Getting started with Software Defined Radio

Joshua S Curry and Denis A Nicole
Electronics and Computer Science
University of Southampton*

13th September, 2021

Contents

1 Introduction

Software Defined Radio peripherals are now readily available at many price points. There is also a wide rang of personal computer software that will quickly get a user started and allow them to progress rapidly to interesting applications. In a cybersecurity context, it is remarkably easy to monitor, decode and, in some cases "spoof" transmissions to achieve a wide range of effects on a target. As professionals, we need to understand the ease, scope and limitations of such attacks, alongside the legalities of research and "penetration testing".

*This project was funded under *Cybersecurity Body of Knowledge (CyBOK)* subaward 2021–2471.

2 Hardware

There are now a variety of SDR "dongles" on the market; the cheaper ones connect via USB and are typically supported on x64 Windows and Linux machines as well as Arm Linux single board computers e.g. *Raspberry Pi*. Along with the different prices, there is a wide variety of performances. The most obvious distinction is whether or not the device has transmit capability. This will be needed for more advanced laboratories, but opens up considerable legal difficulties if users are inadequately trained or supervised.

Many dongles are supplied as bare boards; some sort of protective case will be needed in a teaching environment. Unfortunately, the associated *field programmable gate arrays* or *application specific integrated circuits* dissipate quite a lot of heat; a sealed plastic box may cause premature failure. If a metal box is used, care must also be taken about allowing additional conductive paths between the external connectors.

2.1 Receive performance

Few SDRs offer decent performance at frequencies below about 100MHz; the HF *(short wave,* 3–30MHz) and lower frequency bands are nowadays infrequently[1] used in security applications and this will not normally be an issue for you. Furthermore, you are unlikely to find *dipole* antennas for HF and below to be convenient in a teaching environment; reception in these bands would perhaps best be performed with a tuned *magnetic loop* aerial.

The headline performance figures normally include the overall frequency range, the range of frequencies that can be "captured" simultaneously, and the bit-depth of the analogue to digital converters. For overall range, coverage from the FM broadcast band (88MHz) up to 2.5GHz is desirable. The frequency capture range is often constrained mainly by USB performance and a few MHz is perhaps typical. For example, few general-purpose SDRs will have the ability to decode modern WiFi signals effectively; WiFi dongles are usually dedicated to this specific application. As for *bit depth*, or *ADC resolution:* more is better but the naïve resolution can give a misleading account of the achievable *signal to noise ratio*. In a narrow bandwidth, signal processing is able to enhance substantially the effective resolution and other limitations often dominate over the raw ADC performance.

Most SDRs have a poor ability to receive weak signals. Their noise figures, at around 10dB, mean that the SDR itself is generating ten times more noise power than the thermal background; in contrast, a high quality receiver may generate very little additional internal noise. For specific applications, it may be necessary to use an external *low noise amplifier* and/or a high gain directional aerial to enhance the received signal. In general, however, other sources of interference will dominate over the receiver's internal noise unless great care is taken. These other sources can include signals *(birdies* or *spurii*) generated inside the SDR, or RF interference caused by nearby electronic equipment such as personal computers. A teaching laboratory can be a very noisy environment.

[1] An exception is for *near field communications*, but these applications require specialised coupling transformers and are best addressed using dedicated hardware.

Many SDRs are easily *blocked* by strong signals outside the frequency range of interest. The better (and more expensive) ones have a variety of filters to remove these *out of band* signals. For specific applications, it is relatively cheap and easy to build input filters that will either pass only the wanted frequencies or will *notch out* specific unwanted ones.

2.2 Transmit performance

Many SDRs are receive-only, and this cannot be used for testing active attacks. Those that can transmit will typically generate a few milliwatts of output power; this is to low to cause problems with radiation safety, but can interfere with other services; only transmit if you know (see below) it is lawful and safe to do so.

