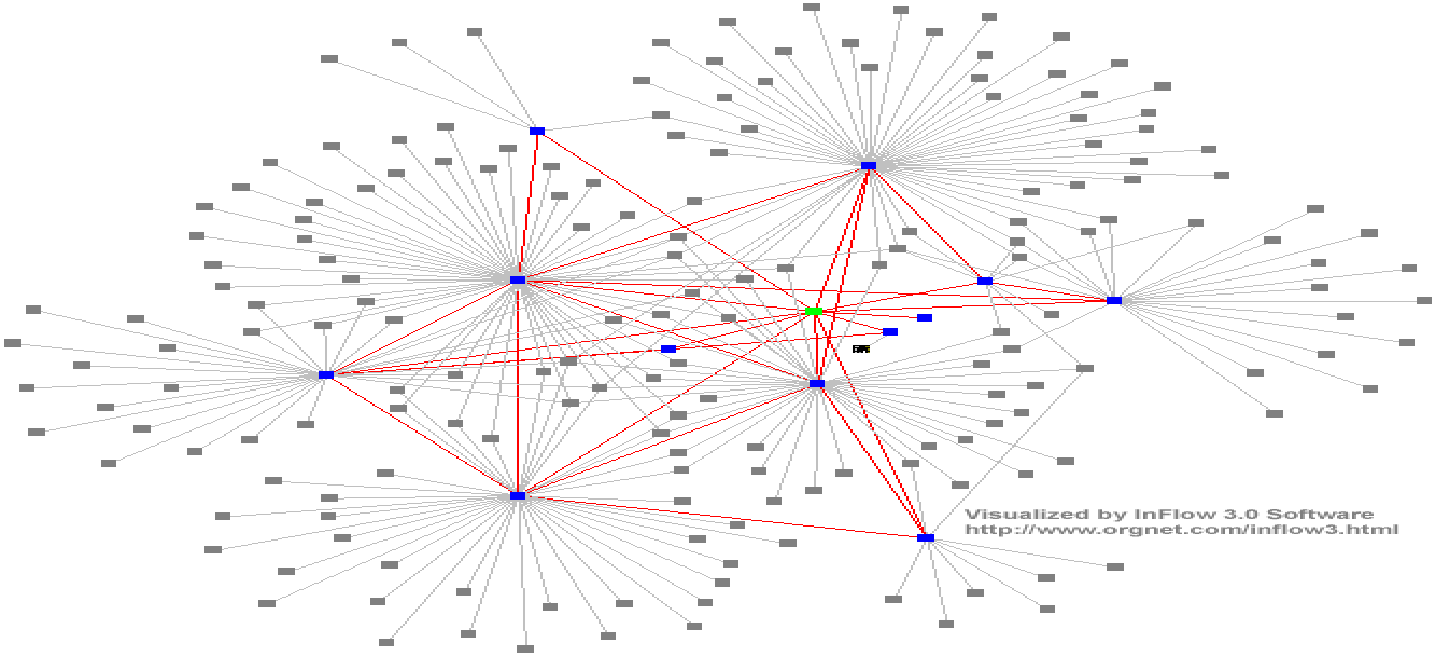
Distributed Computing Systems

Wireless Networking in DS


Visualized by InFlow 3.0 Software
http://www.orgnet.com/inflow3.html

Dr. Sunny Jeong. **spjeong@uic.edu.cn**

Overview

- ❑ Challenges
- ❑ Wi-Fi 802.11
- ❑ Ad-hoc : decentralized network
- ❑ Bluetooth 802.15.1
- ❑ Zigbee 802.15.4
- ❑ RFID

Challenges

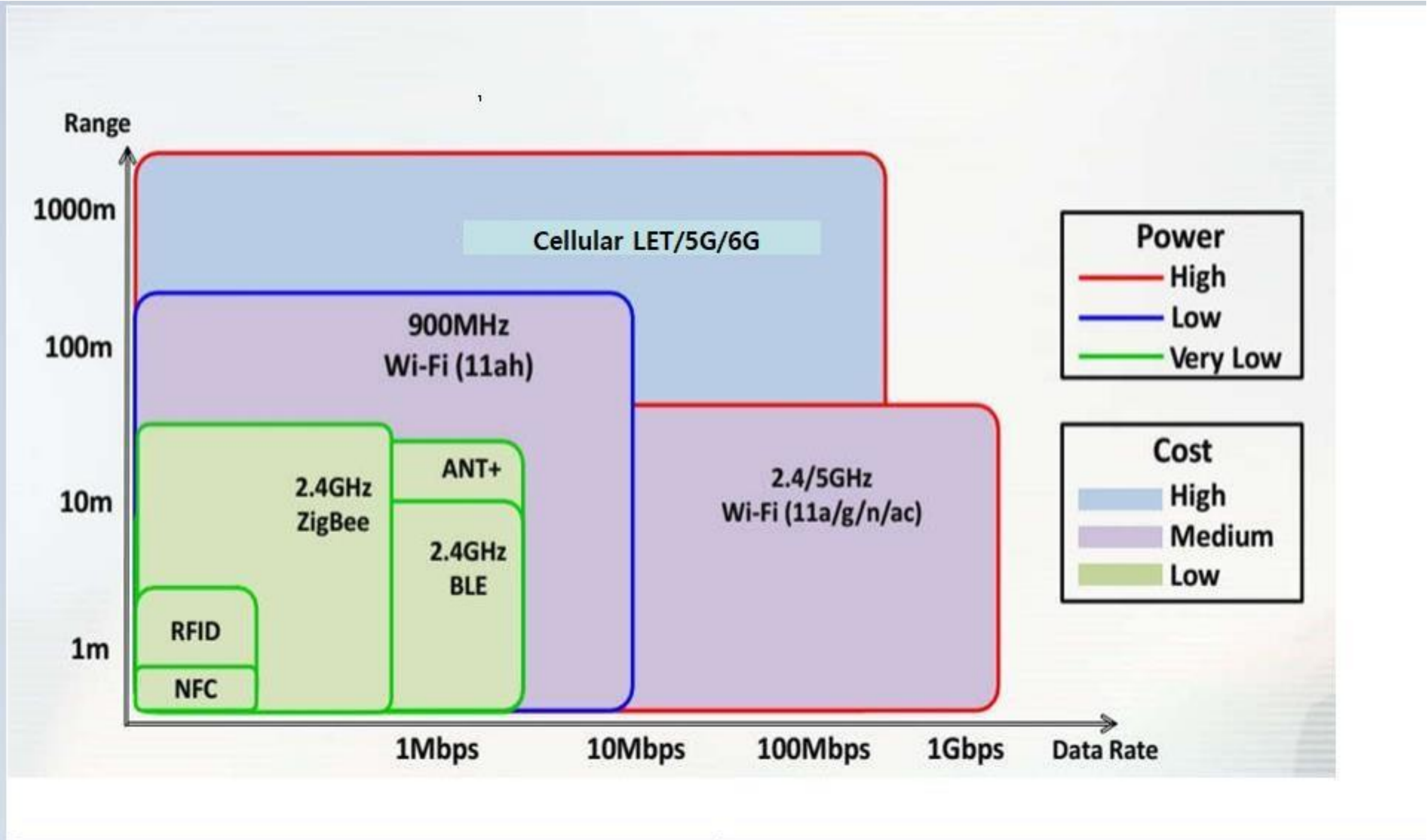
❑ Energy(Cost)

❑ Self-configuring/adapting

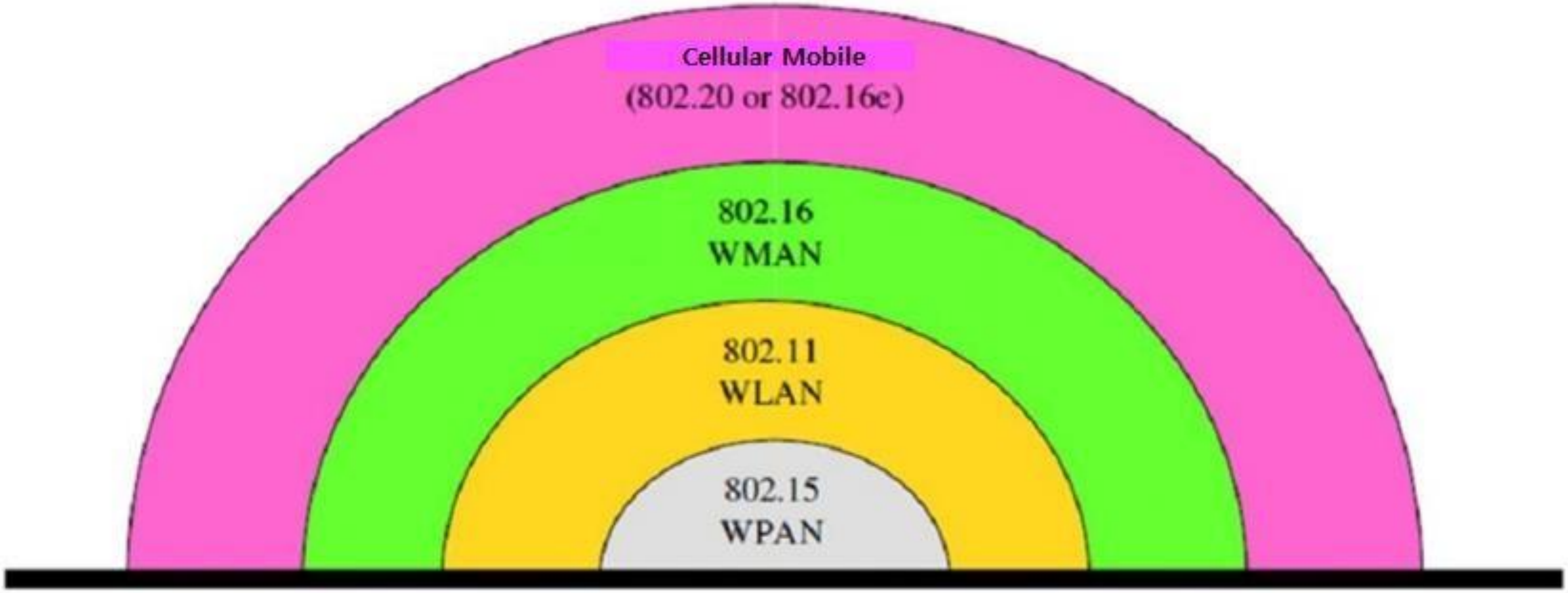
❑ Data processing

❑ Scalability/Mobility

Wireless Power vs. Cost



Wireless Standard Range



WPAN	Bluetooth	Office
WLAN	WiFi	Building/Campus
WMAN	WiMAX	Campus/City
2.5G/3G	Cellular	City/Regional

