CSE 4215 (Network Security)

Chapter 5

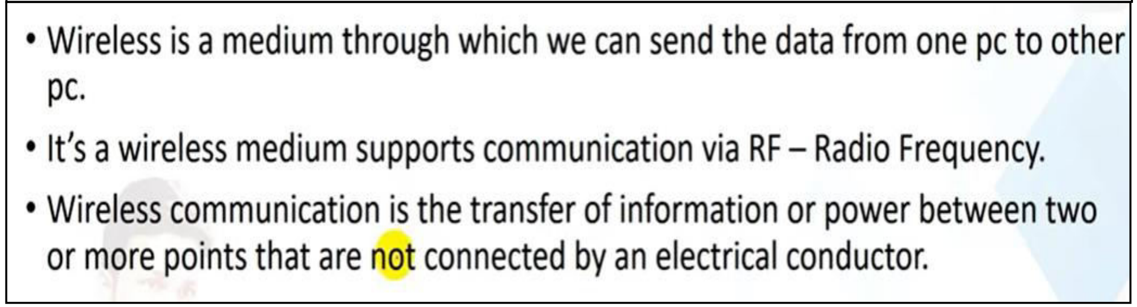
Lecture 11:

Wireless Security Protocols

Wireless Attacks and Security

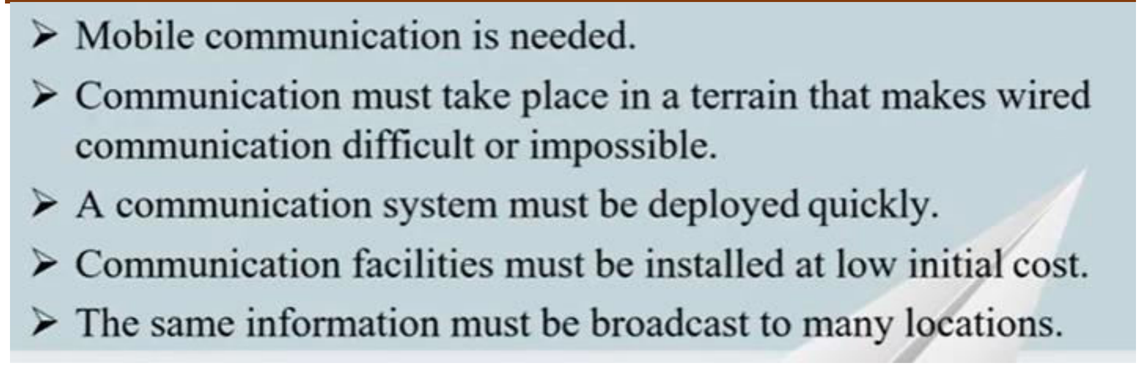
What is Wireless Network?

- With the help of wireless technology we can transfer data from one device to another without using wires or cables. Using this technology we can establish network which is more flexible, intangible and ease to access.



- Wireless is a medium through which we can send the data from one pc to other pc.
- It's a wireless medium supports communication via RF – Radio Frequency.
- Wireless communication is the transfer of information or power between two or more points that are not connected by an electrical conductor.

Need of Wireless Network



- ➢ Mobile communication is needed.
- ➢ Communication must take place in a terrain that makes wired communication difficult or impossible.
- ➢ A communication system must be deployed quickly.
- ➢ Communication facilities must be installed at low initial cost.
- ➢ The same information must be broadcast to many locations.

R-F Signal

- **RANGE**: 30kHz to 300 GHz
- This signal is fall under the category of EM waves
- This signal is invisible and use to send messages from one device to another
- **USES**: FM Radio station use RF signal to broadcast signals. The frequency is used as the station name(like 93.5 RED FM)

Requirements of Wireless Network

- Network Interface Card(NIC) used for wireless networks
- NIC use antenna unlike the RJ45 cable.
- Access Point for Generating signal and establish connection between devices.
- Devices which has wireless signal adapter.

Wireless Attacks and Security

Types of Wireless Network

Based on the size Wireless Networks are divided into 4 categories

- Wireless LAN
- Wireless MAN
- Wireless WAN
- Wireless PAN

WNIC and RJ45 cable

Wireless Network Interface Card (WNIC)

RJ45 cable

Wireless LAN

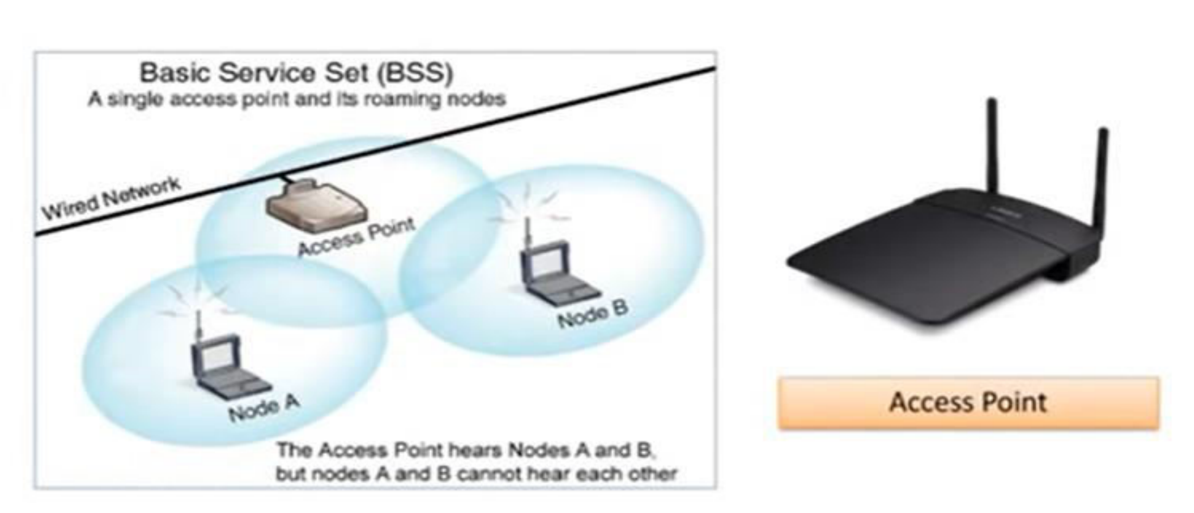
- This is a network where two or more computers are connected that covers only a limited area.
- The NIC is used in this connection where has a small range to cover.
- We often called this peer to peer Network.
- This is also called Ad Hoc Network which is being set up for temporary purposes.

Wireless LAN

- Unlike Switch in a wired Network, A special device is used in WLAN , which is called Access Point.
- WLAN which uses Access Point are called BSS(Basic Service Set)
- This acts as a coordinator between different devices.

Wireless Attacks and Security

Basic Service Set (BSS)


Basic Service Set (BSS)
A single access point and its roaming nodes
Wired Network
Access Point
Node B
Node A
The Access Point hears Nodes A and B, but nodes A and B cannot hear each other
Access Point

What is Wi-Fi

- Wireless Fidelity.
- RF signal Frequency: 2.4 GHz or 5 GHz
- Wi-Fi technology is only used in WLAN.
- Range: About 100 Meters.
- Wi-Fi products are certified and tested by Wi-Fi alliance. We can see their trademarks in most of the Wi-Fi devices.

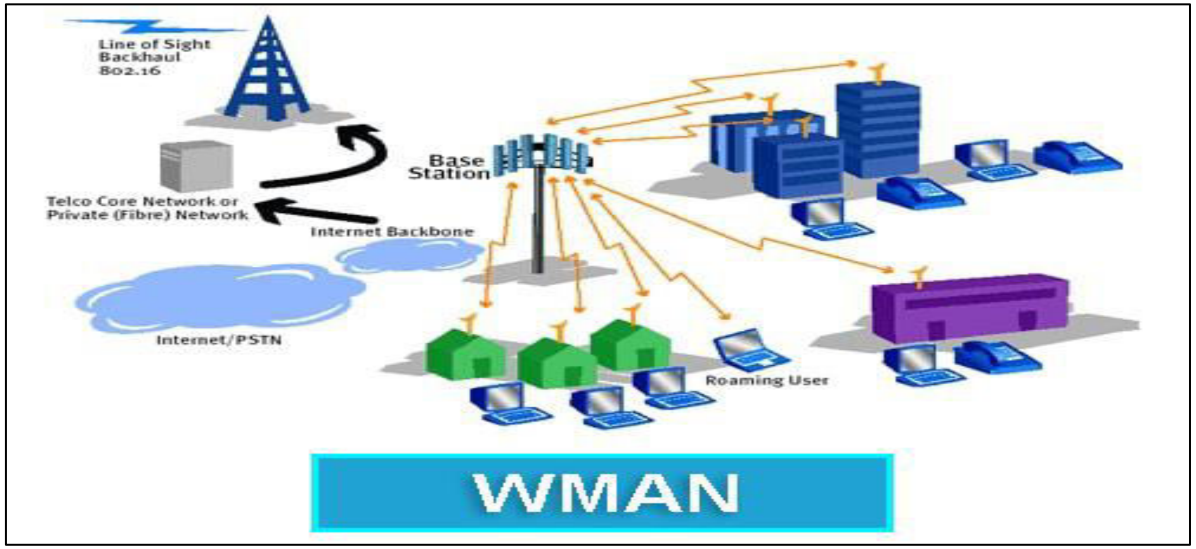
IEEE Standards of Wireless Networks

IEEE Standard	Frequency / Medium	Speed	Topology	Transmission Range	Access Method
802.11	2.4GHz RF	1 to 2Mbps	Ad hoc/infrastructure	20 feet indoors.	CSMA/CA
802.11a	5GHz	Up to 54Mbps	Ad hoc/infrastructure	25 to 75 feet indoors; range can be affected by building materials.	CSMA/CA
802.11b	2.4GHz	Up to 11Mbps	Ad hoc/infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA
802.11g	2.4GHz	Up to 54Mbps	Ad hoc/infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA
802.11n	2.4GHz/5GHz	Up to 600Mbps	Ad hoc/infrastructure	175+ feet indoors; range can be affected by building materials.	CSMA/CA

Wireless Attacks and Security

WMAN (Wireless Metropolitan Area Network)

- Collected unit of many WLANs located at various.
- It uses WIMAX(Worldwide Interoperability for Microwave Access) which is controlled by WiMAX Forum
- Maximum Speed 1 Gbits/sec
- IEEE 802.16