A specific issue with (licensed) transmission on the GSM bands is frequency accuracy. Mobile phones "train" to the frequency of the first network to which they connect; if this is off frequency, they may become unable to "see" other networks.

2.3 Hardware recommendations

The RTL-SDR is popular and can be very cheap, but is unsuitable for our laboratories, mainly because it lacks transmit capability.

We have standardised on the LimeSDR Mini, mainly because of the wide range of advanced software that is available for it. It is also fully capable of acting as the RF portion of a GSM or LTE base station. Interesting specialist software includes:

- Digital television transmission and reception.
- GSM base station
- LTE stack

3 Cables and connectors

For signal connections, SMA connectors are now in almost universal use for small SDRs. The connector on the SDR board will have a grounded male (exterior) thread and a small hole for the central signal connection. The corresponding cable connector will have a freely rotating female (interior) threaded collar and a central signal pin. The threaded collar is equipped with spanner flats, but these are only used with a precision (and gentle) torque spanner in order to improve repeatability for precision applications. In normal use, they should only be tightened by hand to the first resistance.

WiFi commonly uses a very similar connector, the *reverse SMA*, which can cause confusion. In the reverse connector, the positions of the centre pin and hole are reversed between plug and socket, while the threaded outer remains unchanged. At first glance, normal and reverse SMA connectors look identical but they are not interchangeable. Mixing them up will damage the connectors.

SMA terminated coaxial cables, both flexible and semi-rigid, are readily available; in normal use, equal and opposite currents flow in the centre conductor

and the outer screening so that there is no electric or magnetic field outside the cable. It is, however, also possible for an unbalanced signal to be coupled to the cable and it will radiate from the cable itself; this is sometimes referred to as a signal on the outside of the screening. Suct a situation is undesirable and can sometimes be mitigated by passing the cable through magnetic "ferrite beads".

Normal cables have a *characteristic impedance* of 50Ω. This means that, if the cable is terminated in a pure resistance of 50Ω, all the signal power is transmitted into the load. If, on the other hand, the load is either *reactive* or differs from 50Ω, it is "mismatched" and some of the signal power will be reflected. If a cable is mismatched at both ends, there will be multiple reflections; these are undesirable and create interference with the main signal.

Some SDRs have a built-in *bias tee*. This supplies a DC voltage on the input SMA, intended to power a low-noise pre-amplifier. If you are not using it, it should be turned off. If the aerial offers a DC short, much energy will be wasted by a powered bias tee.

4 Aerials

The *half wave dipole* is a standard aerial used over a wide range of frequencies. The wavelength λ (in metres) of a radio signal in air is calculated easily from the frequency f in megahertz as

$$\lambda = \frac{300}{f}$$

A half wave dipole consists of two wires, each of length $\lambda/4$, arranged end to end for a total length of $\lambda/2$. The *feeder* is connected across the two inner ends and presents an impedance of about 70Ω. This feeder should in principle be *balanced* rather than coaxial, but the situation can be improved by threading the "coax" a few times through a suitable ferrite bead, thus forming a *current balun*. Ready made aerials of this sort, complete with balun and connectors are readily available and cheap; we can recommend the Multipurpose Dipole Antenna Set from RTL-SDR, which covers frequencies from around 70MHz to 940MHz.

Some further simplification may be possible. Half of a $\lambda/2$ dipole may be replaced with a conductive reflecting surface; this leads to a $\lambda/4$ monopole rod with the coaxial cable centre connected to the end of the rod and the outer connected to the conductive sheet. In this case, no balun is needed; the feed impedance is also halved to 35Ω. Finally, it may be possible to abandon the conductive sheet and "hope" that the bulk of the SDR's printed circuit will provide a good enough ground plane. Thus, as a last resort, an adequate aerial might be formed from a single $\lambda/4$ wire soldered to the centre of an SMA plug and connected directly to the SDR. These crude simplifications will, however, make the pick-up of local interference much worse.

