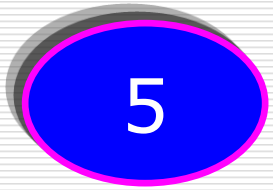


Some Protocols for Industrial Wireless Networks

Dr. H. K. Verma

Distinguished Professor (EEE)

Sharda University, Greater Noida

(Formerly: Deputy Director and Professor of Instrumentation

Indian Institute of Technology Roorkee)

Website : profhkverma.info

CONTENTS

Wired and Wireless LANs

- Depending on the signal transmission medium (STM) used in LAN, it may be:
  - Wired LAN (referred to simply as LAN), or
  - Wireless LAN (referred to as WLAN)
- Wired LAN uses either copper wires or optical fibre as STM.
- WLAN uses either radio-frequency or infrared transmissions and does not require any wires (copper wires or optical fibre).

WLAN: Advantages & Issues

Advantages of WLAN

- Easy and fast deployment
- Nomadic and mobile access
- Connecting field devices in difficult-to-access or inaccessible locations.

Major Issues with WLAN

- Noise and interference
- Interception & eavesdropping
- Jamming.

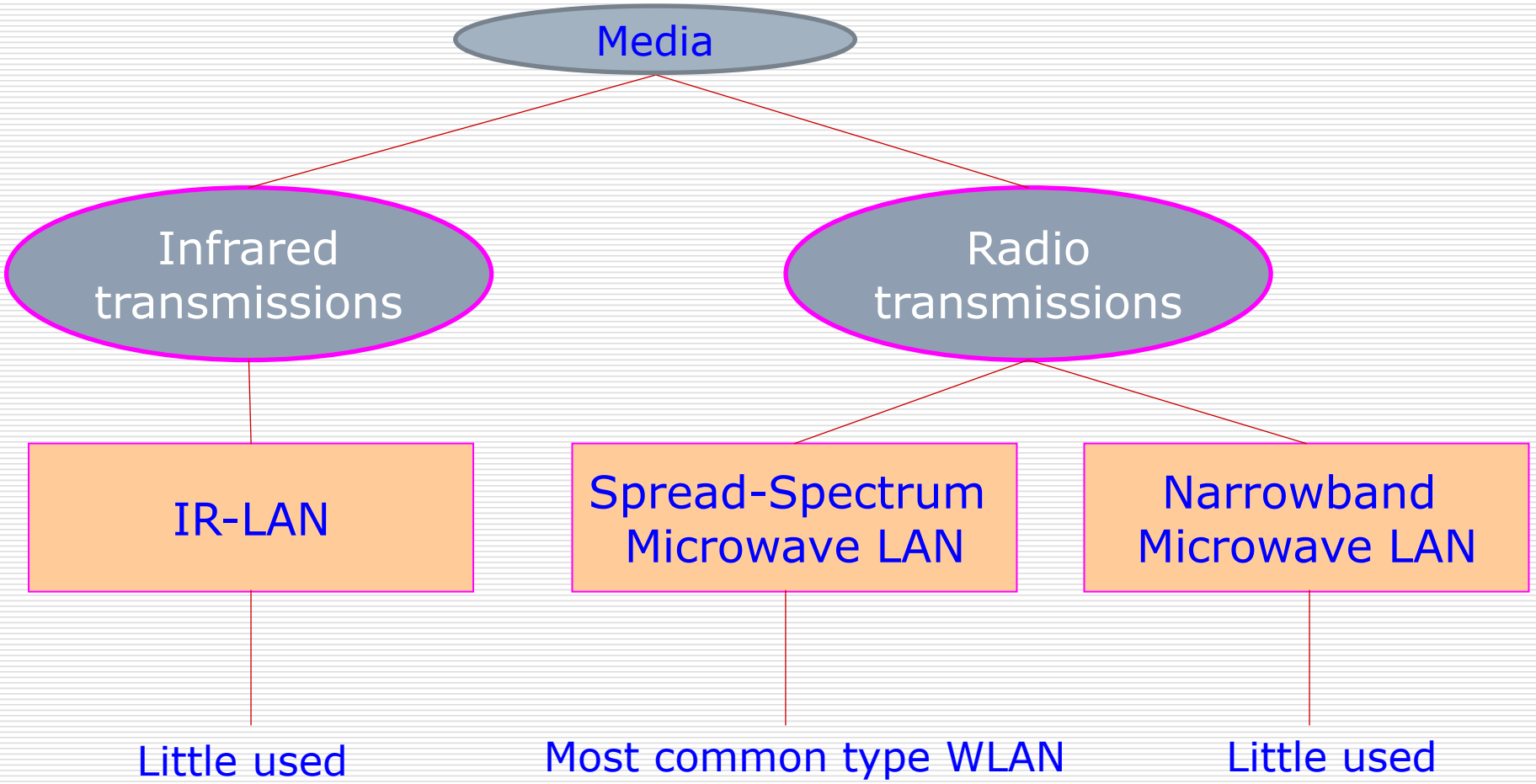
Additional Issue with Industrial WLAN

Strong noise and interfering signals are often present in industrial environment, which may severely effect working of WLANs in industry.

Requirements of WLAN Protocol

1. The protocol should support large number of nodes.
2. Connection to wired-backbone LAN should be easy
3. Adequate range
4. Low power consumption for long battery life
5. Security against noise and interference
6. Security against interception and eavesdropping
7. Security against jamming
8. License-free operation (using ISM frequency bands).

Media for WLAN



Infrared (IR) LAN

- Infrared portion of spectrum is used
- Mostly deployed in homes, within a room
- Common for remote-control devices
- Transmission techniques
  - Directed-beam IR
    - Point-to-point link
    - Ring WLAN
  - Omni-directional IR
    - Broadcasting from ceiling transmitter
    - Radiations in all directions
  - Diffused IR
    - Relies on diffusely-reflecting ceiling

Drawbacks of Infrared LAN

- Background radiations from sunlight and indoor lighting appear as noise
- Large power IR transmitter (for high SNR) can lead to:
  - Issues of eye safety
  - Excessive power consumption

Spread Spectrum LAN

- Spread-spectrum is a **group of modulation techniques** by which a signal generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider spectrum or bandwidth.
- Reasons for using these techniques:
  1. To secure communications by increasing resistance to interference, noise, and jamming,
  2. To increase data security by preventing detection,
  3. To enable multiple-access communication.

Spread Spectrum Techniques

- Following spread-spectrum techniques are available:
  A. Frequency-hopping spread spectrum (FHSS)
  B. Direct-sequence spread spectrum (DSSS)
  C. Time-hopping spread spectrum (THSS)
  D. Chirp spread spectrum (CSS)
  E. Combinations of these techniques
- The first two of these techniques (FHSS and DSSS) are very widely used.
- Both FHSS and DSSS employ pseudo-random number sequences to determine and control the spreading pattern of the signal across the allocated bandwidth.
- Pseudo-random number sequences are created using pseudo-random number generators.

Frequency-Hopping Spread Spectrum (FHSS)

- It is a method of transmitting radio signals by rapidly changing the carrier frequency among many distinct frequencies occupying a large frequency band.
- The changes are controlled by a code known to both transmitter and receiver.
- The code is based on creating a pseudo-random number sequence.
- Available frequency band is divided into smaller sub-bands.
- Signal rapidly changes its carrier frequency (called as hopping) among the centre-frequencies of these sub-bands in a predetermined (pseudo-random) order.
- Interference at a specific frequency will only affect the signal during a short interval, while providing no extra protection against wideband noise.

Benefits of FHSS

1. FHSS signals are highly resistant to narrow-band interference because the signal keeps hopping from one frequency sub-band to another frequency sub-band.
2. Signals are difficult to intercept, if the frequency-hopping pattern is not known.
3. Jamming is also difficult if the pattern is unknown. A malicious individual may be able to jam the signal for a single hopping period only, if the spreading sequence is not known.
4. FHSS transmissions can share a frequency band with many conventional transmissions with minimal mutual interference. This is because FHSS signals add minimal interference to narrowband communications, and vice versa.

Direct-Sequence Spread Spectrum (SS)

- In DSSS, the message bits are modulated by a pseudo-random bit sequence, known as **spreading sequence**.
- Each bit in the spreading-sequence is known as a chip and has a much shorter duration (larger bandwidth) than the original message bits.
- The modulation of the message bits scrambles and spreads the pieces of data, and thereby results in a bandwidth size nearly identical to that of the spreading sequence.
- The spreading sequence created by transmitter is known to receiver. Receiver uses the same spreading sequence to demodulate the received signal in order to reconstruct the information signal.
- The smaller the chip duration, the larger the bandwidth of the resulting DSSS signal and better the resistance against interference.

