CMR
INSTITUTE OF
TECHNOLOGY

USN | | | | | | | | | |

Internal Assesment Test - III

Sub:	WIRELESS COMMUNICATION							Code:	10EC81
Date:	25/ 5/ 2017	Duration:	90 mins	Max Marks:	50	Sem:	VIII	Branch:	ECE
Answer Any FIVE FULL Questions									

		Marks	OBE	
			CO	RBT
1.	With relevant sketches, explain cellular capacity expansion techniques.	10M	CO4	L4
2.a)	Write a note on power control and power saving schemes in a cellular system.	6M	CO3	L2
b)	Determine the frequency reuse distance for a cluster size of 7 and cell radius of 5 km. Repeat the same for cluster size of 4.	4M	CO2	L3
3.	Distinguish frequency hopping and direct sequence spread spectrum techniques.	10M	CO5	L4
4.	Explain the components of Bluetooth architecture with relevant figure.	10M	CO6	L4
5.	Write a note on (i) RAKE receiver. (ii)Smart antenna Technology	5M 5M	CO4	L3
6. a)	Write a note on wireless LAN security problems	5M	CO6	L5
b)	Describe the differences between WLAN and WPAN	5M		

IAT 3 Solutions

1. With relevant sketches, explain cellular capacity expansion techniques. **10M**

- Cellular capacity is a number of users in a cell.
- The approaches to capacity expansion are either architecturally or technologically enabled. They are
  1. ***Cell splitting***
  2. ***Cell sectoring***
  3. ***Overlaid Cells***
  4. ***Channel allocation***
  5. ***Other capacity expansion schemes***
     - *Lee's Microcell Technology*
     - *Smart Antenna Technology*
     - *Migration to Digital Technology*

1. Cell splitting

- The process of subdividing a ***congested*** cell into smaller cells. (each with its own base station and a corresponding reduction in antenna height and transmitter power)
- Cell splitting preserves the geometry of the architecture and therefore simply scales the geometry of the architecture
- The increased number of cells would increase the number of clusters which in turn would increase the number of channels reused, and capacity

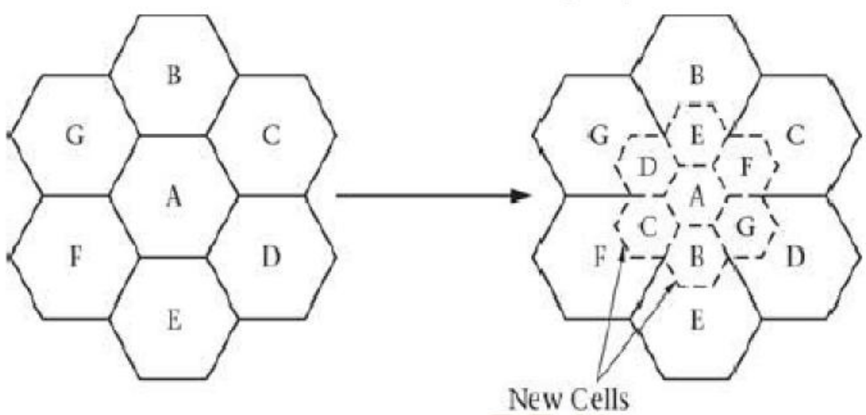


Fig: 3.4 Increase capacities by cell splitting

- Figure 3.4 shown assume that Cell A has become saturated and is unable to support its traffic load. Using cell splitting, six new smaller cells with approximately one-quarter the area of the larger cells are inserted into the system around A in such a way as to be halfway between two co channel cells. These smaller cells will use the same channels as the corresponding pair of larger co channel cells.
- In order that the overall system frequency reuse plan be preserved, the transmit power of these cells must be reduced by a factor of approximately 16 or 12dB.
- As the splitting process moves toward completion the number of channels in the small cells will increase until eventually all the channels in the area are used by the lower-power group *of* cells and the original Cells A has had its power reduced and also joins the new smaller cluster.
- As traffic increases in other areas of the system this process may be repeated over again, eventually the entire system will be resealed with smaller cells in the high-traffic areas and larger cells on the outskirts of the system or in areas of low traffic or low population density.
- **Conclusion:**
  Cell splitting effectively increases system capacity by reducing the cell size and therefore reducing the frequency reuse distance thus permitting the use of more channels.