Line of Sight Backhaul 802.16
Base Station
Telco Core Network or Private (Fibre) Network
Internet Backbone
Internet/PSTN
Roaming User
WMAN

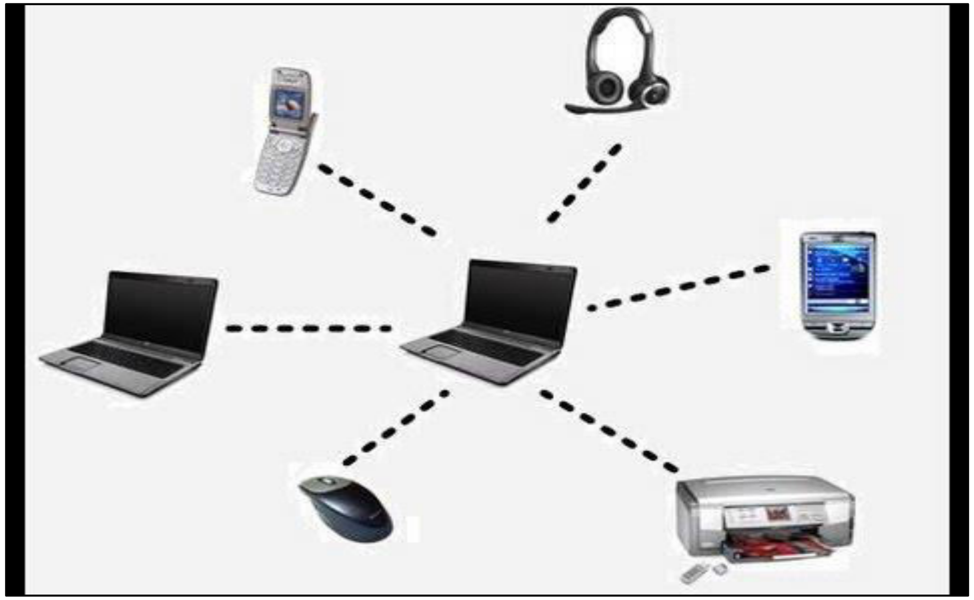
WWAN (Wireless Wide Area Network)

- WWAN is a very large network which is spread over a very large area. It connects many cities together. Mobile Phones use WWAN to make communication possible
- The technology in WWAN are subdivided in many generations
- 2G, 3G and 4G
- The communication system which was used before the emergence of 2G is called 1G used in 1980.
- This technology used in most of the Analog devices.

Wireless Attacks and Security

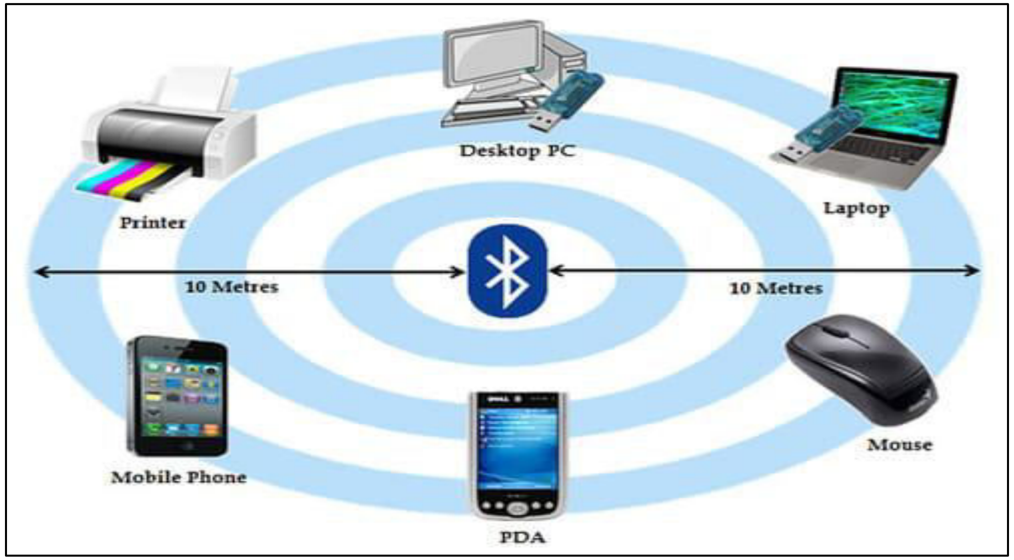
WPAN (Wireless Personal Area Network)

- The Wireless Networks that are used in smaller distances are known as WPAN.
- The communication between a mobile phone and its Bluetooth headset is a typical example of WPAN.
- Two kinds of Wireless technologies are used for WPAN
- Bluetooth and Infrared Data Association.



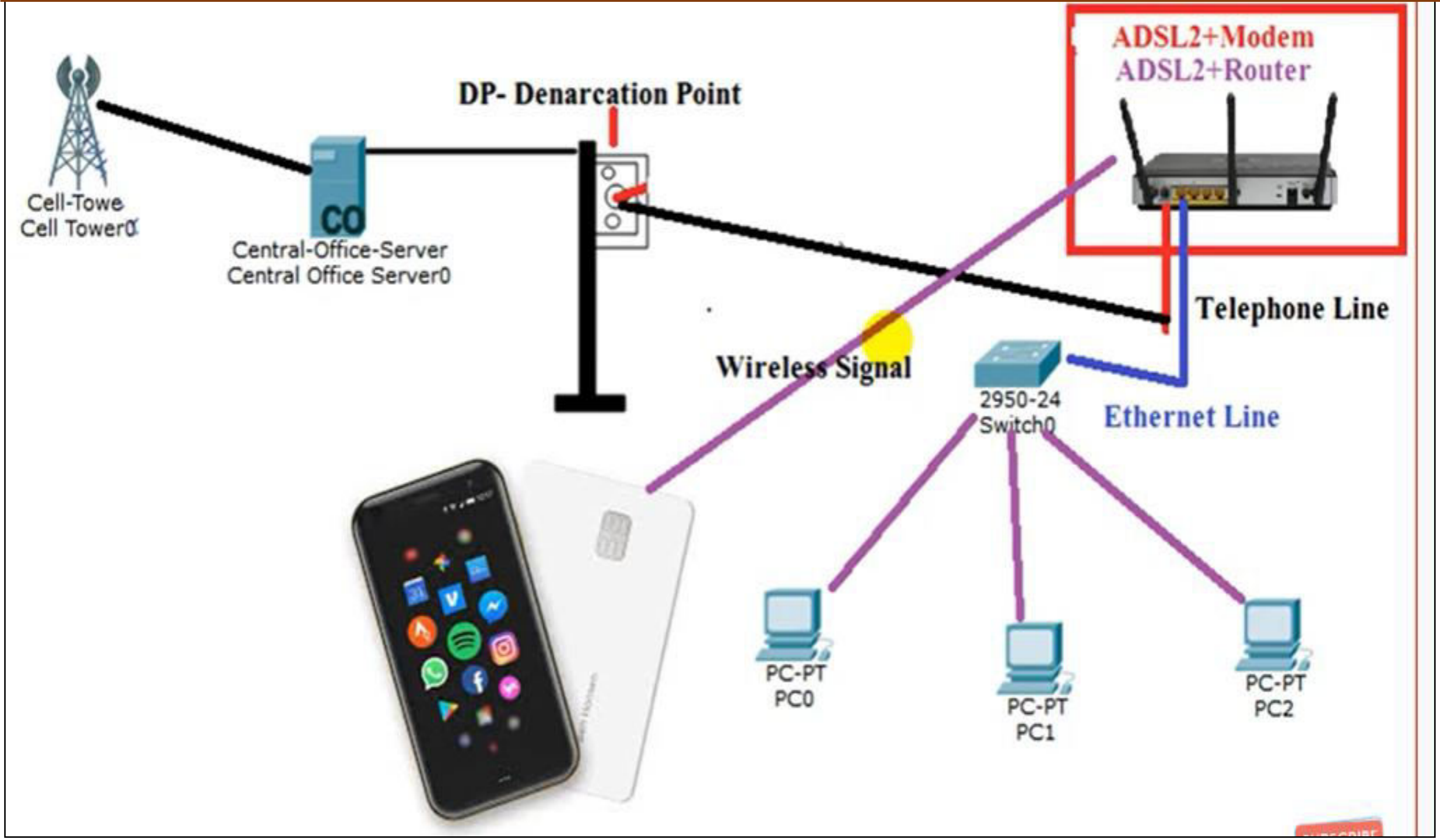
Blutooth

- It is used to connect devices in personal area without using cables
- Use ISM band 2.4 GHz
- Speed up to 721Kbps
- Range 10 to 100 meters