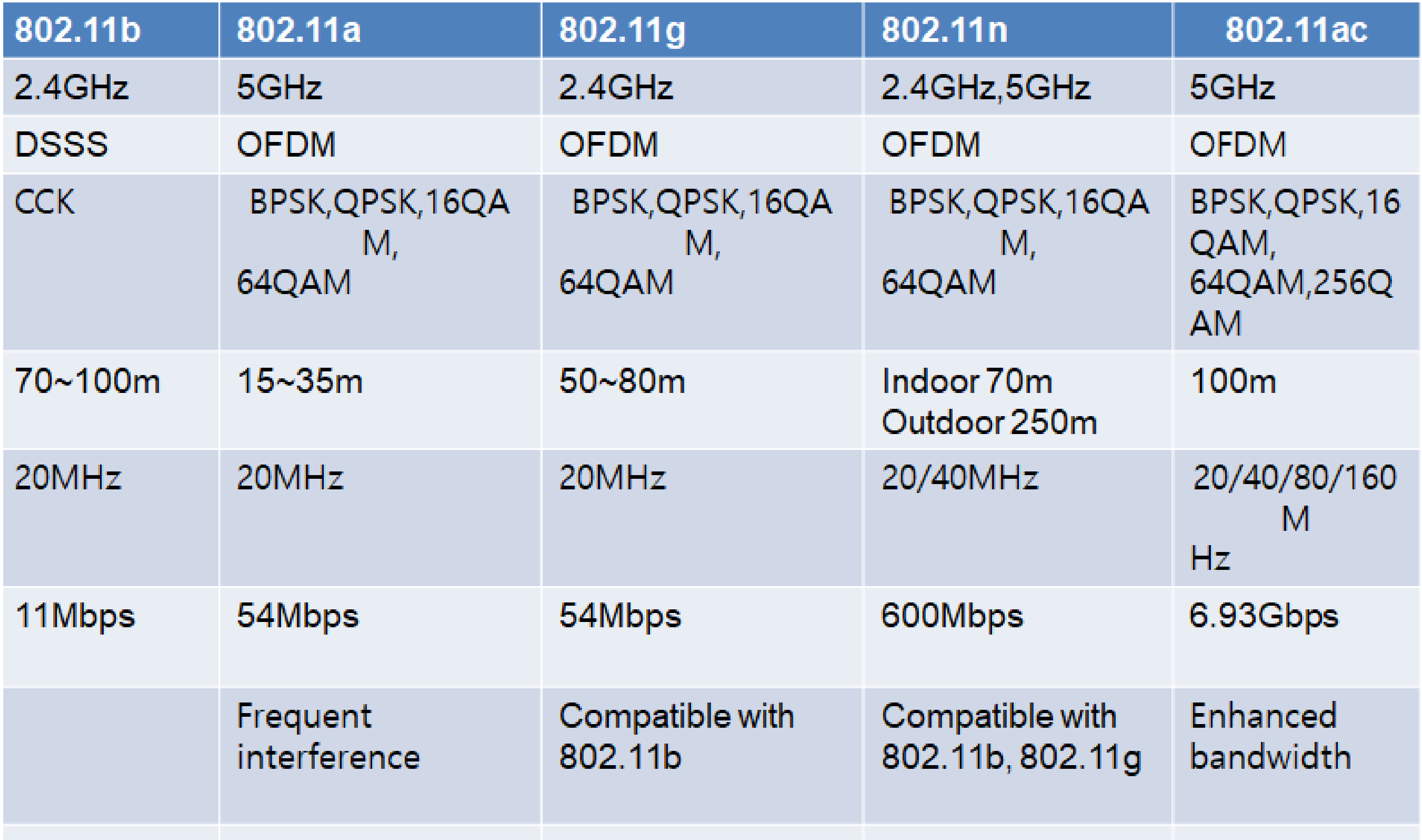
Wireless Connection (Wi-Fi)
IEEE 802.11

- ❑ Short form of Wireless Fidelity. This can be defined as wireless Local Area Networking System. (Wireless LAN)

- ❑ With the help of Wi-Fi, we can access broad band internetconnection with high data transfer rate.

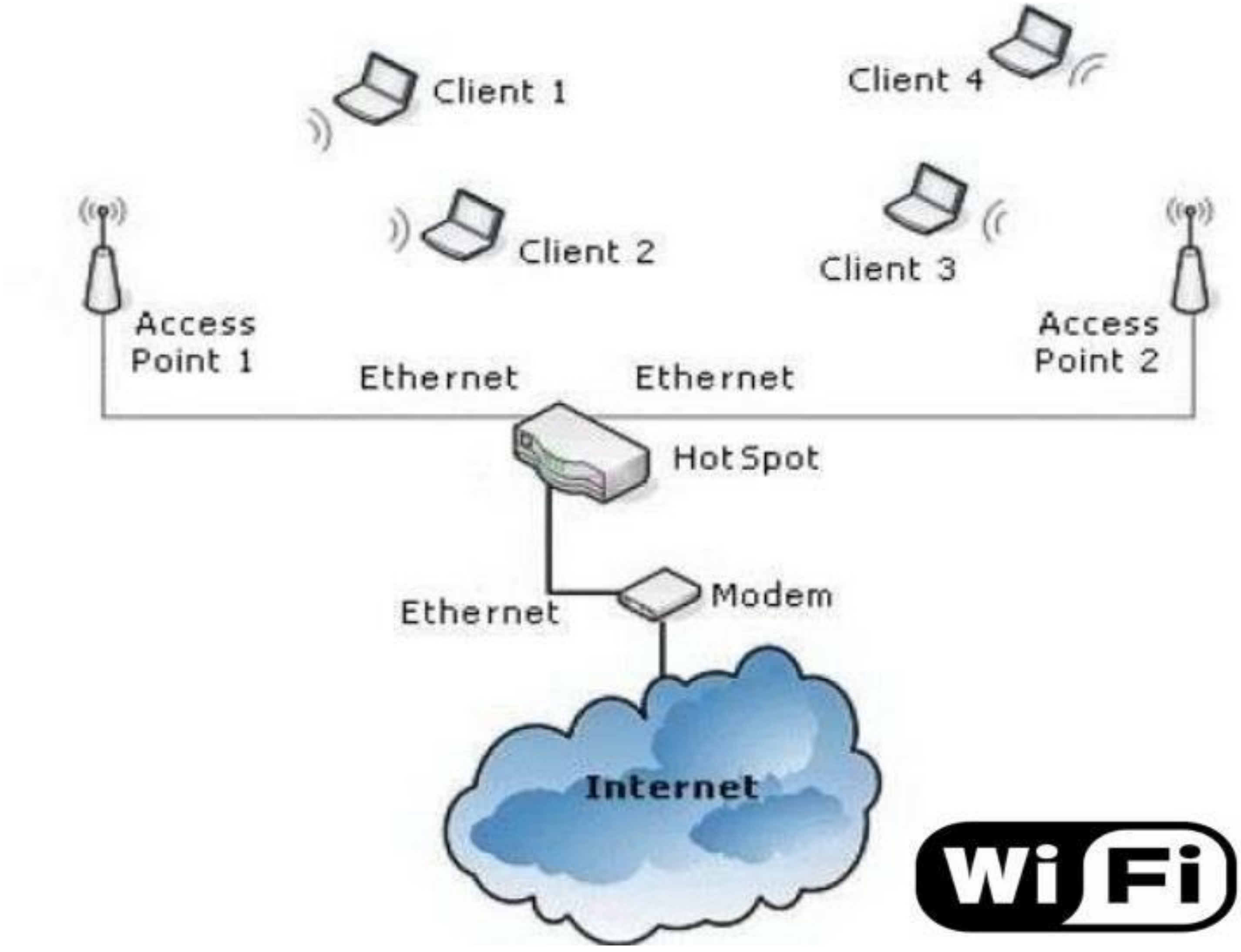
- ❑ The main attractive feature of this technology is that it can provide wireless broadband connection within a specific geographic boundary.

Different Versions of WiFi



802.11b	802.11a	802.11g	802.11n	802.11ac
2.4GHz	5GHz	2.4GHz	2.4GHz,5GHz	5GHz
DSSS	OFDM	OFDM	OFDM	OFDM
CCK	BPSK,QPSK,16QAM, 64QAM	BPSK,QPSK,16QAM, 64QAM	BPSK,QPSK,16QAM, 64QAM	BPSK,QPSK,16QAM, 64QAM,256QAM
70~100m	15~35m	50~80m	Indoor 70m Outdoor 250m	100m
20MHz	20MHz	20MHz	20/40MHz	20/40/80/160 MHz
11Mbps	54Mbps	54Mbps	600Mbps	6.93Gbps
	Frequent interference	Compatible with 802.11b	Compatible with 802.11b, 802.11g	Enhanced bandwidth

Wireless Local Area Networking



Wi-Fi Security

❑WEP stands for Wired Equivalency Privacy(64-128bit)

❑As its name implies, this standard was intended to make wireless networks as secure as wired networks.

❑WPA and WAP2 Wi-Fi Protected Access is an early version of the 802.11i security standard that was developed by the Wi-Fi Alliance to replace WEP.

❑The common key length are 128bit

❑WAP3 **offering stronger encryption and protection against brute-force attacks**

❑ the key length is 256bit : **Simultaneous Authentication of Equals (SAE)**

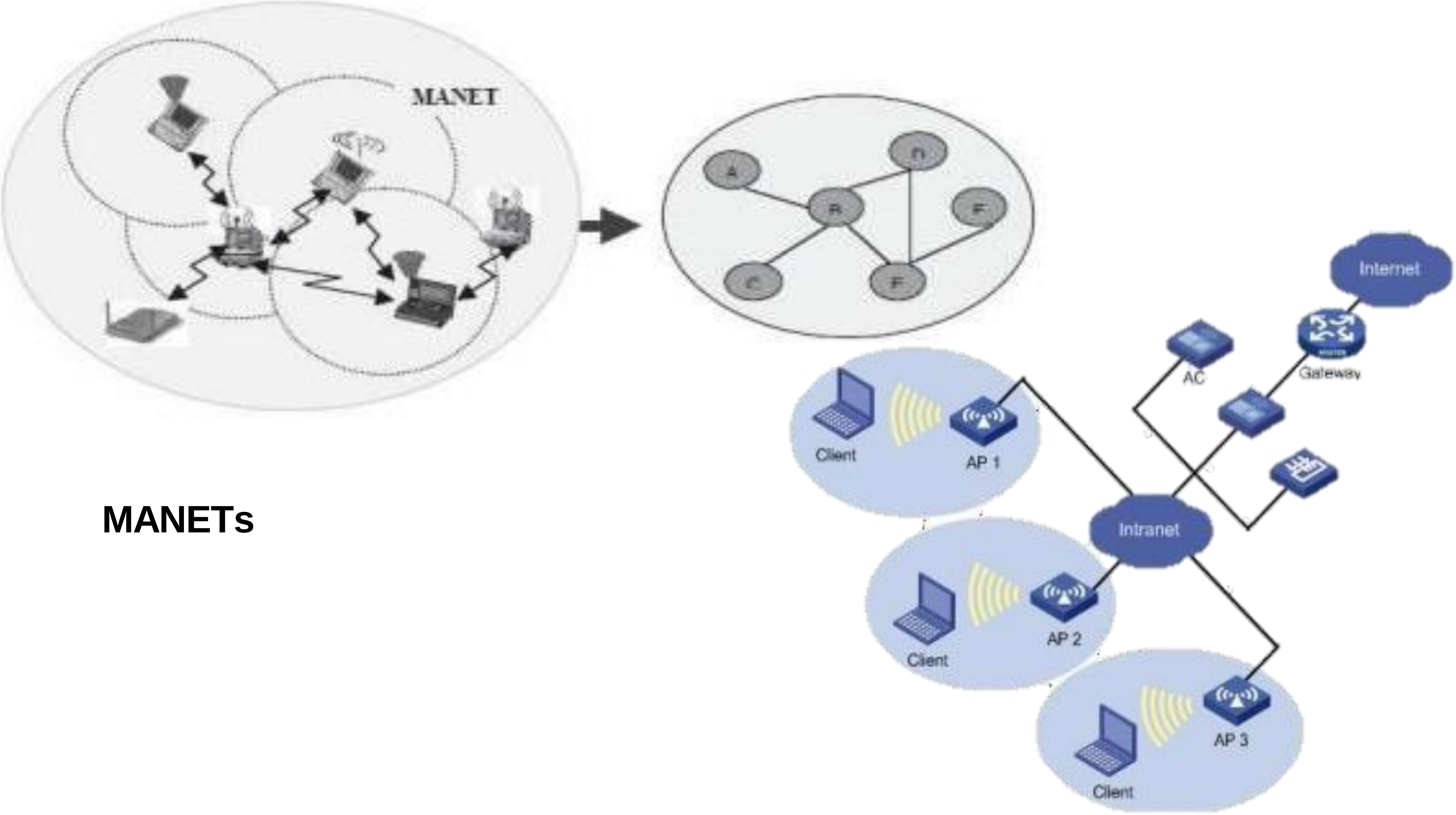
Ad hoc networks

Ad Hoc 网络是指一种没有固定基础设施**（比如基站或路由器）的网**络。

设备之间直接通过无线连接进行通信，就像大家自己组建了一个临时网络一样。

- Mobile ad hoc networks(MANET) are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links.
- No existing fixed infrastructure or centralized administration – No base station.
- Mobile nodes are free to move randomly.
  - Network topology changes frequently.
- May Operate as standalone type or also can be connected to the larger internet.
- Each node works as a router.
- Originated from military purpose

