# Radio control: binding, spreading and frequency hopping

## Table of Contents



Click or Ctrl-click to jump to section


Peter Scott © 2022


Last edit 30 May 2023

# The science of model flying: Signals and transmission

## Nature of our problem

Houston, we have a problem! Well actually we don't, or not usually, because in the words of the late, great Ian Dury, 'There ain't half some clever bas***ds'.

As always, despite careful checking, I might well have made a mistake, or expressed something badly, in this article. Please let me know at peter@peterscott.website so I can make this article as good as possible.

One problem with RC is the abbreviations. Loads of 'em. And they are not acronyms, which are real words made up from the first letters of a phrase. No, they are mostly meaningless and difficult to remember. So tighten the harness and lets go!

## Frequencies

You'd think that the radio spectrum was big enough for everyone to have a share. It runs from about 30 kHz to 300 GHz. However the whole world now runs on radio signals so, in practice, usable frequencies are in short supply. Money-grubbing governments sell them off so they are worth a lot of money. To see the full range in the UK take a look at http://static.ofcom.org.uk/static/spectrum/fat.html.

As model flyers we are insignificant. We get our radio control frequency (RC) allocation grudgingly. Way back, we got parts of 27, 35, 42 and 72 MHz for our sole use. We paid for a licence. Then citizen's band (CB) ruined 27 for us. The 900 MHz and 2.4 GHz bands we have now been given are used for many other things as well. We have to protect ourselves against interference from these.

Connecting a transmitter (Tx) and a receiver (Rx) is straightforward and is covered in another article on aerials. All you need are a transmitter that sends out enough power and a receiver that is tuned to the same frequency and picks up the signal. It is when we want to send out data to operate our servos and throttle that problems might arise. Any problem with the data will make our models crash.

## This article is in four sections

In the first section I will cover the basics for those people who want to know how it works in plain English but nothing more.

Secondly I will cover a brief history of radio control.

The third section will look in more technical detail at the various techniques touched on in section one.

The fourth will be for people like me who aren't satisfied until they have probed deeply into things. Here there be dragons and the need for coffee and an icepack for the head. Or maybe just forget it if you know what's good for you.

## Section one: The basics

The 2.4 GHz band that most radio control flyers use is also used for a huge range of other things.  Not only do we need to be protected from other flyers' Txs but also wifi computer networks, baby alarms, microwave cookers, wireless microphones, garage door openers and so on.

When you bind a receiver to a transmitter a number is exchanged called a Global Unique Identifier (GUID). This is used to encrypt the control data we send and allows the pair to change frequencies when there is interference. It ensures that no other transmitter can take over your model. I use FrSky, which makes binding very easy. I chuckle when I hear users of other makes cursing at the field trying to bind their equipment or rebind when the link fails, which FrSky never does.

There are two systems used for radio control. Different makers call them different things. One is the better but both work well. Direct Sequence Spread Spectrum (DSSS), commonly known as DSMX, selects a frequency band from those available then sticks with it. Frequency-Hopping Spread Spectrum (FHSS) uses the whole band and hops from one frequency to another. Spread Spectrum, which is in both names, is a way of encrypting the data we send to overcome interference. The encryption is done using Code Division Multiple Access (CDMA). These techniques were not invented for radio control. They are used in the other everyday things as listed above.

The last abbreviation you need to know is LBT, which stands for Listen Before Talk/Transmit. It is mandatory in the European Union and requires that a transmitter finds a safe frequency before it starts to transmit. The only reason you need to know this is that if you live in the EU or the UK, and you buy transmitters or receivers from outside the EU, you will need to update their firmware. Apart from the legality you cannot bind if both are not LBT.

All of these are explained in increasing detail as you go through this article. If that doesn't interest you then jump to the summary at the very end.

## Section two: A brief history of radio control

At first a radio control transmitter used the whole of the frequency band so only one person could fly at a time. Clearly we needed to split the band into safe smaller bands. In those days there was very little use of radio transmissions outside of radio and television broadcasts, civil and military forces and air traffic, so there was little or no interference.

