HOGESCHOOL VOOR WETENSCHAP & KUNST | DE NAYER INSTITUUT
SINT-KATELIJNE-WAVER

Jan De Nayerlaan, 5
B-2860 Sint-Katelijne-Waver
Belgium
www.denayer.be

Spread Spectrum (SS)

applications

ir. J. Meel
jme@denayer.wenk.be

Studiedag Spread Spectrum
6 okt. '99

In the period of nov. 1997 - nov. 1999 a 'Spread Spectrum' project was worked out at the polytechnic 'DE NAYER instituut'. The goal of this project was the hardware/software implementation of a Direct Sequence Spread Spectrum (CDMA) demonstrator in the 2.4 GHz ISM band. A measurement environment (Vector Signal Analyzer, IQ-modulator, Bit Error Rate Tester) was build out, resulting in a set of experiments based on this demonstrator. The project results where communicated with SMO's (Small and Medium Organisations) interested in Spread Spectrum. These notes were used to introduce the SMO's in the subject of Spread Spectrum.This Spread Spectrum project was sponsered by:

Vlaams Instituut voor de bevordering van het Wetenschappelijk Technologisch onderzoek
in de industrie – (*Flemisch Gouvernment)*

Sirius Communications – Rotselaar - Belgium

V2 dec 99

CONTENTS

1. Spread Spectrum Applications

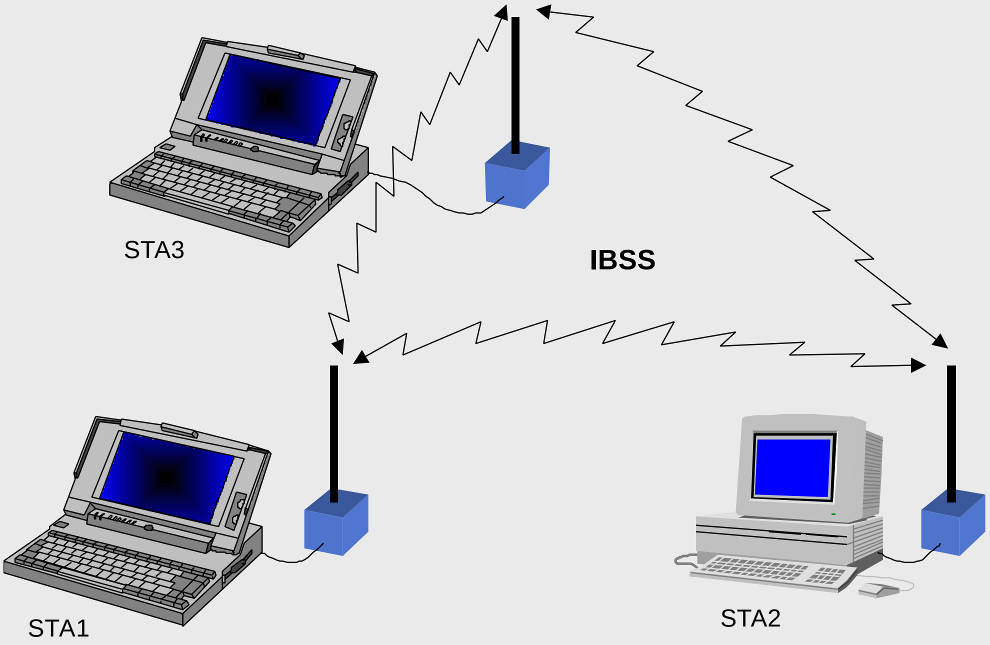
1.1 WLAN IEEE 802.11

IEEE 802.11 is the first internationally recognized standard for Wireless Local Area Networks (WLAN), introducing the technology of mobile computing.

1.1.1 Network Topology

Ad-hoc Network

An Ad-hoc network or Independent Basic Service Set (IBSS) is a simple network where communications are established between two or more wireless nodes or Stations (STAs) in a given coverage area without the use of an Access Point (AP) or server. The STAs recognize each other and communicate directly with each other on a peer-to-peer level.



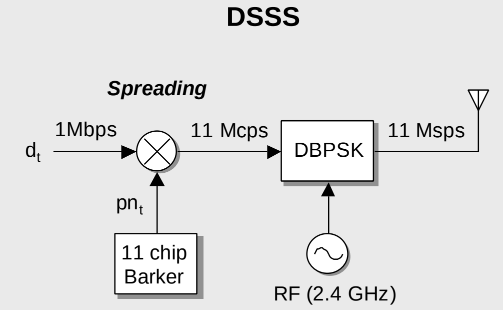
Infrastructure Network

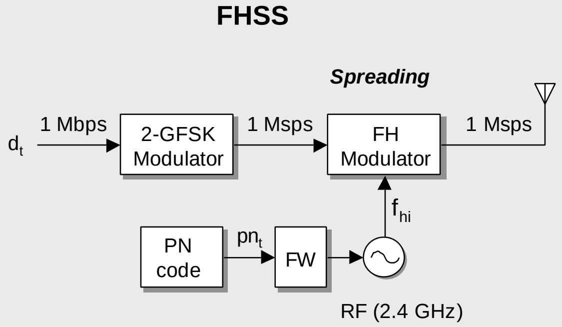
An Infrastructure network (or client/server network) is a more flexible configuration in which each Basic Service Set (BSS) contains an Access Point (AP). The AP forms a bridge between the wireless and wired LAN. The STAs do not communicate on a peer-to-peer basis. Instead, all communications between STAs or between an STA and a wired network client go through the AP. APs are not mobile and form part of the wired network infrastructure.
The Extended Service Set (ESS) consists of a series of BSSs (each containing an AP) connected together by means of a Distribution System (DS). Although the DS could be any type of network (including a wireless network), it is almost invariably an Ethernet LAN. Within an ESS, STAs can roam from one BSS to another and communicate with any mobile or fixed client in a manner which is completely transparant in the protocol stack above the MAC sublayer. The ESS enables coverage to extend well beyond the range of the WLAN radio.

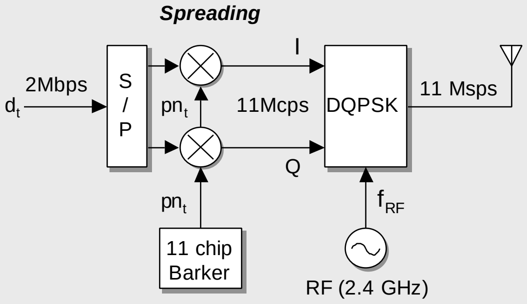
1.1.2 Physical Layer (Radio Technology)

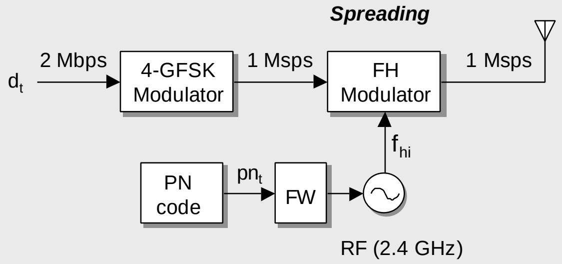
Spreading and Modulation

IEEE 802.11 defines three variations of the Physical Layer: Infrared (IR) and two RF transmissions in the unlicensed 2.4 GHz ISM-band, requiring spread spectrum modulation: DSSS (Direct Sequence Spread Spectrum) and FHSS (Frequency Hopping Spread Spectrum). Only the RF transmission has significant presence in the market.









