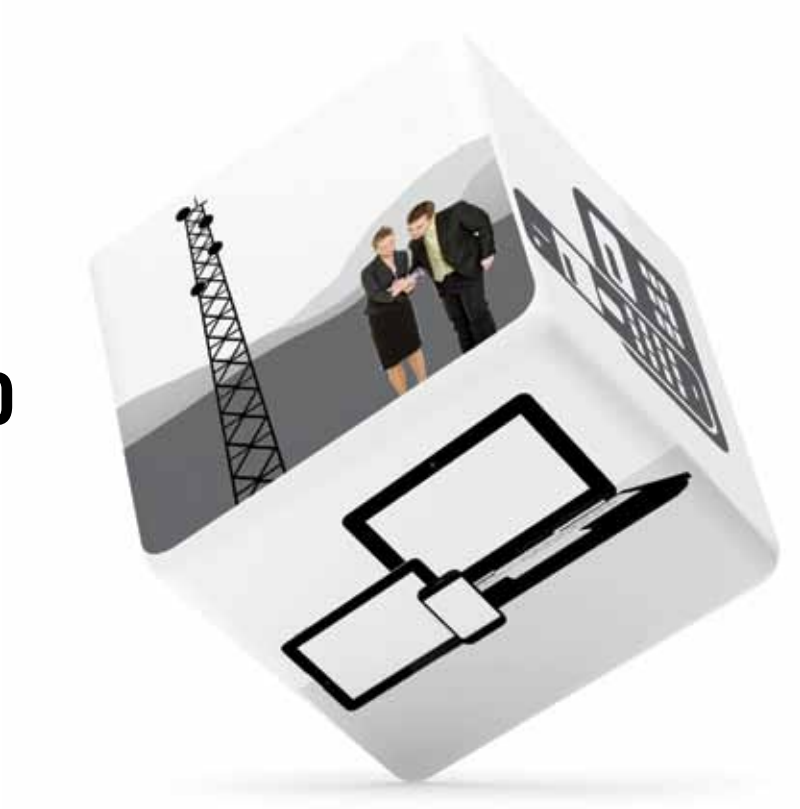
The Institution of Engineering and Technology



Jamming & radio interference: understanding the impact

Introduction

Many of the advances in modern consumer devices are enabled by the increasing use of radio signals in our daily lives - examples are listed in Figure 1. The smooth operation of these radio-based services is often taken for granted. However these services can easily be disrupted by signal jamming, whether intentionally through the operation of a signal jammer or inadvertently due to unforeseen interference from other transmissions.

Deliberate jamming, which for radio signals is the equivalent of an Internet denial of service attack, has traditionally been a military capability typically involving the deployment of specialist personnel and systems to conduct electronic warfare in support of military operations. As will be explained in this Sector Insight the cost and size of jamming equipment has fallen, and the technology can be openly purchased online by the public. For those with modest technical skills, there are a number of websites which describe in detail how to build jammers and provide detailed designs. Deliberate jamming is no longer the specialist preserve of the military and is now available to anyone who chooses to buy or build a signal jammer.

Figure 1: Examples of radio-based services

- satellite navigation/GPS tracking
- mobile telephony & mobile broadband
- WiFi & Bluetooth connections
- remote control, e.g. vehicle locks
- domestic automation and security systems
- wireless CCTV

> "The availability of reliable radio-based services is critical for many systems."

Information & Communications

www.**theiet**.org/info-comms

Inadvertent jamming (interference)

Inadvertent jamming which manifests itself as signal interference is a well-known problem. It may arise from electromagnetic compatibility issues, where legitimate electrical or electronic equipment causes excessive electromagnetic interference. Within the European Union the Electromagnetic Compatibility (EMC) Directive [EC89/336 as amended] requires manufacturers and importers to satisfy specific requirements to ensure that equipment supplied does not cause excessive interference. Inadvertent jamming may also occur where a radio signal transmitted by one user disrupts the use of the radio spectrum by another user.

Regulation of radio transmissions

To reduce the risk of this type of interference, authorised radio transmissions are controlled in accordance with international agreements regarding spectrum allocation and use. These internationally binding legal agreements are coordinated by members of the International Telecommunications Union (ITU). National licensing authorities manage spectrum allocations and use for most radio transmissions. There are some licensing exemptions for Short Range Devices (SRD), devices that offer a low risk of interference with other radio services, usually because their transmitted power (and hence their range) is low, examples include car remote locking transmitters, cordless phones, alarm and CCTV systems and Radio-Frequency Identification (RFID).

Legality of radio transmitter equipment

Equipment which is designed to transit radio signals must comply with a number of national and international standards. In the European Union, such equipment is required to comply with the Radio and Telecommunications Terminal Equipment (R&TTE) Directive [1995/5/EC as amended] and the Electromagnetic Compatibility (EMC) Directive [EC89/336 as amended]. In the UK, these were given legislative effect by SI 2000/730 and SI 2006/3418 respectively. For any equipment which does not fall within the Short Range Devices exemptions, before the transmitter may be used, an appropriate licence is required from the relevant national licensing authority.

