Q-MAC Electronics Pty Ltd

HF HELP FILES

HF Scrambling vs. Frequency Hopping

HEAD OFFICE 142 Hasler Road, Osborne Park WA 6017. Australia
Telephone: +618 9242 2900, Facsimile: +618 9242 3900
Email: info@qmac.com
Web: www.qmac.com

1 Introduction

This document applies to users in;

- Department of Defence
- Army
- Navy
- Air Force
- Police & Armed Police
- Intelligence Services
- Border Guard

Use of speech security, and GPS over HF radio and Frequency Hopping in areas of Government security

1.1 Background

Due to changing security situations in many countries it may be necessary to set up tactical secure communications links over long distances between provinces/states, which span the entire country. These links should be readily relocatable and not subject to interception by either local insurgents or foreign agencies. In order to cover the distances required (well over 1000km in some cases) HF communication is required.

1.2 Communications environment

There are often thousands of HF radio sets in the hands of private individuals. These are mainly amateur or “ham” sets made by Icom, Kenwood or Yaesu in Japan. They are used by companies and private citizens for informal communication. Anyone monitoring the HF bands in Australia can hear this traffic at all times of day from all over the world. Some of these radios are probably unlicensed.

On the internet it is very easy to discover a very simple modification to the above sets to make them work on the military sectors of the HF band as well as the “ham” sectors. The modification is simply the removal of two diodes.

See www.g3ycc.karoo.net/706_7.htm

This means that insurgents in any country have a ready means to monitor military communications.

Also because of the propagation conditions of HF, signals can be heard from one part of the country to another, these same signals will propagate to other countries where they might be intercepted by foreign surveillance and intelligence organisation.

Propagation information can be found at www.ips.gov.au

HEAD OFFICE 142 Hasler Road, Osborne Park WA 6017. Australia
Telephone: +618 9242 2900, Facsimile: +618 9242 3900
Email: info@qmac.com
Web: www.qmac.com

1.3 Options

For speech security some HF suppliers (eg Barrett Communications) are offering speech scramblers based on the FX224 scrambler chip. When used on HF this arrangement is fundamentally insecure.

In order to de-scramble the voice traffic it is only necessary for the insurgent or intercept operator to tune the listening radio up in frequency by a prescribed amount and switch from Upper Sideband to Lower Sideband.

For Example

If the sending radio is on 6000kHz USB in scramble mode it is only necessary to set the interceptor to switch to LSB and tune from 6001.5kHz up to 6003.1kHz and stop at the frequency where the speech becomes clear.

This makes this type of signal security inappropriate to users in Army, Navy, Air Force, Special Forces, Police & Armed Police, Intelligence Services and Border Guard.

1.4 Danger

Insurgents are further able to record and replay Police and Army traffic and replay it in circumstances, which could cause incorrect responses. They can also jam these communications because all they have to do is identify the fixed frequency and transmit a stronger signal using a large hidden wire antenna. This happens regularly in countries where insurgency is a problem.

1.5 Solution

The only solution to the above serious threats is frequency hopping. By operating networks where all net members hop or change frequency in perfect synchronism many times a second, the risk of interception and jamming is totally eliminated. The hop code is entered by the operator and only radios using the same frequency and code can be heard by each other. Outsiders are totally excluded.

In the event of capture of a set by an enemy, there is an erase function which can be activated, or if this is not done, a new set of codes can be utilised.

For more details on hopping see Frequency Hopping – FAQs

Such radio systems are available from Q-MAC Electronics Pty Ltd (Australia) Thales (France) and Harris (USA).

HEAD OFFICE 142 Hasler Road, Osborne Park WA 6017. Australia
Telephone: +618 9242 2900, Facsimile: +618 9242 3900
Email: info@qmac.com
Web: www.qmac.com

2 GPS over HF and Security

Some HF manufacturers (eg Barrett Communications and Codan) offer a GPS location system with their radio. Some of the GPS location systems use a signalling system, which is an extension of the CCIR 493 selective calling system. This signalling format is in the public domain and so it is easy to decode the GPS traffic and determine the location and identity of the stations communicating. This is highly undesirable from a national security point of view.

2.1 Choice

When procuring a communications network to carry sensitive tactical communications via HF links it is critically important to make the correct choice. There are a number of vendors who make suitable equipment but it is important to be aware of limitations prior to procurement.

If position information is sensitive in nature (eg tactical, high value vessels, sensitive cargo) then systems that offer data over frequency hopping and data encryption should be considered.

If position information is not sensitive then unsecured systems may be adequate and cost effective.

HEAD OFFICE 142 Hasler Road, Osborne Park WA 6017. Australia
Telephone: +618 9242 2900, Facsimile: +618 9242 3900
Email: info@qmac.com
Web: www.qmac.com

3 Other Information

3.1 Author

Mr Rod Macduff BSc, BA, MIEEE, MIEE, FIEAust

Rod Macduff is Managing Director of Q-MAC Electronics which is a specialist supplier of HF Communications to the Humanitarian, Aid & Relief and Military organisations. Rod Macduff worked with Racal BCC for 10 years on the Jaguar V tactical hopping radio and travelled extensively consulting with armies on their secure communication issues. The Q-MAC HF-90 hopping radio is in service in 75 nations and has been adopted by Humanitarian, Aid & Relief, Army, Police and Intelligence organisations.

3.2 About Q-MAC Electronics

Q-MAC Electronics is specialist designer and manufacturer of HF Transceivers. The flagship product the HF-90 is the world's smallest high performance HF SSB Transceiver. The HF-90 and Q-MAC Electronics have been awarded many accolades and is currently used by thousands of users in over 80 countries worldwide. The HF-90 is one of the most versatile HF transceivers available and is suited to military, paramilitary and humanitarian aid and relief applications.

Q-MAC offers the HF-90 in a variety of configurations suited to manpack, vehicle and base station applications. A full complement of accessories is also offered for use with the HF-90; including antennas, field battery charging accessories, carry packs/cases and more. All Q-MAC products are backed by the company's strong commitment to after sales service, support and certified ISO9001 quality standards.

3.3 Contact Details

For Further Information Contact;

Q-MAC Electronics Pty Ltd

142 Hasler Road

Osborne Park, WA

Australia 6017

Phone + 618 9242 2900

Fax + 618 9242 3900

Email: info@qmac.com

Web: www.qmac.com