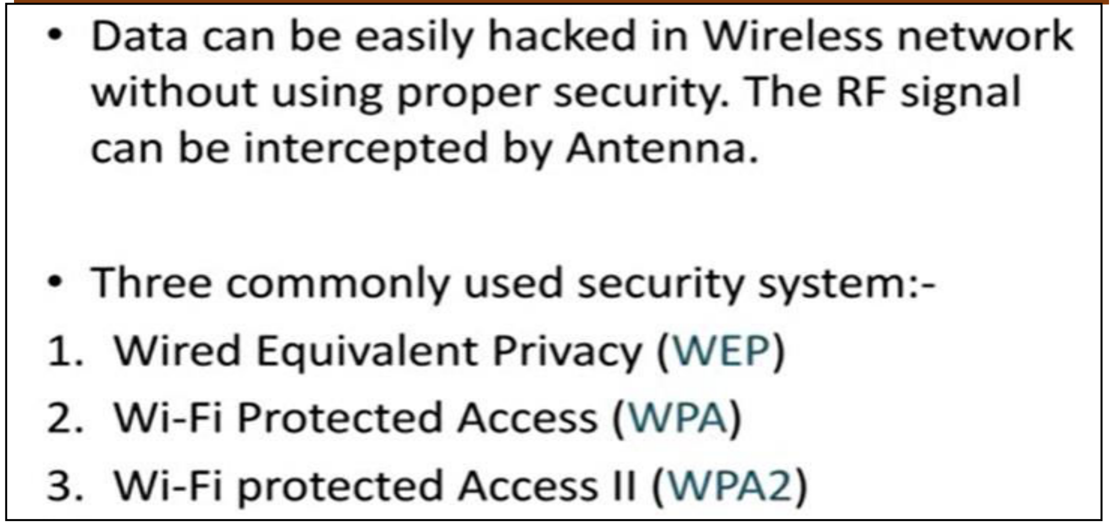
Wireless Attacks and Security

How WiFi Works



Wireless Security Protocols

Security in Wirless Network

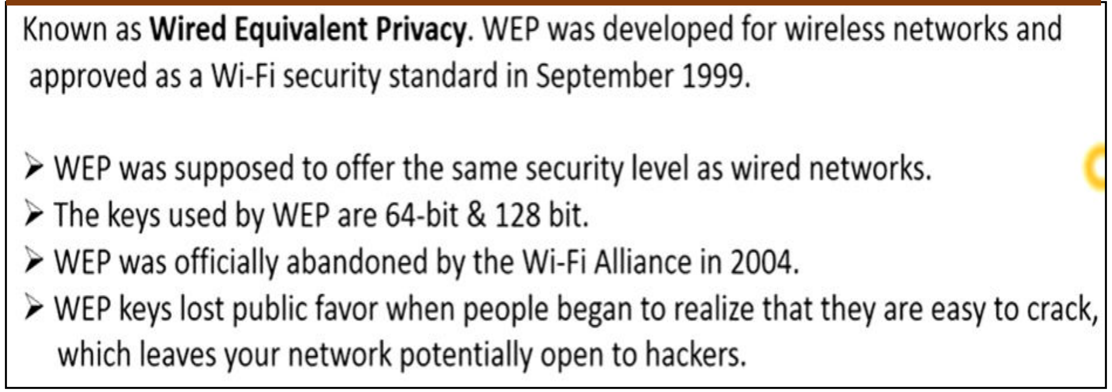


- Data can be easily hacked in Wireless network without using proper security. The RF signal can be intercepted by Antenna.

- Three commonly used security system:-

1. Wired Equivalent Privacy (WEP)
2. Wi-Fi Protected Access (WPA)
3. Wi-Fi protected Access II (WPA2)

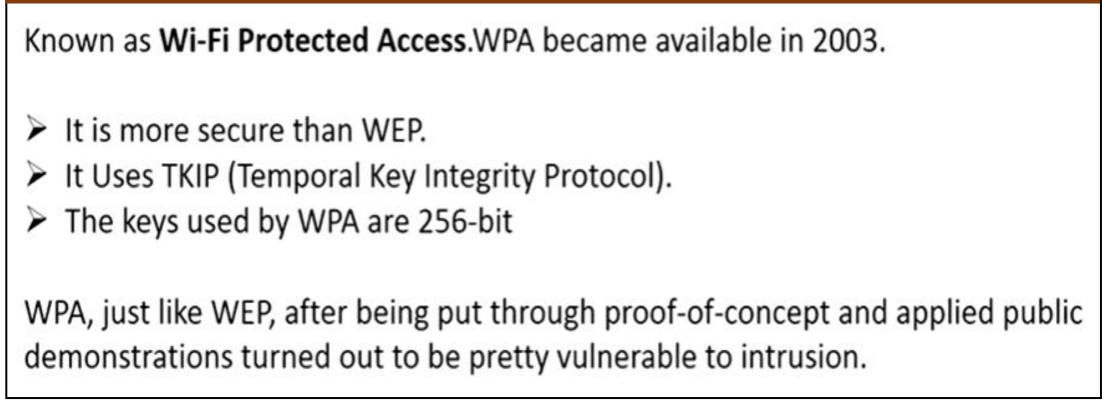
WEP: Wired Equivalent Privacy



Known as **Wired Equivalent Privacy**. WEP was developed for wireless networks and approved as a Wi-Fi security standard in September 1999.

- ➢ WEP was supposed to offer the same security level as wired networks.
- ➢ The keys used by WEP are 64-bit & 128 bit.
- ➢ WEP was officially abandoned by the Wi-Fi Alliance in 2004.
- ➢ WEP keys lost public favor when people began to realize that they are easy to crack, which leaves your network potentially open to hackers.

WPA:Wi-Fi Protected Access

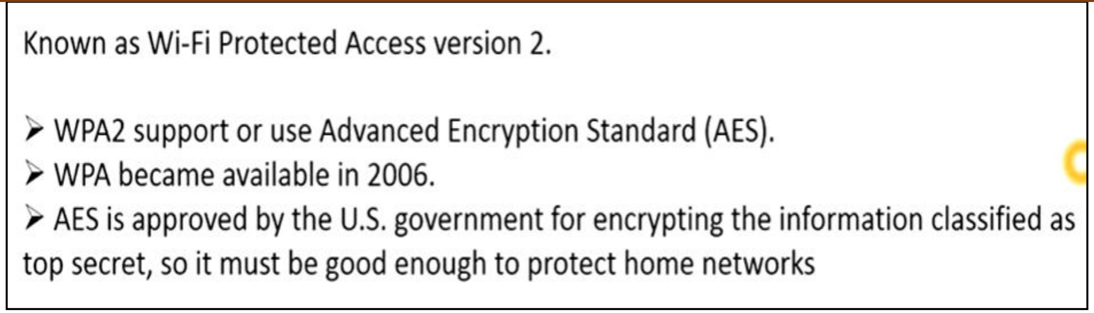


Known as **Wi-Fi Protected Access**.WPA became available in 2003.

- ➢ It is more secure than WEP.
- ➢ It Uses TKIP (Temporal Key Integrity Protocol).
- ➢ The keys used by WPA are 256-bit

WPA, just like WEP, after being put through proof-of-concept and applied public demonstrations turned out to be pretty vulnerable to intrusion.

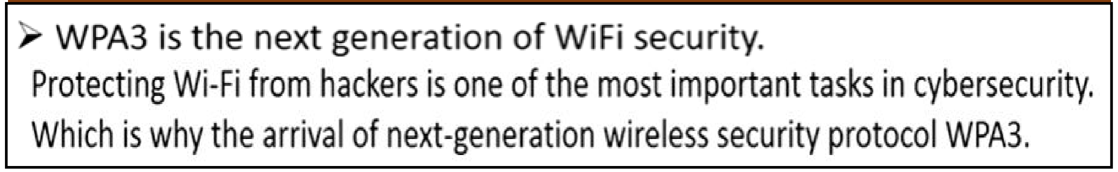
WPA2:Wi-Fi Protected Access Version 2



Known as Wi-Fi Protected Access version 2.

- ➢ WPA2 support or use Advanced Encryption Standard (AES).
- ➢ WPA became available in 2006.
- ➢ AES is approved by the U.S. government for encrypting the information classified as top secret, so it must be good enough to protect home networks

WPA3:Wi-Fi Protected Access Version 3



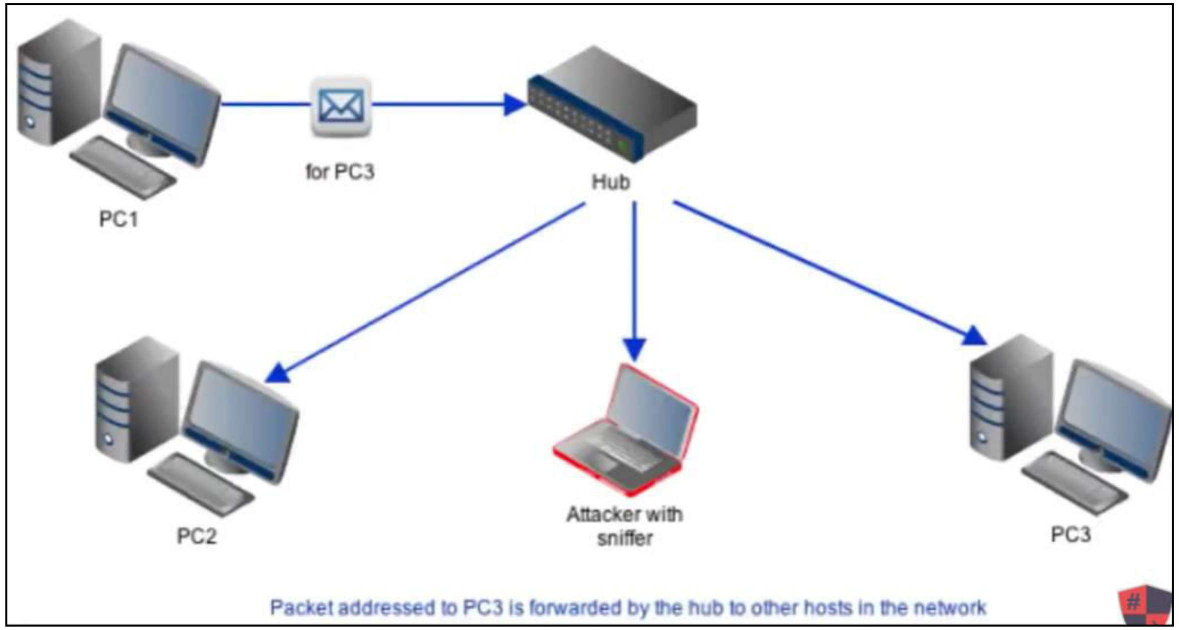
➢ WPA3 is the next generation of WiFi security.

Protecting Wi-Fi from hackers is one of the most important tasks in cybersecurity. Which is why the arrival of next-generation wireless security protocol WPA3.

