4.5. Channel allocation schemes:

In radio resource management for wireless and cellular network, channel allocation schemes are required to allocate bandwidth and communication channels to base stations, access points and terminal equipment.

The objective is to achieve maximum system spectral efficiency in bit/s/Hz/site by means of frequency reuse, but still assure a certain grade of service by avoiding cochannel interference and adjacent channel interference among nearby cells or networks that share the bandwidth. There are two types of strategies that are followed:-

- Fixed: FCA, fixed channel allocation: Manually assigned by the network operator
- Dynamic:
  - DCA, dynamic channel allocation,
  - DFS, dynamic frequency selection
  - Spread spectrum

4.5.1 FCA :

In **Fixed Channel Allocation** or **Fixed Channel Assignment** (FCA) each cell is given a predetermined set of frequency channels.

FCA requires manual frequency planning, which is an arduous task in TDMA and FDMA based systems, since such systems are highly sensitive to cochannel interference from nearby cells that are reusing the same channel.

This results in traffic congestion and some calls being lost when traffic gets heavy in some cells, and idle capacity in other cells.

4.5.2. DCA and DFS:

Dynamic Frequency Selection (DFS) may be applied in wireless networks with several adjacent non-centrally controlled access points.

A more efficient way of channel allocation would be **Dynamic Channel Allocation** or **Dynamic Channel Assignment** (DCA) in which voice channel are not allocated to cell permanently, instead for every call request base station request channel from MSC.

4.6 Spread spectrum:

Spread spectrum can be considered as an alternative to complex DCA algorithms. Spread spectrum avoids cochannel interference between adjacent cells, since the probability that users in nearby cells use the same spreading code is insignificant.

Thus the frequency channel allocation problem is relaxed in cellular networks based on a combination of Spread spectrum and FDMA, for example IS95 and 3G systems.

In packet based data communication services, the communication is bursty and the traffic load rapidly changing. For high system spectrum efficiency, DCA should be performed on a packet-by-packet basis.

Examples of algorithms for packet-by-packet DCA are **Dynamic Packet Assignment** (DPA), Dynamic Single Frequency Networks (DSFN) and **Packet and resource plan scheduling** (PARPS).

3.6.1 Spread spectrum Techniques:

1 In telecommunication and radio communication, spread-spectrum techniques are methods by which a signal (e.g. an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth.

2 These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection, and to limit power flux density (e.g. in satellite downlinks).

3 Spread-spectrum telecommunications this is a technique in which a telecommunication signal is transmitted on a bandwidth considerably larger than the frequency content of the original information.

4 Spread-spectrum telecommunications is a signal structuring technique that employs direct sequence, frequency hopping, or a hybrid of these, which can be used for multiple access and/or multiple functions.

5 Frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), time-hopping spread spectrum (THSS), chirp spread spectrum (CSS).

6 Techniques known since the 1940s and used in military communication systems since the 1950s "spread" a radio signal

over a wide frequency range several magnitudes higher than minimum requirement.

7 Resistance to jamming (interference). DS (direct sequence) is good at resisting continuous-time narrowband jamming, while FH (frequency hopping) is better at resisting pulse jamming.

8 Resistance to fading. The high bandwidth occupied by spreadspectrum signals offer some frequency diversity, i.e. it is unlikely that the signal will encounter severe multipath fading over its whole bandwidth, and in other cases the signal can be detected using e.g. a Rake receiver.

9 Multiple access capability, known as code-division multiple access (CDMA) or code-division multiplexing (CDM). Multiple users can transmit simultaneously in the same frequency band as long as they use different spreading codes.

1. Compression – Encryption:

At the broadcast center, the high-quality digital stream of video goes through an MPEG encoder, which converts the programming to MPEG-4 video of the correct size and format for the satellite receiver in your house.

Encoding works in conjunction with compression to analyze each video frame and eliminate redundant or irrelevant data and extrapolate information from other frames. This process reduces the overall size of the file. Each frame can be encoded in one of three ways:

- As an **intraframe**, which contains the complete image data for that frame. This method provides the least compression.
- As a **predicted** frame, which contains just enough information to tell the satellite receiver how to display the frame based on the most recently displayed intraframe or predicted frame.

