20MCA104-Advanced Computer Networks

Assignment II

Submitted by : ABHINAND K S

ROLL NO : 03

RMCA – A

BLUETOOTH

What is Bluetooth?

Bluetooth is a network technology that connects devices wirelessly over a short-range to form a personal area network (PAN). They use short-wavelength, ultra-high frequency (UHF) radio waves within the range 2.400 to 2.485 GHz, instead of RS-232 data cables of wired PANs.

Features of Bluetooth

- Bluetooth technology was released in 1999 as Bluetooth 1.0, by Special Interest Group (SIG) who continues to manage it.
- It was initially standardized as IEEE 802.15.1.
- Mobile computing devices and accessories are connected wirelessly by Bluetooth using short-range, low-power, inexpensive radios.
- UHF radio waves within the range of 2.400 to 2.485 GHz are using for data communications.
- A PAN or a piconet can be created by Bluetooth within a 10 m radius.
- Presently, 2 to 8 devices may be connected.
- Bluetooth protocols allow devices within the range to find Bluetooth devices and connect with them. This is called pairing. Once, the devices are paired, they can transfer data securely.
- Bluetooth has lower power consumption and lower implementation costs than Wi-Fi. However, the range and transmission speeds are typically lower than Wi-Fi.
- The lower power requirements make it less susceptible to interference with other wireless devices in the same 2.4GHz bandwidth.
- Bluetooth version 3.0 and higher versions can deliver a data rate of 24 Mbps.
- The Bluetooth version 4.0 came in 2010. It is characterized by low energy consumption, multivendor interoperability, the economy of implementation, and greater range.

There are two types of Bluetooth networks −

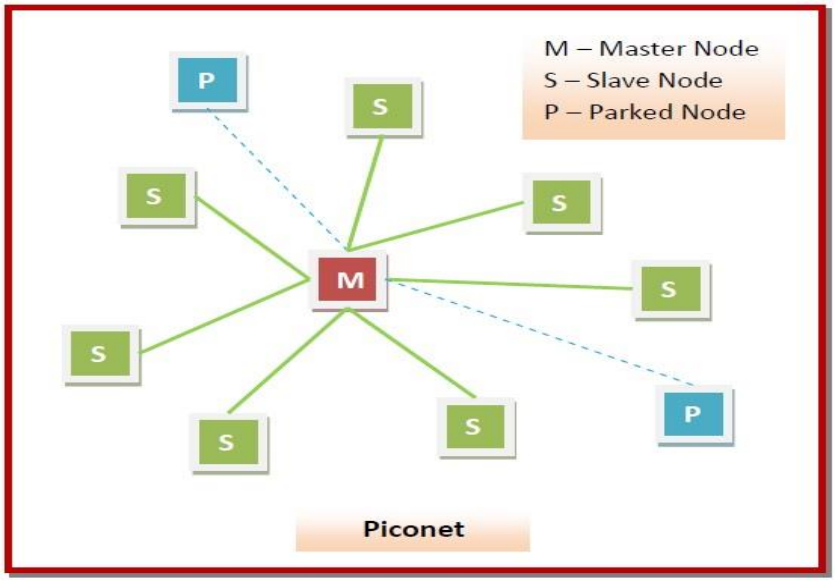
- Piconets
- Scatternets

Piconets

- Piconets are small Bluetooth networks, formed by at most 8 stations, one of which is the master node and the rest slave nodes (maximum of 7 slaves). Master node is the primary station that manages the small network. The slave stations are secondary stations that are synchronized with the primary station.
- Communication can take place between a master node and a slave node in either one-to-one or one-to-many manner. However, no direct communication takes place between

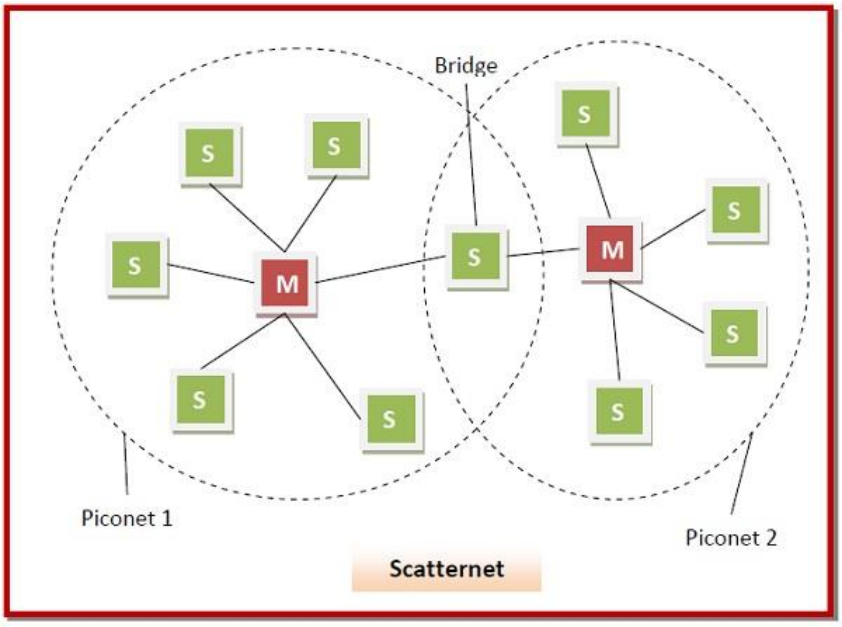
slaves. Each station, whether master or slave, is associated with a 48-bit fixed device address.