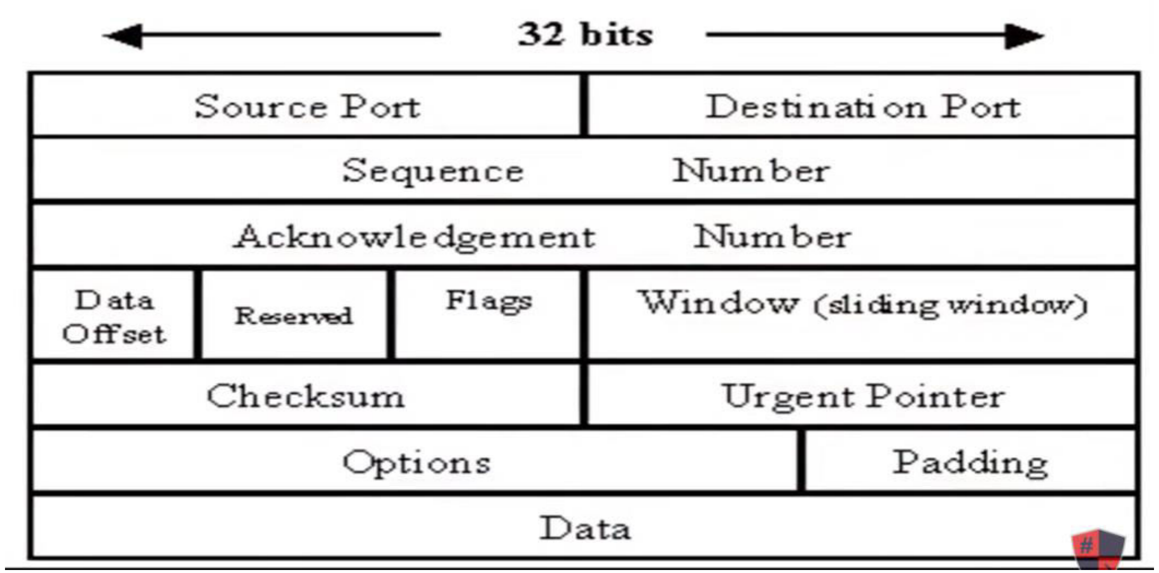
Wireless Attacks and Security

Types of Wireless Security Attack

- **Packet Sniffing:** When information is sent back and forth over a network, it is sent in what we call packets.
- Since wireless traffic is sent over the air, it's very easy to capture. Quite a lot of traffic (FTP, HTTP, SNMP, ect.) is sent in the clear, meaning that there is no encryption and files are in plain text for anyone to read.
- So using a tool like Wireshark allows you to read data transfers in plain text! This can lead to stolen passwords or leaks of sensitive information quite easily.
- Encrypted data can be captured as well, but it's obviously much harder for an attacker to decipher the encrypted data packets.



Packet addressed to PC3 is forwarded by the hub to other hosts in the network



<table>
<tr><th colspan="5">32 bits</th></tr>
<tr><td colspan="3">Source Port</td><td colspan="2">Destination Port</td></tr>
<tr><td colspan="5">Sequence Number</td></tr>
<tr><td colspan="5">Acknowledgement Number</td></tr>
<tr><td>Data Offset</td><td>Reserved</td><td>Flags</td><td colspan="2">Window (sliding window)</td></tr>
<tr><td colspan="3">Checksum</td><td colspan="2">Urgent Pointer</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

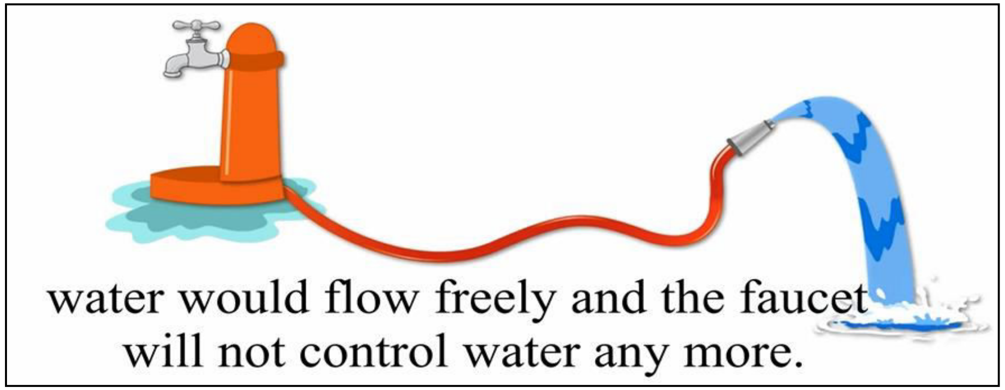
Data Packet

Wireless Attacks and Security

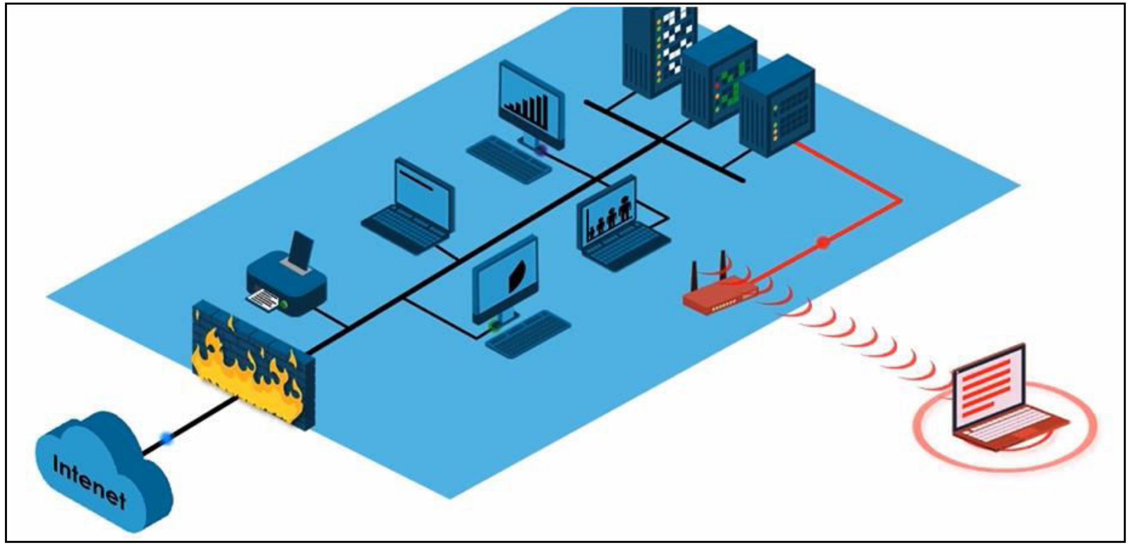
Rouge Access Point

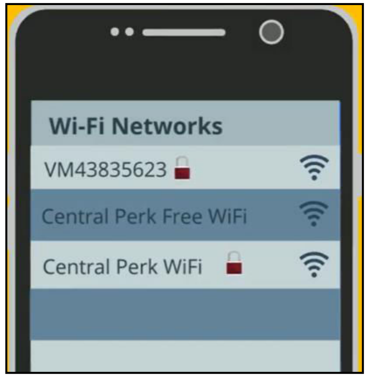
A fraudulent network posing as an authentic Access Point. They will often look exactly the same as a normal network would, but can be configured for malicious intent

In 2014, in Mexico alone , more than 2,000 illegal valves were placed on its oil pipelines.



water would flow freely and the faucet will not control water any more.



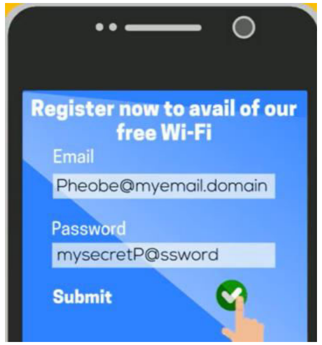


Wi-Fi Networks

VM43835623 🔒

Central Perk Free WiFi

Central Perk WiFi 🔒



Register now to avail of our free Wi-Fi

Email

Pheobe@myemail.domain

Password

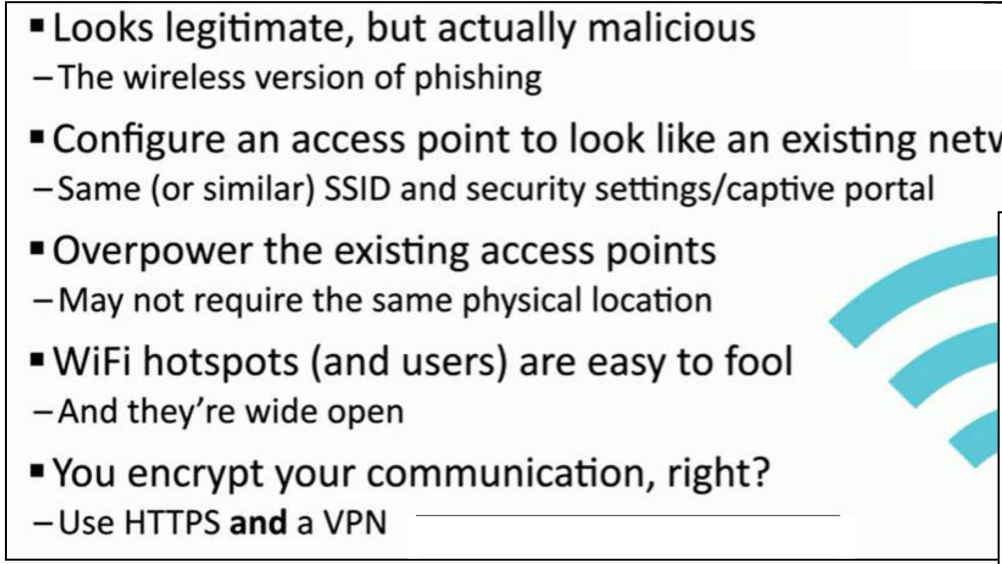
mysecretP@ssword

Submit ✓

In a coffee shop, a customer sees two wi-fi networks, one of which is Rouge Access Point. If the customer login with the fraudulent network, his/her personal credential will be theft.

Wireless Attacks and Security

Evil Twins Wireless Security Attack



- Looks legitimate, but actually malicious
  - The wireless version of phishing
- Configure an access point to look like an existing network
  - Same (or similar) SSID and security settings/captive portal
- Overpower the existing access points
  - May not require the same physical location
- WiFi hotspots (and users) are easy to fool
  - And they're wide open
- You encrypt your communication, right?
  - Use HTTPS **and** a VPN

STARBUCKS COFFEE
STARBUCKS WIFI

The SSID (**Service Set Identifier**) is the name of your wireless network, also known as Network ID. This is viewable to anyone with a wireless device within reachable distance of your network.

Recommendation
Only browse internet using public Wi-Fi network. Do NOT do online shopping or banking.

