# A Comparative Study on Cellular, Sensor and Adhoc Networks

Jayashree V. Shiral

Department of Computer Science and Engineering, DBACER, Nagpur city, India.

jayashreevshiral@yahoo.in

***ABSTRACT***

*A cellular network is an asymmetric radio network which is made up of fixed transceivers or nodes, maintain the signal while the mobile transceiver which is using the network is in the vicinity of the node. An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect.*

*Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other.*

*This paper focuses on various issues, architecture and routing protocols in cellular, adhoc and sensor networks. As issues proves helpful for forthcoming research, this paper work as a backbone to elaborate the various research areas.*

***KEYWORDS***

*Sensor Netwok , Cellular Network, Adhoc Network, Issues , Requirements, architecture, routing protocols.*

## 1. INTRODUCTION

A WSN is a collection of sensors that can communicate through wired or wireless medium. The sensors are allowed to communicate within its communication range. A Cellular network is one of the radio network distributed over land areas called cells, each served by at least one fixed-location transceiver known as a cell site or base station .When these cells joined together provide radio coverage over a wide geographic areas. A wireless adhoc network is a decentralized type of wireless network. The network is adhoc because it does not depend on a preexisting infrastructure, such as routers in wired networks or access points in managed, infrastructure wireless networks.

## 2. WIRELESS SENSOR NETWORK

A WSN is a collection of sensors that can communicate through wired or wireless medium. The sensors are allowed to communicate within its communication range. It has received a greater interest in various applications such as disaster management, border protection, combat field reconnaissance, in military for security surveillance, structural health monitoring, industrial automation, civil structure monitoring, and monitoring the biologically hazardous places and in variety of applications.

DOI: 10.5121/ijassn.2012.2305 

A sensor network must be able to operate under changing environment. Specifically, our protocols must be able to enable network operation during start-up, steady state, and failure.The necessity of operation under these conditions is required because in most cases, the sensor network must operate unattended. Once the nodes have booted up and a network is formed, most of the nodes will be able to sustain a steady state of operation, i.e. their energy reservoirs are nearly full and they can support all the sensing, signal processing and communications tasks as required. In this mode, the group of the nodes will be formed into a multi-hop wireless network. The node begin to establish and maintain paths by which information is passed to one or more sink nodes.

A Sink node is act as a clusterhead which gather, control and forward data collected by other sensor nodes. A sink node is having the large transmission range as compare to other nodes. The sink may also be a mobile node or active node acting as information sink, or any other entity that is extracting the information from the sensor network. Although the multi-hop network can operate in both the sensor-to-sink or sink-to-sensor

Sensor nodes are expected to operate and adjust in changing environments and should be applicable in large areas. Failures are susceptible in wireless sensor networks due to inhospitable, unstable environment and unattended deployment. The data communication from transmitter to receiver and vice versa may cause energy depletion in sensor nodes and therefore, it is common for sensor nodes to exhaust its energy completely and stop operating and thus, need to switch between wakeup and sleep modes. This may cause connectivity and data loss during communication. Therefore, it is necessary that network failures are detected in advance and appropriate measures should be taken to avoid network failures. Figure 1 gives a description of the simple node architecture[2].

To design a system, the mobile assumes full responsibility of making and breaking connections.

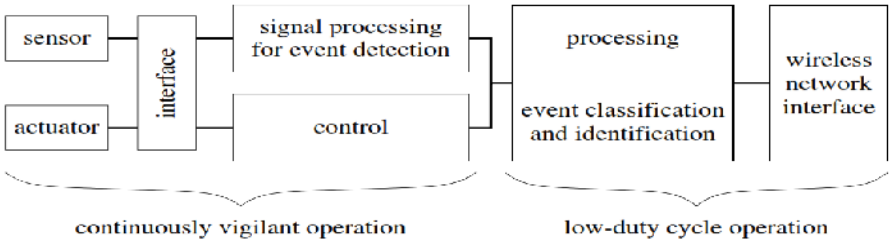


Figure 1. Node Architecture

If the invitation message, which is inherently part of the stationary MAC algorithm, is included as a shared message. Figure 2 shows general mobile scenario[2].