First the band was split into a number of narrower fixed bands. This was called frequency division multiple access. There could still only be six or twelve people flying at once and interference between them was not uncommon.

For those who have never used older 35 and 27 MHz equipment, the large board with rows of hooks on some flying fields will be a mystery. Frequencies were chosen by plugging crystals into the Tx and Rx. There were only six or twelve channels. Switching on without checking whether someone else was already on your frequency was the greatest crime. Txs were often kept in a pound. Each frequency had a colour. You put a coloured ribbon on your Tx aerial and had to register that you were using that frequency on the board.

Eventually we were given use of the 2.400 – 2.485 GHz band called ‘Industrial, scientific and medical’. The clue to the problem is in the name. This is a band used for lots of other things. How then can we reliably fly models in this electromagnetic soup of signals?

The first idea was to sniff the air and only use a frequency not currently being used. The Tx and Rx will hop in a known sequence from a one frequency to another until it finds an unused one with no interference. This is called frequency hopping. It also has the advantage that two Txs cannot interfere with each other’s signals either. The hops are fast so the short signal losses when hopping due to interference don’t matter.

However that only gets us so far. If there are lots of users on a band then there might not be many free frequencies. In any case we also want to protect ourselves against jamming, deliberate or otherwise. So further layers of protection are used called Spread Spectrum and Code Division Multiple Access.

**Hedy Lamarr**
(You can safely skip this except for paragraph four.)

On my Tx I have put a printed strip saying ‘Thanks to Hedy Lamarr’. For those who don’t know the reason I thought it would be good to describe this remarkable woman. Born Hedwig Keisler in Vienna in 1914, she made a name as a beautiful and talented film and stage actor. In the late 1930s, she fled an oppressive husband and, having a Jewish background, the Nazis, ending in the US.

But that isn’t why her name is on my Tx. She was also an inventor. She worked with Howard Hughes and suggested he change the shape of his aircraft from square to a more rounded streamline shape. However it isn’t aviation that put her on my Tx either. Hughes was so impressed by her talent that he gave her a team of scientists and engineers and free rein to do what she wanted. During World War Two a new generation of radio controlled torpedoes was being developed, but the Germans found that they could jam the signals. With composer George Antheil, Lamarr devised a system, that she patented in 1942 (US Patent 2,292,387), for changing Tx frequencies using a device based on a piano roll player. The system became known as frequency-hopping.

As is so often the case, establishments, in this case the US navy, are resistant to ideas from outside and did not take up the idea until the early 1960’s. Her achievement was eventually recognised in 2014 when she was inducted after her death to the US National Inventors Hall of Fame.

Frequency hopping allows the Tx and Rx to switch frequencies, especially when connection is lost due to interference or a block. This is why we never worry about switching our Txs on when others are flying. Ours will simply not connect using frequencies currently in use.

And all ‘Thanks to Hedy Lamarr.’

We will now look at the various techniques in more detail.

## Section three: More details

### First person view

Before we start I must make it clear that this article only covers the sending of control data to the model and the return of telemetry data. First Person View (FPV) uses even more complicated technology to return the video data from the on-board camera to the flyer's screen or goggles. Take a look at https://youtu.be/-eaVseMQycY to see what I mean.

### Practical matters

There are a few words to explain first. Frequency is the rate at which a wave vibrates in a second. It is measured in Hertz. A frequency band is a range of frequencies set aside for a purpose, for example the 2.400 to 2.485 GHz that we are allowed to use. A radio wave is called a carrier or signal. We vary the carrier to send our instructions to our models. This is called modulation. To learn more about this read the companion article about aerials.

The higher the frequency the lower the range due to absorption in the atmosphere and the less the carrier can bend round obstructions. We also see this in mobile phones where increasing frequency for 3G, 4G and 5G means reducing the distance between base stations and possibly making them taller.

### Multiple access

The requirement is safely to squeeze as many flyers as we can into a band that is shared with many other uses. This is called 'multiplexing' or 'multiple access'. There are several ways to divide up a band. The three most common are:

- Time division multiple access: Without knowing it, users take it in turn to use the whole band. That is how the internet works.