- **Advantages:**
  - Increases the system capacity.
  - Reduces the cell size, frequency reuse distance.
  - Increases the number of channels.
- **Disadvantages:**
  - Co channel interference increases
  - Difficult to acquire appropriately located cell sites
  - Prolonged conversion process, different cell size exists in the same area.
  - No. of base station increases
  - Trunking efficiency decreases and Handoff process increases

2. **Sectoring**

- It increase capacity is to keep the cell radius unchanged and seek methods to decrease the D /R ratio.
- Uses directional antennas by replacing a single Omni-directional antenna at the base station. It split the cell in to 3 new cells of 120° apart as shown in fig 3.5.

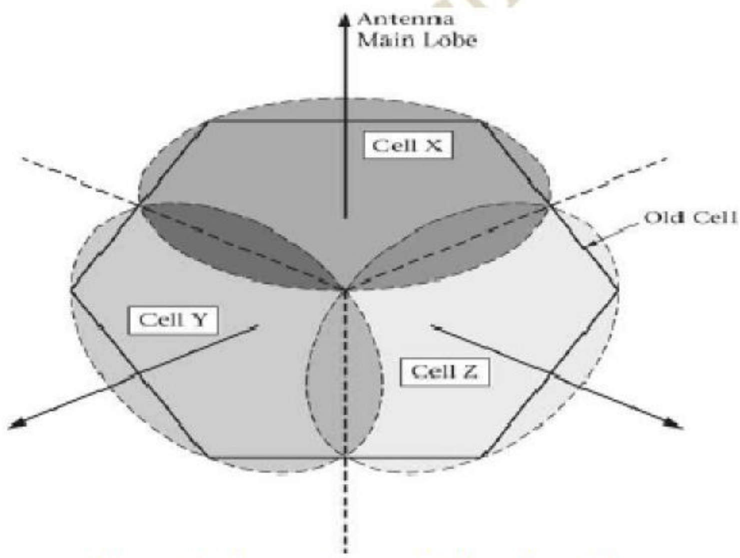


Figure 3.5: Increasing capacity by cell sectoring

- It provides interference reduction, hence S/I ratio increases.
- It does not require new cell sites and additional antennas and triangular mounting only.
- Demerits: Increased network system architecture complexity
- Illustration of interference reduction due to cell sectoring as explained with fig 3.6
- As shown in Figure 3.6 the sectoring of a cell results in a reduction in the amount of interference that the sector experiences from its co channel neighbors in adjacent

clusters and conversely the amount of interference that the sector supplies to its co channel neighbors.

3. Overlaid Cells

- It was first introduced in the section on cell splitting.
- This method can be used to expand the capacity of cellular systems in two ways.
    1. Split-band analog systems.
    2. Reduced cluster size systems

1. Overlaid cells in a split-band system: A wideband analog system could be upgraded to increase its capacity by overlaying and analog system with narrower bandwidth requirements over it. Which is shown in figure 3.7

In such a split-band overlay system, channels are divided between a larger macrocell (using AMPS or TACS) and the overlaid microcell (using NAMPS or NTACS) that is contained in its entirety within the macrocell.

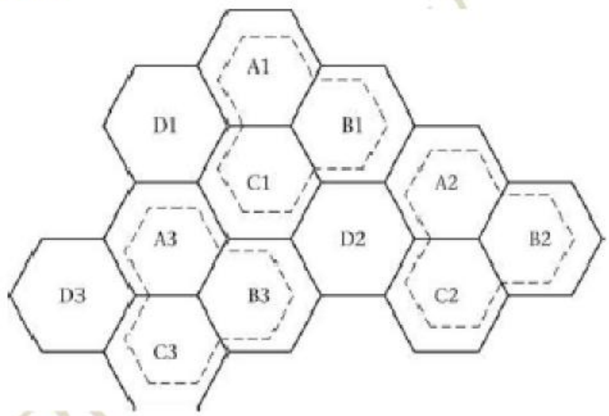


Figure 3.7 Overlaid cells in a split-band system

The channels assigned to the macrocell are used to service users in the area between the microcells, and the channels assigned to the microcells service the microcells. With correct system design of two areas just mentioned will be equal in size. The net effect of this design is an increase in the total number of system channels since now the entire system bandwidth is allocated to both the original wideband system and newer, more efficient narrowband system. This type of system migration requires the use of dual-mode mobile stations.