Spectrum management in the UK

In the UK, spectrum management and licensing is managed by the Office of Communications (Ofcom), which has a statutory duty to ensure the optimal use of the electromagnetic spectrum. The Communications Act 2003 transferred regulatory powers, functions and responsibilities to Ofcom on spectrum and other matters. It also provides the overall statutory framework within which Ofcom operates. The Wireless Telegraphy Act 2006, which came into effect from 8 February 2007, is the principal legislation on the regulation of radio spectrum in the UK and the powers available to Ofcom, consolidating several earlier pieces of legislation. Signal jamming can be addressed by Ofcom using the

www.**theiet**.org/info-comms

power it holds under Section 8 of the 2006 Act, which forbids the installation or use of wireless telegraphy (radio) equipment in the UK, mainland Northern Ireland and territorial waters, the Isle of Man and the Channel Islands, unless an appropriate licence has been obtained from Ofcom, or there are regulations in force exempting it from the licensing requirements.

Licences are usually granted subject to terms, provisions and limitations, which must be complied with. Whilst licensing requirements will vary depending on the nature of the transmissions and the power transmitted, areas typically covered are listed in Figure 2.

Figure 2: Typical license provision

1. use only on a certain frequency;
2. use only with a certain power and certain level of emission;
3. use must not cause undue interference;
4. use only within a certain geographical area;
5. use only of apparatus which meets specified requirements; and
6. access for inspection by Ofcom staff and close down in the event of interference being caused.

Ofcom seeks to minimise inadvertent jamming by managing the use of the radio spectrum and for certain classes of use, and by licensing specific frequency use. As signal jammers are intended to cause interference, their use in the UK contravenes the spectrum licensing requirements of Section 8 of the 2006 Act, and their sale contravenes the European Union EMC Directive.

Who is affected by jammers?

The effects of jamming are potentially becoming more serious given society's increasing reliance on radio signals. The deliberate use of signal jamming equipment can seriously affect the performance of a wide variety of systems, including: satellite navigation, mobile telephony, alarm and CCTV systems. Unintentional jamming can also be a problem, particularly from the activities of illegal broadcasters who typically set out to make it difficult for the authorities to locate and seize their transmitters.

Satellite navigation

In March 2011, the Royal Academy of Engineering issued a report entitled "Global Navigation Space Systems: reliance and vulnerabilities" which looked at the ubiquitous use of satellite navigation and the vulnerabilities of GNSS services to accidental or deliberate interference. Of the forms of interference examined, the jamming of the GNSS signal is the easiest to achieve and GNSS signal jammers are readily available on the Internet.

www.**theiet**.org/info-comms

Mobile telephony

Equipment to jam mobile telephone signals is also on the Internet. Applications suggested for this equipment include jamming access to the mobile telephone networks in prisons, libraries, examination halls, theatres and offices. The equipment varies in capability and style from small hand-held devices which could be used to interfere with signals over a small area (up to ten metres), though devices that can be installed in internal spaces to interfere within an office, hall or auditorium (a range of tens of metres) to weatherproofed high-power units which can interfere with signals over a significant area (ranges of up to 750 metres are advertised).

Alarm and CCTV systems

Alarm and CCTV systems used to protect domestic and commercial premises are increasingly using wireless technologies to connect sensors to control panels and cameras to monitoring equipment. For property owners, this has the advantage of removing the need for the installation of alarm and CCTV wiring, but it exposes the alarm controls to radio frequency interference.

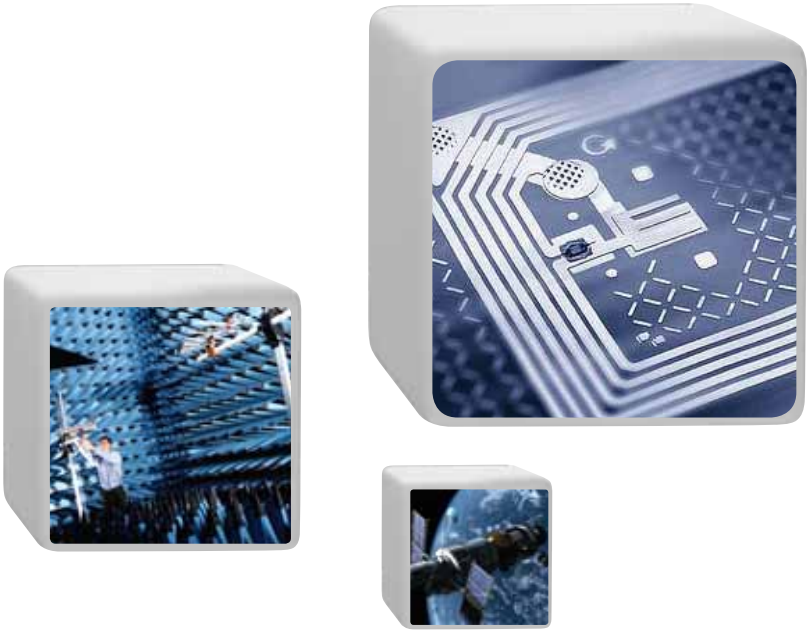
The use of WiFi to carry CCTV signals is a serious vulnerability given the availability of both hardware and software based jammers that can disrupt WiFi signals. Whilst systems may incorporate jamming detection, these features may not have been enabled or may result in frequent false alarms. Where an alarm system uses a GSM auto-dialler to issue alarm alerts, the operation of the auto-dialler could be jammed using a mobile telephone jammer.