5 Software

There is a great deal of SDR software available on the WWW. The *Gnu Radio Companion* should be a valuable learning tool; it supports an enormous variety of signal processing plugins and offers an intuitive user interface in which processing blocks are "wired up" on screen. While it has improved dramatically in recent years, we are unable to recommend for general undergraduate laboratory use because of some continuing instability in the graphical interface. In our experience, the display does not share properly over *Microsoft Teams* and occasionally exits unexpectedly. It is, however, an excellent tool for advanced project work in which students have time to adapt to its idiosyncrasies. For Windows, installation using conda is recommended.

For laboratory use, we have selected *SDR Console*. This may be installed from `https://www.sdr-radio.com/download`. In addition, for the LimeSDR Mini, you will need the latest FTDI drivers which are currently
`FTD3XXDriver_WHQLCertified_v1.3.0.4.zip`.
With these two installs, the SDR works "out of the box".

6 The Legalities

6.1 Reception

In the UK, it is in general illegal to operate a radio receiver or transmitter unless you has been specifically authorised. For example, you are not allowed to receive broadcast television without purchasing a license; this requirement is enforced with enthusiasm. More generally, section 48 of the Wireless Telegraphy Act 2006 states that:

> A person commits an offence if, otherwise than under the authority of a designated person—
> (a) he uses wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addressee of a message (whether sent by means of wireless telegraphy or not) of which neither he nor a person on whose behalf he is acting is an intended recipient, or
> (b) he discloses information as to the contents, sender or addressee of such a message.

There are some general authorisations, including the receiving of licensed (but *not* pirate) radio broadcasts, and licensed amateur radio transmissions. In general, if the information is not being transmitted lawfully, or is not intended for you, you must not listen to it or disclose its contents. This will not normally be a problem in a teaching environment; you will almost always be listening only for signals that are specifically transmitted for the class.

6.2 Transmission

Unsurprisingly, the law about transmission is even more strict; with very few exceptions, you can only transmit signals for which you have an Ofcom license.

As well as the *Wireless Telegraphy Act*, transmission of higher power signals beyond the strength of typical SDR "dongles" will also require you to consider

the possibility of exposing others to excessive non-ionising radiation. If you stray into this territory, your aerial is also likely to need planning consent; you might also have difficulty with your neighbours if your transmitter interferes with their electronic equipment.

Unless you have appropriate test equipment and fully understand the technical issues involved, YOU MUST NEVER AMPLIFY THE OUTPUT FROM AN SDR. Most SDRs create a variety of spurious signals and their frequencies may be close to the intended output frequency or far removed from it; amplification of these signals can cause serious problems.

Finally, you need to take into account *where* you are operating your equipment. If on land, this will normally need the landowners consent. In a vehicle, you may be distracting the driver (using a mobile phone while driving is prohibited), or you may be interfering with vehicle electronics. Additional rules govern operating from ships or aircraft; you will certainly need the permission of the master or pilot and there are additional restrictions associated with the very long *line-of-sight* from airborne transmitters.

6.3 License exempt bands

There are a number of specific frequency ranges for which low-power transmitting equipment does not require an Ofcom licence. As well as the power restriction, equipment may also be restricted to specific uses and subject to some sort of *type approval*. These bands include:

- Short Range Devices: allocations include 433.05–434.79MHz, 862–875.8MHz, 915–921MHz, and 2400–2483.5MHz.
- Citizens Band *Narrow band frequency modulation* channels in the ranges 26.965–27.405MHz and 27.60125–27.99125MHz. There is no longer a 934MHz citizens band in the United Kingdom.
- Radio microphones: 173.7–175.1MHz, 863–865MHz, and 2400-2483.5MHz.

If you have purchased licence-free transmitting equipment, such as a garage door opener, it should be operating within one of these bands. So it is lawful to listen in these bands *for your specific transmitter*, but not to gather information about other users. Otherwise, you lawful use is restricted to amateur bands and lawful broadcast radio but, unless you have a paid license, broadcast television.