DSSS

The DSSS physical layer uses an 11-bit Barker sequence to spread the data before it is transmitted. This sequence gives a processing gain of 10.4 dB, meeting the minimum requirements of FCC 15.247 and ETS 300 328.
The 11 Mcps baseband stream is modulated onto a carrier frequency (2.4 GHz ISM band, with 11 possible channels spaced with 5 MHz) using:

- DBPSK (Differential Binary Phase Shift Keying): data rate = 1 Mbps
- DQPSK (Differential Quaternary Phase Shift Keying): data rate = 2 Mbps

FHSS

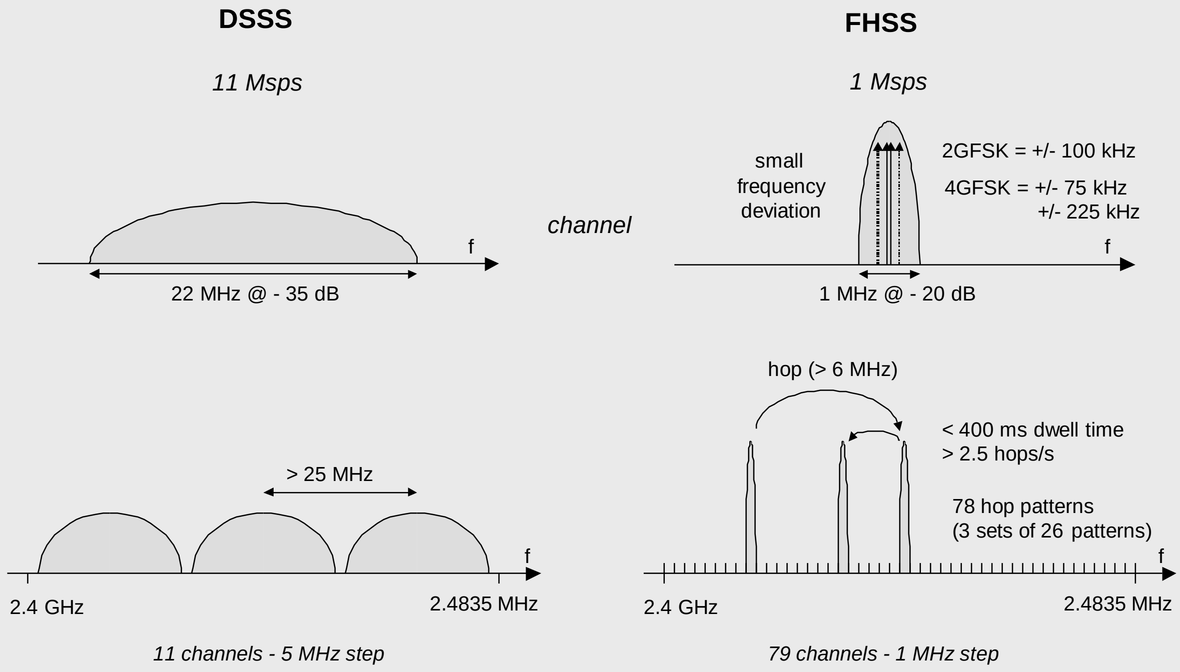
In the FHSS physical layer the information is first modulated using:

- 2-GFSK (2-level Gaussian Frequency Shift Keying): data rate = 1 Mbps
- 4-GFSK (4-level Gaussian Frequency Shift Keying): data rate = 2 Mbps

Both modulations result in a symbol rate of 1 Msps.
The carrier frequency (2.4 GHz ISM band, with 79 possible channels spaced with 1 MHz) hops from channel to channel in a prearranged pseudo-random manner (hop pattern). There are 78 different hop patterns (subdivided in 3 sets of 26 patterns). The FCC and ETS regulations require a minimum hop rate of 2.5 hops/s or a channel dwell time of less than 400 ms.

Spectrum

The spectrum of the transmitted signals determines the network packing.



DSSS

With a symbol rate of 11 Mbps the channel bandwidth of the main lobe is 22 MHz. There are 11 channels identified for DSSS systems, but there is a lot of overlap (only 5 MHz spacing). All IEEE 802.11 DSSS compliant products utilize the same PN code. Since there is not a set of codes available the DSSS network *cannot employ CDMA*. When multiple APs are located in close proximity, it is recommended to use frequency seperations of at least 25 MHz. Therefore the 2.4 GHz ISM band will accommodate 3 non-overlapping channels. Only 3 networks can operate collocated.

FHSS

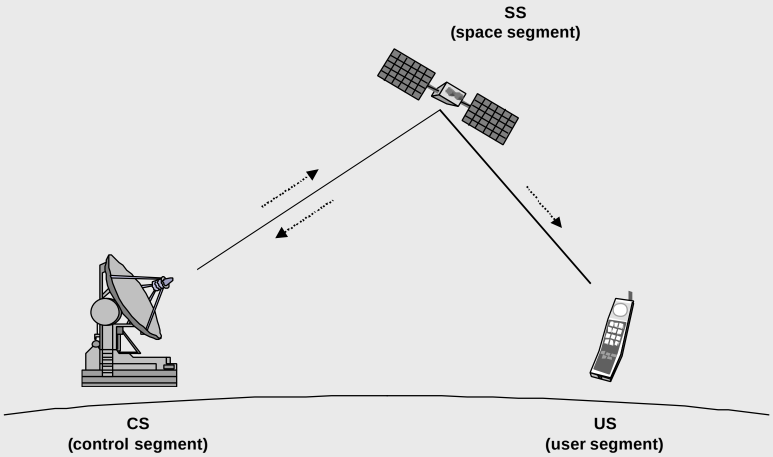
When the hop patterns are selected well, several APs can be located in close proximity with a fairly low probability of collision on a given channel.
Up to 13 FHSS networks can be collocated before the interference is to high. This is based on the probability of collisions where two of the nets choose the same one of 79 channels at the same time. When the probability of collisions gets to high, network throughput suffers.

Comparison of DSSS and FHSS

	DSSS	**FHSS**
Spectral Density Interference Generation	+ reduced with processing gain + *continuous* spread of the Tx power gives minimum interference	+ reduced with processing gain - only the *average* Tx power is spread, this gives less interference reduction
Transmission	+ continuous, broadband	- discontinuous, narrowband
Interference Susceptibility	+ narrowband interference in the same channel is reduced by the PG	- narrowband interference in the same channel is not reduced + narrowband interference in a different channel has no influence
Multipath	+ rejection if the bandwith is wider than the coherence delay of the environment (outdoor applications) - for a chiprate of 11 Mcps the chip period is 91 ns, corresponding with a wave distance of about 30 m (large for indoor applications)	- some of the narrowband channels are unusable + hopping makes transmission on usable channels possible
Modulation	+ BPSK and QPSK are very power efficient	- GFSK is less power efficient in narrowband operation
Higher Data Rates	+ the data rate can be increased by increasing the clockrate and/or the modulation complexity (muli-level)	- a wider bandwidth is needed but not available (it would cut the number of channels to hop in)
Multiple Signals	- only 3 collocated networks + higher aggregate throughput	+ up to 13 collocated networks - lower aggregate throughput
Synchronisation	+ self-synchronizing	- many channels to search
Real Time (voice)	+ no timing constraints - if a station is jammed, it is jammed until the jammer goes away	- if a channel is jammed, the next available transmission time on a clear channel may be 400 ms away
Implementation	- complex baseband processing	+ simple analog limiter/discriminator receiver
Power Consumption	- more power consumption due to higher speed and more compex processing	- more simple circuit

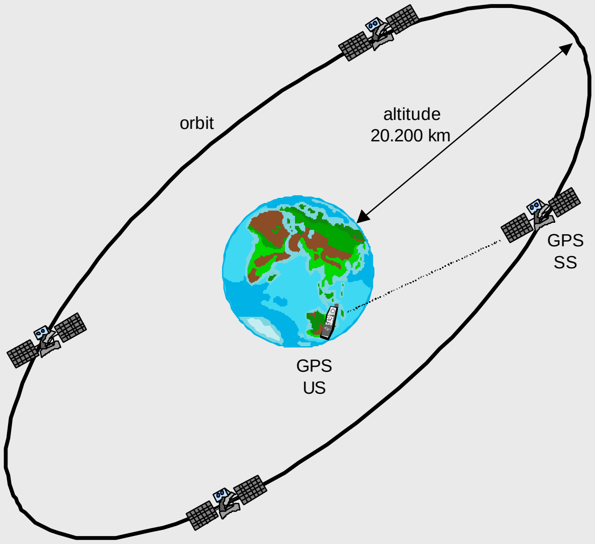
1.2 GPS (Global Positioning System)

GPS is a satellite navigation system, funded by and controlled by the U.S. Department of Defense (DOD).
The GPS system consists of three building blocks: the Space Segment (SS), the User Segment and the Control Segment (CS).