- As a **bidirectional** frame, which displays information from the surrounding intraframe or predicted frames. Using data from the closest surrounding frames, the receiver **interpolates** the position and color of each pixel.

This process occasionally produces **artifacts --** glitches in the video image. One artifact is **macroblocking,** in which the fluid picture temporarily dissolves into blocks. Macroblocking is often mistakenly called **pixilating,** a technically incorrect term which has been accepted as slang for this annoying artifact.

There really are pixels on your TV screen, but they're too small for your human eye to perceive them individually -- they're tiny squares of video data that make up the image you see. (For more information about pixels and perception, see How TV Works.)

The rate of compression depends on the nature of the programming. If the encoder is converting a newscast, it can use a lot more predicted frames because most of the scene stays the same from one frame to the next.

In more fast-paced programming, things change very quickly from one frame to the next, so the encoder has to create more intraframes. As a result, a newscast generally compresses to a smaller size than something like a car race.

1.1 Encryption and Transmission:

After the video is compressed, the provider encrypts it to keep people from accessing it for free. Encryption scrambles the digital data in such a way that it can only be **decrypted** (converted back into usable data) if the receiver has the correct decryption algorithm and security keys.

Once the signal is compressed and encrypted, the broadcast center beams it directly to one of its satellites. The satellite picks up the signal with an onboard dish, amplifies the signal and uses another dish to beam the signal back to Earth, where viewers can pick it up.

In the next section, we'll see what happens when the signal reaches a viewer's house.

1.2 Video and Audio Compression :

Video and Audio files are very large beasts. Unless we develop and maintain very high bandwidth networks (Gigabytes per second or more) we have to compress to data.

Relying on higher bandwidths is not a good option -- M25 Syndrome: Traffic needs ever increases and will adapt to swamp current limit whatever this is.

As we will compression becomes part of the representation or *coding* scheme which have become popular audio, image and video formats.

We will first study basic compression algorithms and then go on to study some actual coding formats.

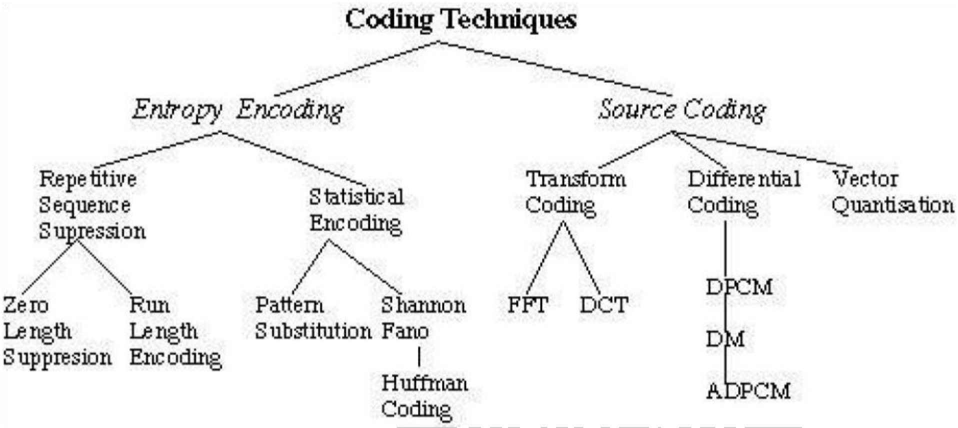


Figure 3.14 *coding* scheme

What is Compression?

Compression basically employs redundancy in the data:

- Temporal -- in 1D data, 1D signals, Audio etc.
- Spatial -- correlation between neighbouring pixels or data items
- Spectral -- correlation between colour or luminescence components. This uses the frequency domain to exploit relationships between frequency of change in data.
- psycho-visual -- exploit perceptual properties of the human visual system.

Compression can be categorised in two broad ways:

Lossless Compression :

-- where data is compressed and can be reconstituted (uncompressed) without loss of detail or information. These are referred to as bit-preserving or reversible compression systems also.

Lossy Compression :

-- where the aim is to obtain the best possible *fidelity* for a given bit-rate or minimizing the bit-rate to achieve a given fidelity measure. Video and audio compression techniques are most suited to this form of compression.

If an image is compressed it clearly needs to uncompressed (decoded) before it can viewed/listened to. Some processing of data may be possible in encoded form however. Lossless compression frequently involves some form of *entropy encoding* and are based in information theoretic techniques.

