Chapter 2

Communication Network: An Introduction

This Chapter describes the brief about networks available for communication. This chapter gives brief idea about Hybrid Network. It describes an overview and classification of networks used for communication. A survey of different types of networks viz., wired and wireless networks, different wireless ad hoc network like wireless sensor network, Wireless local area Network is described.

Today, communication enters our daily lives in so many different ways that it is very easy to overlook the multitude of its facts. The telephone at our hands, the radios and televisions in our living rooms, the computer terminals in our offices and homes, and our newspapers are all capable of providing rapid communications from every corner of the globe [1].

A computer network communication has following properties:

- Facilitates interpersonal communications
  - People can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.
- Allows sharing of files, data, and other types of information
  - Authorized users may access information stored on other computers on the network. Providing access to information on shared storage devices is an important feature of many networks.
- Allows sharing of network and computing resources
  - Users may access and use resources provided by devices on the network, such as printing a document on a shared network printer. Distributed computing uses computing resources across a network to accomplish tasks.
- May be insecure
  - A computer network may be used by computer Hackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from accessing the network (denial of service).
- May interfere with other technologies
  - Power line communication strongly disturbs certain forms of radio communication, e.g., amateur radio. It may also interfere with last mile access technologies such as ADSL and VDSL.
- May be difficult to set up

- A complex computer network may be difficult to set up. It may be costly to set up an effective computer network in a large organization.

With the recent developments in the communication technology, the networking of more devices is possible. The communication networks used to connect devices to form a computer network include electrical cable, optical fiber and radio waves.

A widely-adopted family of communication network used in local area network (LAN) technology is collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802. Ethernet encompasses both wired and wireless LAN technologies. Wired LAN devices transmit signals over cable media. Wireless LAN devices use radio waves or infrared signals as a transmission medium.

2.1 IEEE 802.3: Ethernet

Wired Local Area Networking [1] includes several technologies such as Ethernet [2], token Ring, Token bus, FDDI (Fibre distributed data interface) and ATM (asynchronous transfer mode) LAN (local area networks) [3]. Some of these technologies survived for a while, but Ethernet is by far the dominant technology. Evolution from a 10Mbps Standard Ethernet to bridged Ethernet and then to a switched Ethernet paved a way for faster Ethernet. IEEE 802.3 Standard specifies Carrier Sense, Multiple Access with Collision Detect (CSMA/CD) as the access method for first-generation 10-Mbps Ethernet, a protocol that helps devices share the bandwidth evenly without having the two devices transmit at the same time on the network medium. The Ethernet is a working example of the more general CSMA/CD local area network technology.

The Ethernet is a multiple-access network, meaning that a set of nodes sends and receives frames over a shared link. When the two devices transmit at the same time the collision can occur. This collision generates a jam signal that causes all nodes on the segment to stop sending data, which informs all the devices that a collision has occurred. The carrier sense in CSMA/CD means that all the nodes can distinguish between an idle and a busy link. The collision detect means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node. The Ethernet is said to be a 1-persistent protocol because an adaptor with a frame to send transmits with probability 1 whenever a busy line goes idle.

This Carrier Sense, Multiple Access with Collision Detect (CSMA/CD) protocol was created to overcome the problem of collisions that occur when the packets are transmitted simultaneously from different nodes.

Even though the wired reduces the cost of cabling and gives more flexibility and re-configurability, it is not fully configurable. It includes the cost of cabling damage to the cables temporary abandon of the work progress due to the reconfiguration of the entire system. When operating under the harsh conditions this is not essential and could also lead to the damage of the infrastructure. Suppose if there are any mobile parts then the wires should also be moving a very difficult constraint to meet without any issues. This led to the induction of wireless technologies in industrial networks.