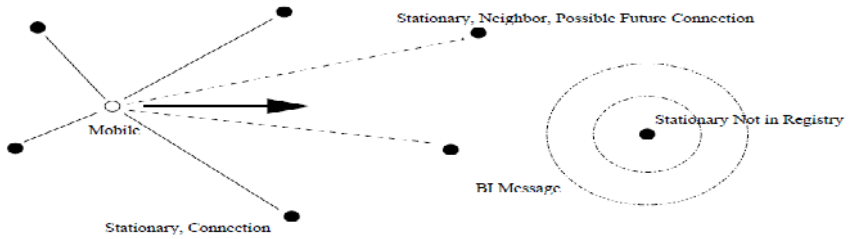


Figure 2. General Mobile Scenario

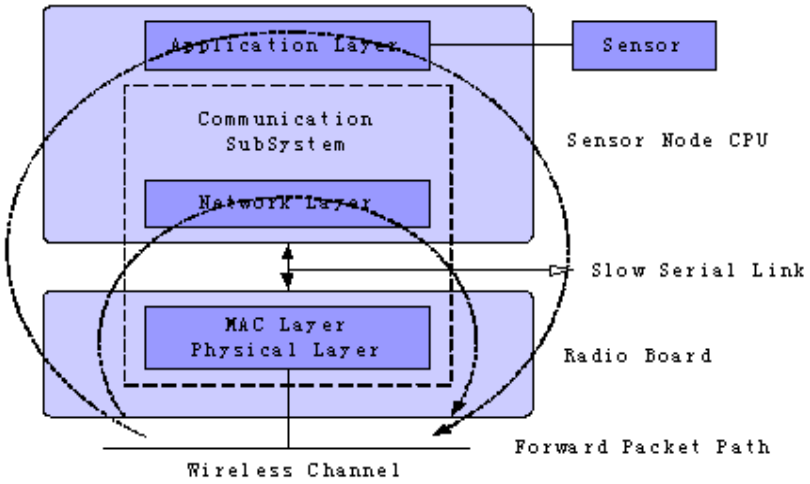


Figure 3. Architecture of sensor node

Routing protocols in WSNs are as follows:

• Flat Routing: each node performs the same role and sensor nodes work together to perform the sensing task.

• Hierarchical (Cluster-based) Routing: higher-energy nodes are used to process and send the information, while low-energy nodes are used to perform the sensing in the proximity of the target. The creation of clusters and assigning special tasks to cluster heads leads to overall system scalability, lifetime of the network, and energy e □ ciency. Hierarchical routing is an e □ cient way to lower energy consumption within a cluster, performing data aggregation and fusion in order to decrease the number of transmitted messages to the sink node

• Location-based: sensor nodes are addressed by means of their locations. The distance between neighboring nodes can be estimated on the basis of incoming signal strengths. To save energy, some location-based schemes demand that nodes should go to sleep if there is no activity. Depending on the protocol operation we can divide routing protocols in:

• Query-based: the destination nodes propagate a query for data from a node through the network, a node with this data sends the data that matches the query back to the node that initiated it.

• Negotiation-based: use negotiation in order to eliminate redundant data transmissions. Data transmission and reception decisions are also made based on the available resources.

• QoS-based: when delivering data, the network balances between energy consumption and data quality through certain QoS metrics as delay, energy or bandwidth.

• Coherent-based: the entity of local data processing on the nodes distinguish between coherent (minimum processing) and non-coherent (full processing) routing protocols.

## 2.1. Issues in WSN Security

Energy efficiency: The requirement for energy efficiency suggests that in most cases computation is favoured over communication, as communication is three orders of magnitude

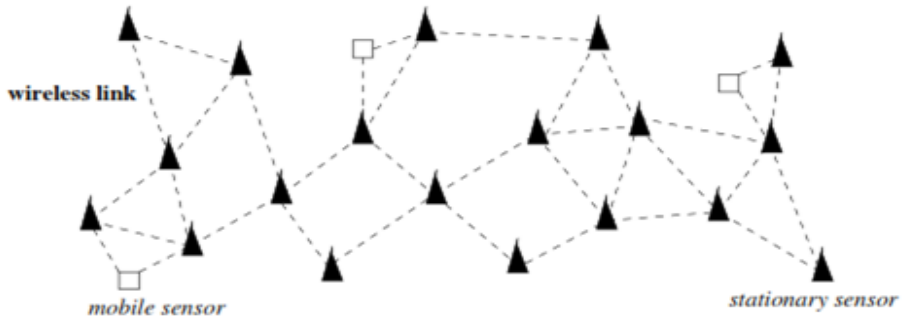


Figure 1. A Wireless Sensor Network

more expensive than computation.

