Communication Principles

8/14/07

These principles concern the transmission of data with reliable reception.

Information can be encoded into messages.

A. A message is a representation intended to communicate information.

B. Messages are encoded into signals that move through a medium. Messages are abstract, signals concrete. Signals can be decomposed into profiles of continuous sine waves of various frequencies and amplitudes.

C. A digital sampling of a waveform records amplitude at periodic sampling times. Digital sampling loses no information if the sampling rate is at least twice the highest frequency in the waveform. (Nyquist theorem)

D. The human ear responds to frequencies up to 22K Hz. Sampling sound at 44K (or more) samples per second preserves the audible frequencies. However frequencies beyond 22K Hz also contribute to the reconstruction; losing them means some loss of fidelity in the reconstruction.

E. Computer systems and networks use digital encodings. This does not constraint the capabilities of those systems because human-generated messages are composed from discrete symbols and because the brain (which perceives information) already samples its sensory input.

Data communication always takes place in a system consisting of a message source, an encoder, a channel, and a decoder.

A. A diagram of a communication system appears below.
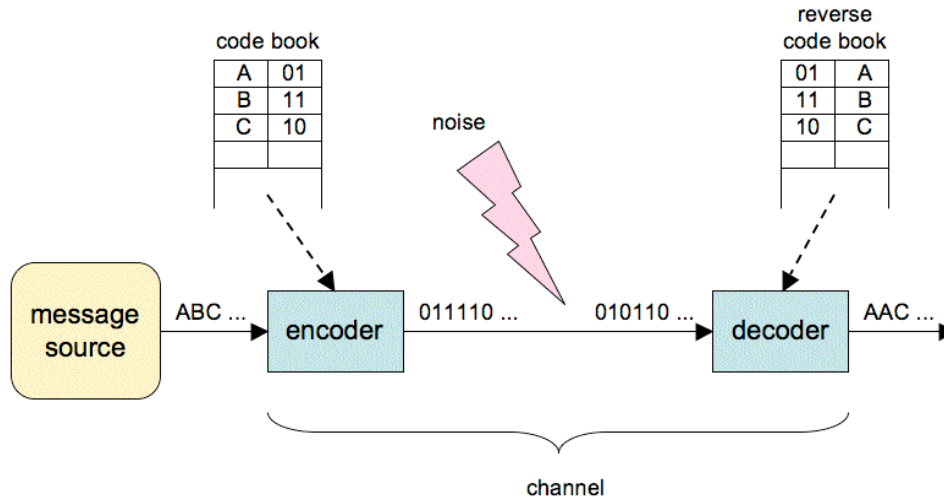
B. A channel is a communication medium that uses specific kinds of signals to represent information. It is no restriction to study only digital (binary) channels.

C. Noise represents any conditions that can disrupt signals (flip or drop bits in the received codes), preventing their accurate reception.

D. A message source is a set of possible messages and their probabilities.

E. An encoder is a device that represents a message with a channel code, that is, with signals in the channel. An encoder uses a codebook that associates a channel code with each message.

F. A decoder is a device that receives channel codes and converts them back to messages. The decoder uses in reverse the same codebook as the encoder. Unless the decoder can correct errors, received messages may not be the same as those sent.

G. A channel code is uniquely decipherable if and only if it has the prefix property: no code is prefix of another. Decoders need uniquely decipherable channel codes for reliable reception.

H. Tree codes, which assign messages to the leaves of binary trees, are prefix codes. The Huffman Code is a tree code that minimizes average code length by assigning high-probability messages shortest path lengths.

Information in a message source places a hard lower bound on channel capacity for accurate reception (Shannon Capacity Theorem).

A. The number of bits of uncertainty resolved by a message is the negative log of the message's probability. (Shannon information)

B. The average uncertainty (entropy) of a message source is the sum of the message uncertainties weighted by their respective probabilities.

C. A code whose average length is less than the entropy cannot be uniquely decipherable.

D. The Huffman code constructs a minimum length codebook for a message source. It is nearly optimal because its average code length is within 1 bit of the code's entropy.

E. The receiver can decode all messages accurately if and only if the channel capacity (bits per second) exceeds the source entropy (bits per message) times the message rate (messages per second).

F. Computer controlled channels generally block the sender so that it cannot transmit beyond channel capacity. In such a system, the maximum rate on the channel is the capacity divided by the entropy.

Messages corrupted during transmission can be recovered during reception (Error Correction).

A. Noise on the channel can reverse or garble some of the bits. A changed or corrupted bit is called an error. The noise rate can be measured by the probability of an error. Noise is "bursty" if errors are clustered into tight sequences.

B. The channel's error rate reduces its effective capacity.

C. An error detecting code contains extra, check bits that reveal whether any original bit has become an error. An error correcting code contains extra, check bits that reveal the original value of an erroneous bit.

D. The Hamming distance of a code is the smallest number of bits of a codeword that must be changed to convert it to another codeword.

E. A single error yields a new codeword with Hamming distance 1 from the original.

F. A code with Hamming distance 2 can detect a single error: the received codeword is not in the codebook. Parity codes are examples.

G. A code with Hamming distance of 3 can detect 1 or 2 errors and correct 1 error: the receiver selects the codebook word within distance 1 of the received codeword.

H. Hamming codes that add n check bits achieve Hamming distance n. Larger n adds more redundancy, corrects more errors, but lowers transmission rates. Smaller n corrects fewer errors and causes more retransmissions when errors are detected.

I. Reed-Solomon codes are elements of finite (Galois) fields that can achieve considerable error correction over bursty channels.

Messages can be compressed.

A. Since messages are representations, they can be compressed and decompressed as indicated in the discussion under Computing Principles. In communication, compression means to re-encode a source file or bit stream with fewer bits.

B. Lossless compression means every original bit is recoverable from a compressed file. This implies that the compressed file size is at least the original message length times entropy. Examples are Huffman and zip codes.

C. Lossy compression means a compression code for which some source bits are irrecoverable. Lossy compression algorithms attempt to delete information believed to be of no value to the receiver, so that the receiver will not notice the loss. Examples are JPEG (images) and MP3 (sound).

Messages can hide information.

A. Information in a code is hidden (enciphered) if the receiver has no fast algorithm for decoding. Therefore the receiver can only guess the message contained in the cyphertext, giving a very low probability of finding the hidden message.

B. Encryption is a computation that converts messages into ciphers, under the control of one or more keys. Decryption by fast algorithm is possible if the receiver has the keys. Encryption is not used for channel encoding; that is a separate process.

C. Secrecy means that no eavesdropper can decipher a message intercepted from the channel.

D. Authentication means that the receiver can uniquely identify the sender of a message.

E. Single-key encryption means sender and receiver have the same key. Security depends on making key exchange secret. If a new key is used for every sender-receiver communication, this system provides both secrecy and authentication.

F. Public-key encryption means the sender enciphers under one key and the receiver deciphers under a different key. The two keys, called public and secret, are linked but knowledge of one does not enable computation of the other. Enciphering with the public key ensures secrecy (only the owner of the secret key can decipher). Enciphering with the secret key ensures authentication (anyone can verify who sent the message).

G. Bit rates of single key channels are orders of magnitude faster than for public key channels. Therefore most encryption systems use public key systems for distributing session keys to the parties, who then use high-speed single-key channels for their communications.