Mobile Ad Hoc NETs



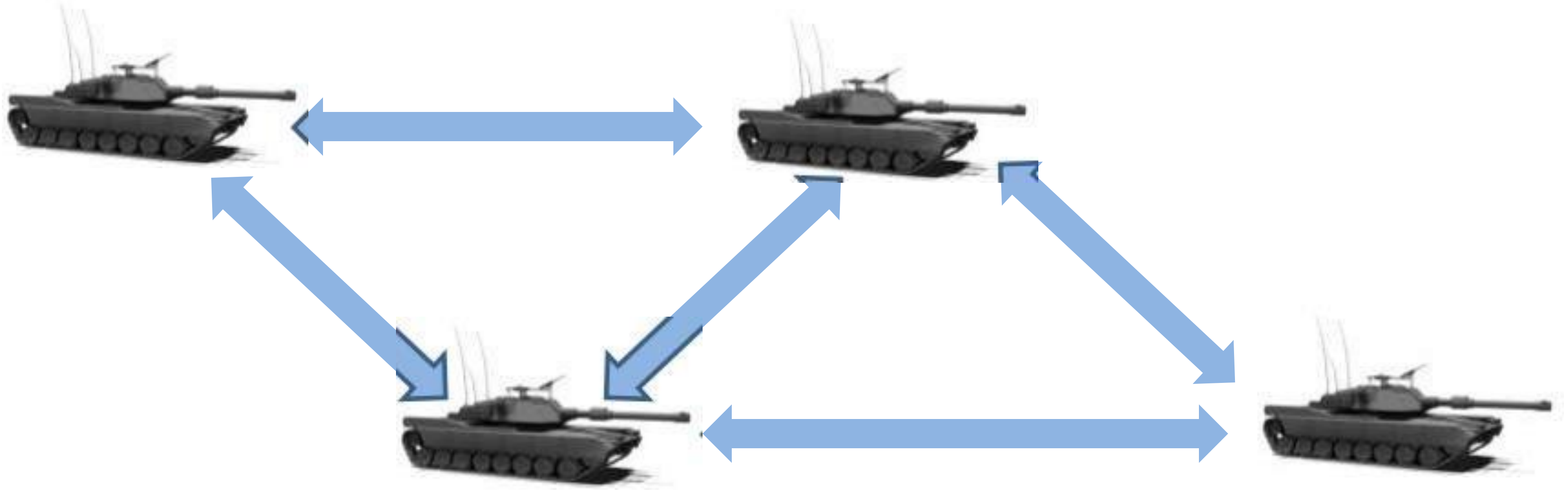
MANETs

WLAN

Origin of Ad Hoc

Incase if we need to exchange information and the network's infrastructure has been destroyed .

It is suitable for military communications at battlefield where there is no network infrastructure.



Advantages

Ad-hoc networks have several advantages over the traditional networks, like:

- Ad-hoc networks can have more flexibility.
- It is better in mobility .
- It can be turn up and turn down in a very short time .
- It can be more economical.
- It considered a robust network because of its non-hierarchical distributed control and management mechanisms .

Applications

- Tactical networks
  - Military communication, automated battlefields
- Emergency Services
  - Search and rescue operations
  - Disaster recovery – Earthquakes, hurricanes .
- Educational
  - Virtual classrooms or conference rooms.
  - Set up ad hoc communication during conferences, meetin
- Home and Entertainment
  - Home/office wireless networking.
  - Personal Area network
  - Multiuser games
  - Outdoor internet access.

Challenges

- Infrastructure less
  - Brings new network designing challenges.
- Dynamically changing topologies
  - Cause route changes, frequent network partitions and packet loss.
- Physical layer limitations
  - Limited Wireless range.
  - Packet loss during transmission.
  - Broadcast nature of the communication.
- Limitations of Mobile Nodes
  - Short battery life
  - Limited capacities.
- Network security.

Effects on the protocol stack

- Application Layer
  - New applications, Authentication, Encryption.
- Transport Layer
  - Congestion Control, Flow control.
- Network
  - Host addressing, Routing, Multicasting.
- Data Link Layer
  - Media Access
- Physical
  - Spectrum usage/allocation

Ad Hoc for Windows

□ >netsh

□ netsh> wlan set hostednetwork mode=allow
ssid=‘*name*’ key=*‘00000000’*

□ netsh> wlan start hostednetwork

Use virtual IP address 192.168.x.x for communication

Medium Access Control (MAC) 协议是什么**？**

这段话主要讲的是 Medium Access Control (MAC) 协议，**尤其是用于** MANET（移动自组网） **中的** 802.11 MAC 协议。

由于 MANET 是无线网络，节点自由移动、没有固定基站，因此存在很多信号冲突和竞争的问题

为什么会有冲突问题**？**

1. 无线信道共享导致冲突

在 MANET **中**，所有节点共用同一个无线传输介质（类似于大家在一个房间里讲话，声音互相干扰）**。**

由于是广播传输，不同设备同时发消息时，**信号会碰撞（冲突）**，导致数据丢失。

这就是所谓的数据包冲突（Packet Collision）和信道竞争（Media Contention）**。**

半双工通信导致无法检测冲突

无线网络通常是半双工通信，也就是说，同一时间只能发送或接收，不能同时进行。

这就导致无法检测冲突，即节点在发送时听不到其他节点也在发，**从而增加了冲突概率。**

因此，传统的有线协议（**如** CSMA/CD）在无线环境中不适用

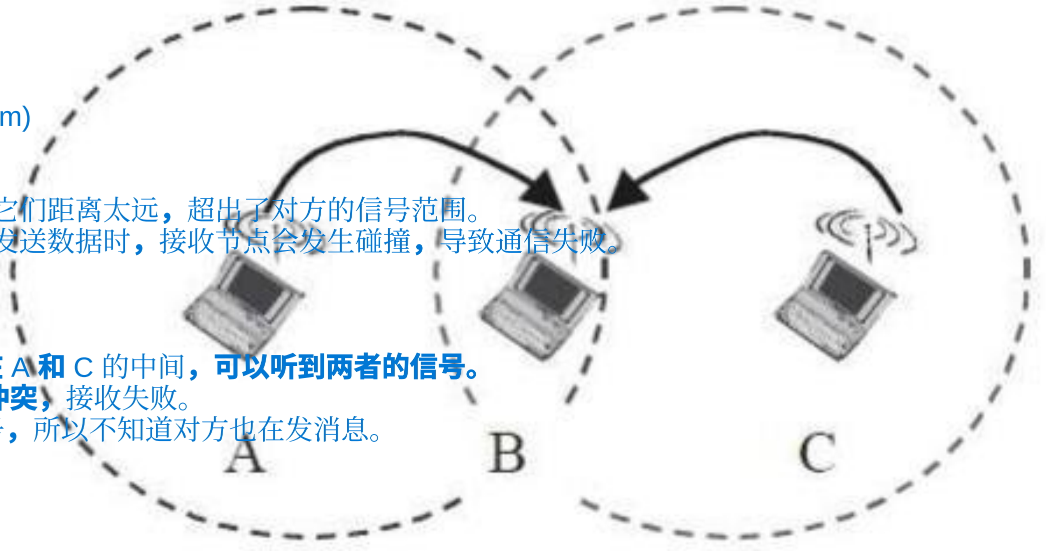
Medium Access Control

(802.11 mac protocol)

- Since MANETs, use broadcasting and shared transmission media, introduces a probability of packet collisions and media contention.
- Since collision detection is not possible with half-duplex radio. This brings new challenges to conventional CSMA/CD-based and MAC based protocols.
- Top issues are the **hidden-terminal** and **exposed-terminal problems.**

Hidden-terminal problem

When two terminals can not detect each other ’s transmission due to being outside of each others range. The collision can occur.



两个主要问题：隐藏终端和暴露终端问题
1. 隐藏终端问题 (Hidden-Terminal Problem)
定义：

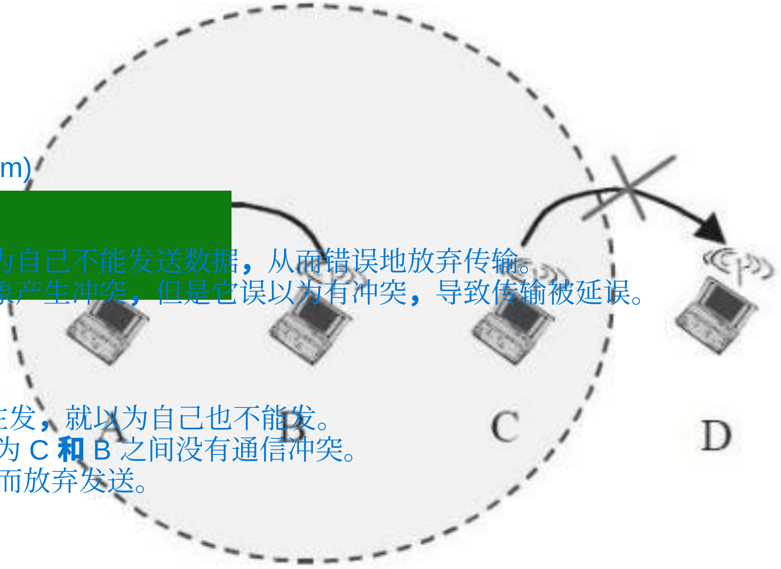
当两个终端彼此听不到对方的传输，因为它们距离太远，超出了对方的信号范围。
但是，这两个终端同时向同一个接收节点发送数据时，接收节点会发生碰撞，导致通信失败。
举个例子：

假设有三个节点：A、B、C。
A **和** C 彼此之间信号范围不重叠，**但** B **在** A **和** C 的中间，**可以听到两者的信号。**
当 A **和** C 同时发送数据到 B 时，B **信号冲突**，接收失败。
问题根源： A **和** C 互相听不到对方的信号，所以不知道对方也在发消息。

A node is visible to a wireless receiver but not to the sender, leading to possible collisions because the sender is unaware of the potential for collision.

Exposed-terminal problems.

Occur when a permissible transmission from a node to another node has to be delayed due to the irrelevant transmission between two other nodes.



. 暴露终端问题 (Exposed-Terminal Problem)
定义：

当一个节点检测到附近有信号传输时，以为自己不能发送数据，从而错误地放弃传输。
事实上，这个信号并不会与自己的接收对象产生冲突，但是它误以为有冲突，导致传输被延误。
举个例子：

节点 A **正在向** B 发送数据。
节点 C **想向** D 发送数据，但检测到 A 正在发，就以为自己也不能发。
实际上，C **和** A 之间的传输互不干扰，因为 C **和** B 之间没有通信冲突。
问题根源：过度保守，因为检测到了信号而放弃发送。

A node is prevented from sending data because it can sense another transmission, even though its communication wouldn't actually cause a collision.

Solution

MACA (Multiple Access with Collision Avoidance) 协议是为了解决隐藏终端和暴露终端问题而设计的。
它通过**信令包（Signalling Packets）**来避免碰撞，主要有两个包：

1. RTS（Request to Send）：请求发送
发送方在发送正式数据包之前，先发一个RTS 包，请求发送权限。
RTS 包比较短，即使冲突也不会占用太多带宽。
发送方："我可以发送数据吗？"
2. CTS（Clear to Send）：清除发送
接收方在准备好接收时，回应一个CTS 包，表示许可发送。
只有在收到 CTS 后，发送方才正式发送数据。
接收方："可以发，准备接收！"