Remote locking systems

In 1996, the AA and RAC estimated that more than 8,800 breakdowns were attended as a result of remote key fobs being blocked by radio interference. This led to the Radio Communications Agency (now part of Ofcom) setting up the RAKE Committee to examine the problem. Following the adoption of a new European Union wider frequency for remote car locking systems this problem has become less severe, but there are still instances where interference may prevent the proper operation of remote key fobs. In 2010, it was reported that Surrey police were exploring the theory that a gang of car thieves are jamming central locking systems to make it easier to steal goods from cars. As these key fobs work within the amateur radio band, it is possible that any jamming was unintentional rather than the work of a criminal gang.

Illegal broadcasting

A report entitled 'Illegal Broadcasting: Understanding the issues' released by Ofcom in April 2007 suggested that at that time, there were approximately 150 illegal radio stations operating in the UK, with approximately half of these operating within the M25 area. Illegal broadcasting can cause interference to safety-of-life networks, e.g. those used by air traffic control and the emergency services. It can also interfere with the signals of licensed broadcasters, frustrating their listeners and potentially causes loss of revenue for commercial broadcasters. Ofcom have a dedicated field force who are responsible for investigating illegal broadcasting.



www.**theiet**.org/info-comms

Availability of jammers

Searches for radio jammers on the Internet show that they are widely available either directly from suppliers or through online markets. Some sites indicate that the purchase or use of the product may be illegal, but many do not. It is not uncommon on the Internet to find suppliers offering a range of signal jammers, including 3G/GSM, GPS jammers, GSM/GPS, UHF/VHF, WIFI/ Bluetooth, remote control, Lojack/XM/4G and general purpose military jammers. In addition to these hardware based jammers, there are scripts available to allow computer users to jam WiFi signals without the need for purchasing additional specialist hardware.

Threat from jammers

Signal jamming poses a number of threats to society regardless of whether it is deliberate or unintentional. In either case, the result is effectively a denial of service which may have an impact which is economic (e.g. loss of revenue by broadcasters), security-related (e.g. failure of alarm systems and remote locking) or simply a nuisance factor (e.g. localised suppression of wireless devices). As outlined earlier, there are legislative mechanisms to allow both types of jamming or interference to be addresses, but the regulatory and enforcement authorities must be willing to take the necessary steps to enforce the legislation.

The issue of unintentional interference created by powerline technology employed to deliver computer networking over domestic power cables is an example of how a failure to enforce the regulations increases the threat posed by specific classes of equipment. Evidence suggests that powerline devices typically fail to meet the European Union's EMC requirements. Despite complaints to Ofcom and concerns raised by a number of stakeholders, the regulator appears unwilling to take action to prevent the sale of powerline equipment which fails to meet the legal requirements of the EMC Directive. If regulatory authorities are unwilling to use the legal framework, the threats posed by deliberate and unintentional jamming will become more serious as we increasingly rely on wireless technologies to support our day-to-day activities.

Over-reaction or spectrum sharing

It may be suggested that adopting a robust approach to managing unintentional interference, unlicensed spectrum use and the operation of signal jamming equipment is unnecessary. The radio spectrum is a finite resource which needs to be carefully managed if we are to enjoy the advances in technology and manage the economic and security risks. Radio signals do not respect geographic boundaries, be they domestic, commercial or national, it is therefore important that complaints about interference and jamming are properly managed by the regulatory authorities so that we can make efficient use of the radio spectrum and users may enjoy the benefits of the various spectrum allocations.

www.**theiet**.org/info-comms

Recommendations

The threat that jamming poses could be addressed in a number of ways:

(a) by enforcing the current regulations prohibiting the sale and use of electronic items which cause interference;
(b) by introducing stricter regulation and significant penalties for deliberate jamming;
(c) by introducing standards requiring new equipment to be made less susceptible to jamming and interference.

A case could also be made for the provision of more resources to investigate interference and jamming. There is also a need to equip and train the law enforcement authorities to investigate possible cases of deliberate jamming, e.g. during crime or public order incidents.

Simon Yarwood, Head of Information & Communications Sector says,

"This Sector Insight demonstrates why it is important that we understand how to identify and mitigate sources of RF interference and jamming."

Get involved by contributing your views on the Information and Communications Sector community at

www.**theiet**.org/infocomms