2.2 IEEE 802.11: Wireless LAN

Wireless local area networks (WLANs) [4] extend the boundaries of traditional wired local area networks (LANs) by unleashing the constrained flow of wire-line data to saturate the surrounding area. Wireless communication offers significant advantages to both users and network designers. Users gain flexible mobility to work anywhere within radio communication range of a network access point and seamlessly retrieve network resources. Roaming around the network, pervasive devices discover each other and permit users to benefit from context aware applications. Network designers gain tremendous advantages in rapid network building, upgrading, and reconfiguration. IEEE 802.11 is a recent standard developed for wireless local area networks (WLANs). IEEE 802.11 is a multiple access protocol in which stations in the network must compete for access to the shared communications medium to transmit data. IEEE 802.11 uses a carrier sensing capability to determine if the communications medium is currently being used [3]. If two or more stations in the network transmit at the same time (i.e., a collision occurs), stations retransmit their data after random periods of time as in Ethernet. Wi-Fi (Wireless Fidelity) Technology, referred as the IEEE 802.11 communications standard for WLAN, is the popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The IEEE 802.11 data link layer is divided in two sub layers: Logical Link Control (LLC) and Media Access Control (MAC). LLC is the same as in 802 LAN allowing for very simple bridging from wireless to wire networks. MAC is different to WLANs. The first method in MAC is CSMA with collision avoidance protocol. This protocol is to ask each station to listen before action. If

the channel is busy, the station has to wait until channel is free. Another method in MAC is called RTS/CTS to solve hidden-Node problem [5].

Wireless communications also offer significant network challenges [6]. Since the broadcast medium is shared by many devices and networks, channel controls must be implemented at both the network and station level to facilitate fair, regulated access to the medium. The Federal Communications Commission [7] regulations allocated the three Industrial, Scientific, and Medical (ISM) bands shown in Table 2.1 for unlicensed use under strict power guidelines to prevent interference.

Band	Frequency Range
UHF ISM band	902 to 928MHz
S-band ISM	2.4 GHz to 2.5 GHz
C-band ISM	5.725 to 5.875 GHz

Table 2.1 Industrial, Scientific and Medical (ISM) bands

Each band is subdivided into channels with much lower throughput capacity than wired channels. Additionally, the wireless environment introduces significant path loss uncertainty, constantly changing in both the space and time domain. Finally, along with the freedom of open wireless network boundaries, the inability to control both active and passive access to the medium increases network security vulnerabilities.

WLAN networks are implemented using IEEE 802.11 standard compliant devices and are classified as either infrastructure or ad hoc networks. Stations in an infrastructure WLAN network transfer data to a central access point (AP). The AP either forwards the message into a distribution system or relays the message to another station within the AP's basic service set (BSS), all stations associated to a particular AP. Ad hoc WLAN network stations form a peer-to-peer relationship with nodes within communications range to form an independent BSS (IBSS).

Although the deployment of wireless technologies completely eradicates the problems of the wired Networks, it is not possible to replace all the systems with wireless technology because they are highly prone to errors. Real time Communication, in which timely delivery of data is important, the missing of deadlines due to network traffic can affect the system performance. The Real time system applications mostly demands lesser bandwidth, long distance communication and more channels for multi device communication. This can be achieved with the help of wireless technology.

As wired LANs are already exist since they are older and because wired LANs allow for more resources because they generally have higher rates and are not limited in terms of size and power consumption as wireless LANs, there has been an increasing demand to connect wireless LANs to wired LANs [8].

It was also noticed that the needs for interconnecting wireless LANs to an existing wired back-bone LAN is increasingly becoming essential in many areas. So far we have discussed that Networks can be classified according to the nature of the medium of their links, to wired and wireless. As the complexity degree of these applications increases over the years, different network traffic must be handled and carried over different mediums in a unique homogeneous way. Hence, the need for interoperability in heterogeneous networks with hybrid structure is in doubtfully a major requirement, when integrating communication scenarios for home and industrial applications.

This type of hybrid network is becoming essential, as it allows for resource sharing and data transfer between the new wireless networks and the already established wired networks.

As IEEE 802.11 [9] and Ethernet [10] are becoming the most common and widely used WLAN/LAN standards, an interoperable architecture is required in order for communication to be treated transparently at the higher-levels. However, it has to be pointed out that from the user point of view, the entire system is seen as a black box and is expected to function equally well, independently from network heterogeneity. With the growing industry needs and expansion of the physical setups the conventional point-to-point technique does not meet the real time requirements such as modularity, decentralization of control, integrated diagnostics, quick and easy maintenance, and low cost because of the number of cables being proportional the square of the devices and other problems [11]. Therefore, the protocol can be redefined and permits to integrate both wired and wireless technologies to meet the industry requirement without affecting the stability of the plant. On the other hand, when dealing with hybrid wired/wireless networks, questions arise regarding QoS and power awareness issues especially concerning the wireless part of the hybrid network.

Theoretically speaking, all types of network topologies used for wired LANs can be used for Wireless LANs, but practically this is not true. The fact that wireless communication channels have different characteristics than wired channels, and the demand for mobility and ad-hoc connectivity in WLANs are the reasons why this is not true [12,13].