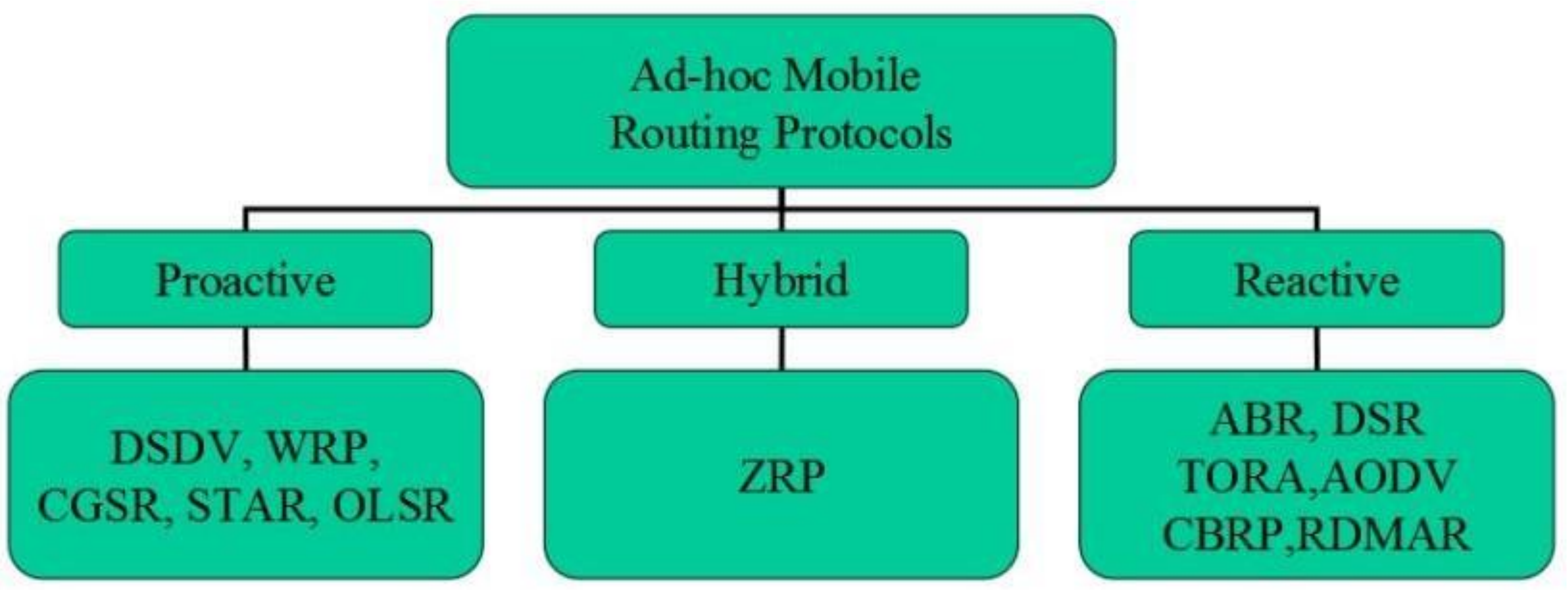
- □ A new protocol MACA (multiple access with collision avoidance protocol) is used to avoid the Hidden-terminal and Exposed-terminal problems.
- □ Use signalling packets to avoid collision.
  - RTS (Request to send)
    - Sender request the right to send from a receiver with a short RTS packet before it sends a data packet.
  - CTS (Clear to send)
    - Receiver grants the right to send as soon as it is ready to receive

RTS/CTS 协议的优势
避免隐藏终端问题：

当节点 A 收到 B 的 CTS 包时，周围的节点（比如 C）也能监听到，从而避免在此时发送数据。
避免暴露终端问题：

由于只有发出 CTS 才算确认发送权限，其他节点不会因检测到 RTS 就盲目停止发送。

Routing In MANETs



Routing in Ad Hoc Networks

- Mobile nodes operate as routers.
- Proactive Protocol – Table Based
  - Maintain routes between every host pair all the time
  - Shortest-path protocols
  - Frequently update routing table; High routing overhead.
- Reactive Protocols – On-Demand
  - On-demand
  - Source initiates route discovery.
- Hybrid protocols
  - Combination of proactive and reactive.

Destination-Sequenced Distance-Vector (DSDV)

- Adapted from Routing Information Protocol(RIP).
  - Adds new attribute- Sequence Number
- Each node maintains a routing table which stores
  - Next hop
  - Cost matric for each destination
  - A sequence number that is create by destination itself.
- Each node advertises a monotonically increasing even sequence number.
  - Used to update path to destination node.
  - Odd sequence number used to represent broken path.
- Routing table updates are transmitted periodically.
- Routing information is transmitted by broadcast.

DSR 协议是什么？
DSR 是一种反应式路由协议（Reactive Routing Protocol），又叫按需路由协议（On-Demand Protocol）。
反应式的意思是：只有在需要时才进行路由发现，**而不是提前构建路由表。**

Dynamic Source Routing (DSR)

- □ DSR is a type of Reactive Routing Protocols.
- □ On demand Protocol
- □ Source node initiate route discovery .
- □ Source node floods Route Request (RREQ) in the network.
- □ Use broadcast method to send RREQ.
- □ Route request use a sequence number and path it traversed.
  - ▣ Sequence number is used to identify the request; to avoid looping.

按需路由：只有当源节点需要与目的节点通信时，才会发起路由发现。
源节点发起路由发现：源节点广播一个路由请求（RREQ），遍历网络寻找路径。
广播请求（RREQ）：**使用广播方法将** RREQ 发送到网络中所有节点。
序列号避免循环：
RREQ 中包含一个序列号和已遍历路径，序列号用于唯一标识请求，避免循环路由。
通过跟踪路径，确保数据包不在相同节点间无限循环。
路径缓存：
路由信息可以保存在源节点的缓存中，**以便将来快速使用。**
这样可以减少重复路由请求，节省资源。

DSR

- □ The indented receiver sends a Route Reply (RREP).
- □ The receiver uses the reverse order of path in the Route Request to send the RREP.
- □ Source use received path to send data.
- □ Route may saved in source`s cache for future use.

DSR **的工作流程：**

1. 路由发现（Route Discovery）：

第一步：发送 RREQ（Route Request）

源节点 S 需要找到到目标节点 D 的路径时，发送一个路由请求（RREQ）。

RREQ **中包含：**

源节点地址（S）

目的节点地址（D）

唯一序列号（用于标识）

已遍历路径（初始为空）

2. RREQ 的传播：

RREQ 通过网络逐跳广播，每经过一个节点就更新路径信息。

路径积累：

例如，S -> E -> F -> J -> M -> D

RREQ **包含完整路径，**确保无环路。

3. **路由回复**（Route Reply）：

当 RREQ 到达目标节点 D **后，**目标节点会回发 RREP（Route Reply）。

反向路径发送 RREP：

目标节点 D **按照反向路径**（D -> M -> J -> F -> E -> S）**返回** RREP。

这样，源节点 S **可以得到完整路径。**

DSR 路由缓存：

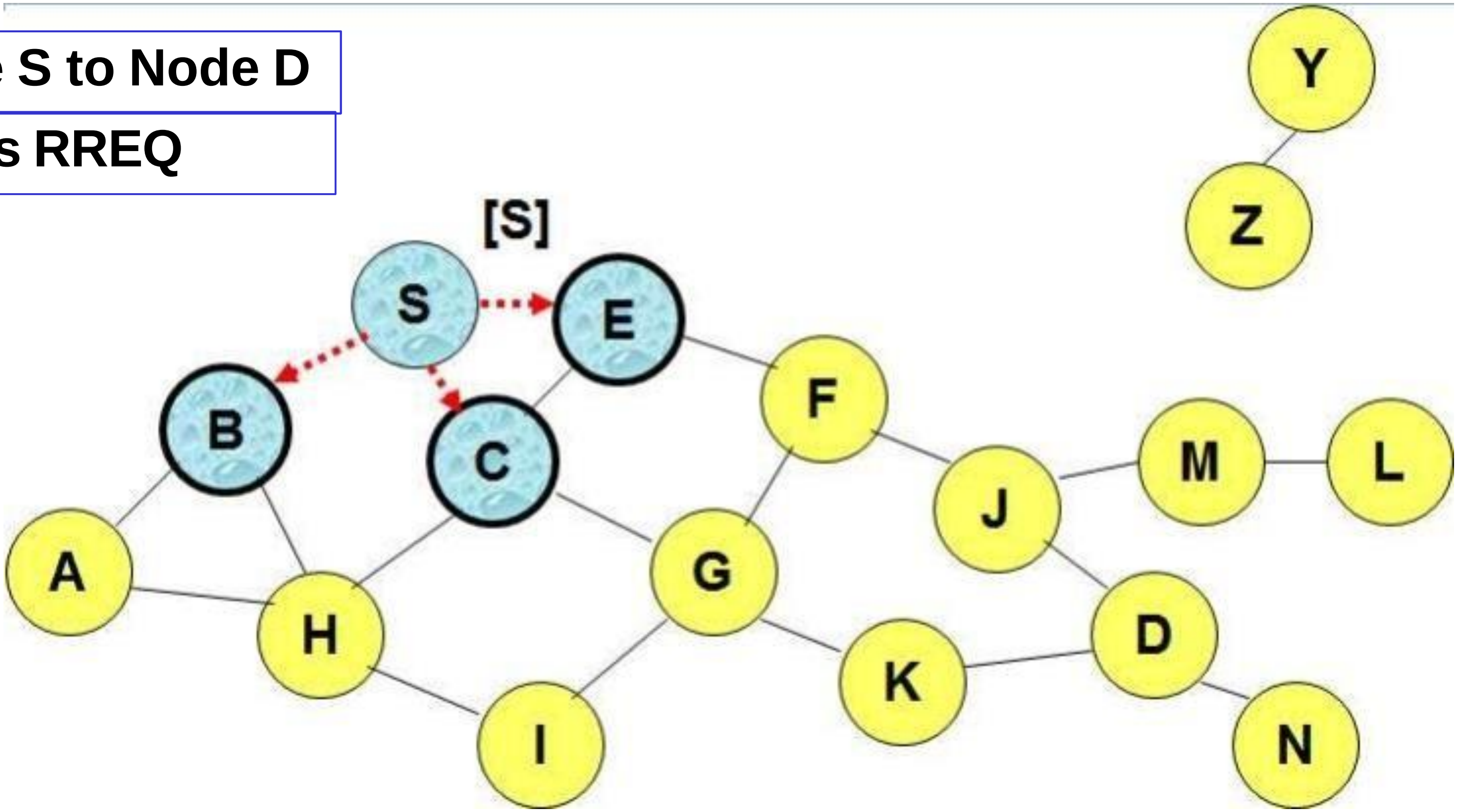
源节点 S **在收到** RREP **后，**会缓存路径，下次通信时可以直接使用缓存路径。

