May 2012 Extra

Q. Explain Wi-Fi protected access (WPA) and WPA2.

- Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the WIFI alliance to secure wireless computer networks.
- The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP(Wired Equivalent Privacy).
- WPA (sometimes referred to as the *draft IEEE 802.11i* standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is common shorthand for the full IEEE 802.11i standard.
- A flaw in a feature added to Wi-Fi, called WIFI Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the security vulnerability.
- The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.
- The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.
- WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently

strong data integrity guarantee for the packets it handled.[4] Well tested message authenticated codes existed to solve these problems, but they required too much computation to be used on old network cards.

- WPA uses a message integrity check algorithm to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and the limitations of Michael to retrieve the keystream from short packets to use for re-injection and spoofing.

WPA2

- Short for ***Wi-Fi Protected Access 2***, the follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks.
- Based on the IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1 x-based authentications.
- There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.
- WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES based encryption mode with strong security. Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark.

Q. Explain various terms with respect to wireless transmission.

1) **Hand Off**

Definition - What does *Handoff* mean?

A handoff refers to the process of transferring an active call or data session from one cell in a cellular network to another or from one channel in a cell to another. A well-implemented handoff is important for delivering uninterrupted service to a caller or data session user.

In Europe and other countries, a handoff is known as a handover.

Cellular networks are composed of cells, each of which is capable of providing telecommunications services to subscribers roaming within them. Each cell can only serve up to a certain area and number of subscribers. Thus, when any of these two limits is reached, a handoff ensues.

For instance, if a subscriber moves out of the coverage area of a particular cell while entering another, a handoff takes place between the two cells. The cell that served the call prior to the handoff is relieved of its duties, which are then transferred to the second cell. A handoff may also be triggered when the number of subscribers using a particular cell has already reached the cell’s maximum limit (capacity).

Such a handoff is possible because the reach of the cell sites serving these cells can sometimes overlap. Thus, if a subscriber is within an overlapping area, the network may opt to transfer one subscriber's call to the cell involved in the overlap.

Sometimes a handoff can take place even if no limit is breached. For example, suppose that a subscriber initially inside the jurisdiction of a large cell (served by an umbrella-type cell site) enters the jurisdiction of a smaller cell (one served by a micro cell). The subscriber can be handed off to the smaller cell in order to free up capacity on the larger one.

Handoffs may be classified into two types:

- Hard Handoff: Characterized by an actual break in the connection while switching from one cell or base station to another. The switch takes place so quickly that it can hardly be noticed by the user. Because only one channel is needed to serve a system designed for hard handoffs, it is the more affordable option. It is also sufficient for services that can allow slight delays, such as mobile broadband Internet.

- Soft Handoff: Entails two connections to the cell phone from two different base stations. This ensures that no break ensues during the handoff. Naturally, it is more costly than a hard handoff.

2)Frequency reuse

- In mobile communication systems a slot of a carrier frequency / code in a carrier frequency is a radio resource unit. This radio resource unit is assigned to a user in order to support a call/ session. The number of available such radio resources at a base station thus determines the number of users who can be supported in the call.
- Since in wireless channels a signal is ”broadcast” i.e. received by all entities therefore one a resource is allocated to a users it cannot be re assigned until the user finished the call/ session. Thus the number of users who can be supported in a wireless system is highly limited.
- In order to supported a large no. of users within a limited spectrum in a region the concept of frequency re-use is used.
- The signal radiated from the transmitter antenna gets attenuated with increasing distance. At a certain distance the signal strength falls below noise threshold and is no longer identifiable.
- In this region when the signal attenuates below noise floor the same radio resource may be used by another transmission to send different information. In term of cellular systems, the same radio resource (frequency) can used by two base stations which an sufficient spaced apart.
- In this way the same frequency gets reused in a layer- geographic area by two or more different base station different users simultaneously.
- Now what is important is to select the set of base stations which will use the same set of radio resources/ channel of frequencies or technically the co- channel cells.
- In this context the minimum adjacent set cells which use different frequencies each is calls a cluster.
- The cellular concept is the major solution of the problem of spectral congestion and user capacity.
- Cellular radio relies on an intelligent allocation and channel reuse throughout a large geographical coverage region.

Cellular Frequency Reuse:

- Each cellular base station is allocated a group of radio channels to be used within a small geographic area called a cell. Base stations in adjacent cells are assigned channel groups which contain completely different channels than neighbouring cells.
- Base station antennas are designed to achieve the desired coverage within a particular cell. By limiting the coverage area within the boundaries of a cell, the same group of channels may be used to cover different cells that are separated from one another by geographic distances large enough to keep interference levels within tolerable limits.
- The design process of selecting and allocating channel groups for all cellular base stations within a system is called frequency reuse or frequency planning.