2. Overlaid cells in a reduced cluster size system: It may be applied to GSM or NA-TDMA systems. As an example of this method, consider a system with a cluster size of N=4. On the top of this system, a cluster of overlaid cells is applied with a cluster size of 3 as shown in figure 3.8. If the channels for the overlaid cell cluster are taken from the underlaid cluster, the system capacity increases since the area needed for the overlaid system for the overlay system, the greater the increase in system capacity. This type of expansion allows operators to migrate their systems using the same base station and mobile station equipment.

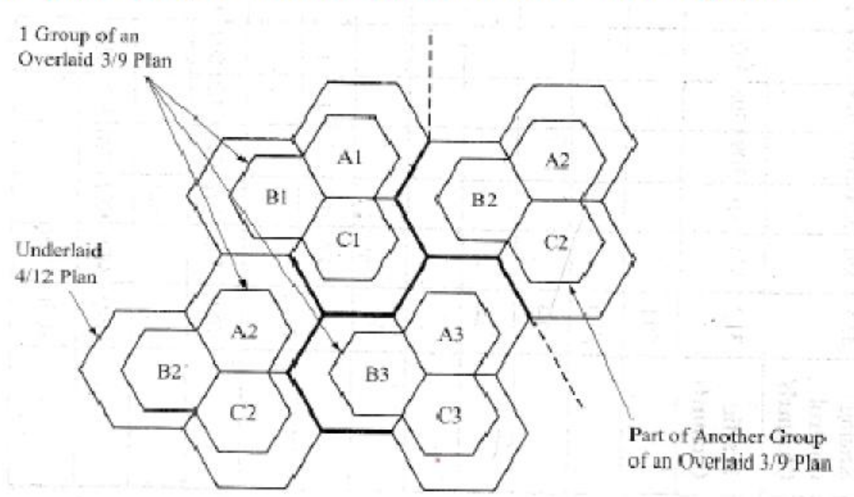


Figure 3.8 Overlaid cells in a reduced cluster size system

1. **Channel allocation**
   - Need for channel allocation to handle random traffic with different scenarios of activities that might cause the amount of traffic to change. They are
   - *Traffic in each cell is dynamic*: For example
     - During the events like rock concerts and sporting events, the amount of traffic offered to cellular systems can change drastically for short periods on the scale of hours.
     - Other events like golf tournaments or state fairs could change traffic intensity for a week or longer.
     - The business district of a metropolitan area may experience changing levels of traffic over the course of workday.
     - The first scenario is so extraordinary that it is very difficult to design anything in to the system to handle the extremely large increase in traffic offered to the system. In many such cases, cellular providers will bring in portable cellular sites (sometimes known as "cells on wheels" or COWs) to handle the increased demand.
     - A national cellular service provider may have dozens of COWs that are deployed all over the country at any given time.
     - COWs are also deployed during natural disasters to restore disrupted communications.

- ***Three main methods to achieve efficient channel allocation***

1. Fixed channel scheme: The procedures of this scheme are

- Examines system wide traffic patterns over time.
- Allocating additional channels where needed to *"fine-tuning"* of the system. This means that instead of equally dividing up the channels over the cells, some cells will receive larger channel allocations than others.
- Use very complex algorithms to determine the final allocation of channels, and these allocations are periodically updated as a traffic usage database grows and new patterns of use emerge and periodically update this process.

2. Channel borrowing scheme: This scheme performs

- A high-traffic cell can borrow channels from low-traffic cells and keep them as needed or until the offered traffic returns to normal.
- While borrowing channel, it should not effect on performance of the borrowed cell.
- After the traffic over the borrowed channel is complete, the channel is returned to use in its original cell.

3. Dynamic channel allocation (DCA): It performs

- All the available channel are placed in channel pool
- Each channel assigned new call based on Signal to interference statistics
- Each Channel can used by each cell until SIR is met.
- This is an extremely complex system that uses many network resources to accomplish its operation.

---

6. Other capacity expansion schemes

1. Lee's Microcell technology
2. Smart Antenna Technology
3. Migration to newer technology

2. a) Write a note on power control and power saving schemes in a cellular system. 6M

- Transmission powers represent a key degree of freedom in the design of wireless networks.
- Power management includes Interference management, Energy management and Connectivity management.
- We know that cellular systems the use of many closely spaced low-power RBSs allows for frequency reuse and hence increased system capacity. At the same time, Interference also increases.
- Interference can reduce by use of power control algorithms for the adjustment of the MS output power and RBS output power allow for nearly constant received signal strength at both the MS and RBS receivers.
- This use of power control provides several system advantages: the amount of co channel interference (CCI) is reduced.
- The last advantage has additional ramifications in the reduction of battery requirements, which translates to longer time between charging and lighter and smaller mobile terminals.
- **Types of power control**