- Cryptography: No public key cryptography is provided in wireless sensor network. Public-key algorithms is expensive on sensor nodes as in case of storage and energy.
- Multilayers for security: Security becomes an important factor because attacks can occur on different layers of a networking stack as defined in the OSI model.

### 2.2. Security Requirements in WSN

- Data Confidentiality: Data confidentiality is one of the important issue in network security. The security can be maintained and provided by applying strong cryptographic algorithms. Confidentiality means that unauthorized third parties cannot read information between two communicating parties while transmitting data from one end to another.
- Data Integrity and authenticity: Data confidentiality only ensures that data can not be read by the third party, but it does not guarantee that data is unaltered or unchanged in the middle of transmission. Integrity means that the receiver should get the original data.

## 3. CELLULAR NETWORK

A Cellular network is one of the radio network distributed over land areas called cells, each served by at least one fixed-location transceiver known as a cell site or base station .When these cells joined together provide radio coverage over a wide geographic areas. Cellular networks provides the advantages such as increased capacity, reduced power use, large coverage area, reduced interference from other signals. Figure 4. shows the cellular network.

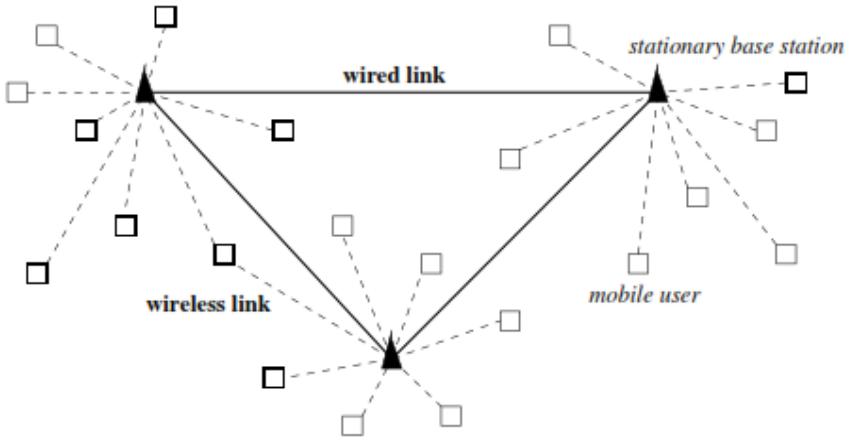


Figure 4. A Cellular Network

Multihop Cellular Networks (MCN) are more demanding on MAC protocols than SCNs. In SCNs, the BS is involved in every transmission of a frame, either as the transmitter or as the receiver. This considerably simplifies the channel assignment, and MAC protocols as simple as slotted ALOHA (used by GSM for access requests) prove to be adequate. The spatial fairness that the MAC protocol provides is to be looked into too. Although it is possible to provide connection-oriented services in MCNs by partitioning the available bandwidth into channels as in SCNs, in this paper, we use one single channel, mpacket switched, contention based MAC protocols. The scalability requirements for MCNs are to be met. Figure 5. Shows the architecture of Wireless Sensor Network.

