BSc (Hons) Computer Science

University of Portsmouth

Third Year

Advanced Networks

M21279

Semester 1

Hugh Baldwin

hugh.baldwin@myport.ac.uk

Contents

Lecture - Introduction

11:00	30/09/24	Asim Ali

Admin

- Lectures given by Dr Asim Ali
- Office - BK 2.20
  - Monday 1300-1400
  - Thursday 1100-1200
- 2 hour lecture every week (PK 2.01)
- 1 hour seminar every week (AG 1.03)

The module information is available at the URL below:
https://course-module-catalog.port.ac.uk/#/moduleDetail/M21279/2024%2F25

Assessments

This module is assessed by one exam and one piece of coursework as below

- 60%, 90 minute Exam covering LO1,2,3&4 - TB1 assessment period (January)
- 40%, Group coursework covering LO5 - 2-4 members *or* individual (but not recommended)
  - 5 pages maximum
  - Template provided
  - Previous samples provided

Lecture - Signal Encoding

11:30 30/09/24 Asim Ali

Signals

(In this context) Signals are typically electromagnetic waves that carry information using some method of encoding. This means that the 'shape' of the signal is changed to represent information. There are three main types of signal–

- Analogue Signals, which vary continuously and smoothly over time
- Digital Signals, which have only 2 levels and change near instantly
- Discrete Signals, which have 2 or more levels and change near instantly

When information is transmitted, it is often converted between many different signals before it reaches the destination. For example, if you have ADSL internet, your computer sends the data as a digital signal to the modem, which is then converted to an analogue signal before it is transmitted across a POTS network (Plain Old Telephone System), then the receiver's modem converts it back to a digital signal before it is sent on to the receiver.

Digital Signal Encoding

There are many methods of encoding a digital signal, but some of the most common are–

- Non-return to Zero Level (NRZ-L)
  - 0 – High voltage level
  - 1 – Low voltage level
- Non-return to Zero Inverted (NRZ-I)
  - 0 – No transition (high-low or low-high voltage level) on clock pulse
  - 1 – Transition on clock pulse
- Bipolar-AMI
  - 0 – Zero voltage
  - 1 – Alternating positive or negative voltage level
- MLT-3 (Multi-Level Transmit 3)
  - 0 – Remain at the same voltage level
  - 1 – Transition to the next voltage level
  - Uses 3 voltage levels, named $+1$,0&-1 but can be any arbitrary voltages
- Manchester
  - 0 – Transition from high-low voltage level in the middle of the clock interval
  - 1 – Transition from low-high voltage level
- Differential Manchester

- 0 – Transition (high-low or low-high voltage level) on clock pulse
- 1 – No transition on clock pulse
- Always transitions in the middle of the clock interval

In this context, the high and low voltage levels can be whatever you like, but are typically either a positive and negative voltage of the same magnitude, or are a positive voltage and zero. The most common voltages used for signalling are 3.3, 5 and 12 volts. In the case of Bipolar-AMI, the 3 voltage levels can be arbitrary, and don't have to be, for example $+5$, 0 and -5 volts.

Diagrams

Below is the binary string 01100110 encoded using all of the above encoding schemes. This assumes that the previous state before the transmission starts is always low, and that each vertical dotted line represents a clock pulse.

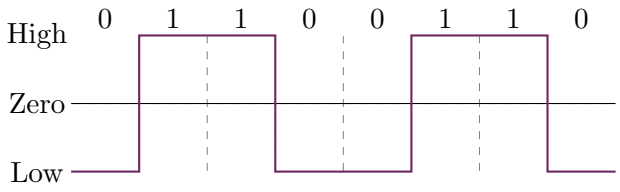


Figure 2.1: Non-return to Zero Level (NRZ-L)

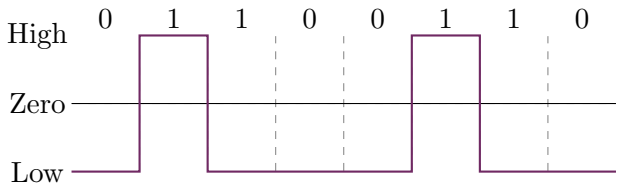


Figure 2.2: Non-return to Zero Inverted (NRZ-I)