Benefits of DSSS

1. High resistance against interference.
2. High resistance to unintended and intended jamming
3. The code division multiple access (CDMA) property of DSSS allows multiple transmitters to share the same channel within the limits of the cross-correlation properties of their spreading sequences.

Requirements of Device-Level WLAN

- Low latency or small end-to-end delay
- Low bandwidth (which will mean a low data rate)
- High data security
- High network security
- Low power consumption:
  Important specially in case of battery-operated wireless sensor nodes used in wireless sensor networks (WSNs).

Protocols for WLANs

- Probably, the most common protocols for WLANs are:
  - Zigbee / IEEE 802.15.4
  - WiFi / IEEE 802.11
  - Bluetooth / IEEE 802.15.1

- Following is the scenario of their application:

(a) Zigbee / IEEE 802.15.4
  - Most suitable and most popular for device-level WLANs used in industrial automation.
  - Less suitable and less popular for business WLANs.

(b) WiFi / IEEE 802.11
  - Most suitable and most popular for business WLANs
  - Less suitable and less popular for industrial WLANs.

(c) Bluetooth / IEEE 802.15.1
  - Has limited application for business WLANs
  - Rarely used in industrial application.

Zigbee/IEEE 802.15.4 Protocol (1)

- Zigbee protocol addresses needs of industrial measurement and control (automation)
- Promoted by Zigbee Alliance, a consortium of 150^{+} companies
- Includes Honeywell, Motorola, Phillips, Samsung, Mitsubishi
- Zigbee conforms to IEEE 802.15.4 standard
- IEEE 802.15.4 is "Low-Rate Wireless PAN Standard"
- **IEEE 802.15.4 defines only Physical and MAC layers**
- Zigbee supports networking of fixed, portable and moving devices.

Zigbee/IEEE 802.15.4 (2)

- Developed to meet special requirement of wireless sensor and actuator networks, namely
  - Low bandwidth
  - Low latency
  - Long battery life
  - High data security

- Not attractive for business communication networks because of low data rate.
- Frequency bands used:
  - ISM-900: Channel BW = 2MHz, Data rate = 20 & 40 kbps
  - ISM-2.4: Channel BW = 5MHz, Data rate = 250 kbps

Zigbee/IEEE 802.15.4 (3)

- Data rates: 20 & 40 kbps with ISM-900 & 250 kbps with ISM-2.4.
- Transmitter power: 1 mw or more
- Range: 10 m or more
- Topologies supported**: Star and Mesh**
- Device addressing: Dynamic
- Modulation technique: **DSSS**
- Supports wireless ad-hoc networks (WANETs), which do not rely on pre-existing infra-structure.
- Supports multi-hop routing, which can be used to effectively increase the range of Zigbee network.

IEEE 802.15.4 Specified Devices

IEEE 802.15.4 standard specifies 2 types of devices:

(a) Full-Function Device (FFD)

- Can talk to any other device
- Can perform job of Network Coordinator (NC) or PAN Coordinator
- Can also function as a normal device.

(b) Reduced-Function Device (RFD) or Normal Device

- Simpler in design and cheaper than FFD
- Can function only as an end device (terminal node)
- Can't function as Network Coordinator
- Can talk to FFD only.

Network or PAN Coordinator

- Network communications are mostly initiated by network coordinator (NC), also called as PAN coordinator.
- Can communicate directly with any device
- Transmits ‘beacon’ in ‘beaconing system’ used for ‘periodic data transfer’ (this is explained in a later slide)
- There is only one node in a network functioning as the network coordinator.

IEEE 802.15.4 MAC Protocol

- MAC protocol specified in IEEE 802.15.4 is **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**
- A node intending to access the medium for transmission of data senses the presence of carrier and **transmits data only if no carrier is present**
- **Data transfer modes are designed to avoid collisions**
- The protocol supports 3 types or modes of data transfers:
  1. Periodic data transfer
  2. Intermittent data transfer
  3. Guaranteed time-slot data transfer

Three Types of Data Transfers

1. Periodic Data Transfer

- Data is transferred **periodically** at a pre-programmed rate.
- A beaconing system is used to handle data transfers in this mode
- Beacon is sent by Network Coordinator (NC) periodically
- Device wakes up, sends data if any, and then goes back to sleep mode.
- Period can vary from 15.36 ms to 15.36 x 2^{14} ms $\cong$ 4 min
- This period is **a trade off between message latency and power consumption**