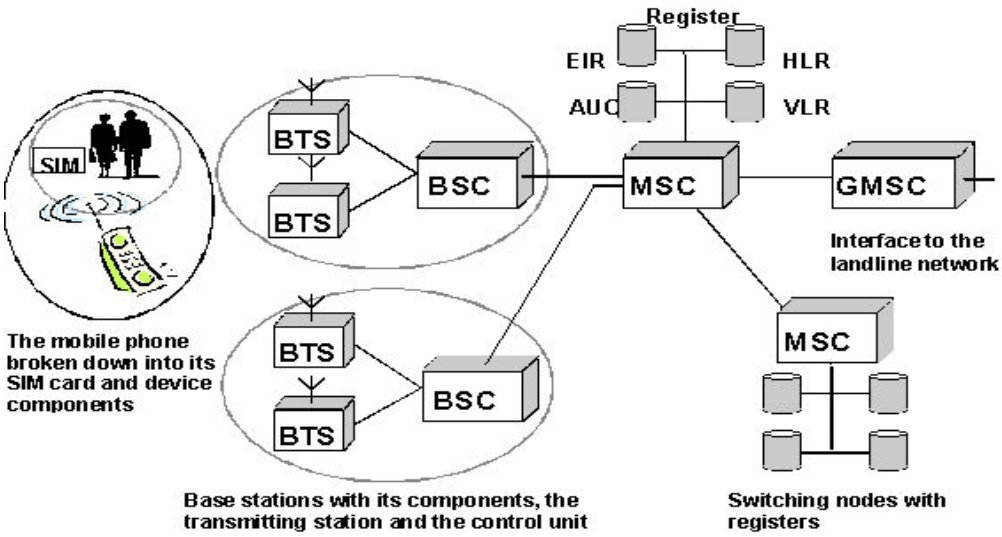


Figure 5.Architecture of Wireless Sensor Network

### 3.1. Security Issues in Cellular Network

- Authentication: Cellular networks have a large number of subscribers, and each has to be authenticated to guarantee the right people are using the network.
- Integrity: With services such as Short Messaging Service, online/offline chat and file transfer it is important that the data arrives without any modifications.

- Access Control: The Cellular device may have files that need to have restricted access to them from users or any kind of unauthorized users.

- Web Services: A Web Service is an element that provides functionality accessible through the web using the standard HTTP Protocol. This opens the device to variety of security issues such as viruses, buffer overflows, denial of service attacks etc.

- Downloaded Contents: Online downloads invites the spywares causing security issues. Another problem is that of digital rights management. User might download unauthorized copies which leads to securities deformity.

## 4. ADHOC NETWORK

A wireless adhoc network is a decentralized type of wireless network. The network is adhoc because it does not depend on a preexisting infrastructure, such as routers in wired networks or access points in managed, infrastructure wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. A Mobile Adhoc Network (MANET) is an autonomous collection of mobile routers and associated hosts connected by bandwidth-constrained wireless links.

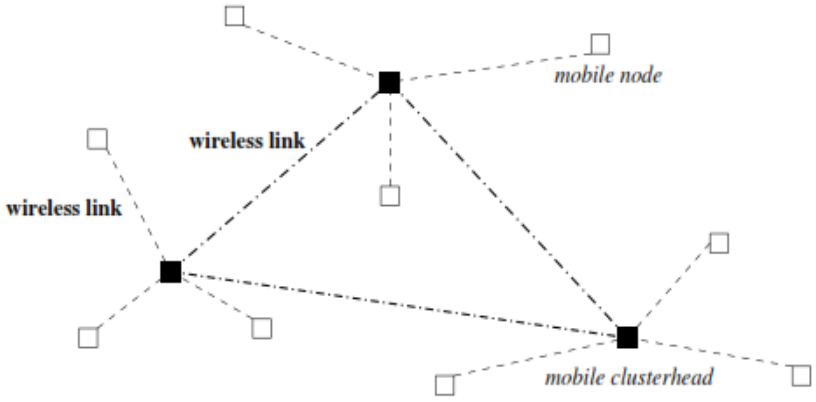


Figure 6. A Mobile Adhoc Network (MANET)

The network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion or may be connected to the larger Internet. Figure 3. Shows the mobile adhoc network. Three categories that existing ad-hoc network routing protocols are as follows:

1. Table Driven Protocols
2. On Demand Protocols
3. Hybrid Protocols

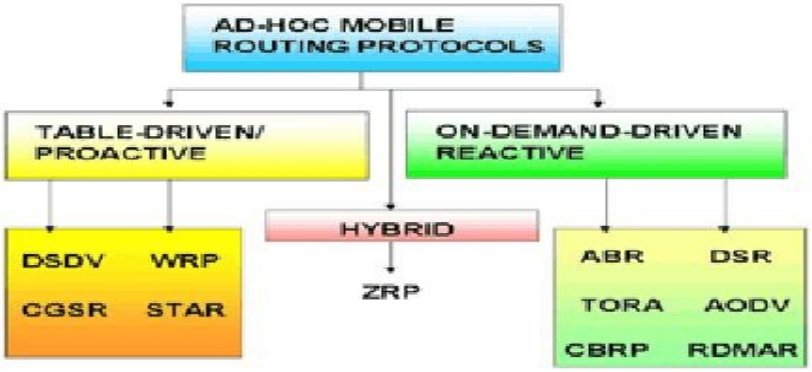


Figure 7. Adhoc routing protocols

Table Driven Routing Protocols, also known as Proactive Protocols, they are independent of traffic demands.This type of protocol is slow to come together. Table Driven Protocols will use limited resources such as power, bandwidth.

On Demand Routing Protocols, also known as Reactive Protocols, they establish routes between nodes only when they are required to route data packets. On Demand protocols are efficient when the route discovery is frequent than the data transfer. On Demand Protocols more useful in large networks with light traffic and with low mobility.

Hybrid Routing Protocols combine the features of Table Based Routing Protocols and On Demand Routing Protocols.

### 4.1. Security Issues in Adhoc Network

- Susceptible to Channels: messages can be eavesdropped and bogus messages can be injected into the network without the difficulty of having physical access to network components which violent the security issue.
- Lack of Infrastructure: Ad hoc networks are considered to operate independently of any fixed infrastructure.

### 4.2. Security Requirements for Adhoc Network

- Confidentiality: Ensures certain information is never disclosed to unauthorized users.
- Integrity: Message received at the receiver side must be original.
- Authentication: Only the authorized user can access the data.
- Non-impersonation: Noone can act to be another authorized member to learn any useful information.
- Attacks using fabrication: Attackers created the false route to access the information. This type of attacks is hard to identify.

## 5. CONCLUSIONS

This paper proposed the comparison between sensor network, cellular network and adhoc network . Also this paper includes various security issues requirements of the above networks. Also it includes the architecture and various routing protocols of these main wireless networks.

## REFERENCES

[1] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz (2008), "Security Issues in WSN," International Journal Of Communications, Issue 1, Volume 2.
[2] Katayoun Sohrabi, Jay Gao, ishal Ailawadhi and Gregory J Pottie, "Protocols for Self-Organization in Wireless Sensor Network", IEEE Journal on Personal Communication, 2000.
[3] http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group11/index.html
[4] Karan Singh, R. S. Yadav, Ranvijay (2007), "Review Paper On Ad Hoc Network Security", International Journal of Computer Science and Security", Issue 1, Volume 1.
[5] Kalpana Sharma, M.K. Ghose, Deepak Kumar, Raja Peeyush Kumar Singh, Vikas Kumar Pande (2010), "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks", International Journal of Advanced Science and Technology, Vol. 17.
[6] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang (2004), "Security in mobile adhoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47.
[5] Roberto Di Pietro, Pietro Michiardi, Refik Molva (2007), "Confidentiality and Integrity for Data Aggregation in WSN using Peer Monitoring".
[6] Nandini. S. Patil, Prof. P. R. Patil (2010), "Data Aggregation in Wireless Sensor Network,"IEEE International Conference on Computational Intelligence and Computing Research, 2010.
[7] Li, Raghu Kisore Neelisetti, Cong Liu, and Alvin Lim (2010), "Efficient Multipath Protocol for WSN", International Journal of Mobile and Wireless, Vol 2, No.1.
[8] Simarpreet Kaur, and Leena Mahajan (2011),"Power Saving MAC Protocols for WSNs and Optimization of S-MAC Protocol", International Journal of Radio Frequency Identification and Wireless Sensor Networks.

## First Author

Author is currently persuing M.E in Wireless Communication and Computing from G.H.R.C.E, Nagpur. She has completed her B.E in Information Technology from Priyadarshini Institute of Engineering and Technology, Nagpur. Currently, she is a lecturer in Dr. Babasaheb Ambedkar College of Engineering and Research (DBACER), Nagpur.
Email id: [1]jayashreevshiral@yahoo.in