Wireless Attacks and Security

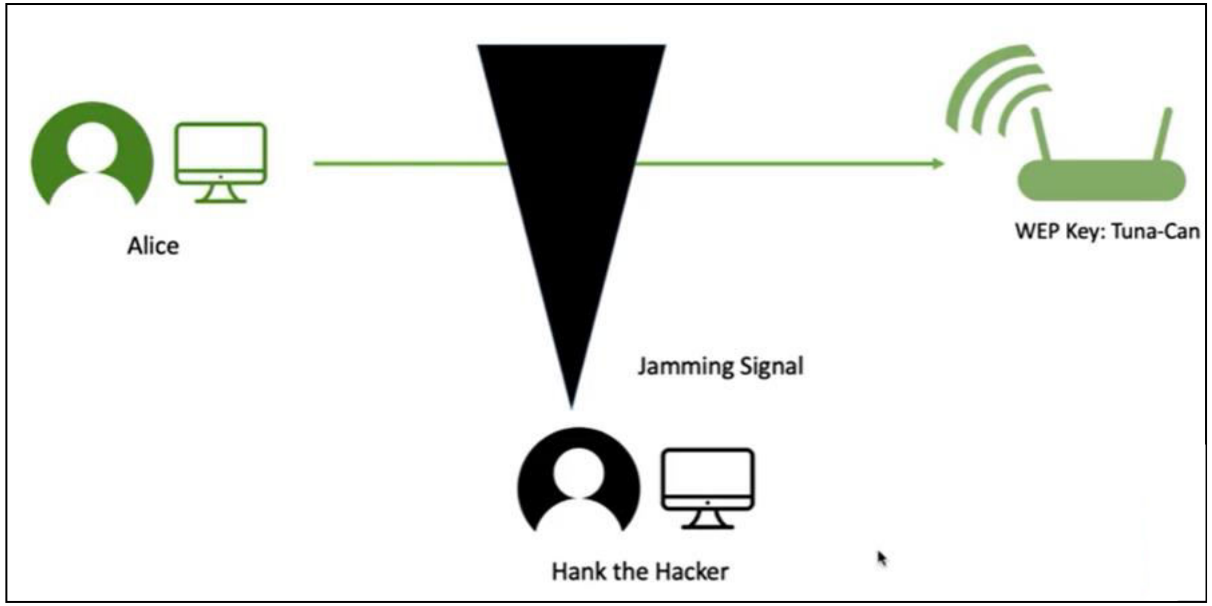
Jamming Wireless Security Attack

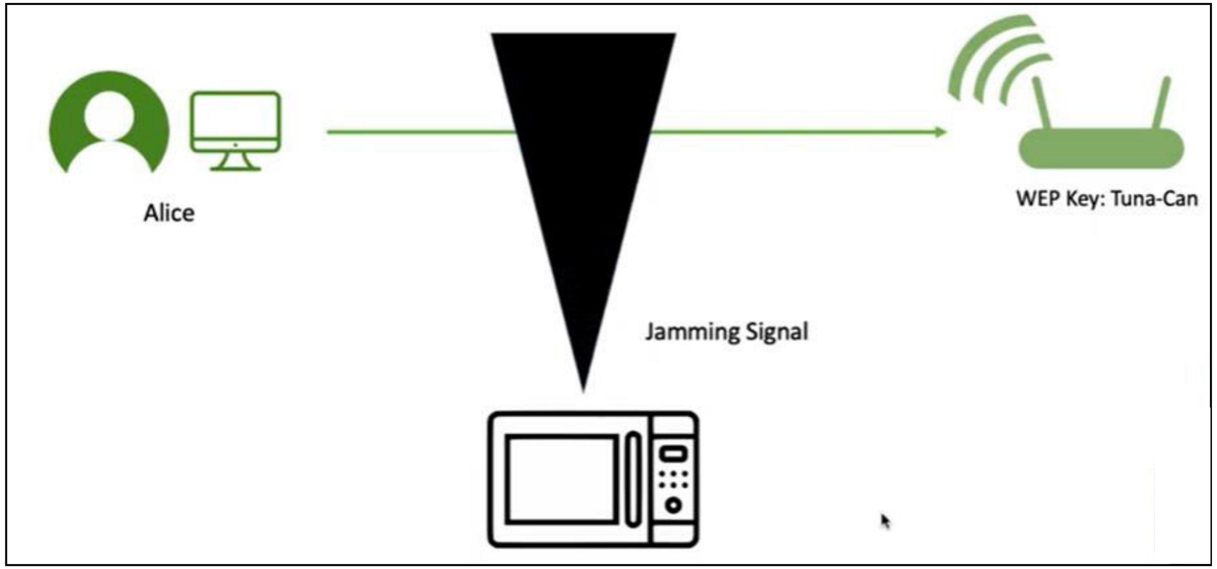
- Broadcasting "Noise" on a Wireless Network
- Increasing the Noise to Signal Ratio
- Denial of Service

Jamming Types

- Intentional
  - Attack
- Unintentional
  - Microwave

- Constant: The Jamming is Occurring all the time
- Reactive: The Jamming only Occurs when System are Trying to Communicate





Wireless Attacks and Security

War Driving Wireless Security Attack

It is a act of driving around for the purpose of searching a Wi-Fi network specially for unsecured networks with weak password.

- **War Driving:** War driving comes from an old term called war dialing, where people would dial random phone numbers in search of modems.
- War driving is basically people driving around looking for vulnerable APs to attack. People will even use drones to try and hack APs on higher floors of a building.
- A company that owns multiple floors around ten stories up might assume nobody is even in range to hack their wireless, but there is no end to the creativity of hackers!

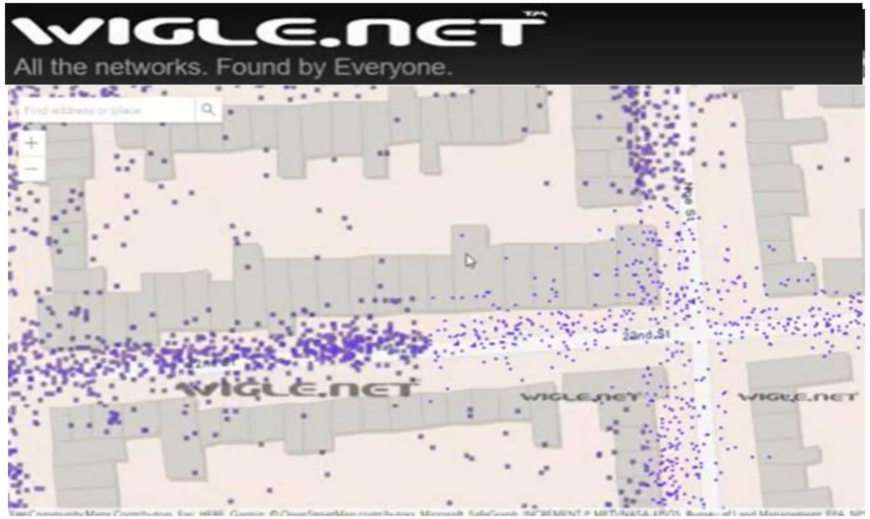
WIGLE.NET
All the networks. Found by Everyone.

Protect War Driving Wireless Security Attack

"Hiding the SSID" is a good practice

However, it is NOT an end-all solution

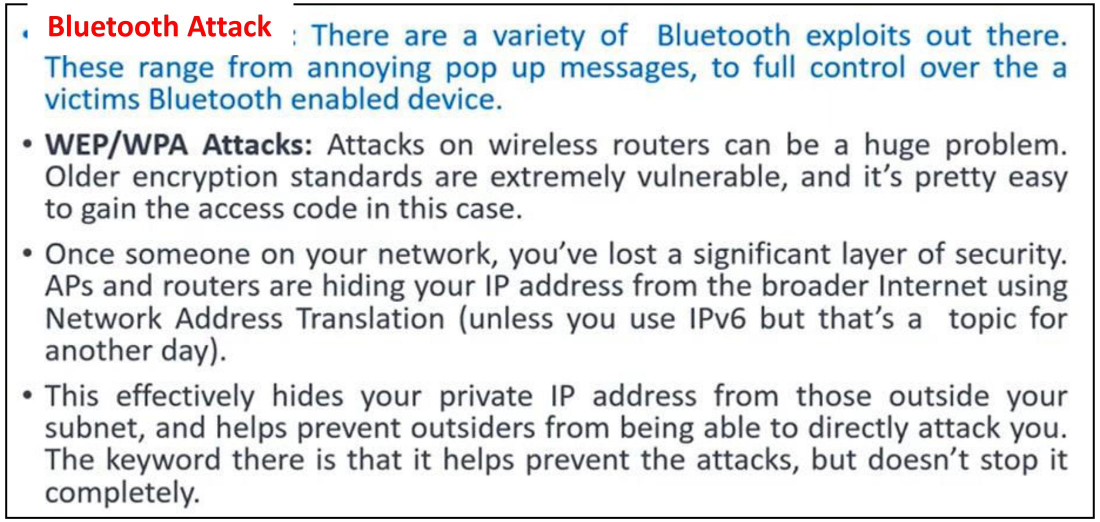
Many wifi-analyzers and wardriving tools are publicly available



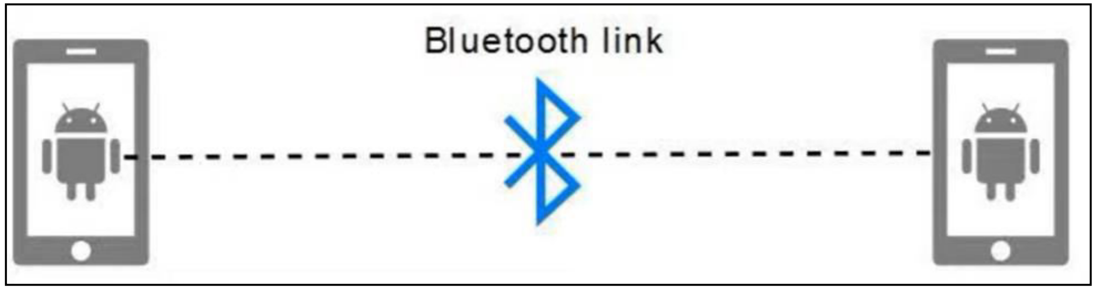
Zoom in

Wireless Attacks and Security

Bluetooth attack Wireless Security Attack



- **Bluetooth Attack** : There are a variety of Bluetooth exploits out there. These range from annoying pop up messages, to full control over the a victims Bluetooth enabled device.
- **WEP/WPA Attacks:** Attacks on wireless routers can be a huge problem. Older encryption standards are extremely vulnerable, and it's pretty easy to gain the access code in this case.
- Once someone on your network, you've lost a significant layer of security. APs and routers are hiding your IP address from the broader Internet using Network Address Translation (unless you use IPv6 but that's a topic for another day).
- This effectively hides your private IP address from those outside your subnet, and helps prevent outsiders from being able to directly attack you. The keyword there is that it helps prevent the attacks, but doesn't stop it completely.