2.3 Hybrid Communication Networks

Hybrid Communication Network (HCN) (Figure 2.1) is one with both wired and wireless connections. Because in most cases, a transceiver-equipped PC or other device known as an access point is used and connected to a wired network, such as the telephone network or a wired LAN, which uses some type of standard cabling. This access point can receive and transmit data between the wireless and wired worlds. The chief advantage of a wireless network is mobility and flexibility. Other than that, both wired and wireless networks are equally easy (or difficult) to set up, depending on the organization's size and complexity.

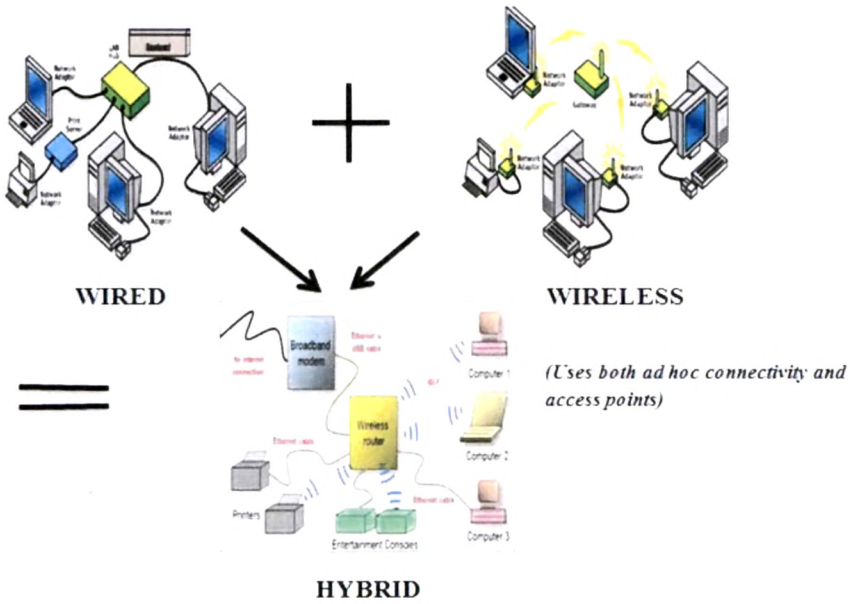

Figure 2.1: Hybrid Communication Network

Classification of Different wireless networks can be done on following basis:

- infrastructure,
- mobility
- size of network.

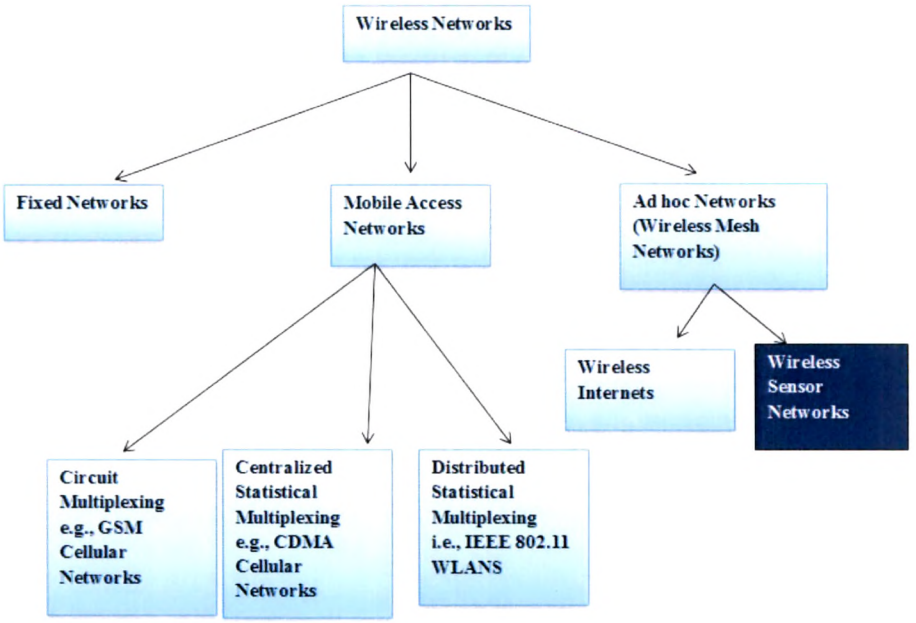

Figure 2.2 : A taxonomy of current practice in wireless networking [13]

Figure 2.2 depicts clssification of the taxonomy of current most popular networks used for communication. Among them, Wireless Sensor Network is one of the most useful in many real time Applications.