- Transmission powers represent a key degree of freedom in the design of wireless networks.
- Power management includes Interference management, Energy management and Connectivity management.
- We know that cellular systems the use of many closely spaced low-power RBSs allows for frequency reuse and hence increased system capacity. At the same time, Interference also increases.
- Interference can reduce by use of power control algorithms for the adjustment of the MS output power and RBS output power allow for nearly constant received signal strength at both the MS and RBS receivers.
- This use of power control provides several system advantages: the amount of co channel interference (CCI) is reduced.
- The last advantage has additional ramifications in the reduction of battery requirements, which translates to longer time between charging and lighter and smaller mobile terminals.
- **Types of power control**

1. ***Open-loop power control***
   - Depends solely on mobile unit
   - No feedback from BS
   - Not as accurate as closed-loop, but can react quicker to fluctuations in SS.
2. ***Closed-loop power control***
   - Adjusts signal strength in reverse channel based on metric of performance
   - BS makes power adjustment decision and communicates to mobile on control channel

- **Power control algorithm:** Design objectives are
  - Achieve SIR tolerance with good quality communications
  - Must constantly adjust to change in RSS caused by fading or mobility of MS
  - Usual Power control algorithm has 2 phases
  - *Phase I*: MS registers with BSS, Determine minimum output power, Avoid possibility of a call drop
  - *Phase II:* Additional measurements to reduce power, Output power of RBS is adjusted, Use complex algorithms achieve maximum SIR for all radio links.

- **Power saving schemes*****
  1. ***Discontinuous transmission (DTX)***
     - Transmit during speech only, Extra over head need
     - Compensate low-power background during silence. It is adopted by MS, TRC, BSC
  2. ***Sleep mode***
     - During no activity
     - RF circuitry is powered off
     - Periodical awakening
  3. ***Energy efficient designs***
     - Semiconductor technologies
     - Power efficient modulation schemes
     - Software/hardware design
     - DSP technology

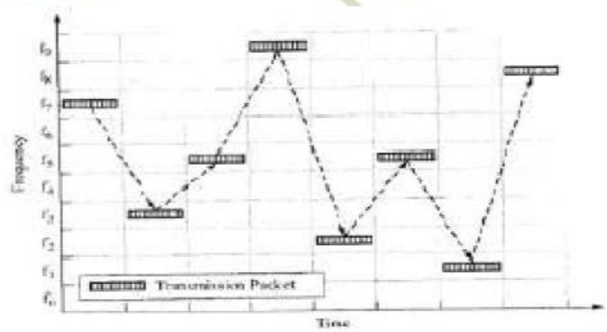
b) Determine the frequency reuse distance for a cluster size of 7 and cell radius of 5 km. Repeat the same for cluster size of 4. **4M**

(1). for N=7, wkt $D = R(3N)^{1/2} = 5(3*7)^{1/2} = 5(21)^{1/2} = 5(4.5823) = 22.913$ *km.*

(2). For N=4, $D = 5(3*4)^{1/2} = 5(12)^{1/2} = 5(3.464) = 17.32$km. *Hence a smaller cluster*

3. Distinguish between frequency hopping and direct sequence spread spectrum techniques. **10M**

1. Frequency Hopping Spread Spectrum (FHSS): It consists of a system that changes the center frequency of transmission on a periodic basis in a pseudorandom sequence. Here data are transmitted through number of different carrier frequencies hops. All the carrier frequency hops independent from one another. For the system to work both the transmitter and receiver must have prior knowledge of the hopping sequence. Figure 8-15 shows an example of a FHSS system.



gure 8-15 Frequency hopping spread spectrum example.

As the transmitter implements the hopping sequence the effective signal bandwidth increases to include all of the utilized carrier frequencies. The use of FHSS does not provide any improvement in a noise-free environment.

2. Direct Sequence Spread Spectrum (DSSS): Here a spreading code is applied to the baseband data stream at the transmitter and the same spreading code is applied to the received signal to perform demodulation. The number of chips per second now determines the basic bandwidth of the transmitted signal. DSSS systems improved noise immunity provided by the increased signal bandwidth. Special orthogonal Walsh codes are used as part of the spreading process. Walsh code property is increase the system capacity in a limited amount of frequency spectrum.