Space Segment (SS)

The Space Segment of the GPS system consists of the GPS satellites. These Space Vehicles (SVs) send radio signals to the User Segment and the Control Segment.
The nominal GPS operational constellation consists of 24 satellites that orbit the earth in 12 hours. The satellite orbits have an altitude of 20.200km and an inclination of 55 degrees with respect to the equatorial plane. There are six orbital planes (with nominally four SVs in each), equally spaced (60 degrees apart). The satellite orbits repeat almost the same ground track once each day (4 minutes earlier each day).



Control Segment

Monitor stations measure signals from the SVs which are incorporated into orbital models for each satellite. The models compute precise orbital data (ephimeris) and SV clock corrections for each satellite. The Master Control station uploads ephimeris and clock data to the SVs. The SVs then send subsets of the orbital ephimeris data to GPS receivers (User Segment).

User Segment

The GPS User Segment receivers convert SV signals into position, velocity and time estimates. Four satellites are required to compute the four dimensions of X,Y,Z (position) and time. Authorized users with cryptographic equipment and keys and specially equipped receivers use the *Precise Positioning System* (PPS).

PPS Predictable Accuracy (95%):

- 22 meter horizontal accuracy
- 27.7 meter vertical accuracy
- 100 nanosecond time accuracy

Civil users worldwide use the Standard Positioning System (SPS) without charge or restrictions. Most receivers are capable of receiving and using the SPS signal. The SPS accuracy is intentionally degraded by the DOD by the use of Selective Availability.

SPS Predictable Accuracy (95%):

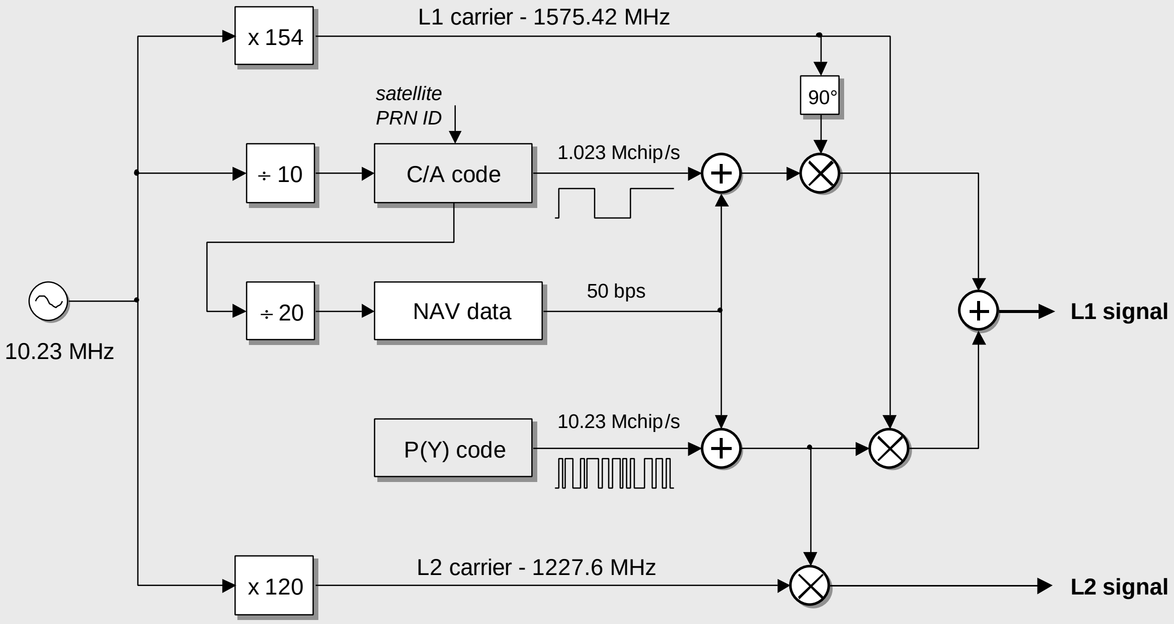
- 100 meter horizontal accuracy
- 156 meter vertical accuracy
- 340 nanoseconds time accuracy

GPS Satellite Signals

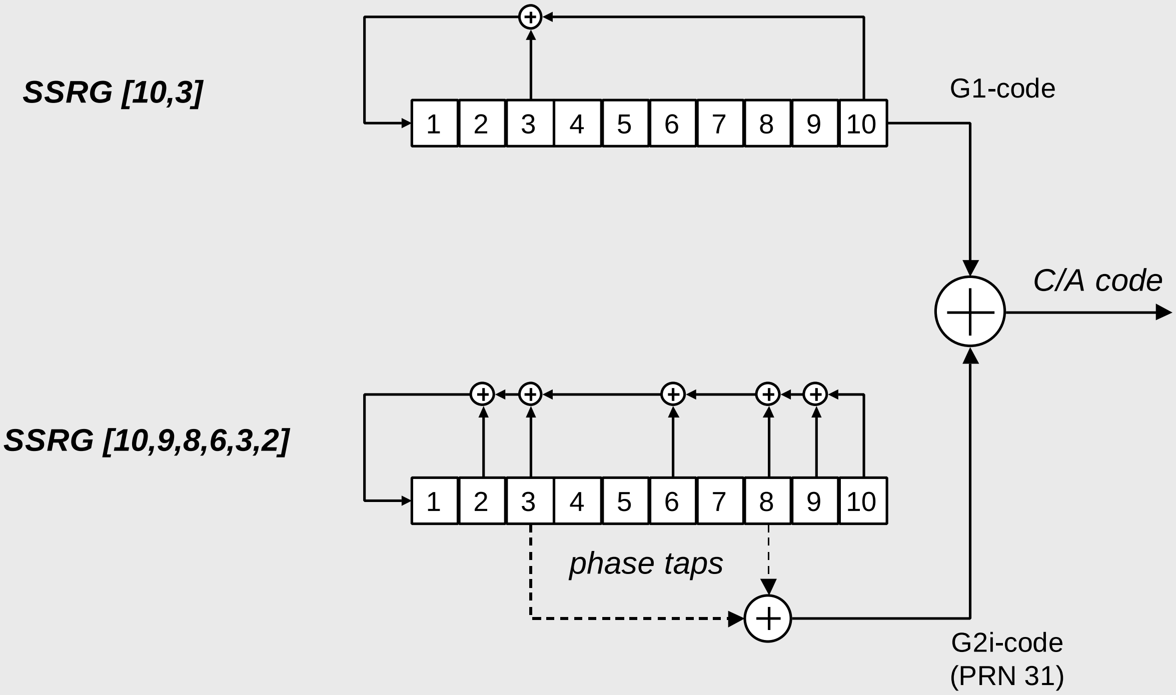
The SVs transmit two microwave carrier signals. The L1 frequency (1575.42 MHz) carries the navigation message and the SPS code signals. The L2 frequency (1227.60 MHz) is used to rneasure the ionospheric delay by PPS equipped receivers.