2.4 Wireless Sensor Networks

Wireless sensor networks (WSN) may consist of several to thousands of homogeneous or heterogeneous sensors that share the need to organize for data collaboration or network data collection sink routing [14]. Small system platforms which integrate sensors, processors, and transceivers are referred to as motes. Remote sensing platforms are typically characterized by reduced processing capabilities, limited memory capacities, and fixed battery supplies. The WSN energy consumption falls into three categories: sensing, computing, and communicating. Analysis conducted by Soharabi et al. [15] demonstrates that the communications costs dominate a WSN sensor platform's power budget. WLAN networks were designed to minimize delay and maximize throughput, but they do not provide the energy efficiency demanded by WSN networks. As technology makes the hardware smaller, WSN research continues developing innovative, energy-saving techniques at all network protocol layers in order to engineer sensor platforms which can operate unattended for months or even years. The WSN networks must also be scalable to support extremely dense sensor fields. Applications for energy-efficient WSN networks include homeland defense nuclear/biological/chemical

(NBC) sensing, military surveillance, and environmental sensing [16-18]. These applications generally work in a self-organizing, clustered environment that supports either a single application or collaborative applications. WSN network design requires trade-offs in throughput and latency to extend network lifetimes.

Given such a diverse set of applications and requirements [19], it should come as no surprise that the constraints which guide the design and deployment of wireless sensor networks differ, sometimes substantially, from those that hold in wireless ad hoc networks [20]. Following are the constraints, discussed in more detail.

- ***ENERGY EFFICIENCY:*** Probably the most important difference is due to the fact that sensor nodes typically operate on limited battery power, which means that the maximization of network lifetime (and, consequently, minimization of power consumption) is a sine qua non for sensor networks. On the contrary, power consumption is seldom the critical requirement for ad hoc networks.

  According to [21], the constraint of minimal energy consumption translates into two distinct, yet closely related design requirements:

  1. The communication efficiency has to be maximized through the design of simple yet flexible and effective communication protocols and functions.
  2. Those protocols and functions have to be implemented by small chips with limited computational and memory resources.

  Simultaneous achievement of these objectives necessitates some kind of cross-layer protocol optimization in which the MAC layer would use the information obtained from, and control the operation of the PHY layer. At the same time, optimal operation of the upper, network and transport layers requires the knowledge of appropriate information from both the PHY and MAC layers. Again, such tight integration is not too common in ad hoc networks. An important consequence of the requirement for energy efficiency is the limited transmission range of most sensor node radio subsystems; few real devices have a transmission range of more than 100 meters (300 feet), and ranges of 10 meters (30 feet) and even less are not uncommon.

- ***PROTOCOL EFFICIENCY:*** Regarding communication protocols, the main sources of inefficiency are packet collisions, but also overly complex handshake protocols, receiving packets destined for other nodes, and idle listening to the medium [22]. Actual power consumption of sensor nodes, often called motes,

depends mostly on the radio subsystem and its operating mode. In most (but not all) cases, transmitting and receiving use about the same amount of energy, depending on the power level used for transmission. However, most savings can be made by putting the node to sleep, when power consumption drops by one to two orders of magnitude, depending on the hardware [23, 24].

- ***USE OF REDUNDANT SENSORS:*** Since nodes are small and cheap to produce and the network lifetime needs to be maximized, it is often feasible to deploy the sensors in a given physical space in much larger numbers than necessary to obtain the desired rate of information flow. If redundant sensors are used, they can be periodically sent to sleep in order to minimize their duty cycle, which extends the lifetime of individual sensors and of the entire network and reduces or eliminates the need for operator intervention, thus reducing the operational cost of the network [25] . The use of redundant sensors has profound implications on the design of MAC protocols.
- ***NODE SPECIALIZATION:*** Another important distinction is related to the role of individual nodes. An ad hoc network allows its nodes to choose the specific role, or roles, they would like to play – i.e., data source, destination, or intermediate router – at any given time. In most cases, a node is free to switch to a different role, or roles, whenever it finds appropriate or is instructed to do so by the specific application currently executing on it. On the contrary, nodes in a sensor network have specific roles that do not change often, or never change at all. Most of the nodes act as sensing nodes, some act as intermediaries which route the traffic and (possibly) perform some administrative duties, and a small number of nodes (sometimes only a single node) act as the network sink (or sinks) toward which all the sensed data ultimately flows [26] . A group of sensor nodes under the control of an intermediary is sometimes referred to as a sub-network or cluster, while the intermediary itself is known as cluster head. The number of intermediate levels interposed between the sensing nodes and the network sink(s) depends on a number of variables such as the size of the network, the size of the physical space which the network has to monitor, the transmission range of individual nodes, and (to some extent) the actual MAC protocol used.
- ***TRAFFIC CHARACTERISTICS:*** The traffic in sensor networks is rather asymmetric, as the bulk of it flows from the sensing nodes toward the network