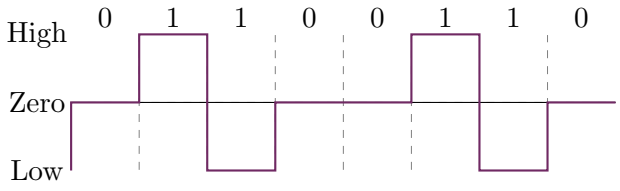


Figure 2.3: Bipolar-AMI

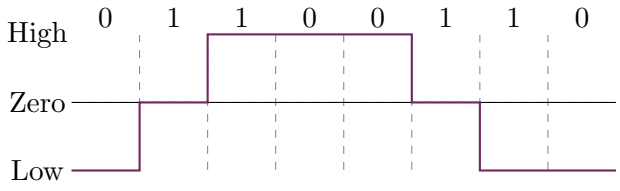


Figure 2.4: Multi-Level Transmit 3 (MLT-3)

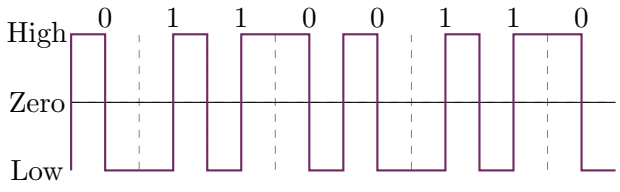


Figure 2.5: Manchester

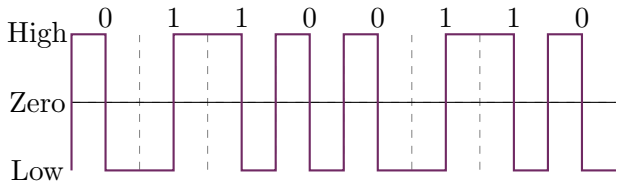


Figure 2.6: Differential Manchester

Carrier Waves and Modulation

A carrier wave is a continuous waveform that, on it's own, carries no information. This carrier wave is then modified by another signal to convey information. This modification can be of it's amplitude, frequency, phase, or a combination of all 3. This is known as modulation, hence the names AM (Amplitude Modulation) and FM (Frequency Modulation) for the two types of analogue radio.

Digital-to-Analogue Encoding

There are several methods of encoding a digital signal on an analogue transmission medium. In the case of sending digital data over a POTS network, the signal is encoded onto a carrier wave in the range of 300-3400Hz using a MoDem (Modulator-Demodulator). The main methods of encoding are–

- Amplitude-Shift keying (ASK)
- Frequency-Shift keying (FSK)
  - Binary FSK (BFSK)
  - Multiple FSK (MFSK)
- Phase-Shift keying (PSK)
  - Binary PSK – 1 = A sine wave, 0 = The same sine wave shifted by $180°$
  - Differential PSK (DPSK) – 1 = The previous sine wave shifted by $180°$, 0 = The previous sine wave
  - Multiple-level PSK
- Quadratic AM (Combination of ASK and PSK)

The sender and receiver may use different frequencies as to allow full-duplex data transmission on the same physical medium or radio channel. Full-duplex meaning full-speed transmission in both directions simultaneously.