Three binary codes shift the L1 and/or L2 carrier phase.

- The C/A Code (Coarse Acquisition) modulates the L1 carrier phase. The C/A code is a repeating 1.023 Mchip/s Pseudo Random Noise (PRN) Code. This noise-like code modulates the L1 carrier signal, "spreading" the spectrum over a 1 MHz bandwidth. The C/A code repeats every 1023 chips (one millisecond). This chip length N_c of 1023 chips results in a processing gain of 30 dB. That’s why GPS receivers don’t need big satellite dishes to receive the GPS signal. There is a *different C/A code PRN for each SV*. GPS satellites are identifed by their PRN number, the unique identifier for each pseudo-random-noise code. This code-division-multiplexing technique allows the identification of the SVs even though they all transmit at the same L1-band frequency. A low cross-correlation gives a minimum of interference between the SV signals at the receiver side. The C/A code that modulates the L1 carrier is the basis for the civil SPS.
- The P-Code (Precise) modulates both the L1 and L2 carrier phases. The P-Code is a very long (seven days period = $6.19.10^{12}$ chips) 10.23 Mchip/s PRN code. In the Anti-Spoofing (AS) mode of operation, the P-Code is encrypted into the Y-Code. The encrypted Y-Code requires a classified AS Module for each receiver channel and is for use only by authorized users with cryptographic keys. The P (Y)-Code is the basis for the PPS.
- The Navigation Message (NAV data) also modulates the L1-C/A code signal. The Navigation Message is a 50 bps signal consisting of data bits that describe the GPS satellite orbits, clock corrections, and other system parameters (1500 bits = 30 sec).



The Long code (P or Y code) is identical for each satellite.
The Short code or C/A code is a Gold code with the generator shown below.



The C/A code generator produces a different 1023 chip sequence for each phase tap setting. The C/A codes are defined for 32 satellite identification numbers (PRN ID).

SV PRN ID	G2 phase Taps	First 10 chips
1	2 & 6	1100100000
2	3 &7	1110010000
3	4 & 8	1111001000
4	5 & 9	1111100100
5	1 & 9	1001011011
6	2 &10	1100101101
7	1 & 8	1001011001
8	2 & 9	1100101100
9	3 &10	1110010110
10	2 & 3	1101000100
11	3 & 4	1110100010
12	5 & 6	1111101000
13	6 & 7	1111110100
14	7 & 8	1111111010
15	8 & 9	1111111101
16	9 &10	1111111110
17	1 & 4	1001101110
18	2 & 5	1100110111
19	3 & 6	1110011011
20	4 & 7	1111001101
21	5 & 8	1111100110
22	6 & 9	1111110011
23	1 & 3	1000110011
24	4 & 6	1111000110
25	5 & 7	1111100011
26	6 & 8	1111110001
27	7 & 9	1111111000
28	8 & 10	1111111100
29	1 & 6	1001010111
30	2 & 7	1100101011
31	3 & 8	1110010101
32	4 & 9	1111001010

Measuring the distance d between the SV and the RX is based on measuring the travel time t_d of the radio signal (L1/L2) send by the SV and the propagation speed c of the signal:

$$d = c.t_d$$

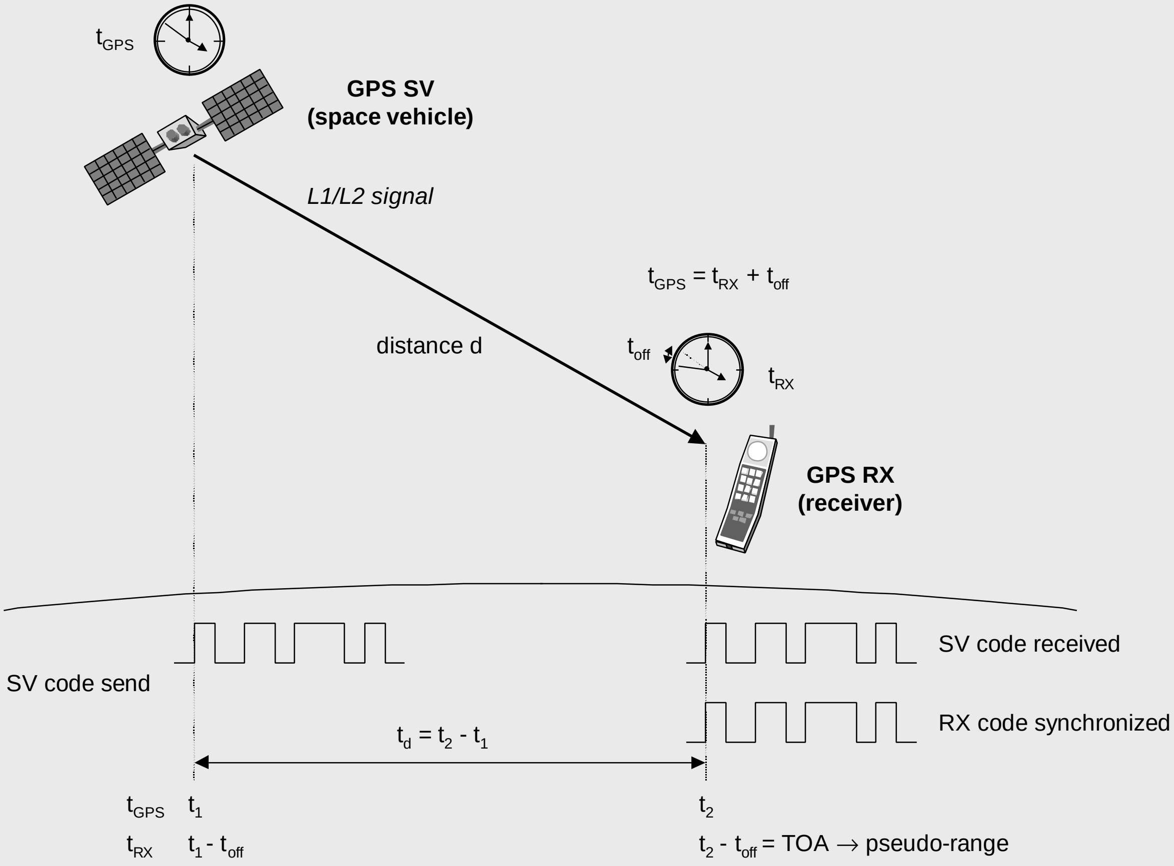
The travel time t_d is measured by synchronizing the C/A code (or P(Y) code) of the receiver to the C/A code in the signal received from the SV. The start time of this synchronized C/A code in the receiver gives the Time Of Arrival (TOA) of the C/A code of the SV at the receiver. The start time t_1 of the C/A code in the SV is known (time information is included in the Navigation Message). The travel time t_d can be calculated from t_1 and TOA.
Because $c = 3.10^8$ m/s, the time must be measured very accurate:

$d = 20.200$ km → $t_d = 67.333\ \mu s$
$d = 300$ m → $t_d = 1\ \mu s$ = chip period of C/A code
$d = 30$ m → $t_d = 100$ ns = chip period of P(Y) code