Methods of Bluetooth attack

1. Bluejacking
2. Bluesnarfing
3. Bluebugging

Blue jacking Bluetooth attack

A hacker can launch a bluejacking attack in just a few simple steps.

1. The attacker finds a Bluetooth-enabled device in their immediate vicinity.
2. They pair their own device with the victim's. If they need to authenticate themselves with a password to establish the connection, they can use brute force software, cycling through multiple password combinations until they find the right one.
3. Once they've connected, they can spam the victim with messages and even send them images.

Bluesnaring Bluetooth attack

Bluesnarfing is a way of stealing information using an unsecured Bluetooth connection. Hackers exploit vulnerabilities in Bluetooth tech to break into Bluetooth-connected devices like mobiles, laptops, personal digital assistants, etc. Using bluesnarfing, cybercriminals can potentially get access to personal data like **contacts**, **messages**, **pictures**, **videos**, and even **passwords** from the device of their victim!

Wireless Attacks and Security

Bluebugging Bluetooth attack

Bluebugging is a type of cyber attack done on the Bluetooth enabled devices. The attack allows the hacker to access the cell commands and infiltrate the phone calls, read and send SMS. The attack even allows any hacker to modify the contact list, connect to the internet and eavesdrop on any phone conversation and record it.The attack was developed after the onset of **bluejacking** and **bluesnarfing**.

Procedure For The Attack

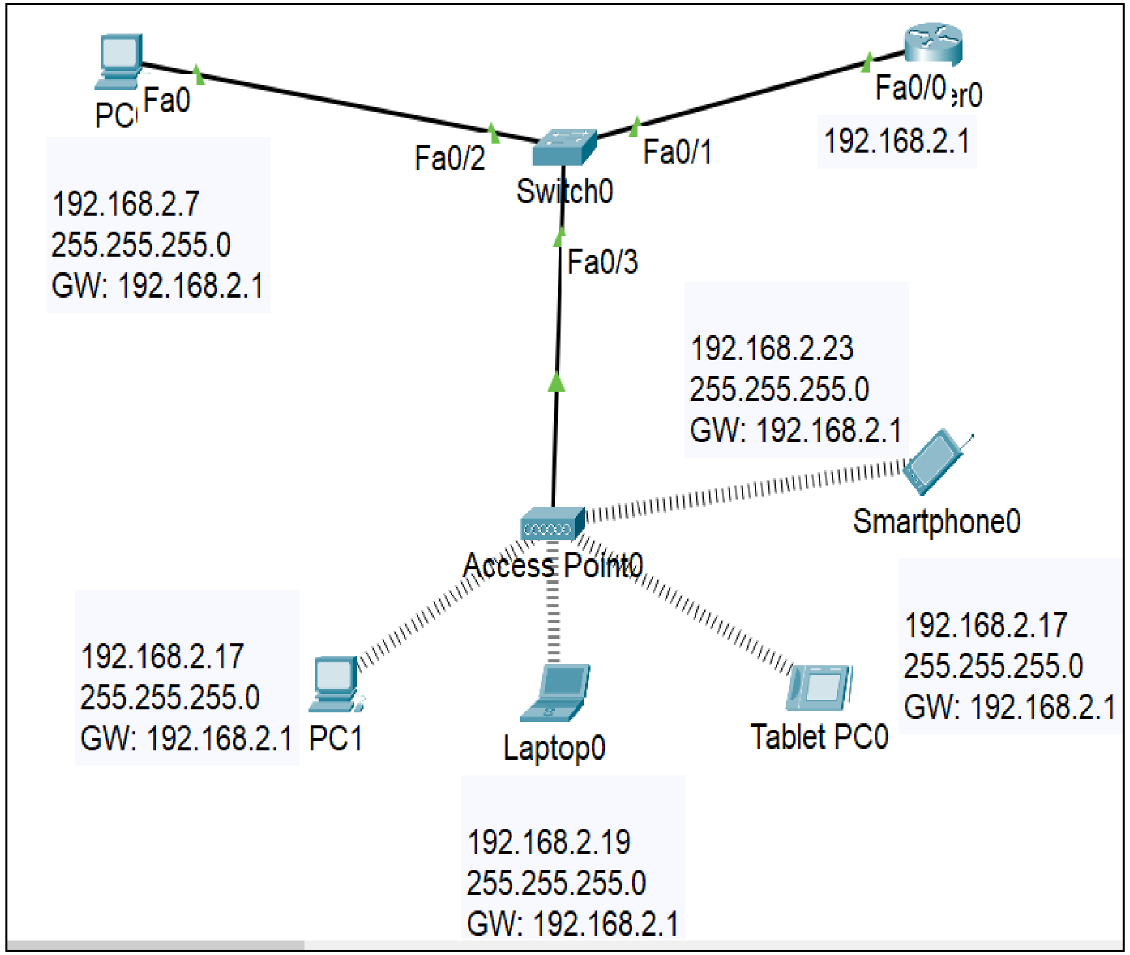
1. For this attack to happen the most important condition is that the victim cell should ON and the bluetooth should be in discoverable mode in victim cell.
2. If these conditions are met then the hacker first initiates the connection to the victim device. If the connection is established, then the hacker uses this connection to install the backdoor in the victim device. The backdoor then exploit several security vulnerabilities such as remote code execution vulnerability, local privilege escalation vulnerability etc. and give the unauthorized access of the victim device to the hacker.
3. Due to the backdoor, the hacker device remain listed in the victim cell and as a trusted device. The hacker then uses this attack to control the victim cell by entering AT commands and can even control the victim Bluetooth headset to perform malicious activities.

Blue jacking Bluetooth attack

The attack can be prevented by:

- Keeping the Bluetooth OFF when not in use.
- Reset the Bluetooth settings to take off all the devices from the trusted list.
- Set the device to the hidden, invisible or the non-discoverable mode when using the Bluetooth.
- Keep the Bluetooth off in public places, including restaurants, stores, airports, shopping malls, train stations, etc.

Wireless Network with PT



//Wireless network
//Router: 1941, Switch: 2950-2A, Access-Point-PT
//For PC1 Go to Pysical Device View-->Power off-->Remove Network Card-->
// -->Insert WMP300N wireless card-->Power on
//For Access-Point Go to Configuration-->Port 1
// -->WEP--> Set Key=1234567890 and SSID="CSE 4215"
//Select PC1-->Desktop Tab-->PC Wireless-->Select Connect Tab & Refresh
//Configure PC1, Laptop and Tablet with IP,Subnet and Gateway
//check whether the laptop has wireless card or not
//After connect to access point check IPs for the host devices
//For Tablet Select Config-->Wireless0-->Select WEP-->Set key 1234567890
//-->Set SSID to "CSE 4215 (Free)" and Check Ips
// Do as same for SmartPhone as Tablet

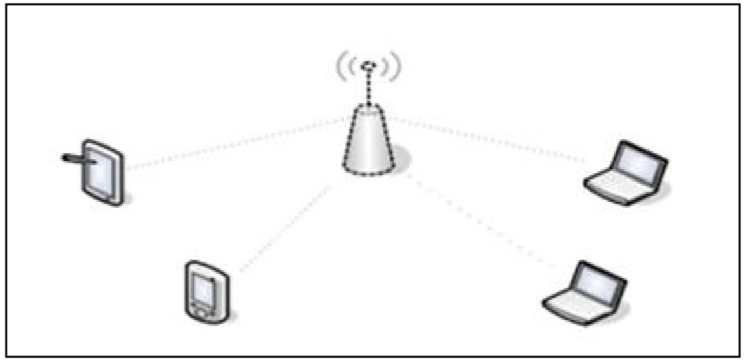
Wireless Ad hoc Network

What is wireless ad hoc network?

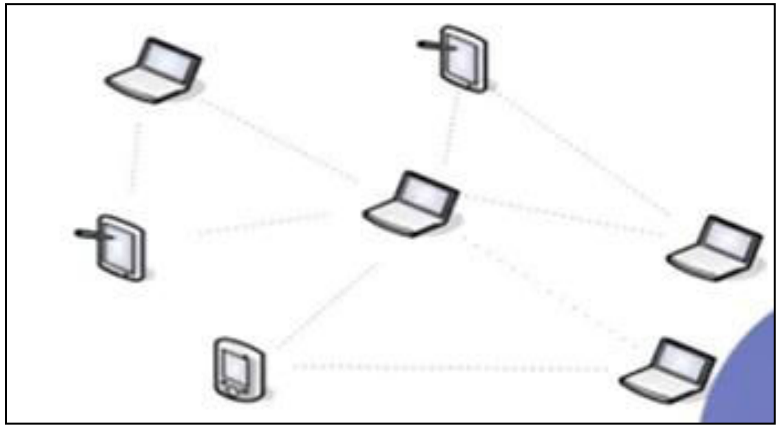
A **wireless ad hoc network** (WANET) is a type of local area network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring typical network infrastructure equipment, such as a wireless router or access point. When Wi-Fi networks are in ad hoc mode, each device in the network forwards data that is not intended for itself to the other devices.