Diagrams

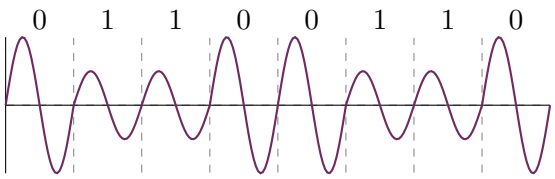


Figure 2.7: Amplitude-Shift Keying

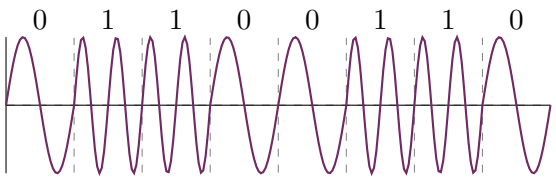


Figure 2.8: Binary Frequency-Shift Keying

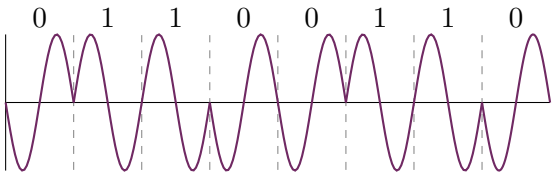


Figure 2.9: Binary Phase-Shift Keying

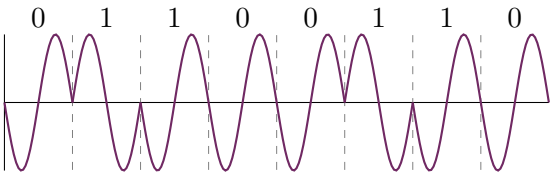


Figure 2.10: Differential Phase-Shift Keying

Seminar - Encoding Exercises

12:00 03/10/24 Asim Ali

Figure 3.1: Encode the binary data 11000011 with the MLT-3 encoding scheme

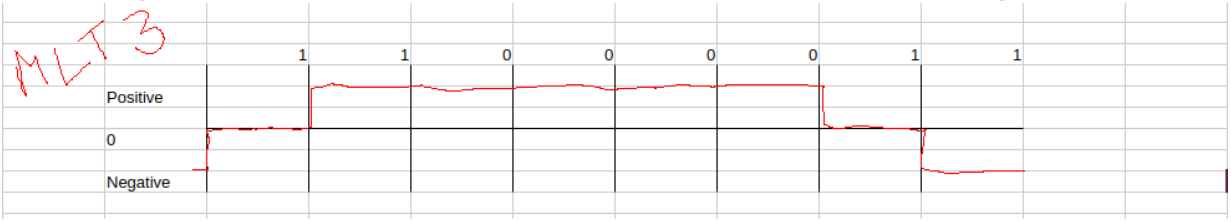


Figure 3.2: Encode the binary data 11000011 with the Non-Differential Manchester encoding scheme

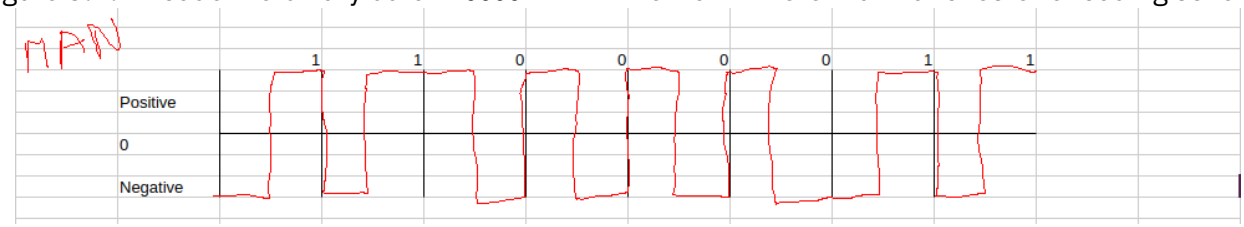
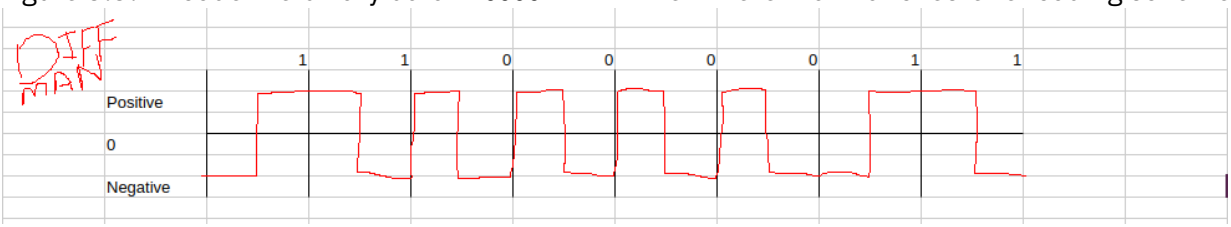


Figure 3.3: Encode the binary data 11000011 with the Differential Manchester encoding scheme



Lecture - Signal Encoding II

11:00 07/10/24 Asim Ali

Transmission Media

There are many different mediums which can be used to transmit information. In the case of networks, there are two main types, guided and unguided media.