- Besides the seven active slaves, there can be up to 255 numbers of parked nodes. These are in a low power state for energy conservation. The only work that they can do is respond to a beacon frame for activation from the master node.



Scatternodes

A scatternet is an interconnected collection of two or more piconets. They are formed when a node in a piconet, whether a master or a slave, acts as a slave in another piconet. This node is called the bridge between the two piconets, which connects the individual piconets to form the scatternet.



FIREWALL

What is a firewall?

Firewalls are tools that protect networks by deciding how and what information can enter and exit the network. They can be used to protect large networks and individual computers from malware and data theft. Many of today's digital devices have them built in. Popular operating systems, such as macOS, Windows, and Linux, have prepackaged firewalls for their users, including essential components of network security.

Types Of Firewalls

- Next-generation firewall (NGFW)
- Packet-filtering firewall
- Proxy firewall
- Stateful inspection firewall
- Application firewall

Firewall Rules

The firewall rules are the access control mechanism used by firewalls to safeguard your network from harmful applications and unauthorized access.

The firewall rules were structured in the following three areas:

- Incoming traffic
- Forwarding
- Outgoing traffic

Firewall 1

These rules were used for Firewall 1:

Incoming traffic

1. Stop all incoming traffic.
2. Allow all related and established traffic for Firewall 1.

Forwarding traffic

1. Stop all forwarding traffic.
2. Allow forwarding of TCP traffic from 192.168.40.60 (proxy server) to the internal servers.

3. Allow forwarding of all related and established traffic.

Outgoing traffic

Allow output traffic for ICMP.

All servers on the internal zone have Firewall 1 as their default route.

Firewall 2

These rules were used for Firewall 2:

Incoming traffic

1. Stop all incoming traffic.
2. Allow all related and established traffic for Firewall 2.

Forwarding traffic

1. Stop all forwarding traffic.
2. Allow forwarding of all related and established traffic.
3. Allow forwarding of TCP traffic on IP interface 10.10.60.0 (OSA card) to go to 192.168.40.21 (Firewall 1) and 192.168.40.60 (proxy server), and when Apache is moved into the DMZ, to 192.168.40.100.

Outgoing traffic

Allow output traffic for ICMP.

The client needs to be able to route request through the Firewall 2 to the proxy server.

VPN

A VPN (virtual private network) provides a secure, encrypted connection between two points. Before setting up the VPN connection, the two endpoints of the connection create a shared encryption key. This can be accomplished by providing a user with a password or using a key sharing algorithm.

Once the key has been shared, it can be used to encrypt all traffic flowing over the VPN link. For example, a client machine will encrypt data and send it to the other VPN endpoint. At this location, the data will be decrypted and forwarded on to its destination. When the destination server sends a response, the entire process will be completed in reverse.

Types of VPNs

- **Site-to-Site VPN:** A site-to-site VPN is designed to securely connect two geographically-distributed sites. VPN functionality is included in most security gateways today. For instance a next-generation firewall (NGFW) deployed at the perimeter of a network protects the corporate network and also serves as a VPN gateway. All traffic flowing from one site to the other passes through this gateway, which encrypts the traffic sent to the gateway at the other site. This gateway decrypts the data and forwards it on to its destination.

- **Remote Access VPN:** A remote access VPN is designed to link remote users securely to a corporate network. For instance when the COVID-19 pandemic emerged in 2020, many organizations transitioned to a remote workforce, and set up secure remote access VPNs from the remote clients to connect to critical business operations at the corporate site.

- **VPN as a Service:** VPN as a Service or a cloud VPN is a VPN hosted in cloud-based infrastructure where packets from the client enter the Internet from that cloud infrastructure instead of the client's local address. Consumer VPNs commonly use this model, enabling users to protect themselves while connecting to the Internet via insecure public Wi-Fi and provide some anonymity while accessing the Internet.

VPN protocols

VPN protocols ensure an appropriate level of security to connected systems when the underlying network infrastructure alone cannot provide it. Several different protocols can be used to secure and encrypt data. They include the following:

- IP Security (IPsec)
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- OpenVPN

Benefits and challenges of using a VPN

Benefits of using a VPN include the following:

- the ability to hide a user's IP address and browsing history;
- secure connections with encrypted data;
- bypassing geo-blocked content; and
- making it more difficult for advertisers to target ads to individuals.

The challenges of using a VPN, however, include the following:

- Not all devices may support a VPN.
- VPNs do not protect against every threat.
- Paid VPNs are more trusted, secure options.
- A VPN may slow down internet speeds.
- Anonymity through VPNs has some s limitations -- for example, browser fingerprinting can still be done.