Lossy compression use source encoding techniques that may involve transform encoding, differential encoding or vector quantization.

1.3 MPEG Standards :

All MPEG standards exist to promote system interoperability among your computer, television and handheld video and audio devices. They are:

- **MPEG-1:** the original standard for encoding and decoding streaming video and audio files.
- **MPEG-2:** the standard for digital television, this compresses files for transmission of high-quality video.
- **MPEG-4:** the standard for compressing high-definition video into smallerscale files that stream to computers, cell phones and PDAs (personal digital assistants).
-
- **MPEG-21:** also referred to as the Multimedia Framework. The standard that interprets what digital content to provide to which individual user so that media plays flawlessly under any language, machine or user conditions.

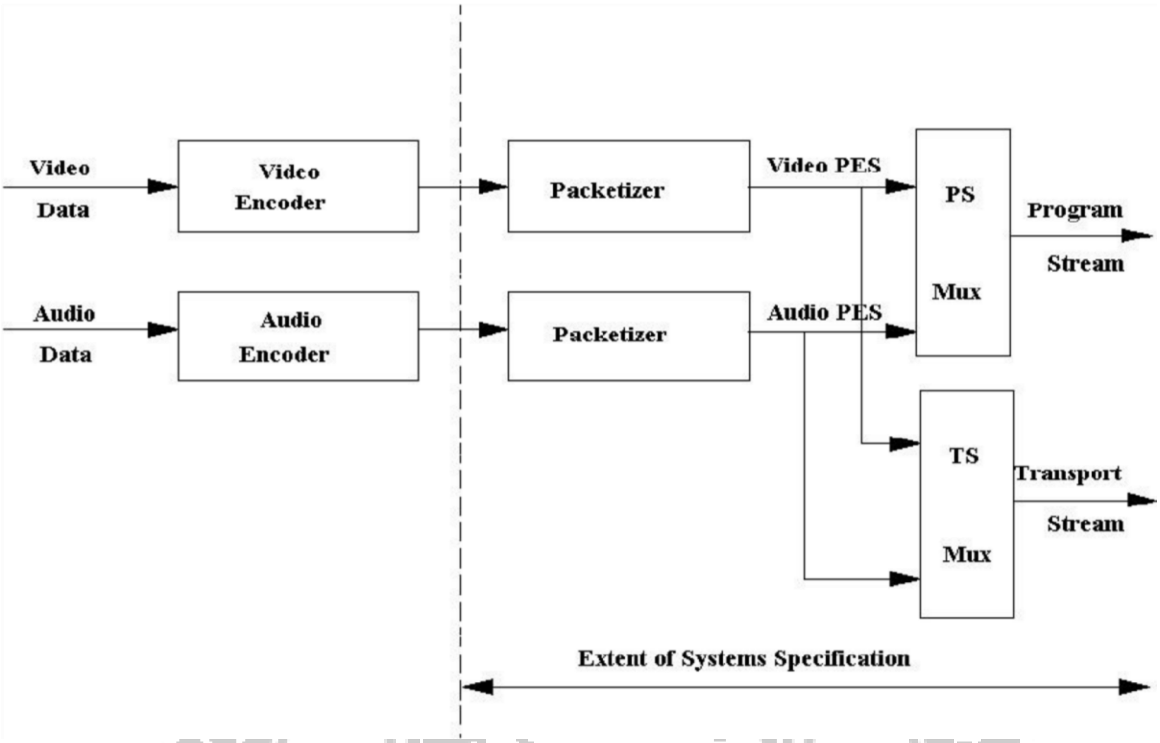


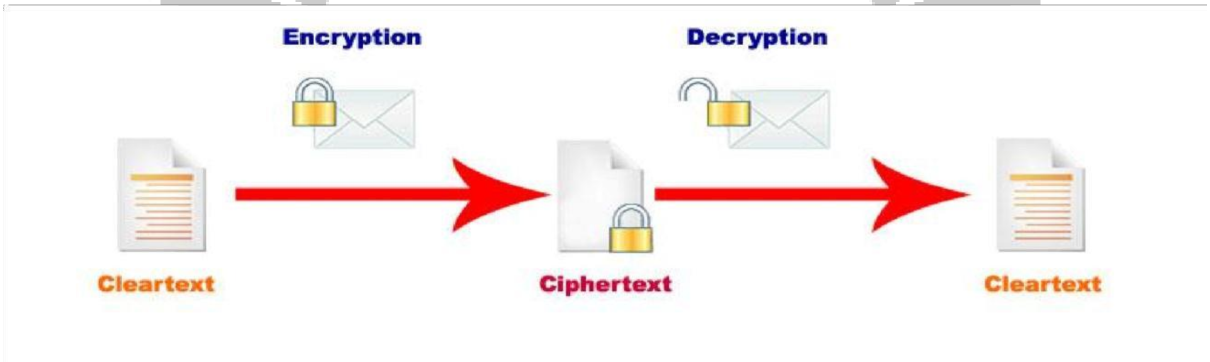
Figure 3.15 MPEG scheme

3 Encryption:

It is the most effective way to achieve data security. To read an **encrypted** file, you must have access to a secret key or password that enables you to decrypt it.

Unencrypted data is called **plain text** ; **encrypted** data is referred to as **cipher text.**

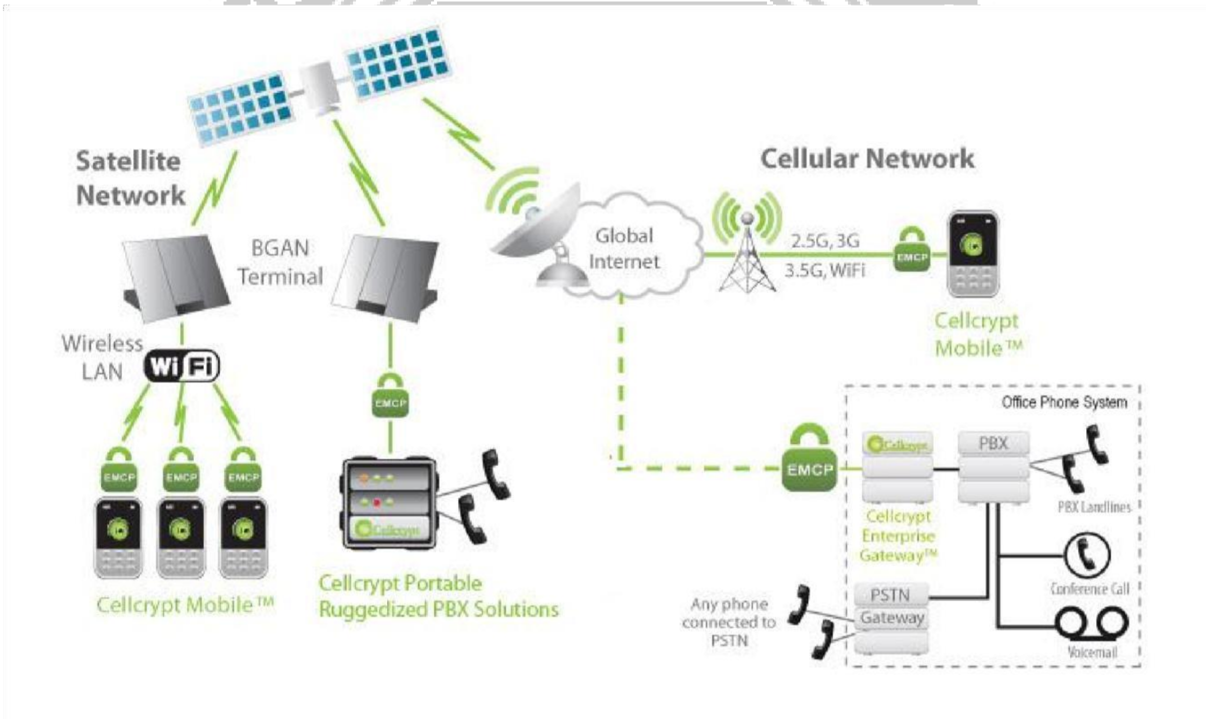
Figure 3.16 Encryption methods



4.9.1 Symmetric key encryption:

In symmetric-key schemes, the encryption and decryption keys are the same. Thus communicating parties must have the same key before they can achieve secret communication.

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read.



Decryption:

It is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer are able to read and understand.

This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of company data and trade secrets