如果路径失效（例如节点移动导致断链），源节点会重新发起路由发现

DSR

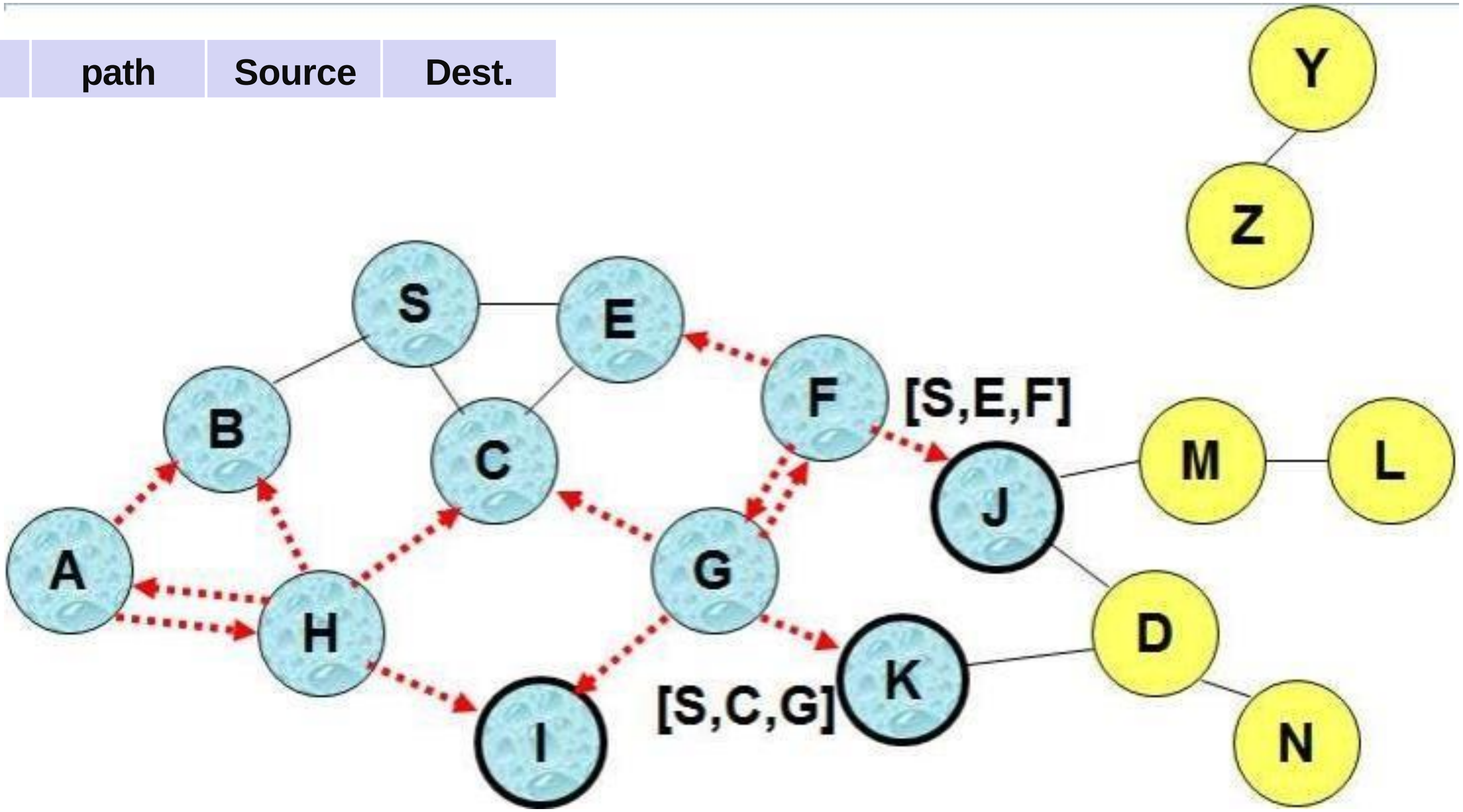
Node S to Node D

Sends RREQ

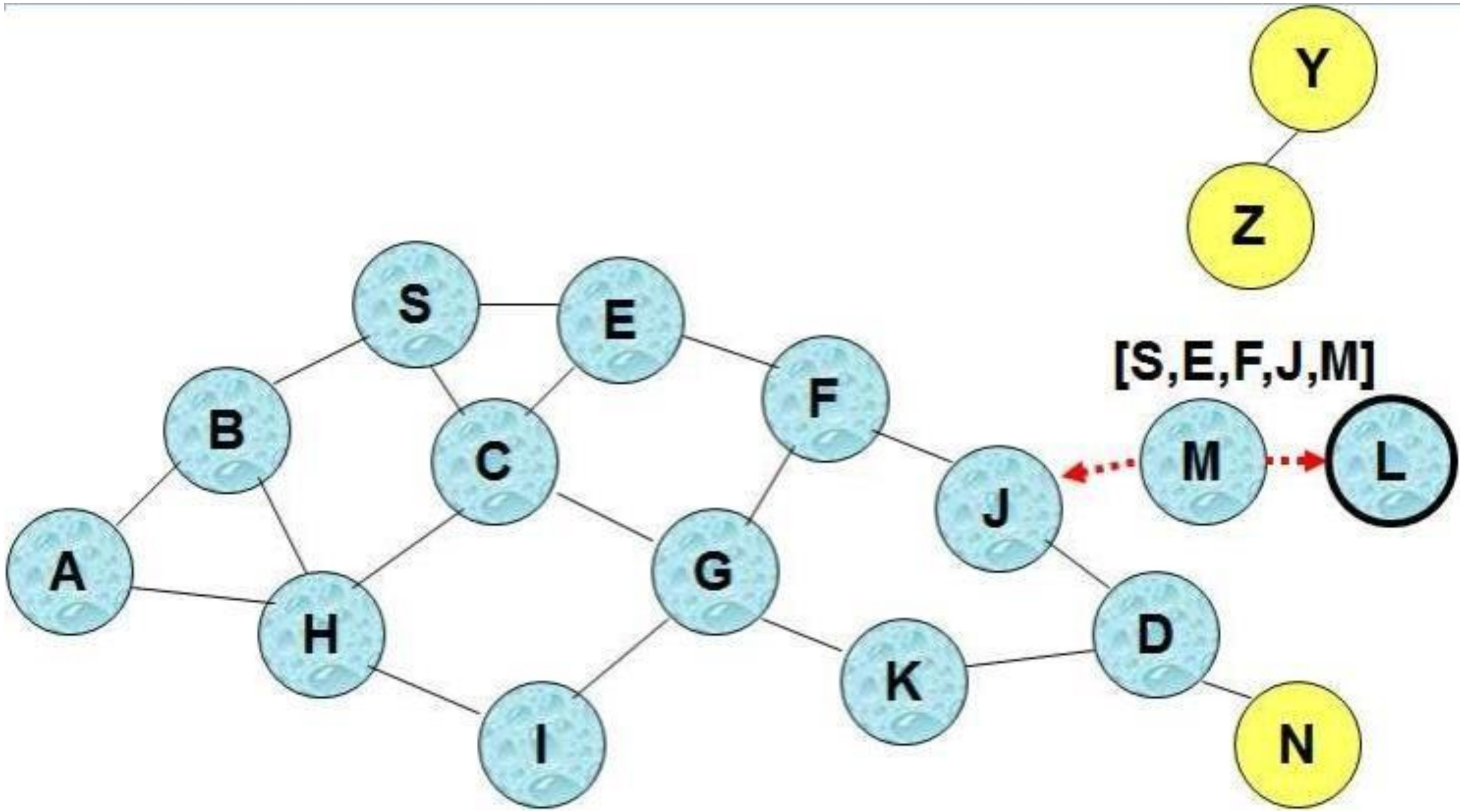


DSR

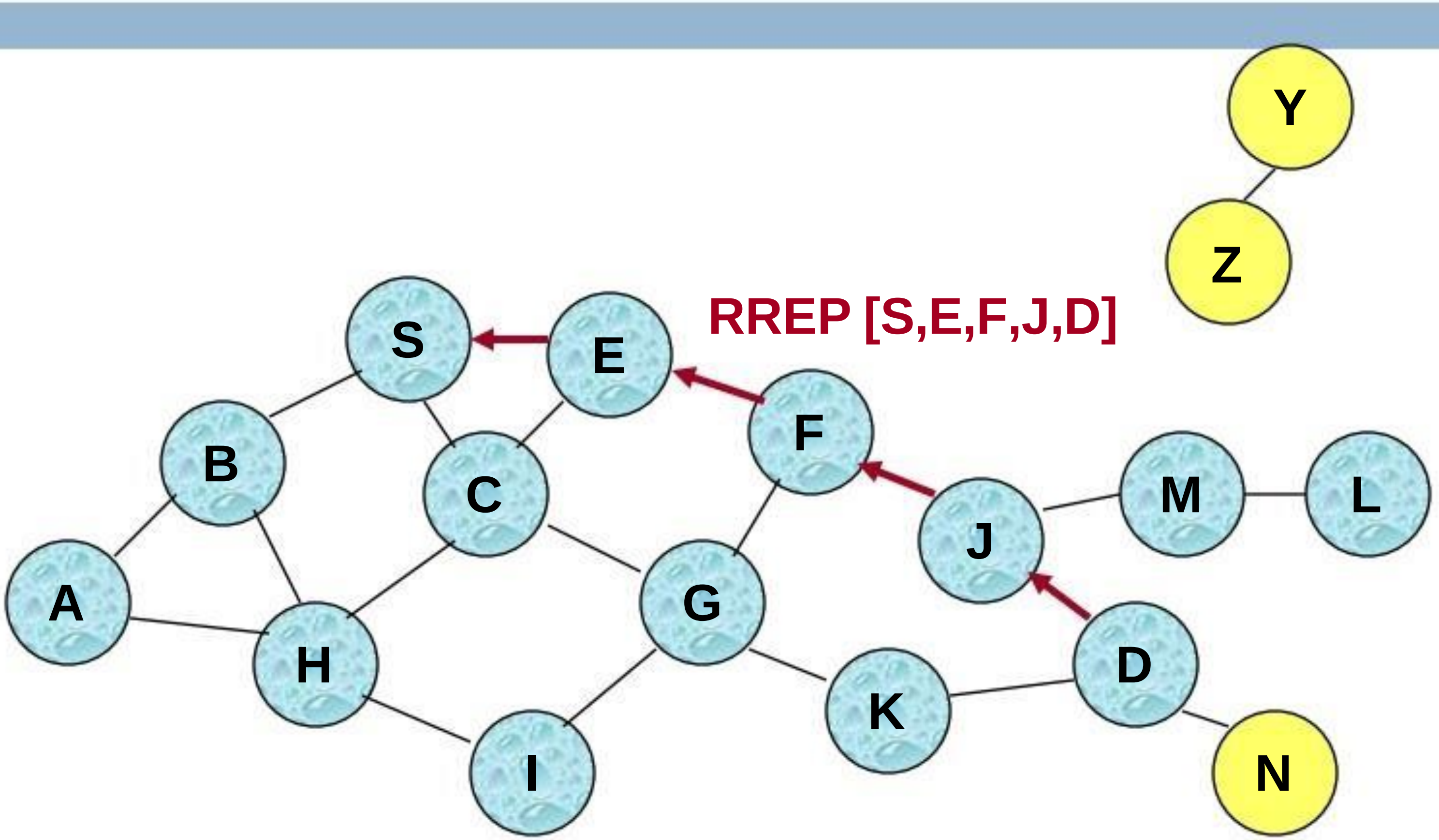
ID	path	Source	Dest.



DSR



DSR (Reply)



Node D to Node S

Sends back RREP

Bluetooth IEEE 802.15.1

Wireless Connection to Multiple Bluetooth Devices
Up to 7 devices can be connected without cables at the same time
Bluetooth headphones
Bluetooth Mouse
Bluetooth Keyboard
PC
Smart phone & Tablet
Printer
Laptop

蓝牙是什么**？**
蓝牙是一种短距离无线通信技术**，**用于在设备之间进行数据传输。
它主要用于手机、电脑、耳机、鼠标、键盘等设备之间的无线连接。

Bluetooth Characteristics

- It separates the frequency band into hops. This spread spectrum is used to hop from one channel to another, which adds a strong layer of security.

蓝牙的主要特点**：**
跳频扩频（Frequency Hopping Spread Spectrum）**：**

蓝牙会将频段分成多个跳频信道。
通过不断切换信道来传输数据**，增加了安全性，**因为黑客很难跟踪信道变化。
设备组网（Piconet）**：**

一个主设备（Master）最多可以连接7个从设备（Slave）**，形成一个微微网**（Piconet）**。**
所有设备都同步到主设备的跳频序列和时钟**，**一起跳频。
信号可穿透障碍物：

蓝牙信号可以穿过墙壁、背包**，**不需要设备之间对准。
信号是全向传播的**，**即使不面对面也能正常连接。
全球统一标准**：**

由IEEE（电气电子工程师学会）和蓝牙SIG（特别兴趣小组）制定标准**，全球通用。**

- Up to eight(Main +7) devices can be networked in a piconet.

- Signals can be transmitted through walls and briefcases, thus eliminating the need for line-of-sight.

- Devices do not need to be pointed at each other, as signals are omni-directional.

- **World standard by IEEE and Bluetooth SIG, so it is possible to** utilize the same standard wherever one travels

Different Versions of Bluetooth

- These are the different versions of bluetooth technologies we have since 1999.

1. Bluetooth v1.0 (with mandatory bluetooth hardware device address)
2. Bluetooth v1.1 (ratified as IEEE standard 802.15.1-2002)
3. Bluetooth v1.2 (faster connection and discovery)
4. Bluetooth v2.0 + EDR (enhanced data rate)
5. Bluetooth v2.1 (secure simple pairing-SSP)
6. Bluetooth v3.0 (high speed data transfer)
7. Bluetooth v4.0 (low energy consumption)
8. Bluetooth v5.0 (low energy consumption – easy connection, collision avoidance)

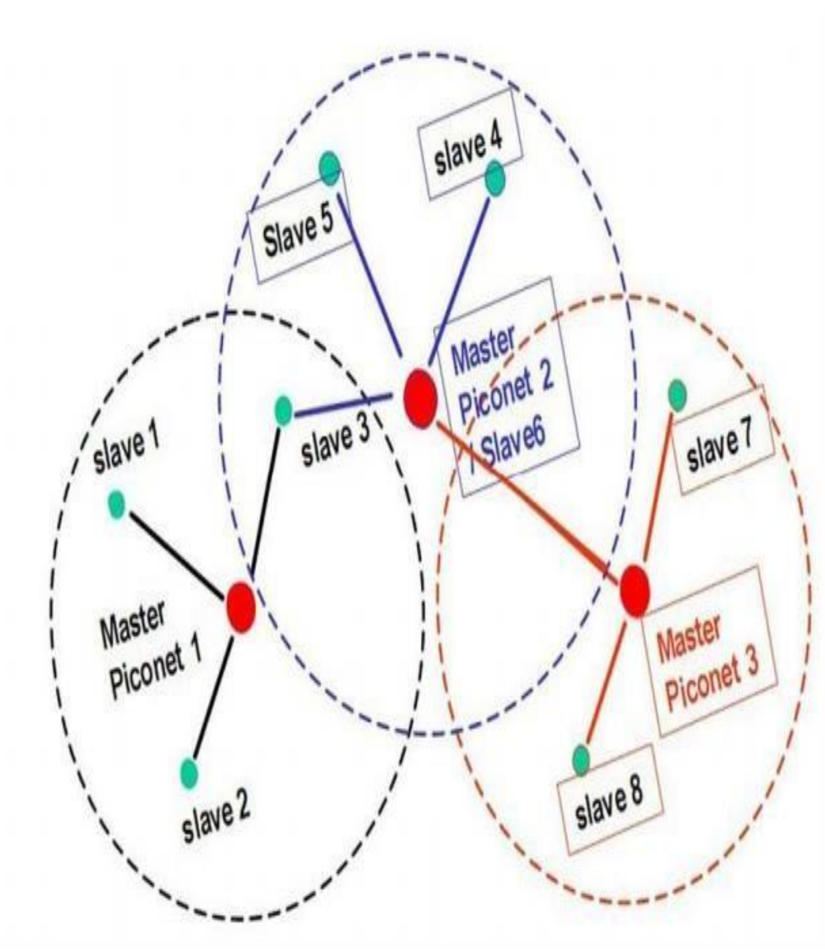
- Bluetooth will support wireless point-to-point and point-to-multipoint (broadcast) between devices in a piconet.