- Guided Media
  - The signal is contained within a medium, such as
  - Copper cable (twisted pair, coaxial, etc)
  - Fibre optics
- Unguided Media
  - The signal is sent out without containment, through the air
  - This does not mean that the signal is not directional, microwave networks are often highly directional to reduce signal drop-off and interference
  - Microwave, Radio, Cellular and Satellite

add spectrum diagram

Signal Properties

- **Data Rate** – The speed in bits per second (bps or b/s) at which data can be communicated
- **Error** – The reception of a 1 when 0 was transmitted, or vice versa
- **Error Rate** – The rate at which errors occur, usually as a ratio or percentage
- **Frequency Bandwidth** – The difference between the upper and lower frequency in a continuous frequency band
- **Channel Capacity** – The maximum rate at which data can be transmitted through a channel
- **Signal-to-Noise Ratio** – The ratio of the signal power to noise power in decibels (dB)

Interference and Noise

Definition

Interference is when two signals are added together. There are two main types of interference – constructive and destructive. When two signals combine to create a signal with a higher amplitude, this is constructive interference. If the amplitude is reduced, this is destructive interference.

Definition

Noise is any other signal which interferes with the desired signal along the medium of transmission. Typically, any noise in a signal will make it more difficult to decode, since the signal may be reduced in amplitude or shifted in phase.

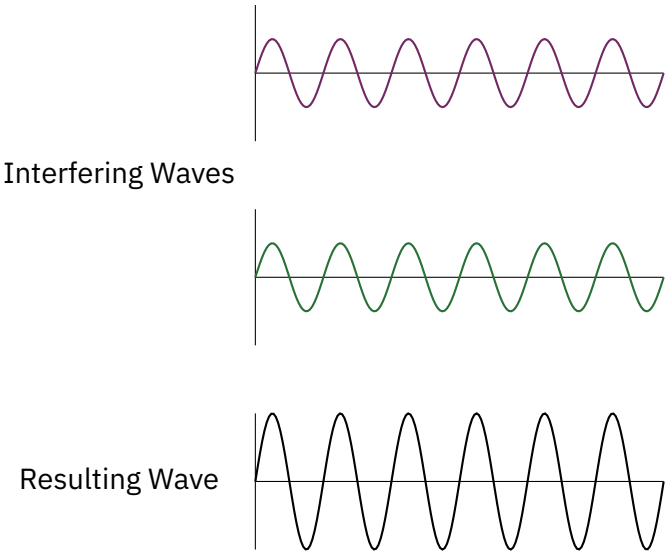


Figure 4.1: Constructive interference

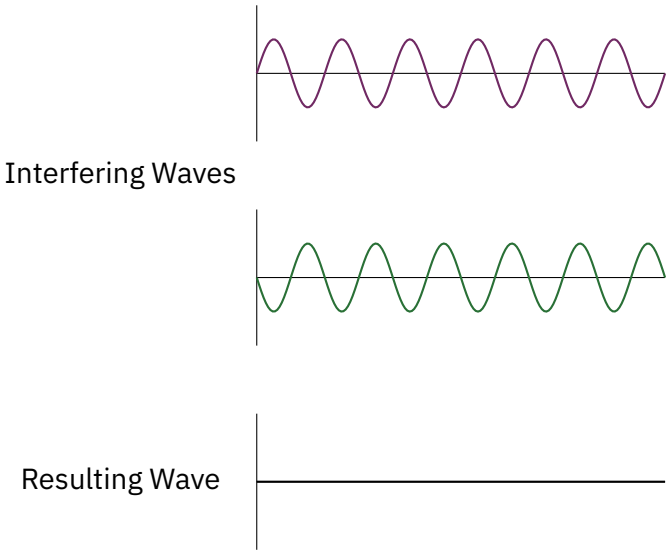


Figure 4.2: Destructive interference

Securing a Signal

When a signal is sent through any media, if a third party has access to the same media, they can intercept, block and even fake signals. This is because there is no inherent security in an electromagnetic wave, so we need to find ways of securing it.