- Frequency division multiple access: Here the band is divided into even narrower bands each of which is used by one user only. Users' equipment has to choose a band and exclude others or find an unused one before it starts to send data.

- Code division multiple access: Here many users share a band but each encrypts data with a code number so it can only be read by their own receiver using the same code.

An example of where all three are used might help. Fibre optic Internet connections allow almost unlimited data speeds compared with mobile, satellite or copper connections. Why is that? The data is carried on light that goes on and off very rapidly. One fibre can carry many different colours (frequency division). On each colour, some of which are invisible to us, data is sent in small packets one after the other for many users (time division). Interference and hacking are prevented by encryption (code division) for example in WhatsApp or Virtual Private Networks.

Back to us. Our radios use frequency and code division. Time division is not practical for us at the moment, though it might be when 5G mobile becomes more common and reliable. I suspect the CAA/FAA would like to force us to use it in some form.

The two main methods are DSSS and FHSS. In situations where there are few users and little external interference there is nothing to choose between FHSS and DSSS. Only when there are many flyers or a lot of external interference will FHSS be preferable.

**Global Unique ID (GUID)**

A GUID is a unique number that can be used as a label for anything. Binding and the techniques explained below are dependent on the GUIDs of the Tx. There is no central register. It relies on there being so many possible numbers that a repeat is very unlikely. Each GUID is created by a computer program or algorithm or just made up. It might be built in to a chip in the equipment as it is in our Txs.

FrSky GUIDs have this format in hexadecimal B7 99 00 00 00 00 00 00. Each digit has 16 values (0 to F) so that gives $16^{16}$ possible values or $1.8 \times 10^{19}$. Only the first four characters are used by FrSky at present. All 2.4 GHz Txs have a GUID, as do telemetry-capable Rxs to allow them to send data back to the Tx. That is why you are asked during FrSky binding whether telemetry is required.

**Spread spectrum**

Spread spectrum is a way to improve resistance to interference by increasing the number of data bits sent for each bit of the control data. Instead of squeezing the signals into a narrow frequency band used by one user, the data is encoded so it is more like noise and spreads over a wider band. There will be noise and other users' signals in this same band. In fact our signal can even be at a lower power level than the interference noise and still be readable, like when you hear your name being spoken at the far side of a very noisy room. The signal is hidden in the noise. There is more about this under CDMA.

**Direct Sequence Spread Spectrum (DSSS)**

One or more fixed frequencies are chosen by the Tx and Rx at switch on. The two most common are DSM2 that selects two frequencies and DSMX that uses up to sixty. DSM2 cannot use LBT (later) so is no longer sold in Europe. DSSS is less tolerant of very noisy environments.

**Frequency-Hopping Spread Spectrum (FHSS)**

In effect FHSS is just an extra layer of protection added on top of DSSS like hops turning ale into beer (see what I did there?). It has been described as 'Agile DSSS'. Each frequency hopped to is used like the whole band in DSSS.

The Tx and Rx hop from one frequency to another, following a fixed sequence of hops called 'pseudorandom'. To avoid every one doing the same hops the start point in the sequence varies, determined by a 'seed', which is derived from the GUID. Therefore different Tx/Rx pairs of the same make will start at different places in the sequence.

FHSS is highly resistant to interference and still works when perhaps 80% of the band is occupied. If very congested the signal might be lost through the time taken for repeated hopping. Signals cannot be intercepted nor jammed unless the hop pattern is known. Does this it make it more difficult to disable or jam by authorities? Is that why they have to use very high power signals to swamp 'rogue drones' by brute force? The band we use is 80 Mhz wide and has 36 hopping channels. The seed for the pseudorandom sequence would

be created by ‘hashing’, which means using a maths procedure on the GUID to get the correct format of digits for the seed.