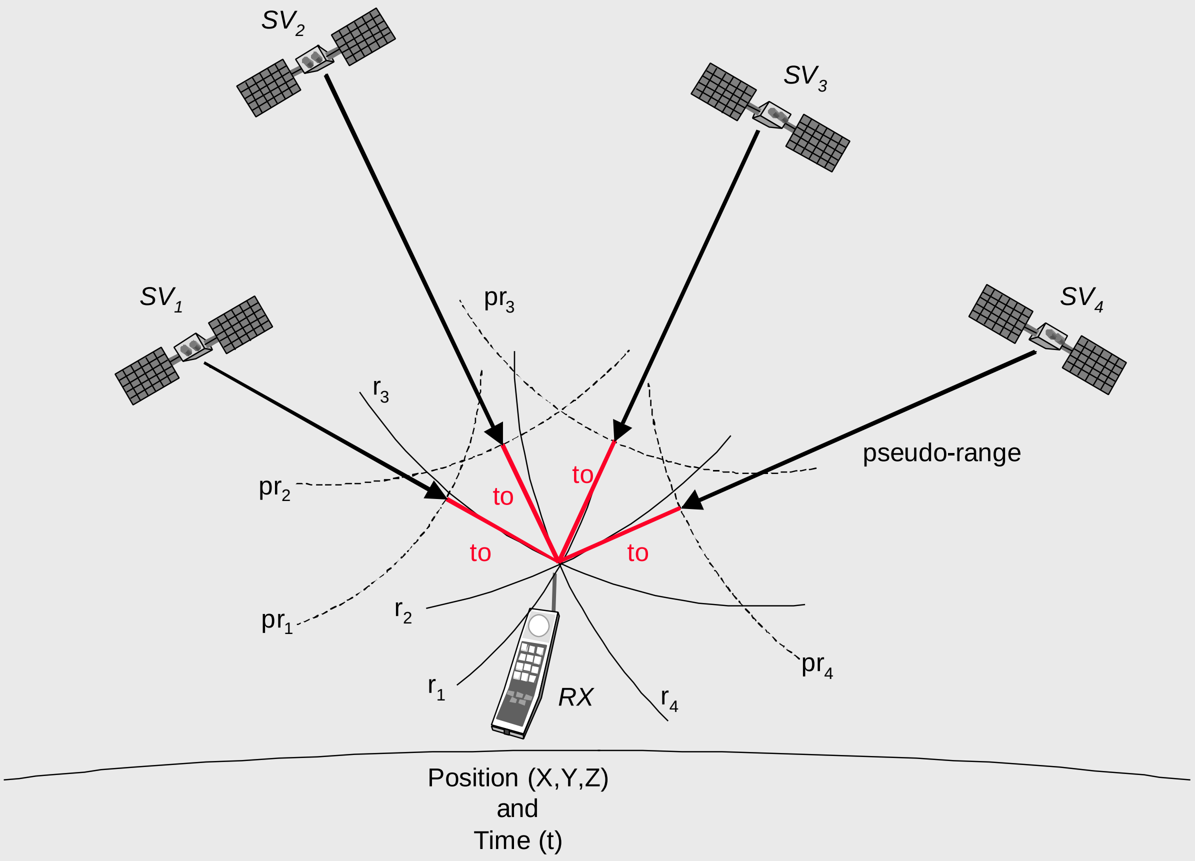
On the Space Vehicle (SV), timing is almost perfect because they have precise atomic clocks on board. A low-cost GPS receiver cannot have an atomic-accuracy clock. The receiver clock time t_{RX} shows an offset t_{off} from the SV's GPS time t_{GPS}:

$$t_{RX} = t_{GPS} - t_{off}$$

Due to this inaccuracy the TOA is called the pseudo-range.



If the receiver clock is perfect, than all the satellite (SV) ranges would intersect at a single point (which is the position of the receiver). Three perfect measurements can locate a point in 3-dimensional space.
With imperfect receiver clocks, a fourth measurement (done as a cross-check), will not intersect with the first three. Since any offset from GPS time will effect the four measurements in an equal way, the receiver must look to a single correction factor (timeoffset to) that it can substract from all its timing measurements that would cause them all to intersect at a single point.
Making four satellite measurements gives accurate position and time information.


SV2
SV3
SV1
SV4
pr3
r3
pseudo-range
pr2
to
to
to
to
pr1
r2
r1
RX
r4
pr4
Position (X,Y,Z)
and
Time (t)

1.3 IS-95

IS-95 CDMA is a digital cellular radio system for mobile voice communication as well as many new services like mobile fax and data transmission.
In the US, the initial standards were the Telecommunications Industry Association/ Electronic Industry Association (TIA/EIA) Interim Standard 95 (IS-95) and related versions for base station and mobile performance (IS-97 and IS-98, respectively).
The IS-95 system operates in the same frequency band as the analog cellular system AMPS (Advanced Mobile Phone System).

1.3.1 Network Architecture

Mobile Station (MS)

The Mobile Station (MS) is the subscriber’s interface with the CDMA network. Both hand-held MS units having a low-power radio transmitter and vehicle-mounted MS units are permitted. The manufacturer assignes a unique 32-bit Electronic Serial Number (ESN) to each MS. It is a permanent and private identification code of the mobile terminal.

Base Station Subsystem (BSS)

Each Base Station has a unique pilot PN-offset, a delay applied to a random number sequence (PN Short Code) at the base station. This sequence is applied to forward direction transmissions that enables the terminals in a cell to decode the desired signal and reject the signals from other base stations. Pilot PN offsets ensure that the received signal from one cell does not correlate with the signal from a nearby cell.
It is possible for adjacent cells to use the same CDMA radio channel frequency (f_1). Reusing the same frequency in every cell eliminates the need for frequency planning in a CDMA system. Pilot PN-offset planning must be done in stead.
In an area where the ranges of two cells overlap, there is an increased interference, but this only reduces the number of users that can share the radio channel.

Base Transceiver Station (BTS)

The BTS comprises several base radio transceivers. Each transceiver consists of a transmitter and a receiver which has a duplicated front end to match up with the two receiving antennas used in the base antenna assembly.

Base Station Controller (BSC)

The BSC comprises control logic, data communication facilities and multiplexing and de-multiplexing equipment. The BSC can control the radio power levels of the various transceivers in the BTS, and also can autonomously control the mobile stations’ radio transmitter power levels. A single BSC can control several BTS radio equipment transmitters.

GPS Receiver

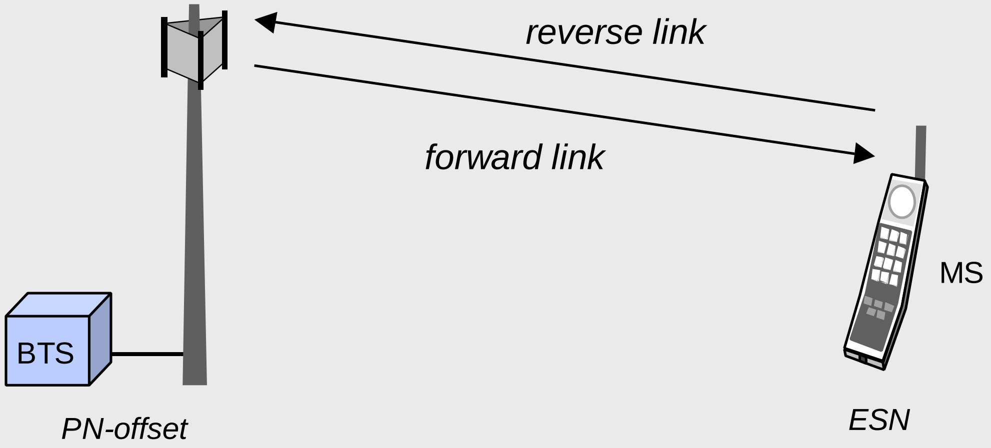
CDMA ‘soft handover’ (an MS establishes contact with a new base station before giving up its radio link to the original base station) requires base stations to operate in synchronism with one another. Therefore each base station contains a GPS receiver.

Mobile Switching Centre (MSC)

The MSC is a switching network that interconnects calls between Mobile Stations and between Mobile Stations and the Public Switched Telephone Network (PSTN). The MSC is also needed for 'automatic roaming' capabilities.

1.3.2 Forward Link Radio Transmission

The forward link is by convention the transmission from Base Station to Mobile Station (MS).

