ROYAL SCHOOL OF ARTILLERY

BASIC SCIENCE & TECHNOLOGY SECTION

Future Developments in Air Defence Radar

INTRODUCTION

Military, Air-Defence, radar systems have to operate in a hostile environment against stealthy targets. Each development in radar is soon matched by an increase in anti-radar techniques (e.g. jamming) or by a decrease in the reflective properties of the target (e.g. stealth). Sometimes, in battle, the air defence radar has to be switched off to eliminate the risk of detection or attack from radiation-seeking missile. Future AD radars must address these two problems.

A conventional radar transmits a burst of energy towards an area of space and then interprets any reflected signal as a potential target. In a modern scenario then not only would such a radar would be quickly detected and neutralised but it would also fail to detect many of those targets that had adopted stealthy techniques.

If we could design a radar which operated in such a way that an enemy cannot detect its transmissions then it would be difficult for him to interfere with them or to locate the radar in order to attack it. In order to detect stealthy targets (that reflect very little radar energy back to the radar) then the radar system could be designed to detect the effects of other properties of stealthy targets.

HOW TO HIDE THE RADAR

An enemy who is trying to jam a radar must obviously know some basic and current facts about that radar, for example, what frequency it is using and whether it is switched on or not. One way of determining a radar's parameters is for an enemy to use a radar receiver to listen for its transmissions. If he detects any radar transmissions that might be a threat then he can operate his jamming equipment. If he were to operate the jammer at the wrong frequency or when the radar was switched off then his transmissions would reveal his presence. Jamming when there is nothing to jam might be counter-productive.

Operating a radar that the enemy cannot detect is obviously a very good protection measure. Current methods of hiding radar transmissions exploit the properties of 'noise'. When there is no 'real' signal entering a radar receiver then its output is not zero. Random signals, called noise, appear at the output. All electronic systems are subject to noise but it is only a problem when the noise is comparable to the wanted signal. For example, to receive an acceptable picture on a domestic television then the signal must be about 100 000 more powerful than the noise (50 dB). If the signal is less than this then the picture appears increasingly 'speckly' and 'grainy' as brightness and colour information is randomly altered by the noise. If the signal is so weak as to be only about ten times more powerful than the noise then the picture becomes un-recognisable.

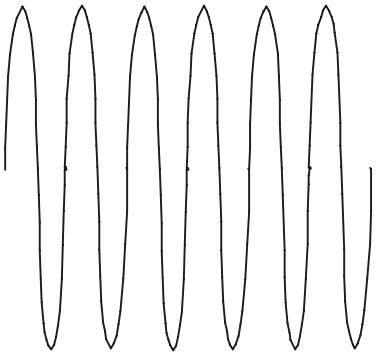

Figure 1: Part of an Ordinary Radar Pulse

If an enemy listens for our radar transmissions and all he receives is noise then he might assume that we are not transmitting or that our signals are too weak to be effective. Thus, if we can make our radar signals resemble noise then they will be more difficult to detect and, consequently, more difficult to jam.

FREQUENCY AGILITY

An ordinary radar transmits a burst of signal (e.g. at 10 GHz) for a few micro-seconds (e.g. 2 ms) and, during that time, the radar transmission remains fixed and constant (see Figure One). Signal analysis reveals that the signal consists of a spread of frequencies centred on 10 GHz of width 0.5 MHz. (The spread of frequencies is equal to the reciprocal of the pulse duration, $1 \div (2\ \mu s) = 500$ kHz.) This signal is quite easy to detect with a simple receiver at a much greater range than that at which the radar can operate provided that the receiver is tuned to 10 GHz with a bandwidth of 500 kHz.

A frequency-agile radar is one that periodically changes its frequency by an amount greater than its bandwidth. With a frequency-agile radar then the transmitted frequency is not know precisely by the enemy so his receiver cannot receive it unless he either widens its bandwidth or scans, in sequence, the range of frequencies that might be used.

The detection of such signals is quite difficult since the the two obvious methods by which it might be accomplished are not very effective:

- **Bandwidth and Noise**: to detect a simple radio or radar signal then it must be observable against the background noise. The amount of noise is directly proportional to the bandwidth of the receiver so if an enemy widens the bandwidth of his radar-detecting system then he will increase the noise but not increase the signal. If we can be frequency agile over an extremely wide band then the enemy will

have to use a very wide bandwidth receiver to cover it. Consequently, he might not be able to recognise that we are transmitting because the noise in his receiver will mask out the signal.

- **Time and Noise**: An alternative to widening the receiver's bandwidth might be to for an enemy's receiver to use a narrow-bandwidth scanner to search for a frequency-agile signal by hopping from one frequency to another, hoping to catch a signal from the radar. This does not work because such a receiver cannot dwell in any particular bandwidth for a long time, in case it misses the signal in another part of the spectrum. The relative amount of noise increases as the time spent listening decreases because the bandwidth depends on the inverse of the time.