sink (this is often referred to as the uplink direction). The traffic in the opposite direction is generally much smaller and consists of control information and, possibly, queries issued by the network sink on behalf of the corresponding sensing application [27]. Furthermore, traffic patterns in sensor networks are rather different than in ad hoc networks. For example, temperature or humidity monitoring might require periodic or nearly periodic transmissions – in essence, synchronous traffic with low data rate – while object surveillance and other event-driven sensing applications exhibit low average traffic volume and random bursts with considerably higher peak rates. Furthermore, data packets are often much smaller in sensor networks. Original data from sensing nodes typically consists of only a few data values reported by appropriate sensors. Intermediate nodes may choose to aggregate those values in order to improve energy efficiency and reduce bandwidth and energy consumption; data aggregation is more common in networks with a larger number of hierarchical levels. At the same time, the number of sensor nodes and their spatial density may be very large, depending on the size of the space to be monitored and the requirements of the sensing application.

- ***QUALITY OF SERVICE REQUIREMENTS:*** Delay considerations are of crucial importance in certain classes of applications, for example, in military applications such as battlefield communications and detection and monitoring of troop movement, or in health care applications where patients in special care units must be monitored for important health variables (via ECG or EEG) due to a serious and urgent medical condition. Maintaining prescribed delay bounds in a network of resource-constrained nodes with limited transmission range is a complex issue. Low delays can be achieved either by bandwidth reservation, as utilized in variations of the TDMA approach, or by some kind of admission control that will prevent network congestion, if the CSMA approach is used. At the same time, the requirement for maximum throughput is relaxed due to the following. First, the exact value of the throughput requirement is usually prescribed by the sensing application, unlike general networks where the goal is to obtain as much throughput as possible. Second, energy efficiency dictates the use of protocols that incorporate power control, which will strive to keep the nodes inactive for as long as possible [25]. In order to obtain the desired throughput, it suffices to adjust the mean number of active nodes. Even packet losses can be

catered to in this manner, since we don't care whether a given packet from a given node will reach the network sink – as long as the sink receives sufficient number of packets from other nodes. Any packet loss can be compensated for (in the long term) by varying the mean number of active nodes. In a certain sense, fairness is not needed at the node and packet level as long as it is maintained at the cluster level [28]. On the contrary, fairness at the node/packet level is important in ad hoc networks.

- ***DIFFERENCES FROM AD HOC NETWORKS:*** The requirements outlined above lead to a number of important differences between sensor networks and ad hoc networks, most notably the following:
  - Power efficiency and lifetime maximization are the foremost requirements for sensor networks.
  - Self-organization is important in both ad hoc and sensor networks. In the former case, this is due to dynamicity and node mobility, which cause frequent topology changes and make self-organization more difficult; in the latter, this is mostly caused by sensor nodes exhausting their battery power (i.e., dying), although mobile sensors are used in some applications.
  - Throughput maximization is often required in ad hoc networks but is not too common in sensor networks.
  - Delay minimization is typically assigned much higher priority in sensor networks than in their ad hoc siblings. The use of redundant sensors allows for a certain level of fault tolerance; on the contrary, packet losses are intolerable in ad hoc networks.
  - Scalability is an important issue due to the potentially large number of sensors; scalability is also important in ad hoc networks, but it is limited by the available bandwidth and the desired throughput.
  - Nodes in ad hoc networks are often mobile, while most sensor networks have no mobile nodes.

In more than one sense, wireless ad hoc networks are a class of networks with flexible topology but without infrastructure, that should cater to all kinds of networking tasks. On the other hand, sensor networks are highly specialized networks that perform a rather restricted set of tasks under severe computational and communication restrictions.

Summary:

This chapter describes classification of Networks on the bases of Wired, Wireless and Hybrid Communication Network. The various constraints, characteristics and parameters of WSN are also discussed.