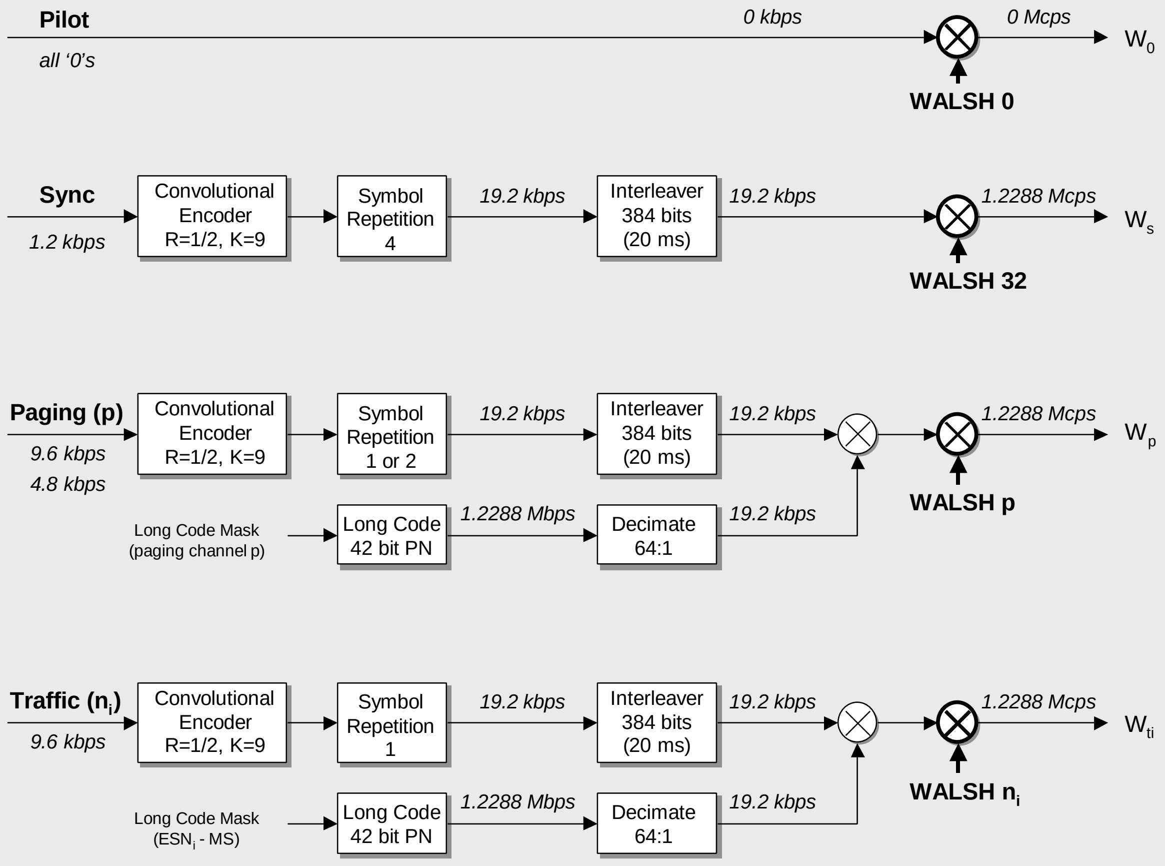


Traffic Channel

The traffic channel can accept data rates of 9600 bps, 4800 bps, 2400 bps and 1200 bps comming from a variable-bit-rate speech coder (QCELP = Qualcomm Code Excited Linear Prediction). Check digits and tail bits (convolutional encoder tail sequence to drive the convolutional encoder into a known state at the end of each frame) are included. The signals are processed in frames of duration of 20 ms.
A *convolutional code*, with constraint length K=9 and rate ½ protects each signal.
When the rate is less than 19200 bps, the transmitter *repeats* code bits (factor 1, 2, 4 or 8) to bring the rate up to 19200 bps, corresponding to 384 bits in a frame of 20 ms.
An *interleaver* permutes the code bits in each frame. This will spread the influence of burst errors, typical for wireless communications.
The baseband sequence is *scrambled* by the PN sequence derived from a *Long Code Generator* (a PN sequence with length $2^{42} - 1$ at a rate of 1.2288 Mbps) and Long Code Mask (a time-offset determined by the ESN of the MS for traffic channels). The Long Code period is:

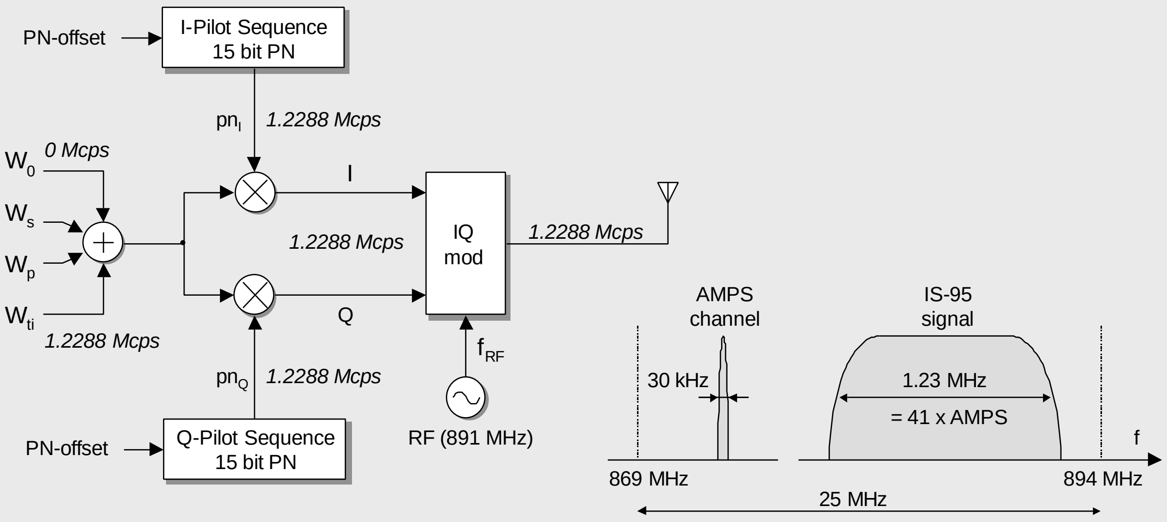
$$\frac{2^{42}-1}{1.2288\ \text{Mcps}} = 3.5\ \text{x}\ 10^{6}\ \text{s} = 41.4\ \text{days}$$

To match the rate of the Long Code sequence to the 19200 bps baseband rate, a decimator extracts 1 bit out of 64 bits of the Long Code sequence.



The baseband symbol stream is *spread* by multiplication with a *Walsh sequence of length 64*, thus creating a baseband chip rate of 1.2288 Mcps. There are 64 orthogonal Walsh sequences of length 64, certain of which are assigned to different users of the channel. All user's transmissions occur *synchronously* from the base station, so these transmissions are also synchronized at any individual subscriber's receiver *(synchronous CDMA).* The use of a set of orthogonal sequences thus allows perfect rejection of other-user interference associated with any given transmission path within the cell.

The same baseband sequence is duplicated on the I and Q channels of an IQ-modulator. Then they are *spread with 'different' pilot sequences on the I and Q channels*. This pilot sequence or Short Code sequence has a length of 2^{15} chips. A 'PN-offset' in the pilot sequences is assigned to each base station and is synchronized to Universal Coordinated Time (UCT). To demodulate a received signal, an MS synchronizes its receiver with the assigned base station and generates I-channel and Q-channel pilot sequences with the value of 'PN-offset' assigned to the local base station. Signals received from other base stations, with different values of 'PN-offset', appear as low-level noise in the receiver of the MS, due to the correlation properties of the sequences. There are 512 possible 'PN-offsets', with offset i corresponding to a time delay of 64i chips (a delay of 64 chips ≅ 52 µs ≅ 15km). Since the period of the sequence is 2^{15} chips, there are $2^{15} / 2^6 = 2^9 = 512$ possible offsets.