Frequency-agile, radar signals do not resemble noise but they force an enemy to use a noisy receiver so that the noise masks the signal. More advanced receivers can perform statistical analyses on received signals and identify those that are not random - they might be our radar transmissions. However, this takes time and computing power to achieve.

Our own receiver can, of course, receive its transmitter's frequency agile signals because it knows the exact frequency that was transmitted. This means that it can use a narrow bandwidth receiver set to that frequency to receive any echoes from targets. The receiver's frequency is changed in step with that of the transmitter. This frequency information (and how the system decides what frequencies to use when operational) must be kept secret from the enemy, for obvious reasons.

CHIRPED SIGNALS

Another way to make it harder for an enemy to detect a signal is to use a pulse whose frequency changes rapidly. As described above, a conventional radar might transmit a pulse of frequency 10 GHz for 2 μs and, during that 2 μs, the frequency remains at 2 GHz. A chirped pulse might start at 10 GHz and decrease to 9.98 GHz during that 2 μs. The bandwidth of the transmission becomes 20 MHz (subtract the final frequency from the starting frequency) compared to its original 0.5 MHz. The waveform of a chirped signal might resemble that in Figure Two (the amount of frequency change has been very much exaggerated in the Figure).

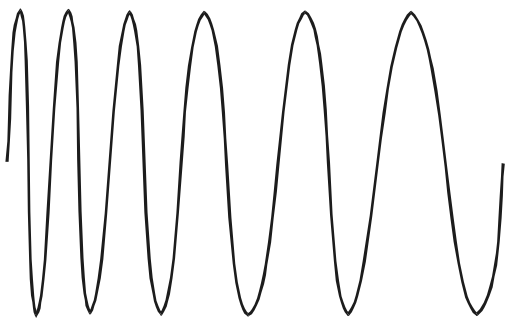

Figure 2: A 'Chirped' Pulse

As before, the chirped signal does not resemble noise but it could be masked by noise. For more information on chirped signals then refer to the BST Handout on Pulse Compression.

SPREAD SPECTRUM

One feature of noise is that it occurs approximately equally at all frequencies within the bandwidth of interest. In other words, the power of the noise is spread-out over the bandwidth in use. If we can give our radar signals this feature then they will more closely resemble noise and, therefore, be more difficult for an enemy to detect.

Spread Spectrum: by altering our radar signal in what is called a 'pseudo-random' way then we can widen its bandwidth to hundreds of MHz whilst giving it random-like features. A pseudo-random signal is a string of binary Ones and Noughts that can be generated by a computer in such a way that the pattern appears almost indistinguishable from a truly random pattern. This signal is then used to change the phase of the transmitted wave as indicated in Figure Three. Each time that a One appears on the pseudo-random sequence then the phase of the signal is changed.

This signal differs greatly from the ordinary sine wave which is usually detected by a radar using its consistency over many cycles. If you imagine pushing a child on a swing using pushes like the waveform of figure One then you might decide that the regular pushes would give an increasing amount of swing. Pushes such as those of Figure Three are just as likely to slow down the swing as to speed it up. (This is by intention, because they are random.)

Most pseudo-random sequences are of limited length (e.g. 1024 bits) and if the sequence is known by the enemy then he can use that to detect the signals. However, if the sequence is unknown then there are so many possible variations that it could not be guessed in a reasonable time (unless some clever mathematician comes up with a new way of cracking such codes).

Detecting our Own Signal: by widening the bandwidth of our radar signal then we make it very difficult for an enemy to detect. Obviously, we need some means to detect it ourselves, otherwise we would never receive any echoes. The solution is to de-code the pulse with the same code that was used in the transmitter. The transmissions are, effectively, encrypted and require the correct key to de-crypt. By using a key that appears ran-

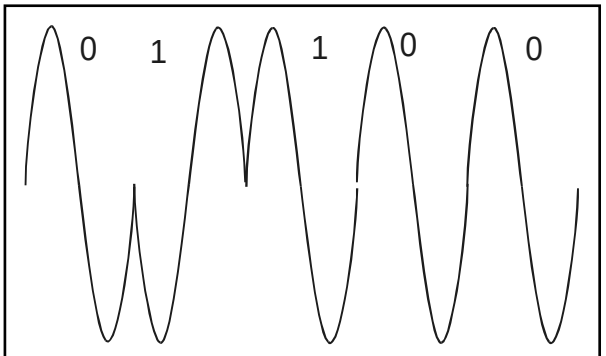

Figure 3: A Pseudo-Random Coded Wave

dom then the radar signals are effectively both hidden and encrypted.

Such signals can, unfortunately, be detected by an enemy - provided that he is prepared to devote significant time and effort and to use a complex receiver in conjunction with a powerful computer. Hopefully, the expense and complexity will militate against this.