## Section four: Techniques in depth

### Hashing

If you look this up on a search engine you risk your brain hurting, so let’s look at it simply. It is a maths method for changing a series of digits, or characters, pictures or sound in digital form, into an agreed number format in a way that makes it unique. It usually means only using the lowest digits in the result of the calculation. If anything changes, either deliberately or due to interference, the hash value will change and you know the data has been corrupted. I don’t know why it is called hash, which is how h is pronounced in France and the symbol # looks like an h. It is also how a number is indicated in the US, for example #3, whereas in the UK we would say No. 3.

Suppose we want to send a message to our mates, ‘Lets meet at seven pm.’ We want to ensure that they get it correctly, so we find the numerical position of each character in the alphabet and then add numbers up. Then we send that as well in the form of a hash value.

| L | e | t | s | m | e | e | t | a | t | s | e | v | e | n | p | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 5 | 20 | 19 | 13 | 5 | 5 | 20 | 1 | 20 | 19 | 5 | 22 | 5 | 14 | 16 | 13 |

Hash total 214

If the people who get the message do exactly the same to the received message and also get 214 they can be pretty certain they got it correctly, as two equal value corruptions are unlikely. If there were many more characters in the message and the hashed value got very large we could agree just to use the last three digits.

A much more complicated method, called the cyclic redundancy check (CRC), is used by computers to check that files have been copied or saved without corruption, usually called something like ‘error checking’, ‘verification’ or ‘validation’.

## Code Division Multiple Access (CDMA)

This is how the data is sent in DSSS and FHSS. It is a kind of encryption, and is used widely, not just for radio control.

Let’s examine the words. Multiple access means more than one device using a data channel. Code division means the Tx using an agreed code of bits effectively to encrypt data so it can only be understood by a Rx using the same code. The channel is divided by code not by frequency.

Each data bit is replaced by a ‘spreading code’ or ‘sequence’ of several 1 and 0 bits. The more encoding bits that are used the more reliable the method becomes. How many coding bits there are to each data bit is called ‘Process Gain’. Computer wifi uses the low value of 11 but corrupted bits are re-sent and its range of about 250 m means that corruption is less likely anyway. An RC Tx uses 64 bits as it cannot ask for a retransmit so needs higher reliability. The range is several kilometres meaning corruption is more likely. The leading and trailing edges of the bits are not steep to avoid the harmonics broadening the frequency band further. Because of its anti-jamming and security capability it is used by the military, GPS, Bluetooth, mobile phones and wifi networks.

Of course for commercial and security reasons I haven't seen the program code that runs to decode the incoming signal. I imagine that it patiently looks at the signals that flash by until it spots some that decode to something usable. Remember that computer devices run millions of times faster than our brains so 'patiently' will mean minute fractions of a second. It reminds me of virology and immunology. The antibodies wait in our blood until they spot a virus spike molecule that matches their own shape then they strike.

To understand how the coding and decoding works requires an explanation of digital logic, or to be more exact the function 'Exclusive Or' or XOR. It's tricky but worth a try as it gives you a insight into how all digital computers work at their very centre. XOR is described later.

**GUID and the above methods**

During binding the Rx uses the transmitted GUID to seed the pseudorandom sequence and probably the CDMA key, though I can't find a firm confirmation of the latter. This would be done by 'hashing' as described above, which means using a maths procedure on the GUID to get the correct format of digits for the seed.

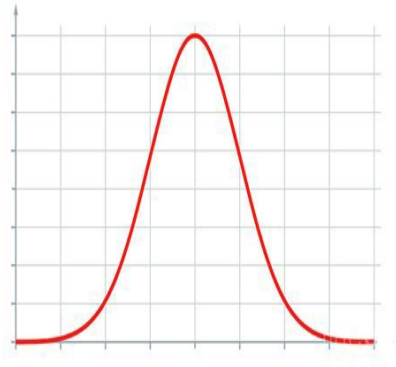
**Listen Before Talk/Transmit (LBT)**

In the European Union, and former satellites like the UK, all systems must also check for a clear frequency before transmitting using LBT. The technology is also found in Bluetooth connections and many other radio-based wireless networks. An EU Rx will not bind to a non-EU Tx and vice versa.