Properties of Wireless Ad hoc Network

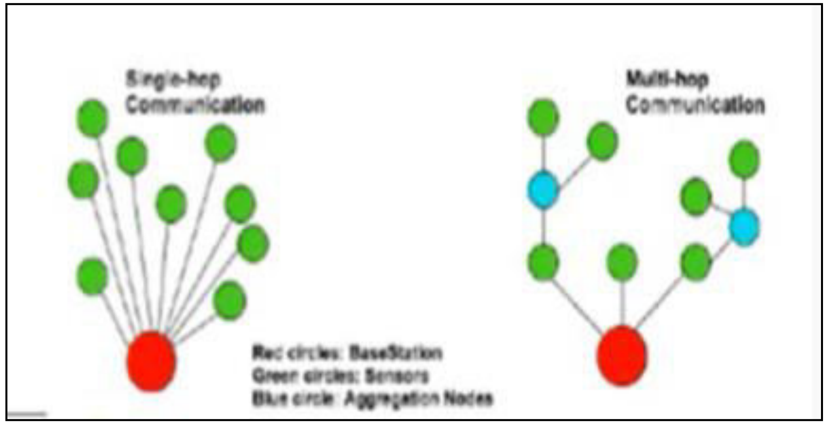
1. Decentralized wireless network
2. No need of network infrastructures
3. Zero configuration required
4. One fly network, create any where anytime
5. Multi hop communication
6. Dynamic Topology
7. Self-synchronized
8. Mobile in nature
9. No central controller



Centralized Network



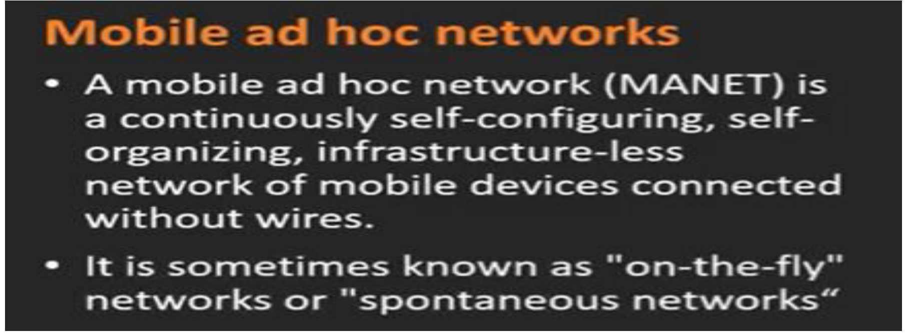
Decentralized Network



Single/Multi hop system

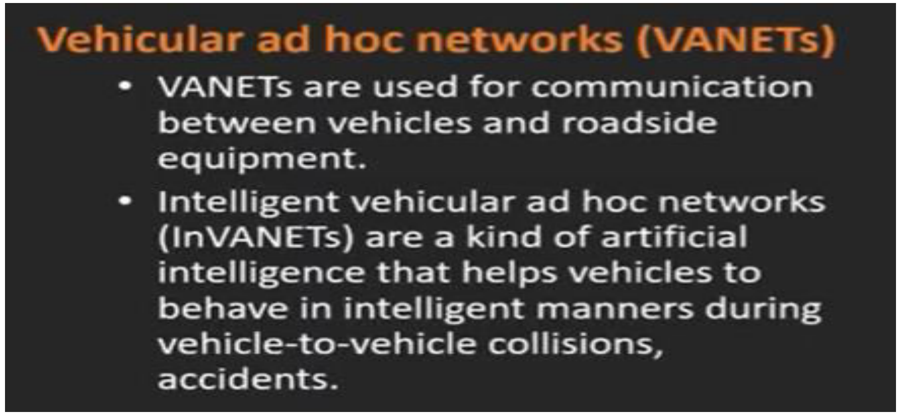
Wireless Ad hoc Network

Applications



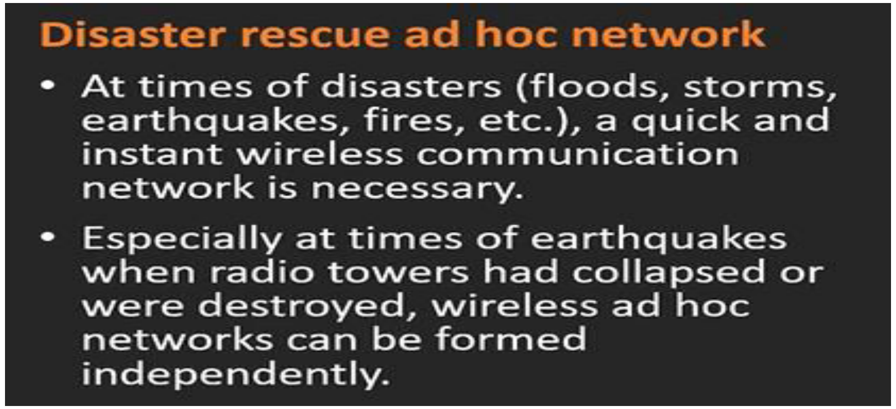
Mobile ad hoc networks

- A mobile ad hoc network (MANET) is a continuously self-configuring, self-organizing, infrastructure-less network of mobile devices connected without wires.
- It is sometimes known as "on-the-fly" networks or "spontaneous networks“



Vehicular ad hoc networks (VANETs)

- VANETs are used for communication between vehicles and roadside equipment.
- Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.



Disaster rescue ad hoc network

- At times of disasters (floods, storms, earthquakes, fires, etc.), a quick and instant wireless communication network is necessary.
- Especially at times of earthquakes when radio towers had collapsed or were destroyed, wireless ad hoc networks can be formed independently.

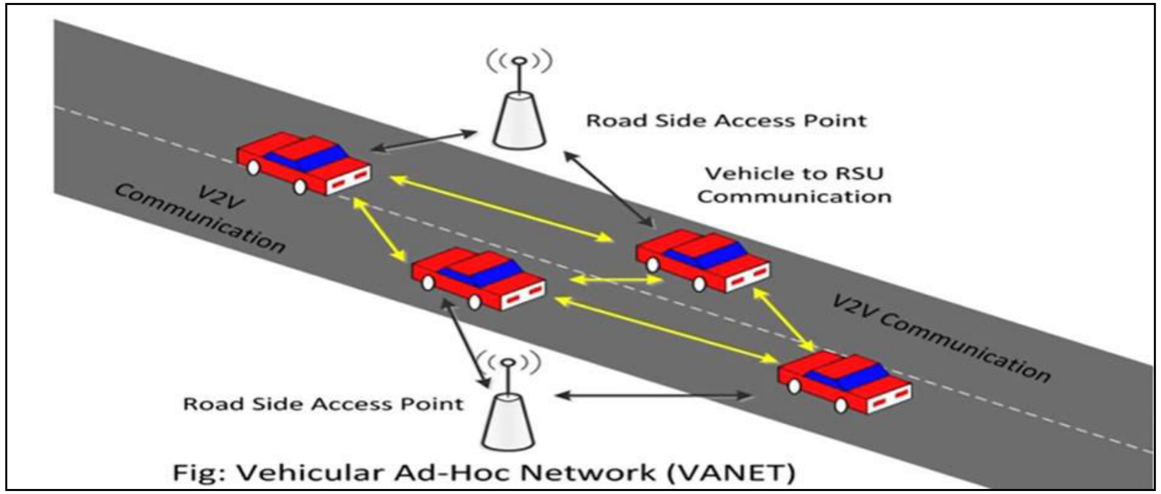


Fig: Vehicular Ad-Hoc Network (VANET)

Wireless Ad hoc Network

Applications

Smart phone ad hoc networks

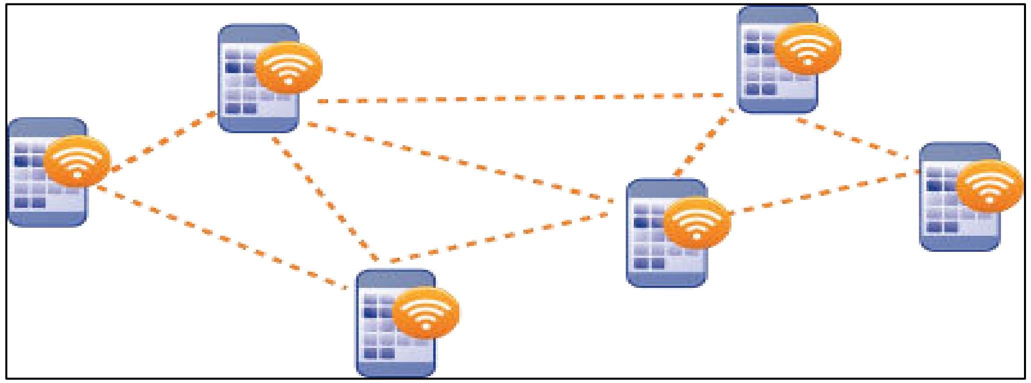
- With the use of Wi-Fi and Bluetooth of Smartphone peer-to-peer networks can be created.
- It is created Without relying on cellular carrier networks, wireless access points, or traditional network infrastructure.

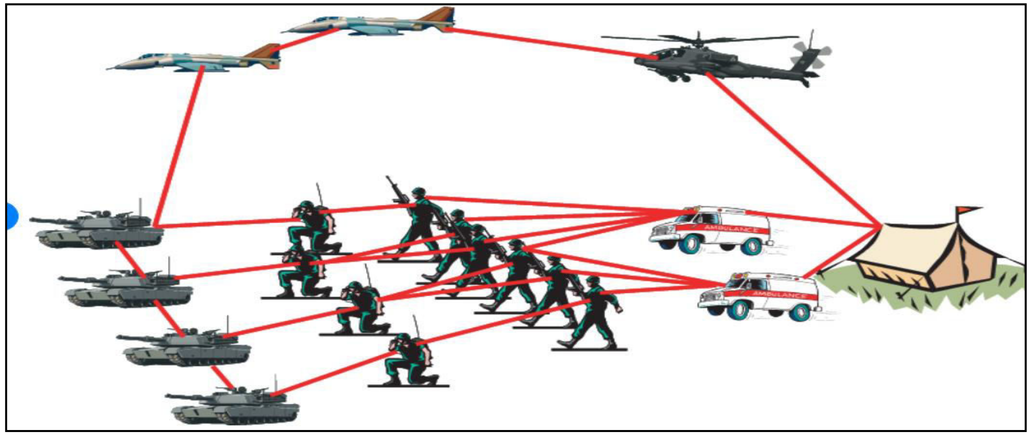
Army tactical MANETs

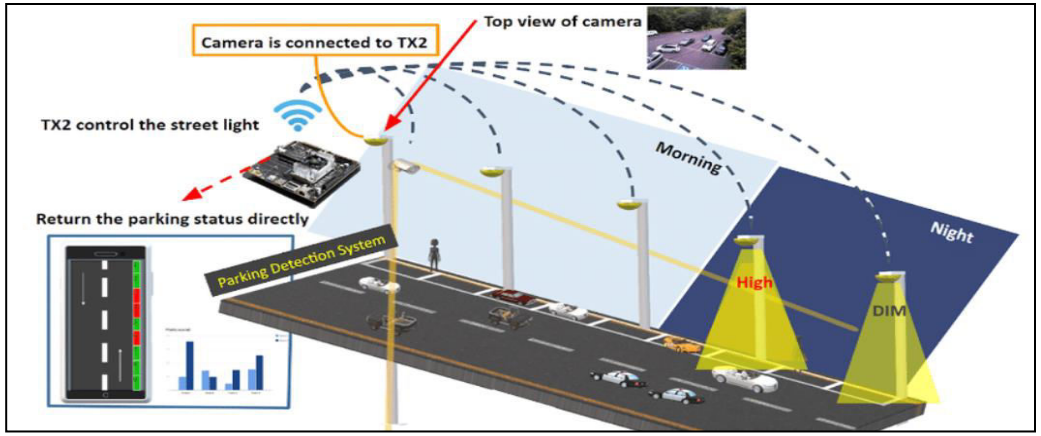
- Army has needed "on-the-move" communications for a long time.
- Ad hoc mobile communications come in well to fulfill this need, especially its infrastructure less nature, fast deployment and operation.

