any new nodes or devices at any time.
- It is flexible and hence open to physical partitions.
- All the WSN nodes can be accessed through centralized montoring system.
- As it is wireless in nature, it does not require wires or cables.
- WSNs can be applied on large scale and in various domains such as mines, healthcare, surveillance, agriculture etc.
- It uses different security algorithms as per underlying wireless technologies and hence provide reliable network for consumers or users.

Disadvantages of WSN

- As it is wireless in nature, it is prone to hacking by hackers.
- It can not be used for high speed communication as it is designed for low speed applications.
- It is expensive to build such network and hence can not be affordable by all.
- There are various challenges to be considered in WSN such as energy efficiency, limited bandwidth, node costs, deployment model, Software/hardware design constraints and so on.
- In star topology based WSN, failure of central node leads to whole network shutdown.

WSN with IOT



WSN with IOT

- Internet Connectivity
- In an IoT system, all of the sensors directly send their information to the internet. For example, a sensor may be used to monitor the temperature of a body of water. In this case, the data will be immediately or periodically sent directly to the internet, where a server can process the data and it can be interpreted on a front-end interface.

- Conversely, in a WSN, there is no direct connection to the internet. Instead, the various sensors connect to some kind of router or central node. A person may then route the data from the router or central node as they see fit. That being said, an IoT system can utilize a wireless sensor network by communicating with its router to gather data.

- You can think of a wireless sensor network as more of a group of sensors or "a big sensor" and less like a "competitor" or "rival" to the Internet-of-Things.

WSN as a Subset of IoT

- IoT exists at a higher level then WSN. In other words, WSN is often a technology used within an IoT system. A large collection of sensors, as in a mesh network, can be used to individually gather data and send data through a router to the internet in an IoT system.

- It's also important to note that the term "wireless sensor network" is not nearly as encompassing as "the internet of things." WSN consists of a network of only wireless sensors. If the network was to include a wired sensor, it could no longer be labeled a "wireless sensor network." This is unlike IoT. Essentially any device that connects to the internet can be considered an IoT device. An "IoT system" can therefore be interpreted as a group of many IoT devices.

WSN with IOT

- Examples
- A fridge with the capability of sending temperature reading to the internet is unlikely to use a wireless sensor network but it IS an IoT device.
- A large collection of sensors used to monitor precipitation on an acre of land is likely to be considered a "wireless sensor network" if in fact all the sensors are wireless. This system may or may not be connected to an IoT system.