- Point to Point Link
  - Master - slave relationship
  - Bluetooth devices can function as masters or slaves

- Piconet
  - It is the network formed by a Master and one or more slaves (max 7)
  - Each piconet is defined by a different hopping channel to which users synchronize to
  - Each piconet has max capacity (1 Mbps)

微微网（Piconet）：
主设备控制从设备，所有设备的频率和时钟与主设备同步。
跳频序列和相位由主设备决定。
散射网（Scatternet）：
多个微微网组合在一起，由某个设备同时参与多个微微网形成。
比如：一个设备既是A网络的从设备，**又是**B网络的主设备。
设备之间不冲突，通过切换时隙来管理连接

Piconet and Scatternet Structure



✓ Master is connected to up to 7 slaves to form one Piconet

✓ All devices on Piconet are synchronized with the Master's frequency hopping sequence and time.

✓ All devices in piconet hop together.

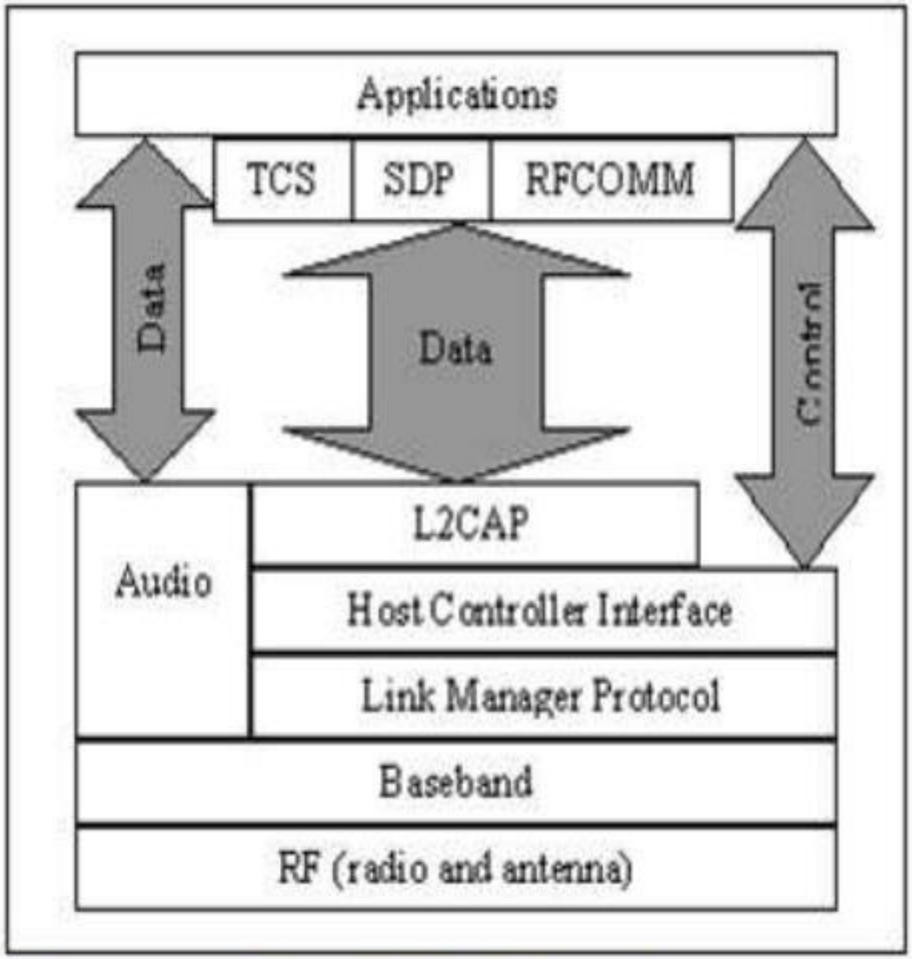
✓ Master ’s ID and master ’s clock determines frequency hopping sequence & phase.

✓ Scatternet structure consists several piconets together. Scatternet is a state where
one device is participating in more than one piconet.

Advantages of BLUETOOTH

- ❑ No line of site restrictions as with IrDA(Infrared Data Assoc.)
- ❑ power consumption makes integrated in battery powered devices very practical.
- ❑ 2.4 GHz radio frequency ensures worldwide operability.
- ❑ Tremendous momentum not only within the computer industry but other industries like cellular telephones and transportation.

Bluetooth Protocol Stack



- The heart of the Bluetooth specification is the Bluetooth protocol stack By providing well-defined layers of functionality, the Bluetooth specification ensures interoperability of Bluetooth devices and encourages adoption of Bluetooth technology.

- Bluetooth is defined as a layered protocol architecture consisting of core protocols, cable replacement and telephony control protocols, and adopted protocols .

Core System Protocols

无线电协议（Radio Protocol）：
负责无线电波的传输和跳频管理。
确定调制方式和发射功率。
2. 基带协议（Baseband Protocol）：
负责建立连接和数据传输，**管理地址分配和包格式。**
包含功率控制，确保设备功耗优化。
3. 链接管理协议（LMP）：
负责链接建立和维护，比如配对和加密。
4. 逻辑链路控制和适配协议（L2CAP）：
提供面向连接和无连接服务。
数据分片和重组，确保大数据包的可靠传输。
5. 服务发现协议（SDP）：
提供设备信息和服务特性查询，帮助设备快速配对。

❑ Radio (RF) protocol : Specifies details of the air interface, the use of frequency hopping, modulation scheme, and transmit power.

❑ Baseband protocol : Concerned with connection establishment within a Piconet, addressing, packet format, timing, and power control.

❑ Link Manager protocol (LMP) : Responsible for link setup between Bluetooth devices and ongoing link management.

❑ Logical link control and adaptation protocol (L2CAP)

L2CAP provides both connectionless and connection-oriented services.

❑ Service discovery protocol (SDP) : Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices

Applications of Bluetooth

- ❑ Wireless control of and communication between a mobile phone and a hands free headset . This was one of the earliest applications to become popular.
- ❑ Wireless communication with pc input and output devices, the most common being the major home appliance.
- ❑ Transfer of files , contact details, calendar appointments, and reminders between devices

ZigBee 是一种专为 低速无线个人区域网络 (LR-WPAN) 设计的自组网技术。
它的主要特点是低功耗、低成本、高可靠性，适用于物联网 (IoT)、智能家居和工业自动化等场景。

ZigBee IEEE 802.15.4

❑ ZigBee is a Ad-hoc networking technology for Low Rate – Wireless Personal Area Networks(LR-WPAN).

❑ Based On IEEE 802.15.4 standard that defines the Physical(PHY) and Medium Access Control(Mac) Layers for ZigBee.

❑ Intended for 2.45 Ghz , 868 Mhz and 915 Mhz Band.

❑ Low cost & power consumption as compared to competing technologies.

❑ Simple (self-configuring), Reliable & robust (self-healing) & Flexible (mesh topology) with high Security (built-in cryptography).

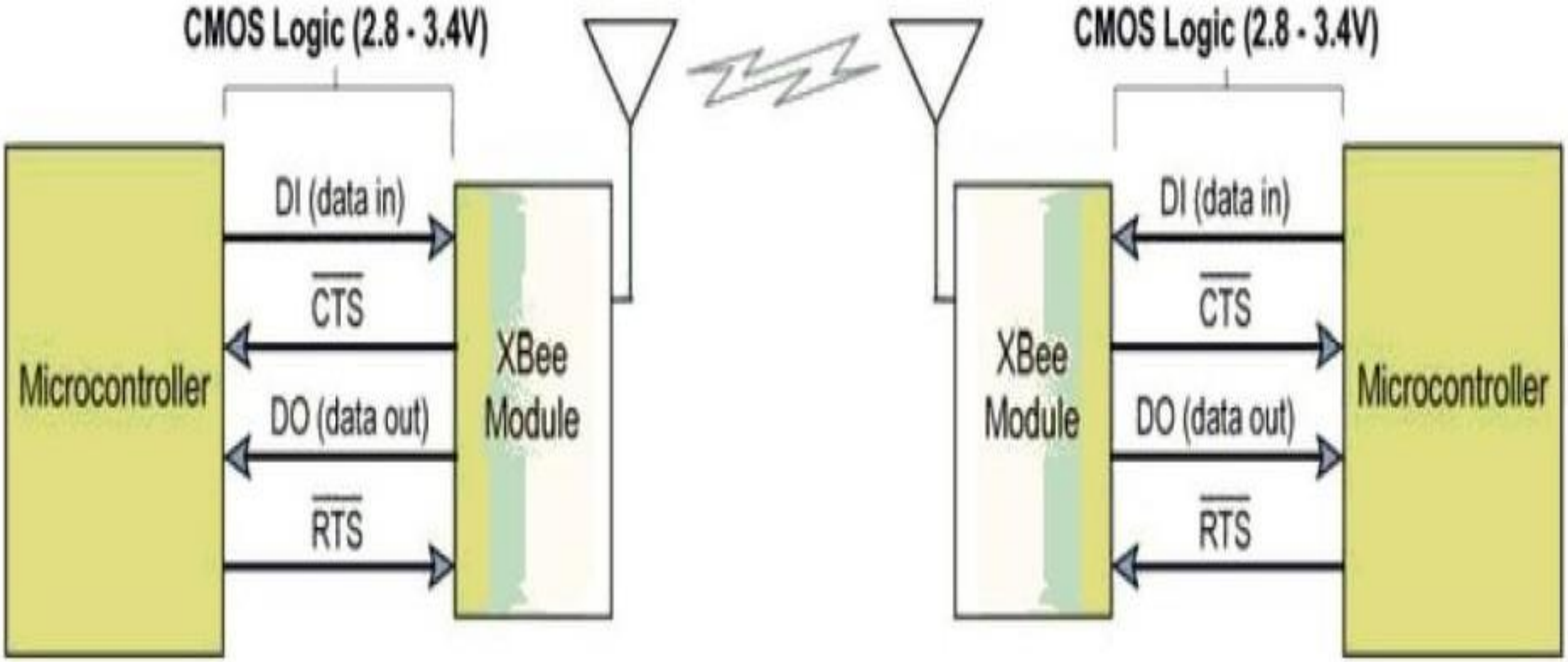
❑ Data rates touch 250Kbps for 2.45Ghz Global Band ,40 Kbps for 915Mhz North American band and 20Kbps for 868Mhz European band.