4. **Explain the components of Bluetooth architecture with relevant figure.** **10M**

- Figure 10.7 below shows the Bluetooth protocol stack.
- The Bluetooth standard call for a set of communication protocols and a set of interoperable application that are used to support the usages address in the specifications.
- Figure below shows both Bluetooth-specific protocols and other non-Bluetooth-specific protocols.
- The link manager protocol (LMP) and the Logical Link Control And Adaptation(L2CAP) layer protocol are
- Bluetooth specific whereas the protocols within the "Other" box are not.
- Some of these other protocols are the point-to-point protocol (PPP) and wireless application protocol (WAP).

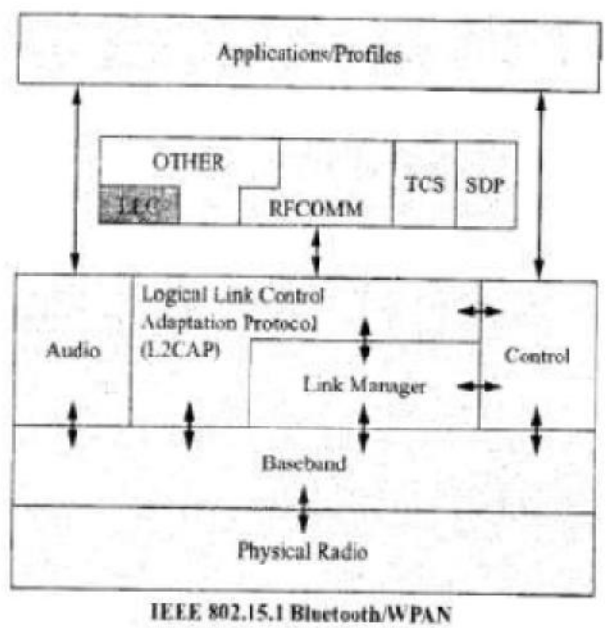


Figure 10–7 The Bluetooth protocol stack (Courtesy of IEEE).

Layer Description:

- *Physical radio layer*: It for Tx and Rx data and voice.
- *Baseband layer*: It enables RF link between Bluetooth devices.
- *Link manager*: It is the protocol that handles link establishment b/w Bluetooth devices which include authentication and encryptions.
- *LLC and L2CAP*: It is connection based communication protocol that implements multiplexing. No flow control. But provide reliable base band link.
- *Audio profile*: It responsible for managing connection for Tx /Rx data from audio devices.
- *Control*: For control signal generations for various activities.
- Other LLC: Link controller for optional device, fax, headsets like cordless phone etc.

5. Write a note on (i) RAKE receiver (ii) Smart antenna Technology

RAKE Receiver

- It is a radio receiver designed to counter the effects of multipath fading.
- It recognizing that multiple signals will arrive at a receiver over the mobile radio channel.
- These receivers isolating the signal paths at the receiver.
- It using several "*sub-receivers*" called *fingers*, that is, several correlators each assigned to a different multipath component.
- Each finger independently decodes a single multipath component; at a later stage the contribution of all fingers are combined in order to make the most use of the different transmission characteristics of each transmission path.
- This could very well result in higher S/I ratio in a multipath environment.
- The rake receiver is so named because it reminds the function of a garden rake, each finger collecting symbol energy similarly to how tines on a rake collect leaves.