Spread Spectrum

If we were to transmit a signal using a wide range of the spectrum, rather than a single frequency, it makes it harder for a third party to entirely block the signal. This method is often used in military applications, as well as wired and wireless networks. Three common techniques are–

- Frequency Hopping Spread Spectrum (FHSS)
  - Data is sent using one of the previously discussed analogue transmission techniques, but the carrier frequency is changed rapidly across a wide spectrum, using a code or pattern known by both the transmitter and receiver
  - This makes it harder to intercept or block transmissions, as long as the pattern of frequency hopping is not known
  - It is also very resilient to narrowband interference (interference over a small band of frequencies)
- Direct Sequence Spread Spectrum (DSSS)
  - Each bit of the data is represented by multiple bits of the transmitted signal, using a spreading code
  - The bits in the PN sequence are known as chips, and the sequence of them the chip sequence
  - One technique is to combine the data with the spreading code bit stream using an exclusive-or

- Code Division Multiple Access (CDMA)

Multiplexing

Definition

Multiplexing is sending multiple data streams or signals over a single transmission medium.

Frequency Division

With frequency division multiplexing, you have a transmission medium which can send data over a wide spectrum of frequencies, and multiple signals you need to send at the same time. If you modulate the different signals using a different carrier frequency for each, and leave a suitable gap between them, you can then combine the waves together to create a single composite wave which encodes the data of all the streams. The receiver then needs to know only the frequency of the signal they need to receive, and pass the composite wave through a filter for that specific frequency to recover the signal intended for them.

Time Division

With time division multiplexing, each of the signals gets a certain share of time in which it can be transmitted. This often means that the data needs to be buffered on both ends, so may be more costly to implement. This also greatly limits the bandwidth available to each signal, as it would be split between all of the signals on the same channel.

Code Division Multiple Access (CDMA)

CDMA is a multiplexing technique which can be used with a spread-spectrum signal. Given a data stream of bit rate R, we assign each bit a unique user code of n according to a Walsh matrix. If a user, k, sends a 1, the transmitter sends the chip code ck, and if they send a 0, the transmitter sends the inverse of that chip code, $c'k$. The chip codes of all users will add up to a bipolar signal, D. The receiver decodes the signal for a specific user with a function, by taking the cartesian product of D and the specific chip code ck, $D.ck$. If $D.ck = n$ then a 1 is received, and if $D.ck = -n$ then a 0 is received.

Come back to this and find some other material that explains it less terribly

Add something about Nyquist and Shannon bandwidth and capacities

Seminar - Encoding Exercises II

12:00 10/10/24 Asim Ali

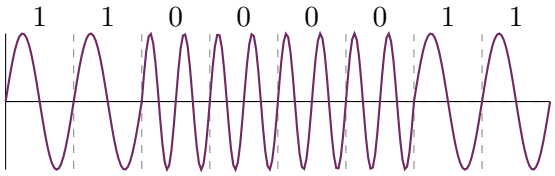


Figure 5.1: BFSK representation of the binary number 11000011

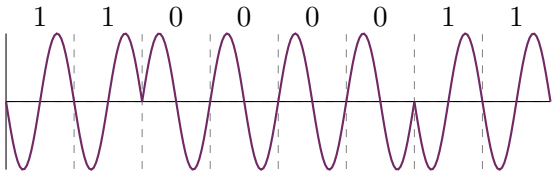


Figure 5.2: BPSK representation of the binary number 11000011

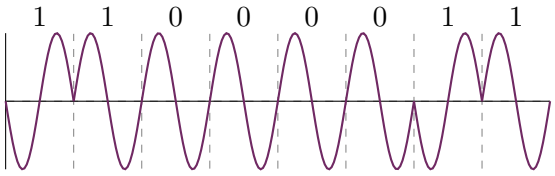


Figure 5.3: DPSK representation of the binary number 11000011

INPUT	1				0				1				1			
PN Stream	0	1	1	0	1	0	0	1	0	1	1	0	1	0	1	1
Transmitted	1	0	0	1	1	0	0	1	1	0	0	1	0	1	0	0
Received	1	0	0	1	1	0	0	1	1	0	0	1	0	1	0	0
PN Stream	0	1	1	0	1	0	0	1	0	1	1	0	1	0	1	1
OUTPUT	1				0				1				1			

Figure 5.4: DSSS encoding and decoding of the binary number 1001

Lecture - Security

11:00 14/10/24 Asim Ali

Security Factors

There are three main security factors we need to consider–

- Confidentiality
  - Only authorised parties should be able to read the information
- Integrity
  - Only authorised parties should be able to modify, create and delete information
- Availability
  - Authorised parties should always have access to the information

Types of Attackers

- Passive Attackers
  - The attacker only listens to the messages, so they can only read the information
- Active Attackers
  - The attacker listens, modifies and sends messages, so they can read the information, modify it or fabricate it entirely

To overcome both of these types of attacker, you can encrypt the data, meaning that it is unreadable by any third parties, and if someone attempts to modify or spoof a message, it will not be encrypted with the same key and so the receiver will know it was not sent by the correct person.