**Gaussian frequency-shift keying (GFSK)**

This is a version of frequency modulation that reduces the range of frequencies needed (bandwidth) needed. The word Gauss is used as the leading and trailing edges of the datum are a bit like a Gaussian distribution or 'bell curve'.

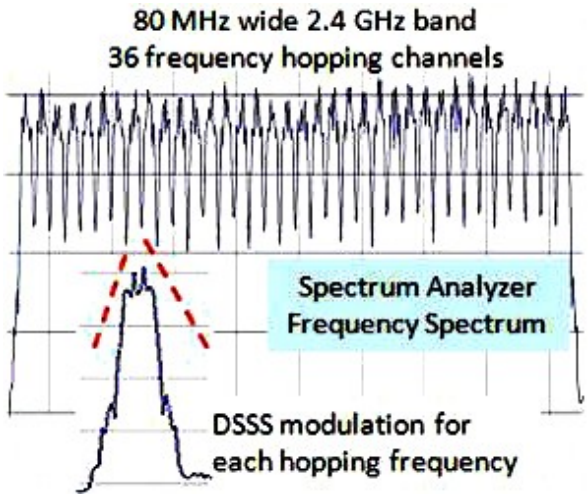
Here is one such bell curve and a real trace from received data.



Gaussian 'bell' curve

From pixels.com

Picture of real signals copied from an oscilloscope




From rchelicopterfun.com

This method is used in DSSS but not in FHSS.

**Computer logic and spread codes**

All computer-type devices only understand two things, 1 and 0. Each is called a binary digit, shortened to bit. If you think of 0 as being the absence of a 1 then they only understand one thing that is either there or not there. So when your Tx, phone, television, laptop, washing machine, remote control lights, satnav, fitbit, hifi, wifi, car etc is working, at its heart it is just juggling 1s and 0s. A voltage of 1 V to 5 V gives a 1 and 0 V gives a 0. When I use the word computer it applies to all of the above devices and of course to our radio equipment.

To work at the speeds they do, computers do a small variety of very simple maths operations. The calculating part of a computer processor chip is mostly made of transistor logic gates, which are surprisingly easy to understand.

**NOT**

Here is the simplest. This inverts the bit and is called NOT.  A is the input and Q is the output. In words ‘If input is 1, then output is not’ (i.e. 0)


The results are shown in a ‘truth table’. For the NOT gate it looks like this:

| Input | Output |
|---|---|
| A | Q |
| 0 | 1 |
| 1 | 0 |

Most gates have two inputs to be compared. This means there are four options in the truth tables.

**AND**

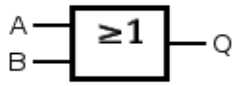
This one is called an AND gate. In words it is ‘If both A AND B are 1 then output is 1, else output is 0.’


| Inputs | | Output |
|---|---|---|
| A | B | Q |
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

A practical example might help. In a washing machine water must be supplied at a sufficient pressure. This is checked by a sensor, which outputs a 1 if it is high enough. That could be input A. You now press the button to start the machine. That is input B. Only if A AND B are 1 will the output Q start the machine. If the output is zero then the circuitry gives you an error message like ‘check water’ or more usually and less helpfully ‘Error E0045Z’.

**OR**

This is an OR gate. In words it is ‘If A OR B OR both are 1 then output is 1, else output is 0.’




| Inputs | | Output |
|---|---|---|
| A | B | Q |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

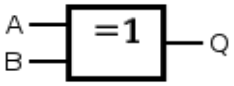
This could be a lamp with two switches in parallel. If switch A is 1 then light the lamp. If switch B is 1 then light the lamp. If both are 1 then still light the lamp.

**Where is this going?**

Let’s suppose want to send the following data: 1001
To keep this simple we will use a four bit spreading code 0010 remembering that in our Txs this might actually be 64 bits long.