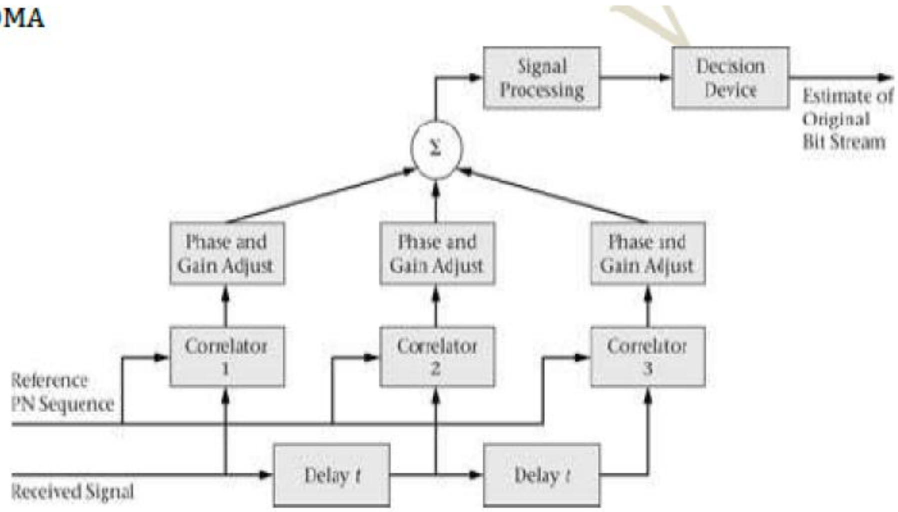


Figure 7.10: RAKE receiver block diagram

- Few RAKE taps possess the ability to dynamically adjust the taps (move the rake fingers) in response to a search algorithm used to locate multipath components.
- These smart receivers standard diversity combining techniques to provide a more reliable receiver output and therefore improve system performance.
- There are potential problems with this type of receiver that are tied to the multipath delay and spread introduced to the radio link.
- The multipath components that can be resolved have a time dependence that is proportional to the inverse of the system chip rate and the system-tolerated multipath spread is proportional to the inverse of the symbol time.
- For the IS-95 CDMA system, using a chip rate of 1.2288 Mcps allows the resolution of multipath components of the order of approximately 1/1.2288 Mcps or 800 ns by the RAKE receiver.
- Typical multipath spreads for outdoor is tens of microseconds and for indoor is few ns.
- In an indoor environment the CDMA RAKE receivers would not able to resolve multipath components.

SMART ANTENNA TECHNOLOGY

- It is one of the 3G specifications.
- This technique to improve system performance makes use of phased array or "beam steering" antenna system.
- Beam steering antenna can use narrow pencil beam patterns to communicate with a subset of the users within the cell.
- Figure 7.9 depicts of a smart antenna system.

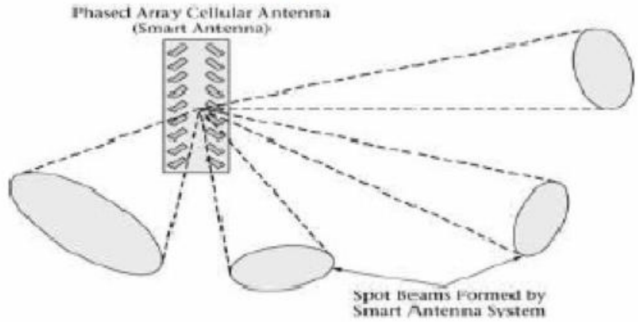


Figure 7.9: depiction of a 3G smart antenna system

- The narrow beam shown in figure 7.9 may be pointed the users always their moving direction through the use of sophisticated antenna technology. It will increase the system performance

6. a) Write a note on wireless LAN security

b) Describe the differences between WLAN and WPAN

Types of Wireless LAN Security Problems

Before discussing the details of wireless LAN security, a quick review of some of the popular types of attacks on these networks will be instructive:

- Eavesdropping: the attacker listens to private communications or steals sensitive information by listening to wireless data traffic.
- MAC spoofing: the attacker is able to identify a valid MAC address of a legitimate network user and makes a copy of it to gain access to the wireless network.
- Dictionary attack: the attacker systematically tries all possible passwords in an attempt to determine the correct one and gain access to the network.
- Man-in-the-middle attack: the attacker impersonates a legitimate access point in order to gain sensitive user information (i.e., passwords and user names) from a legitimate user that has inadvertently attempted to associate with the rouge access point.
- Theft of service: the attacker gains Internet access through the Enterprise or home wireless LAN infrastructure resulting in ISP charges for unauthorized use or the unauthorized sending of e-mail (spam) from the compromised network.
- Session hijacking: the attacker waits until a client has successfully authenticated to the network, sends a disassociation message to the client using the MAC address of the access point, and then starts sending traffic to the access point by spoofing the MAC address of the client.

Differences between WLAN and PAN

Parameters	LAN	PAN
full form	Local Area Network	Personal Area Network
Distance coverage	10m to 100m and even more in wireless LAN case	10m to 100m in wireless PAN network (i.e. zigbee, bluetooth)
Data rate	LAN supports 10, 100 and 1000 Mbps while WLAN supports 54Mbps(as per 802.11a) and above 100Mbps (802.11n/11ac/11ad)	250Kbps in zigbee, From Kbps to 24 Mbps in bluetooth case
Technologies	Wireless LAN or WLAN as per IEEE 802.11 standards	Zigbee, Bluetooth, zwave etc.
Applications	Mainly used for wireless LAN and LAN where in data transfer at high speed is desired.	Used for low data rate and short distance applications