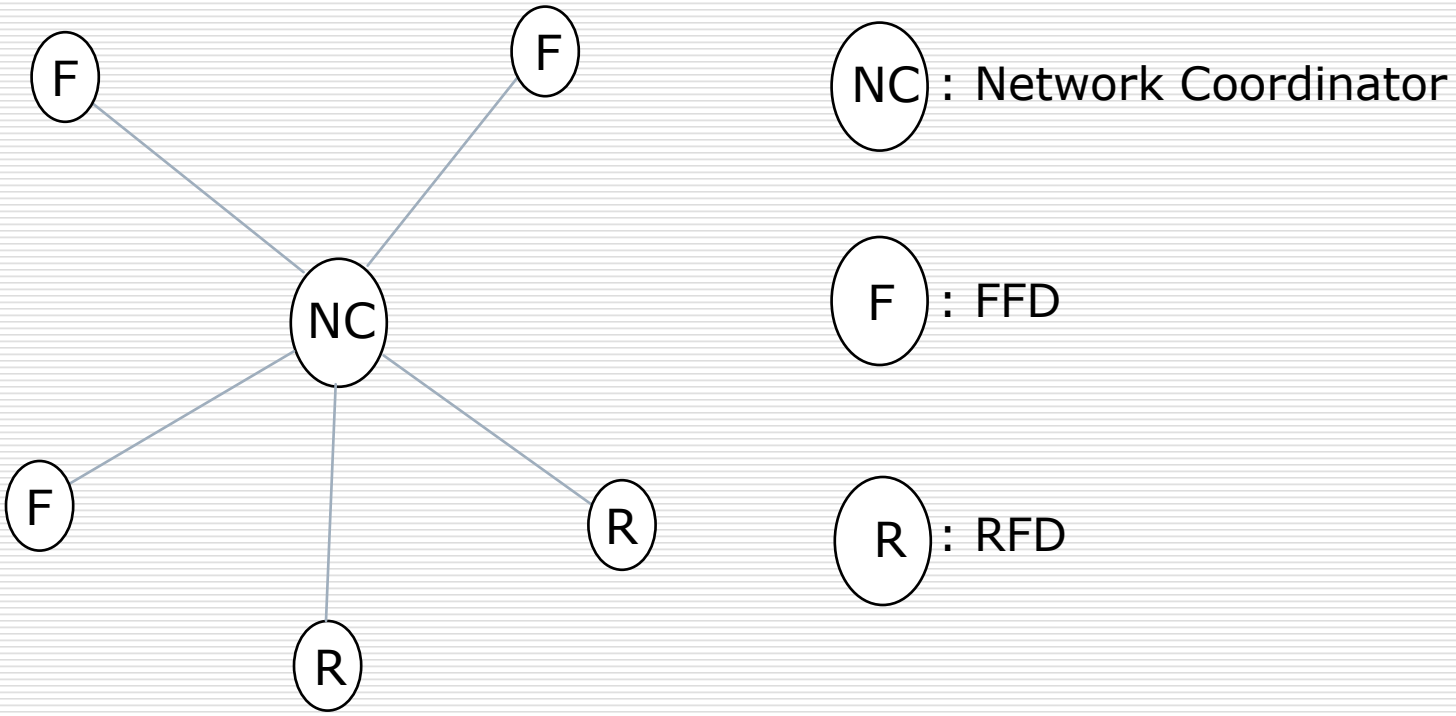
2. Intermittent Data Transfer

- NC sends message to a selected node **as and when data is required** from the node.
- Beaconless mechanism
- Device sleeps most of time, so it is **power saving mode** of data transfer.