Symmetric (Shared Key) Encryption

Symmetric key encryption requires the sender and receiver to already have a shared key, which will then be used to both encrypt and decrypt the messages.

DES (Data Encryption Standard)

Plaintext is split into 64-bit blocks. The key is 56-bits long and 16 subkeys are generated for 16 rounds of cryptography. The subkeys are then used in reverse order to decrypt the data. Because this quickly became insecure, Triple-DES was created as a new standard, which is as literal as the name suggests. You simply encrypt the data three times with three different keys, then decrypt 3 times in reverse order.

AES (Advanced Encryption Standard)

Plaintext is split into 128-bit blocks. The key is 128,192 or 256-bits long, giving the algorithm the name AES-128/192/256. AES is a much more advanced algorithm than DES, and it was created with the express purpose of replacing DES

Confidentiality

Because the messages are encrypted, they cannot be read or examined by a third party. This does rely upon the keys being shared ahead of time, in a secure way such that no third parties know what the key is.

Asymmetric (Public Key) Encryption

In asymmetric encryption, the sender and receiver have two different but related keys. The sender uses the public key of the receiver to encrypt the message, and the receiver uses their own private key to decrypt the message.

RSA (Rivest-Shamir-Adleman)

1. Select two large primes p and q (the larger the better)
2. $n = pq$ and $z = (p-1)(q-1)$
3. Select a number relatively prime (what?) to z and call it d
4. Find e such that $e * d = 1 \mod z$
5. The public key is then (e, n) and the private key (d, n)
6. To encrypt a message, convert the plaintext M into an integer m such that $0 \leq m < n$, using a known and reversible padding scheme. Then compute the ciphertext c such as $c = m^e(\mod n)$
7. To then decrypt the message, you use the private key d by computing $c^d = (m^e)^d = m(\mod n)$. Then given m, you recover the message M by reversing the padding scheme

Add example here?

Confidentiality

Because the messages are encrypted, they cannot be read or examined by a third party. Since the public key can only be used to encrypt messages (theoretically it can be used to determine the private key but this is effectively impossible with current computational power), it can be sent out on the internet for anyone to use to encrypt messages for the receiver. As long as the private key is kept secret by the receiver, the messages are perfectly confidential.

Ensuring Integrity

To make sure that a message was sent by the correct person, and without being modified we can use either signatures, message digests or both.

Digital Signatures

When making a digital signature, the inverse of public-key cryptography is done. This means that only the owner of the signature knows the private key, but everyone knows the public key. The private key is used to cryptographically sign a file or message, which anyone can use the public key to verify, but only the owner of the keypair can use their key to sign. This means that if a message is signed, it must've come from the correct person.

Message Digests

A message digest (or hash function) takes a message M and produces a small 'fingerprint' known as the message digest $H(M)$. A secure hash function H encrypts a small block of the message which is produced as a function of the message, known as the authenticator. The properties of H are such that $H(M) \neq$

$H(M')$ and given $H(M)$ is is computationally impossible to find M. The message digest is encrypted with the sender's private key, and serves as a signature that verifies the content and order of the message. Two popular digest functions are MD5 and SHA-1.

Authentication

Authentication verifies that a message has come from a verified source. This can be achieved using conventional encryption techniques as discussed previously. This does not protect against so-called playback attacks however. If a third party records an encrypted message, they can re-send it again at a later time, and since the message is correctly encrypted, the receiver will still believe it to be a valid message.

This can be avoided by adding a number to the cipher that relates to the time the message was sent, either directly or by using it as the seed for a random number generator. When the message is received, if the time is too far in the past, the message will either be ignored, or requested for re-sending to ensure the correct message was sent.