ZigBee™ Alliance
Wireless Control That Simply Works

Characteristics

- Data rates of 20 kbps and up to 250 kbps
- Star or Peer-to-Peer network topologies
- 255 devices per network
- Support for Low Latency Devices
- Carriers Sense Multiple Access/Collision Avoidance(CSMA-CA) Channel Access
- Fully handshake protocol for transfer reliability
- Low Power Usage consumption
- 3 Frequencies bands with 27 channels
- Extremely low duty-cycle (<0.1%)

Basic Block diagram

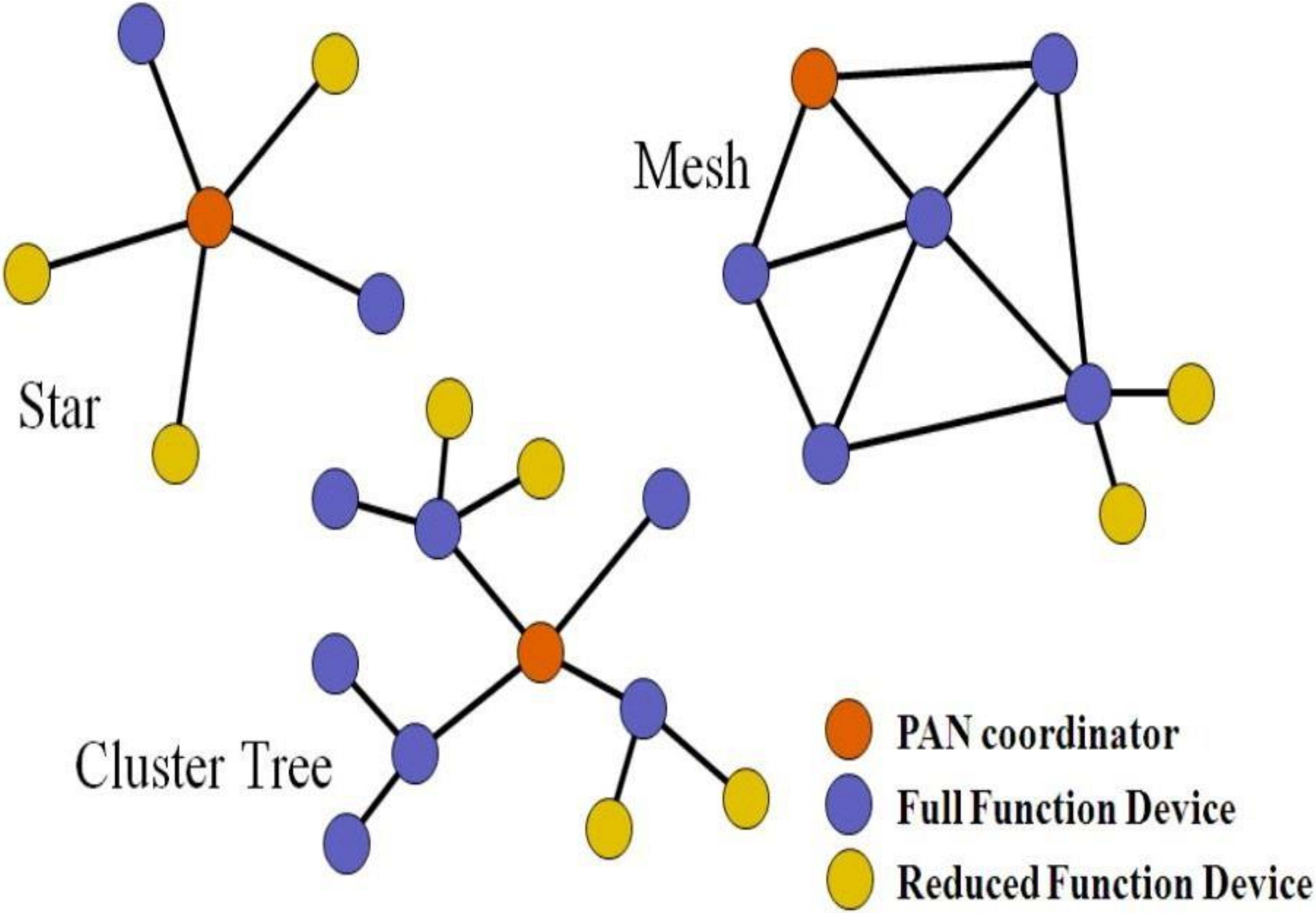


ZigBee Protocol & Topology

Different Node Types in a ZigBee Network

- ❑ **Full Function Device (FFD) : Can communicate with every type of device. A FFD can operate in three different modes:**
  - ✓ **PAN Coordinator : Sends beacon frames, provides routing information, manages short, network-specific addresses.**
  - ✓ **Coordinator : Acts as router.**
  - ✓ **Normal device .**
- ➢ **Reduced Function Device (RFD) : Can only talk to a single FFD.**

Topology Models

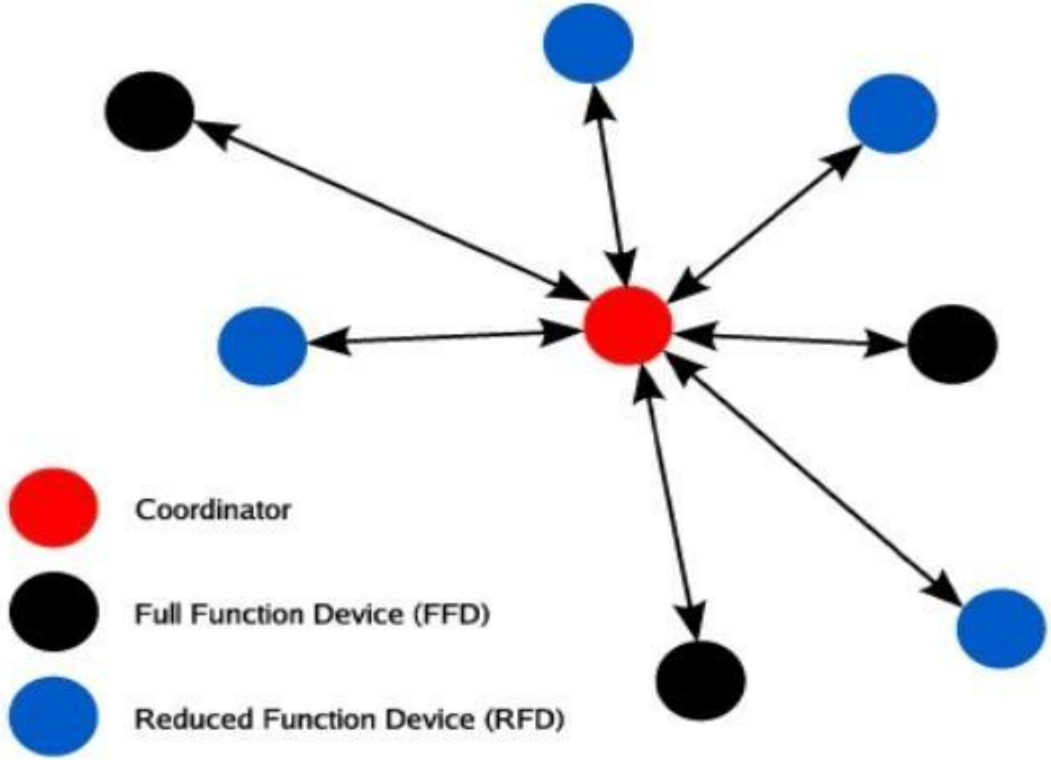


ZigBee Protocol Overview

Different Network Topology in a ZigBee Network

Star Network

In the star topology, the PAN coordinator chooses a unique (within its radio sphere of influence) PAN id. All attached nodes can only talk to the central PAN coordinator.

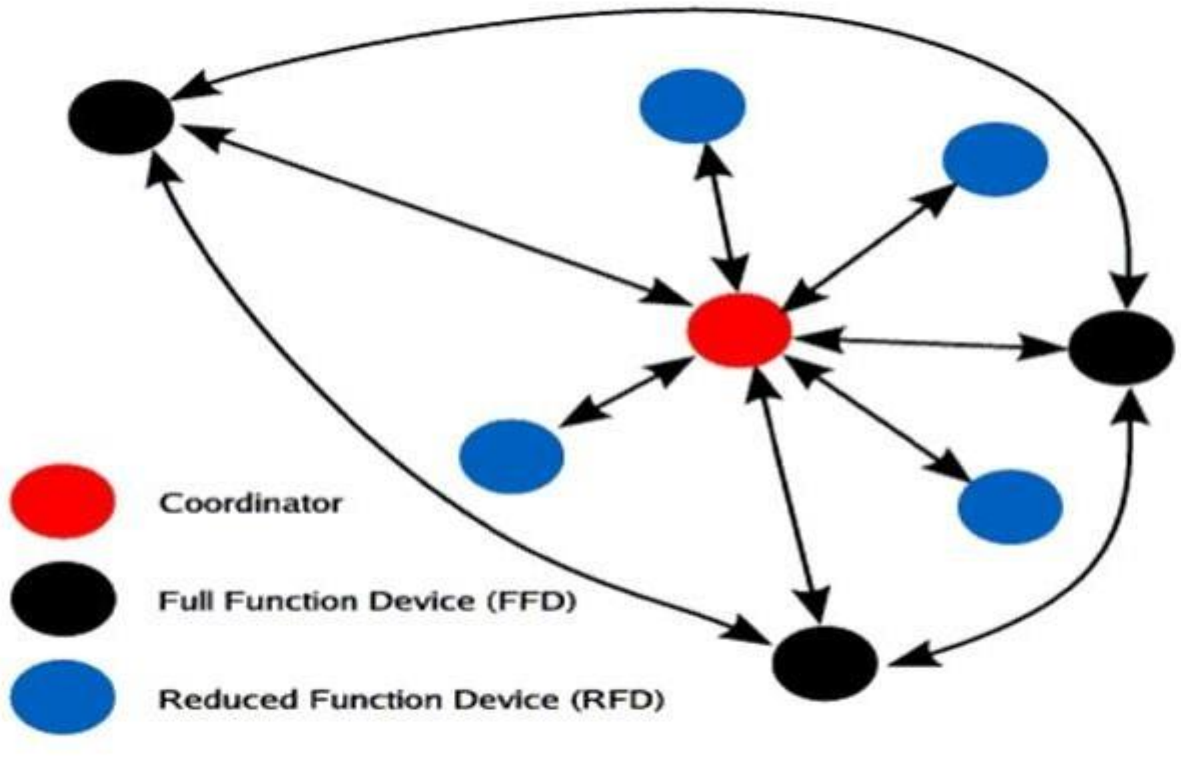


ZigBee Protocol Overview

Different Network Topology in a ZigBee Network

Peer-to-Peer Network

Within a peer-to-peer topology, each FFD can communicate with any other device within its range. A RFD may only communicate with a single FFD at a given time.

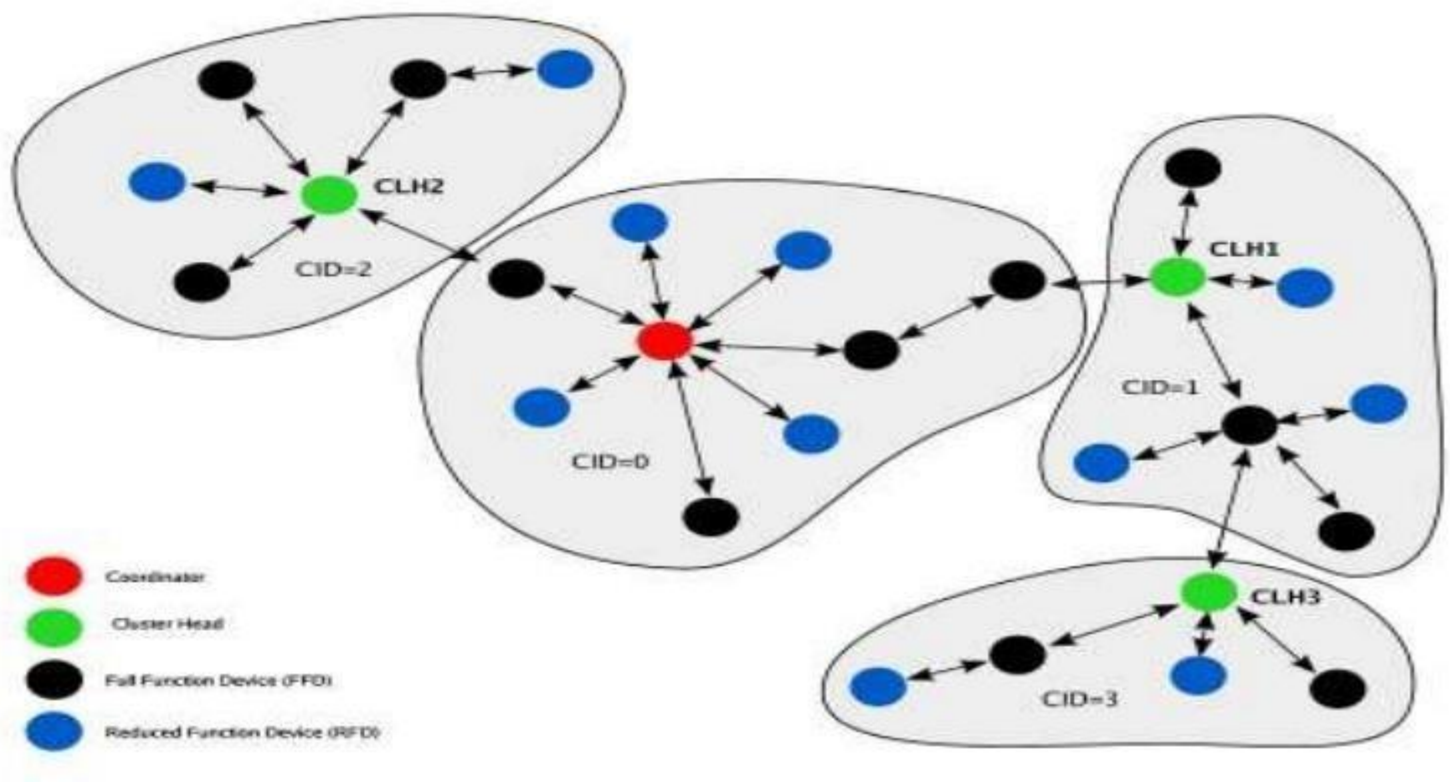


ZigBee Protocol Overview

Different Network Topology in a ZigBee Network

Multi-Cluster Network

Larger networks may be established by forming multi-cluster topologies.
Each cluster has a single cluster head that is responsible for coordination within the cluster.