3. Guaranteed Time-Slot Data Transfer

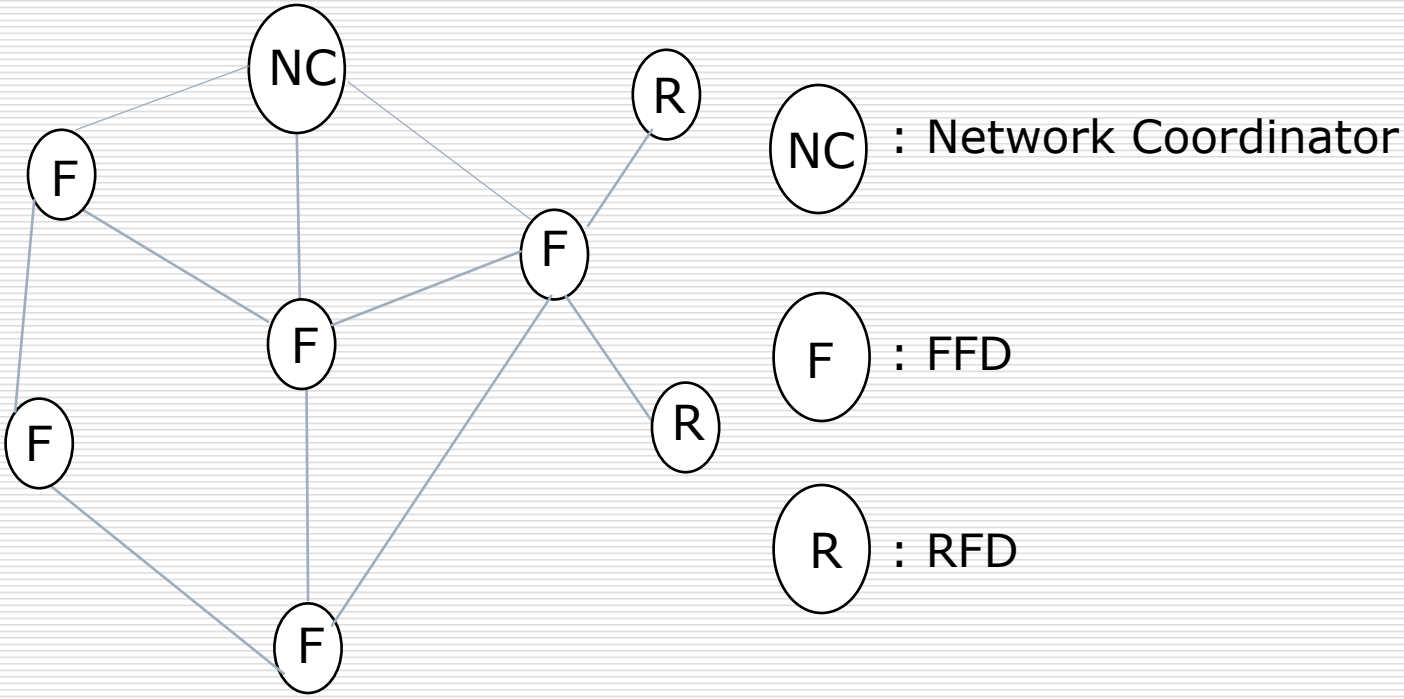
- Time is **allotted to each device** to transmit data without contention.
- It is **low-latency mode** of data transfer.

Zigbee Star Topology



- Network Coordinator (NC) forms central node
- Network Coordinator has to be an FFD
- Each other node can be either an FFD or an RFD.

Zigbee Mesh Topology



- Every node in the mesh is connected to other nodes by radio signals
- All **nodes in the mesh** are FFDs
- One of FFDs is configured as Network Coordinator (NC)
- RFDs can be connected as **end devices** to a node in the mesh.

Advantages and Limitations of Zigbee

- Advantages of Zigbee
  - Low latency
  - Low energy requirement
  - Ad-hoc networking
  - Multi-hop transmission

- Limitations of Zigbee
  - Low data rate
  - Small range

WiFi/IEEE 802.11

- WiFi means Wireless Fidelity.
- IEEE 802.11 is “Wireless LAN Standard”
- WiFi Alliance, formed in 1999, promotes WiFi protocol/technology
- WiFi Alliance was earlier known as “Wireless Ethernet Compatibility Alliance”
- It also certifies IEEE 802.11 products for interoperability
- **IEEE 802.11 specifies only Physical and MAC layers**

IEEE 802.11 MAC Layer

- MAC (Medium Access Control) protocol specified in IEEE 802.11 is **CSMA/CA** (Carrier Sense Multiple Access with Carrier Avoidance)
- MAC layer supports three WLAN topologies:
  1. Basic Service Set (BSS) : Consists of an access point (AP) plus several wireless nodes.
  2. Extended Service Set (ESS) : It is a set of two or more BSSs forming a single subnetwork.
  3. Independent Basic Service Set (IBSS) : It includes a number of wireless nodes that communicate directly with one another on a peer-to-peer basis building a full-mesh or partial-mesh topology. None of the nodes has to work as server.
- MAC layer supports two modes of WLAN operation:
  A. Infrastructure mode for BSS and EBSS
  B. Ad-hoc mode for IBSS