**XOR**

We now have to look at the XOR gate which is one of the oddest of the logical functions. In words it is ‘If A OR B are 1 then output is 1, else output is 0.’ It is called ExclusiveOR (XOR) because it excludes the case where both A and B are 1.




| Inputs | | Output |
|---|---|---|
| A | B | Q |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

For each bit in the data – 1001 - we do an XOR with each bit in the spreading code. This gives us the spread output that we send.

| | | | | |
|---|---|---|---|---|
| Bit | 1 | 0 | 0 | 1 |
| Spread code | 0010 | 0010 | 0010 | 0010 |
| CDMA spread output | 1101 | 0010 | 0010 | 1101 |

When the Rx gets the CDMA spread output data it decodes it using XOR as follows:

| | | | | |
|---|---|---|---|---|
| CDMA data | 1101 | 0010 | 0010 | 1101 |
| Spread code | 0010 | 0010 | 0010 | 0010 |
| Decoded data | 1111 | 0000 | 0000 | 1111 |

If the decoded data gives the same bit in all four positions the Rx knows this is from the correct Tx. It ignores the repeated digits and ends with 1001 which is the data that was sent. This process is known technically as ‘correlation’. In practice some corruption might occur so not all decoded data will be the same. In this case corrupt data is ignored.

However if the received CDMA spread output was encoded by a different Tx using a different spread code then the bits in each group would not all be the same and the data would be rejected. Suppose the spread code used by the other Tx was 1001 instead of the 0010 that we use.

Transmitted data

| | | | | |
|---|---|---|---|---|
| Bit | 1 | 0 | 0 | 1 |
| Their spread code | 1001 | 1001 | 1001 | 1001 |
| CDMA spread output | 0110 | 1001 | 1001 | 0110 |

| | | | | |
|---|---|---|---|---|
| Received CDMA data | 0110 | 1001 | 1001 | 0110 |
| Our spread code | 1010 | 1010 | 1010 | 1010 |
| Decoded data | 1100 | 0011 | 0011 | 1100 |

These would be rejected as corrupt or not intended for us.

XOR is used for many types of digital encryption. No other gate will do. If you have plenty of time to spare you might like to try using AND or OR and see what happens.

If like me you like spreadsheets (yes – we do exist), you can try out the effect of the various gates by setting up truth tables like those above. LibreOffice Calc and its imitator Excel have all of the logic functions available for you to try.

There are several more gates. To learn more try https://en.wikipedia.org/wiki/Logic_gate. Oh dear, do I hear the sound of running feet and cries of 'Aaaargh'?

## Other information

### Who uses what method?

Name used by maker in brackets – these will change so please tell me if I miss any

DSSS  used by Spektrum, Horizon, Flysky, JR  (DSM2 and DSMX)

FHSS  used by Futaba (FAAST), Hitec (AFHSS), FrSky (ACCST, ACCESS), Multiplex (M-Link)

### Radio frequency chips used

This is here for interest only. These are all standard commercial chips used in cordless phones, wireless keyboards, and game controllers, etc.

| | |
|---|---|
| Micro Linear ML2724 | Futaba FASST |
| Cypress CYRF6936 | Spektrum DSM |
| Texas Instruments CC2500 | FrSky, Hitec, Futaba (S-FHSS), JR |
| Texas Instruments CC2520 | JR (DMSS) |

### At my flying field

At my flying field there is a corner where several models have crashed inexplicably. I call it the Northrepps Triangle. We are close to a coastal radar dome and have wondered if that might be the cause. My radio uses FHSS (ACCST) so should be robust but others are still using DSM2 or X. Next time there is a crash I must ask and see if there is a pattern. The dome has now been moved inland due to the steady erosion of the cliffs so maybe I'll never know.

## Summary

The key to all of this is that each Tx/Rx pair shares the same frequency band with others. Rxs will only accept data that has been encoded using the Tx's key.

Each maker uses a different name for the methods used – ACCST, FASST, DMX etc but all use the same set of basic technologies even if only in part. The best systems can reliably extract our control signals even when they are smaller than the surrounding electrical noise.

To be ‘futureproof’ it is probably best to use FHSS as the band becomes more congested or noisy, or in situations such as competitions where there are many fliers at once. Happily, problems are rare at the moment.