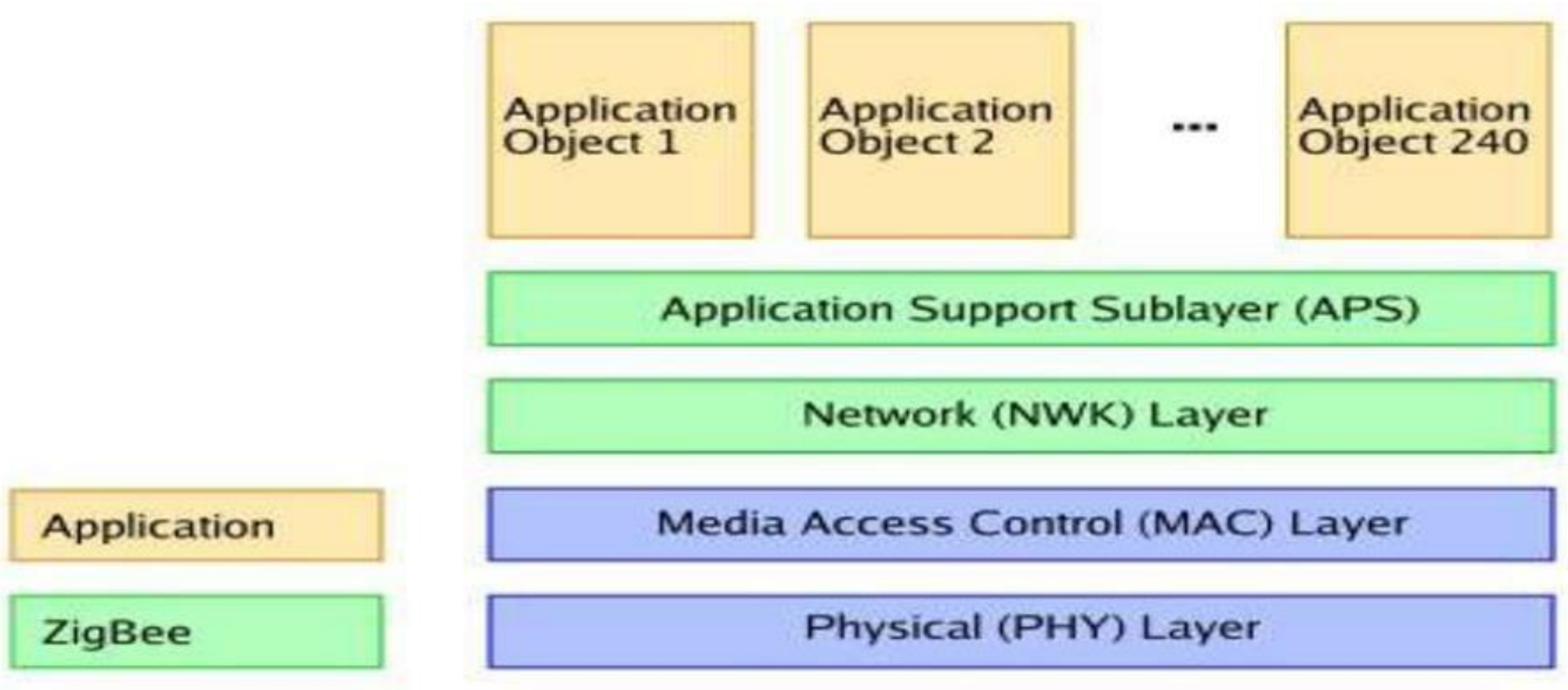


ZigBee Protocol Overview

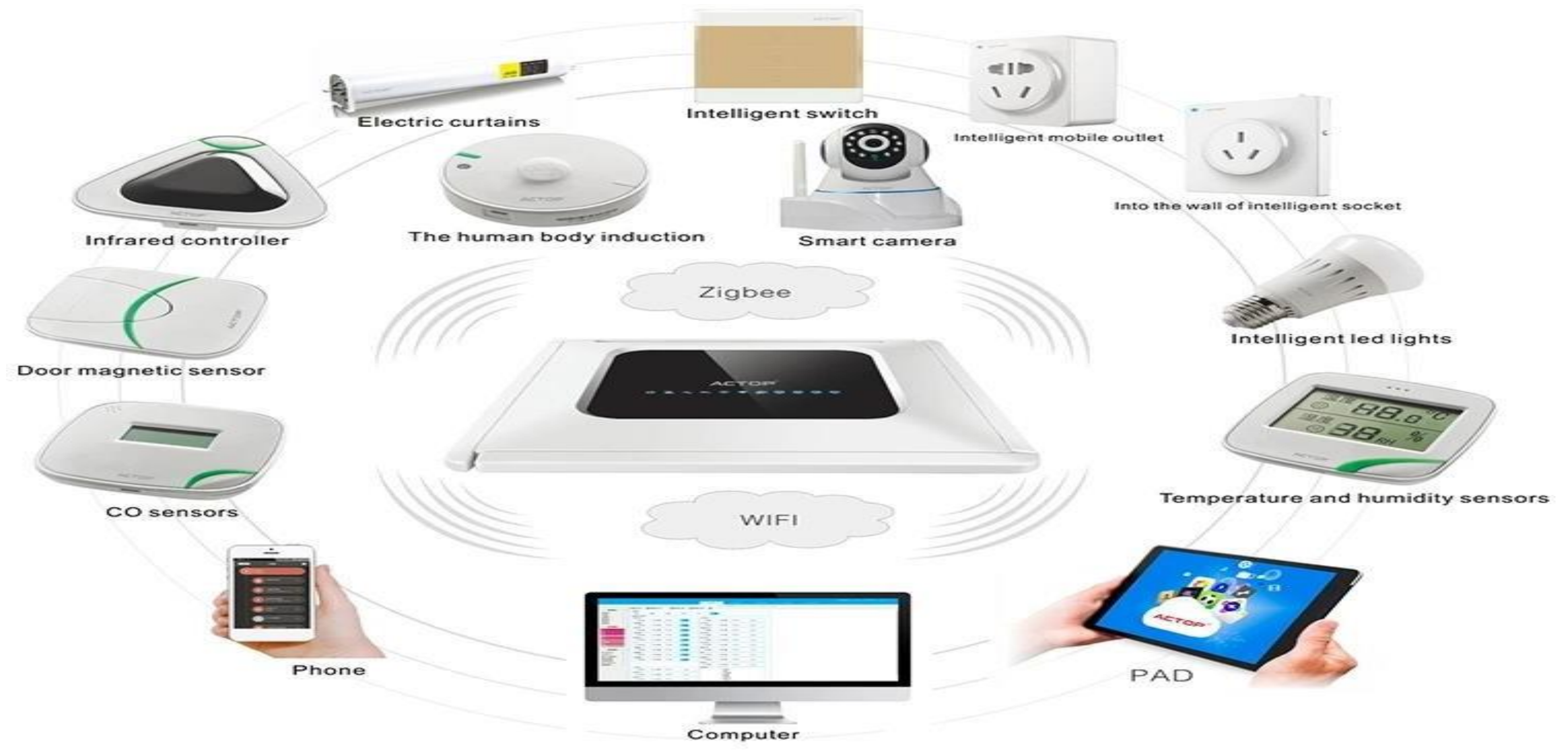
ZigBee / IEEE 802.15.4 Protocol Stack Architecture

The IEEE 802.15.4 standard describes the physical and MAC layer.

ZigBee builds on the IEEE standard and defines the network and application layer.



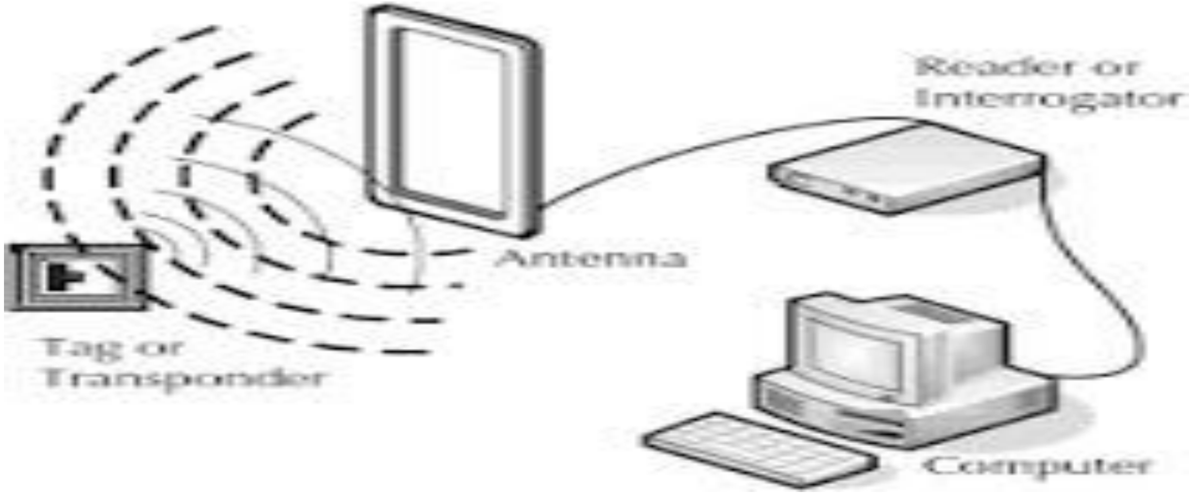
Applications



Zigbee 3.0 : interoperable products for smart homes and cities.
*** Low-power operation and secure networking.**

Radio Frequency Identification (RFID)

- RFID uses backscatter - passive transmission technique.
- RADAR
  - Send a beam and receive reflections.
  - Physical radar



RFID

- ❑A receiving antenna is not just a receiver.

  If current is moving along the antenna, then

  it is transmitting as well.
- ❑If the circuit the antenna is attached to has a resonates at the carrier frequency, then this circuit will oscillate. These oscillation will cause RF transmissions.
- ❑If the circuit is suddenly switched so it does not have a resonates, then now transmissions occur.
- ❑The RFID can switch the circuit to modulate the transmission.

Summary

蓝牙 (Bluetooth)、Wi-Fi **和** ZigBee 都是常见的无线通信技术，它们在功能、速率、功耗和应用场景上各有特点。让我们来详细对比一下这三者吧！

Standard	**Bandwidth**	**ProtocolStack Size**	**Stronghold**	**Applications**
ZigBee	250kbps	4-32KB	Longbattery life,lowcost	Remotecontrol, battery-operated products,sensors
Bluetooth	1Mbps	~100+KB	cable replacement	WirelessUSB, handset,headset
Wi-Fi	Upto Gbps	100+KB	Highdatarange	Internetbrowsing, PCnetworking, filetransfers