BI-STATIC RADAR

One feature of stealthy targets is their sloping plates that are designed to reflect radar signals at a glancing angle. This means that the reflections do not return to the radar. Most conventional radars are mono-static, with the transmitter and receiver in the same location (often using the same antenna). A bi-static radar has the transmitter in a different location from that of its receiver - there might even be a number of receivers.

This defeats the sloping-plate part of the stealthy design because there is a good chance that the target will now reflect some energy towards one of the receivers. For example, a radar transmitter could illuminate a valley along which a stealthy target might approach for an attack. A number of receivers along the rim of the valley would be quite likely to receive echoes from the target as it flew along the valley. These receivers would then transmit their data back to a central point where a fast computer would correlate the data to compute a location for the target. The target could not deduce from the radar transmitter's signals that it was being illuminated by such a radar as the signals could be identical to those of any other radar.

The drawbacks of bi-static radar include the expense of setting up the required number of sites, the cost of the equipment, communications links and computers and the lack of mobility. However, to protect a large city then this could be quite effective and some of the receivers could be un-manned.

NON-COOPERATIVE RADAR

Modern radars operate at frequencies similar to those used for television signals and FM radio. Most areas of the Earth are covered by TV and radio transmitters and these signals will be reflected from any aircraft that fly through them. The reflections will have a Doppler shift because the aircraft is moving. These transmitters often transmit continuously at power level of hundreds of kilo-Watts and can be quite effective at illuminating targets.

A recent article in the 'New Scientist' magazine reported that a system called 'Silent Sentry' has detected targets of 10 m^2 at ranges of 190 km using this technique. Admittedly, the target was flying near a US city where one would expect there to be many suitable transmitters, but the reported figure does indicate the capability of the system. The system requires very sensitive antennae and receivers to be combined with fast computers to decode the signals.

The longer wavelengths used by FM radio and some TV transmitters are not absorbed very well by the type of coatings that are currently applied to stealthy targets. In the event that the wavelength of such a signal is four times the length of the target then an exceptionally strong echo is obtained. Some radio stations might fit this size criterion for some targets.

The big advantage of such a system is that the radar itself emits no EM energy and is, consequently, inherently indetectable by the target. Unfortunately, the only countermeasure that the enemy could use appears to be the destruction of the TV and radio transmitters.

One drawback of the system is that the position data are not sufficiently accurate to identify a target or to direct a missile or gunfire onto the target. However, the system could be used to alarm any AD system that the target approaches so that alternative means of identification (e.g. thermal, audio or visual) could be used locally.

MULTI-BAND RADAR

A target might be stealthy in one band of frequencies but not so stealthy in another. Consequently, a radar that can operate in several bands (or a system that can combine data from several different radars) could be used to extract useful target data from what might otherwise be interpreted as 'passing shadows'.

SURVEILLANCE FROM SPACE

Many stealthy targets are designed to reflect radar energy upwards, away from a ground-based radar system. A satellite could easily receive this energy and detect the target. The obvious problem is how to return the data to the radar system so that it can be correlated against the transmitted signal to extract range information (etc.) Alternatively, the entire radar system could be mounted on a satellite, but there would be only limited transmitter power available and difficulties in positioning the satellite over the area of interest.

Teaching Objectives		Comments
H07.1 Describe the problems with current radar systems		
H.07.01.01	Describe how the enemy can detect our radar transmissions.	
H.07.01.02	Describe how the enemy can design stealthy targets that give poor radar returns.	
H.07.02 Describe the concepts of noise and signal		
H.07.02.01	State that signal is a term used to describe wanted information that might not be present.	
H.07.02.02	State that noise is random and always present.	
H.07.02.03	State that the noise power is proportional to bandwidth	
H.07.03 Describe the features of frequency agility		
H.07.03.01	Describe the features of frequency agility.	
H.07.03.02	Describe how the use of freq agility makes the radar difficult to intercept.	
H.07.03.03	State that frequency agile signals can be distinguished from noise because they are not random enough.	
H.07.04 Describe the features of spread spectrum		
H.07.04.01	Describe the features of spread spectrum transmissions	
H.07.04.02	Describe how the use of spread spectrum makes the radar difficult to intercept.	
H.07.04.03	State that spread spectrum signals are difficult to distinguish from noise because they are pseudo-random.	
H.07.05 Describe the features of a bi-static radar		
H.07.05.01	Describe the multi-site nature of a bi-static radar	
H.07.05.02	Describe how a bi-static radar can be used to detect stealthy targets.	
H.07.05.03	State that bi-static radar systems require complex computer processing to achieve optimum results.	
H.07.06 Describe the features of non co-operative radar		
H.07.06.01	State that non co-operative radars exploit signals from existing transmitters, usually TV and radio.	
H.07.06.02	State that the signals require extensive computer analysis.	
H.07.06.03	State that the effect of the target on the signals is very small but can be identified using Doppler.	
H.07.07 Describe the features of other advanced radars		
H.07.07.01	Describe the concept of data fusion from other radar frequencies and/or systems.	
H.07.07.02	Describe the use of satellites in AD radar systems.	