IEEE 802.11 Physical Layer

- Physical layer specifies three main things:
  1. Frequency spectrum or ISM band
  2. Transmission method
  3. Data rate
- Original IEEE 802.11 and its popular **extensions** are as under:
  - IEEE 802.11 - 1997 (original) : specifies Physical and MAC layers
  - IEEE 802.11b - 1999 : Specifies Physical layer only
  - IEEE 802.11a - 1999 : Specifies Physical layer only
  - IEEE 802.11g - 2002 : Specifies Physical layer only

Summary of IEEE 802.11 Standards

MAC layer	CSMA/CA					
Physical layer	**IR**	**2.4 GHz**	**2.4 GHz**	**2.4 GHZ**	**5 GHz**	**2.4 GHz**
	850-950 nm	FHSS	DSSS	DSSS	OFDM	OFDM
	1, 2 Mbps	1, 2 Mbps	1, 2 Mbps	11 Mbps max.	54 Mbps max.	54 Mbps max.
Standard	IEEE 802.11 (original)			802.11b	802.11a	802.11g
Year published	1997			1999	1999	2002

OFDM : Orthogonal frequency division multiplexing

Bluetooth / IEEE 802.15.1

- Bluetooth technology was conceived in 1994
- Developed as robust, secure, short-range wireless communication protocol
- Supported by Bluetooth Special Interest Group (SIG) setup in 1998
- Bluetooth SIG has 9 members: Ericson, Nokia, IBM, Intel, Microsoft, Lucent, 3 COM, Motorola and Toshiba
- Bluetooth protocol is currently an industry standard for wireless linking of office and home equipment/gadgets/devices.
- A **"host device"**, such as laptop PC, desktop PC or mobile phone is linked wirelessly to one or more **"Bluetooth devices"**, such as wireless mouse, printer, wireless headset, etc.
- Bluetooth protocol conforms to IEEE standard 802.15.1.

Key Features

- Ad-hoc network technology
- Protocol supports both voice and data communication
- Frequency band: ISM-2.4 GHz
- Transmission method: FHSS
- Frequency Hopping: BW split into 79 hops
  1600 hops/s
- Each hopping frequency displaced by 1 MHz
- Some countries use smaller number of hops
- Modulation method: GFSK (Gaussian frequency shift keying)
- Transmission rate: upto 1 Mbps

Power and Range

- Three power classes (transmitter powers) specified
  - Class 1: 100 mW or 20 dBm
  - Class 2: 2.5 mW or 4 dBm
  - Class 3: 1 mW or 0 dBm

- Ranges specified
  - Class 1: 100 m (extended range devices)
  - Class 2: 10 m (normal range devices)
  - Class 3: 1 m (short range devices)

Bluetooth-Supported Products/Gadgets

- Laptop PC
- Desktop PC
- Printer
- Mouse
- Cellular (mobile) phone
- PDA
- Watch
- Wireless headset
- Wireless speaker
- Camera
- Etc.

Merits & Limitations

- Merits
  - Low power consumption
  - Secure connection
  - Low cost
  - Ease of use
  - Globally accepted specifications
  - Wide range of devices

- Limitations
  - Low data rate
  - Small range (pico-nets)
  - Short packets

Comparison of Zigbee, WiFi & Bluetooth (1)

S.No.	Feature	Zigbee	WiFi	Bluetooth
1	Governing standard	IEEE-802.15.4	IEEE-802.11	IEEE-802.15.1
2	Data rates	20, 40 and 240 kbps	2, 11 and 54 Mbps	1 Mbps
3	Range	50-100 m	200-500 m	1-10 m
4	Network size	Personal area network	Local area network	Pico-net
5	Topologies supported	Star and Mesh	BSS, EBSS and IBSS	Mesh
6	ISM frequency bands	900 MHz 2.4 GHz	2.4 GHz & 5 GHz	2.4 GHz
7	MAC	CSMA/CA	CSMA/CA	CSMA/CA
8	Modes supported	Ad-hoc	Ad-hoc Infrastructure	Ad-hoc
9	Routing	Multi-hop	Single-hop	Single-hop

Continued

Comparison of Zigbee, WiFi & Bluetooth (2)

S. No.	Feature	Zigbee	WiFi	Bluetooth
10	Modulation technique	DSSS	DSSS/ FHSS/ OFDM	FHSS
11	Latency	Very low (≤30 ms)	High (≤3 s)	Very high (≤10 s)
12	Network scalability	Very high (65,000 nodes)	Good (255 nodes)	Poor (7 nodes)
13	Power consumption	Very low	High	Medium
14	Data security	Very high	Very high	Very high
15	Major application area	Industrial measurement and control (automation)	Business communi-cations	Pico-net in office/home