The bandwidth of a CDMA signal is 1.23 MHz. The bandwidth of an AMPS channel (using the same frequency band) is 30 kHz. Therefore the bandwidth of a CDMA signal corresponds to an aggregate bandwidth of 41 AMPS channels.

Pilot Channel

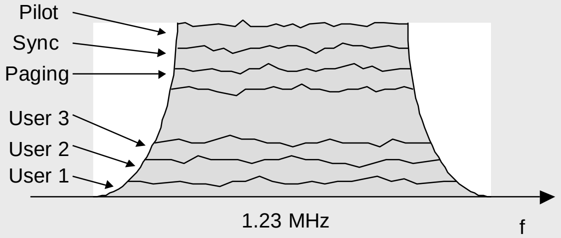
The pilot channel uses WALSH 0, a sequence of all 0s (or 1s). The channel contains no information, only the PN pilot sequence. It provides the MS with a beacon, timing and phase reference (for coherent detection). The I and Q channels of the traffic channels (containing the same information) can be despread independently to determine the amplitude of the channels. The pilot sequence can be employed for channels sounding purposes to determine the amplitudes and phases of various multipath components received at the MS (RAKE receiver).

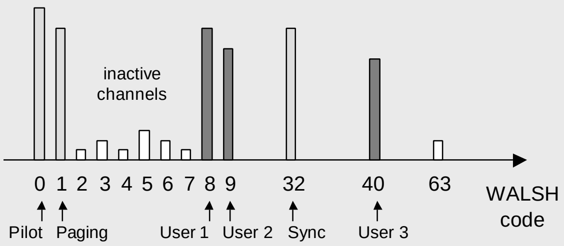
Sync Channel

The sync channel uses WALSH 32, a sequence of 32 0s, followed by 32 1s. It provides the MS with critical time synchronization data: system time (obtained from GPS), the PN-offset of the pilot sequence and the rate of the base station paging channels (4.8 kbps or 9.6 kbps).

Paging Channel

A CDMA signal carries up to 7 paging channels and using WALSH 2 to WALSH 7. The paging channels transmit information to terminals that do not have calls in progress.





1.4 W-CDMA

The target of the third-generation (3G) mobile communication systems (cellular) is the introduction of *multimedia capabilities*. ETSI (European Telecommunications Standards Institute) has been responsible for UMTS (Universal Mobile Telecommunications System) standardization since the early 1990s. In January 1998 (historical milestone) the basic technology for the UMTS Terrestrial Radio Access (UTRA) system was selected:

For the paired bands 1920 –1980 MHz and 2110-2170 MHz wideband CDMA (W-CDMA) shall be used in frequency-division duplex (FDD) operation.

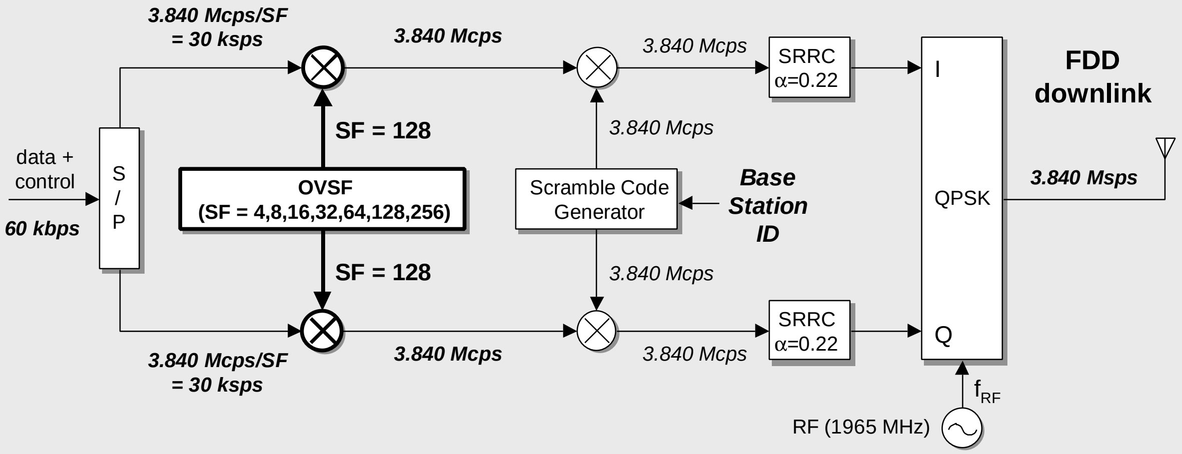
The bearer capability targets have been defined as:

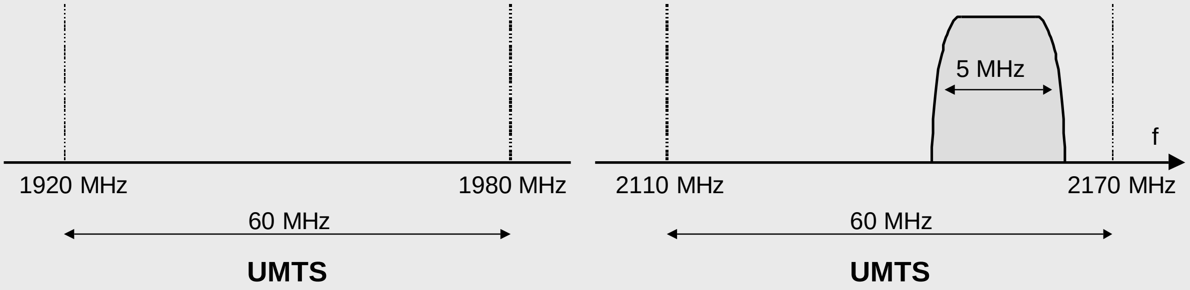
- 384 kbps for full area coverage (→ Internet access)
- 2 Mbps for local coverage (→ video/picture transfer)

A variety of data services from low to very high bitrates must be supported.

<u>*Downlink Dedicated Physical Channel*</u>

The spreading and modulation of the downlink dedicated physical channel is illustrated in the figure below.





Traffic data (voice) is multiplexed with control information (pilot bits, transmit power control bits, rate information, …). The serial-to-parallel converter maps the 60 kbps to the I and Q branch of the QPSK modulator. This produces a 30 ksps symbol rate. The I and Q branches are then spread to the 3.840 Mcps chip rate with the same Orthogonal Variable Spreading Factor (OVSF) code. Since the spreaded bandwidth is the same for all users, multiple-rate transmission needs multiple Spreading Factors (SF). The OVSF has an SF of 128 in this case (length of the spreading code). This results in the relation:

2 (QPSK) x datarate x SF = chip rate

The OVSF code is the *channelization code*. Next a *scrambling code* is applied, which is unique to the Base Station within the geographic area. Baseband filtering is done with a Square Root Raised Cosine (SRRC) with roll-off 0.22.

Different physical channels in the same cell use different channelization codes. Several downlink physical channels can be transmitted *in parallel* on one connection using a ‘grouped' channelization code (with lower SF and thus less transmission quality) in order to achieve higher channel bit rates.

Orthogonal Variable Spreading Factor (OVSF) Codes

The OVSF codes preserve mutual transmit orthogonality between different downlink physical channels, even if they use different Spreading Factors and thus offer different channel bit rates. The use of OVSF codes is thus a key factor in the high degree of service flexibility of the W-CDMA air interface.