Ad hoc street light networks

- Wireless ad hoc smart street light networks are beginning to evolve.
- The concept is to use wireless control of city streetlights for better energy efficiency, as part of a smart city architectural feature.
- A single gateway device can control up to 500 streetlights.

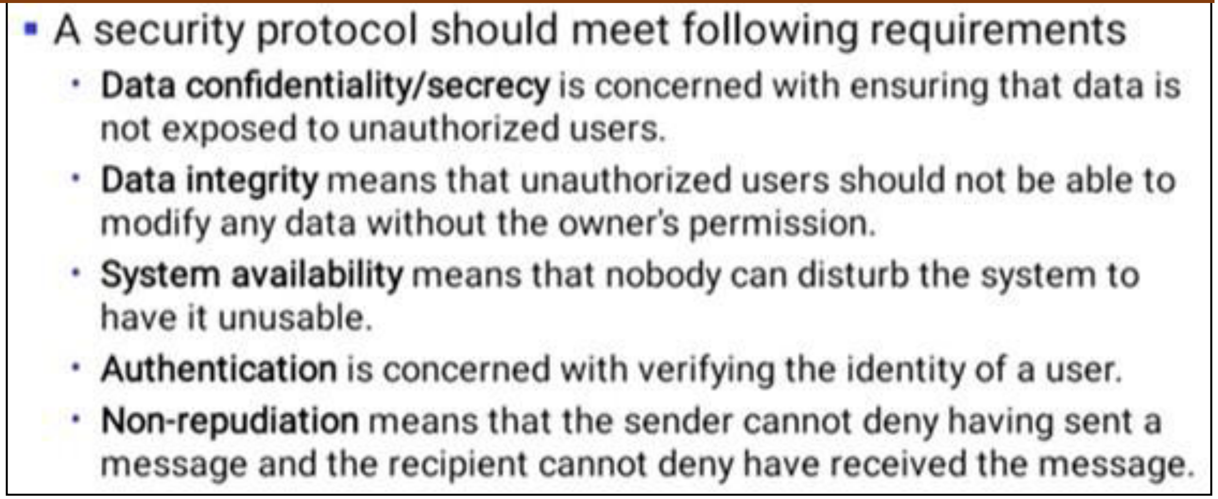





Camera is connected to TX2
Top view of camera
TX2 control the street light
Return the parking status directly
Parking Detection System
Morning
Night
High
DIM

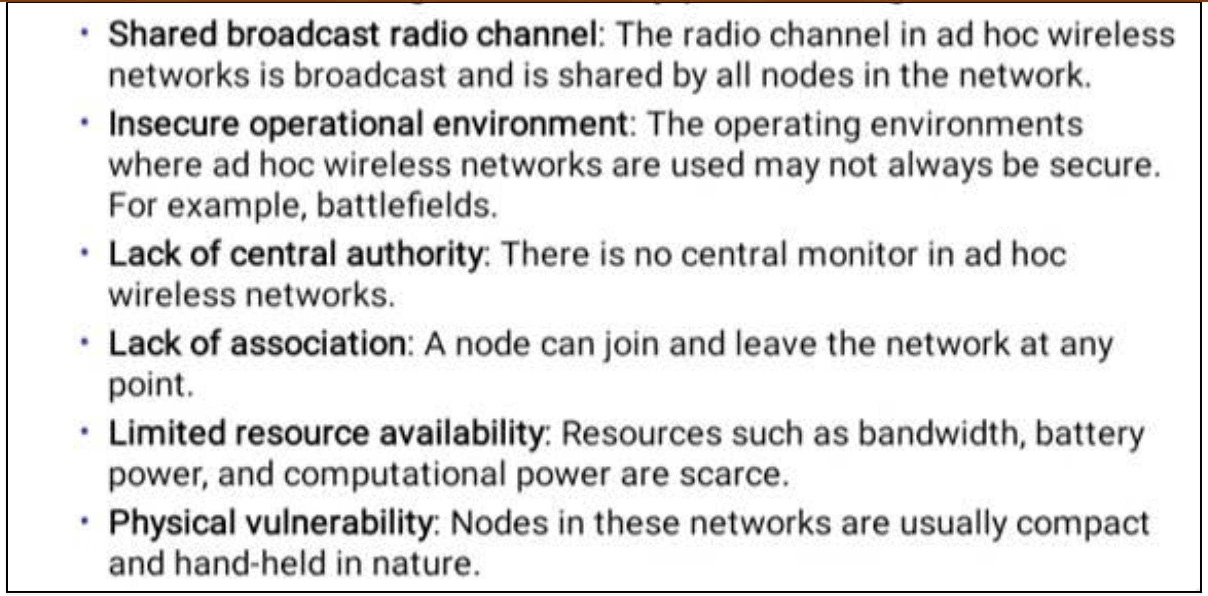
Wireless Ad hoc Network

Securities in Wireless Ad hoc Network



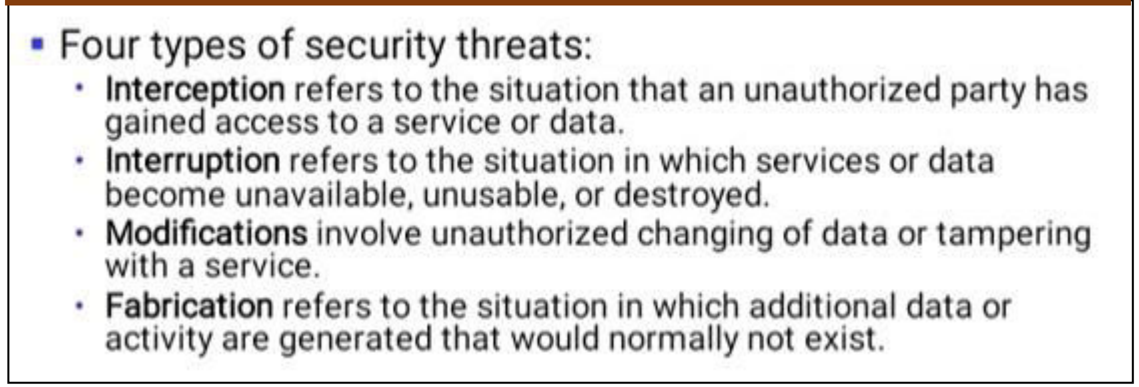
- A security protocol should meet following requirements
  - **Data confidentiality/secrecy** is concerned with ensuring that data is not exposed to unauthorized users.
  - **Data integrity** means that unauthorized users should not be able to modify any data without the owner's permission.
  - **System availability** means that nobody can disturb the system to have it unusable.
  - **Authentication** is concerned with verifying the identity of a user.
  - **Non-repudiation** means that the sender cannot deny having sent a message and the recipient cannot deny have received the message.

Issues and Challenges in Wireless Ad hoc Network



- **Shared broadcast radio channel**: The radio channel in ad hoc wireless networks is broadcast and is shared by all nodes in the network.
- **Insecure operational environment**: The operating environments where ad hoc wireless networks are used may not always be secure. For example, battlefields.
- **Lack of central authority**: There is no central monitor in ad hoc wireless networks.
- **Lack of association**: A node can join and leave the network at any point.
- **Limited resource availability**: Resources such as bandwidth, battery power, and computational power are scarce.
- **Physical vulnerability**: Nodes in these networks are usually compact and hand-held in nature.

Types of Security Threats



- Four types of security threats:
  - **Interception** refers to the situation that an unauthorized party has gained access to a service or data.
  - **Interruption** refers to the situation in which services or data become unavailable, unusable, or destroyed.
  - **Modifications** involve unauthorized changing of data or tampering with a service.
  - **Fabrication** refers to the situation in which additional data or activity are generated that would normally not exist.

Wireless Ad hoc Network

Creating Ad hoc network with Windows 10

The **ad hoc** wireless connection switches your PC to a virtual Wi-Fi router permitting internet connection to other devices, although each with a different IP address..

Steps to create Ad hoc wireless networkcm

- Follow the steps below and check if it helps you with the Setup.
- Right click on the start button.
- Choose the **Command Prompt (Admin)**.
- Write "***netsh wlan set hostednetwork mode=allow ssid= key=***"
- Now substitute the markup tags with your desired entries.
- In the place of "**network name**" provide your desired network name and instead of "**pass key**" provide your key which should not be less than 8 characters.
- Afters etting up the hosted network, you need to start it.
- And to do so, type the following command "***netsh wlan start hostednetwork***"

Steps contd…

- Now open **Windows 10 Control Panel**.
- Choose **Network and Sharing Center**.
- On the left pane of **Network and Sharing Center** window, click the link **Change Adapter Settings**.
- This will open up **Network Connections.**
- Here, or the recently created **Wi-Fi** connection you need to turn on the **Internet Connection Sharing.**
- And to do so right click on the internet connection device which is currently connected to the internet.
- Navigate to the **Sharing**
- Select the checkbox which asks you to
- ***Allow other network users to connect through this computer's Internet connection.***
- And then use the drop down menu and select the recently created **ad hoc**
- You can get the **IP address** of the recently created **ad hoc** connection by double clicking the **TCP/IPv4 Properties** under the **Networking Tab.**
- Now you can connect any of your **Wi-Fi** able devices with your **Windows 10**