Let C_N be a matrix of size NxN and denote the set of N binary spreading codes of N chip length, $C_N(i)$ is the row vector of N elements and $N = 2^n$. The matrix C_N is generated from $C_{N/2}$:

$$C_N = \begin{bmatrix} C_N(1) \\ C_N(2) \\ \vdots \\ C_N(N) \end{bmatrix} = \begin{bmatrix} C_{N/2}(1).C_{N/2}(1) \\ C_{N/2}(1).\overline{C_{N/2}(1)} \\ C_{N/2}(2).C_{N/2}(2) \\ C_{N/2}(2).\overline{C_{N/2}(2)} \\ \vdots \\ C_{N/2}(N/2).C_{N/2}(N/2) \\ C_{N/2}(N/2).\overline{C_{N/2}(N/2)} \end{bmatrix}$$

These variable length codes can be generated from a tree structure as shown in the figure below. Starting from $C_1(1) = 1$, a set of 2^n spreading codes with the length of 2^n chips are generated at the nth layer. The generated codes from the same layer constitute a set of Walsh functions and they are orthogonal, although the rows of C_N are not in the same order of H_N. Any two codes of different layers are also orthogonal except for the case that one of the two codes is a ‘mother' code of the other. For example $C_2(2)$ is a mother code for $C_4(3)$, $C_4(4)$, $C_8(5)$, $C_8(6)$, $C_8(7)$, $C_8(8)$, …, so these codes are not orthogonal against $C_2(2)$. A mother code is mapped on all the codes in the sub-tree produced by that code (they all start with that code). In other words, a code can be used in a channel if and only if no other code on the path from the specific code to the root of the tree or the sub-tree produced by the specific code is used in the same channel.

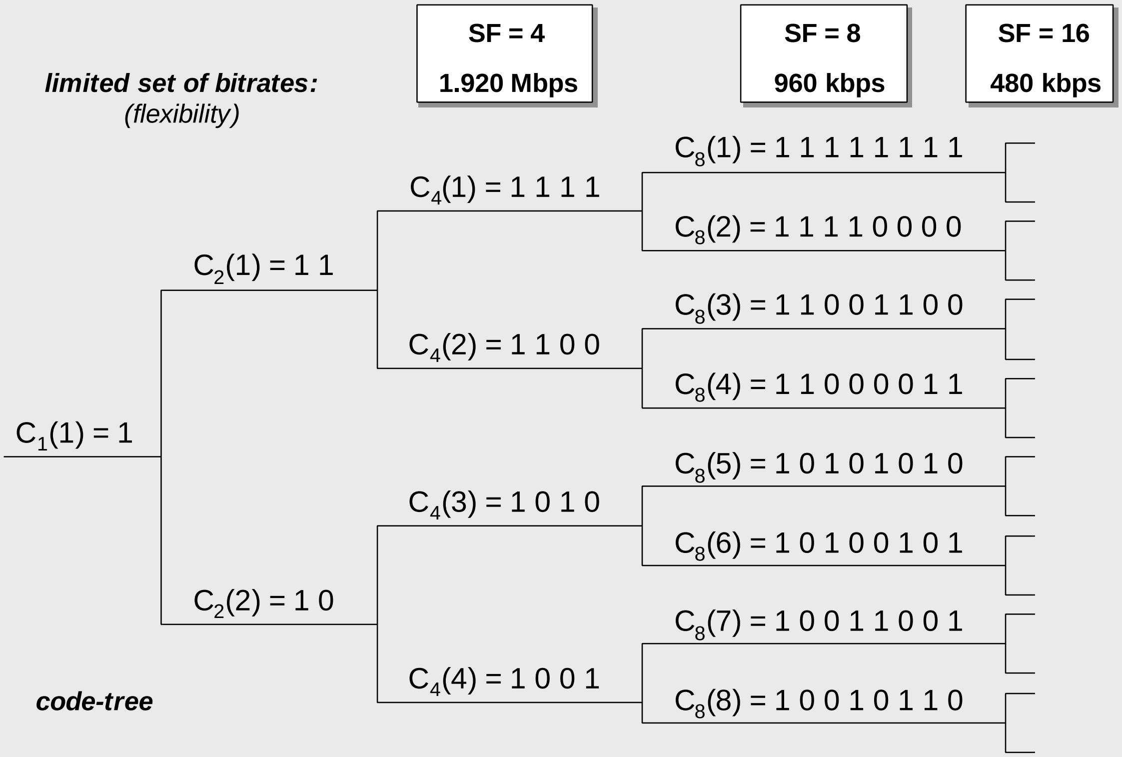
For example if $C_8(1)$ is assigned to a user, all the codes $\{C_{16}(1), C_{16}(2), C_{32}(1), …, C_{32}(4), …\}$ generated from this code cannot be assigned to other users requesting lower rates; in addition, mother codes $\{C_2(1), C_4(1)\}$ of $C_8(1)$ cannot be assigned to users requesting higher rates. The OVSF code $C_8(1)$ has a Spreading Factor (SF) of 8. With a given (fixed) symbol rate of 3.840 Msps, this results in a data rate:

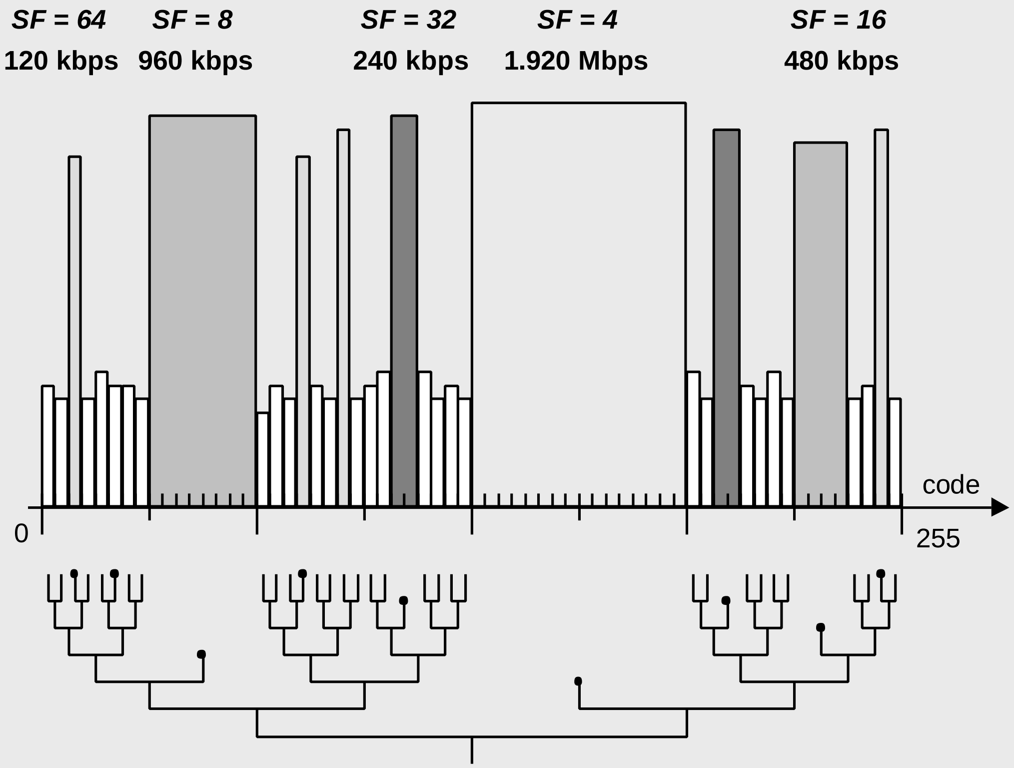
2bits/symbol(QPSK) x 3.840 Msps / (SF = 8) = 960 kbps

$C_8(1)$ is utilizing 12.5% of the available code space (channel capacity).

The OVSF code $C_4(2)$ gives a datarate of 2.048 Mbps and uses 25% of the channel capacity.

These restrictions are imposed in order to maintain orthogonality.





code-tree