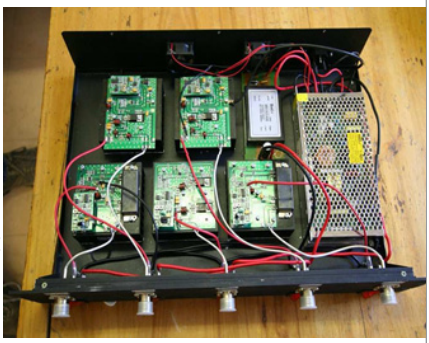
FREQUENCY JAMMING IN THE INTRUDER ALARM INDUSTRY

What is Jamming?

Radio jamming is the (usually deliberate) transmission of radio signals that disrupt communications by decreasing the signal-to-noise ratio. Unintentional jamming occurs when an operator transmits on a used frequency without checking, equipment generating radio noise, etc.

The History of jamming



Radio Frequency jamming is nothing new and was first used in the 2nd world war. In occupied Europe attempts were made to jam broadcasts to the continent from the BBC and other allied stations.
The use of jamming for military radios is still used worldwide.
It is a common form of censorship in totalitarian countries, in order to prevent foreign radio stations in border areas from reaching the country.
It is often used in company boardrooms, banks, cinemas and theatres to prevent the public or criminals from using their cellular phones to receive or send data or make calls.
A transmitter, tuned to the same frequency as the opponents' receiving equipment and with the same type of modulation and with enough power, can override any signal at the receiver.

The threat.....

Jamming has now become a very real threat in the Intruder alarm industry worldwide as more and more frequency jammers are being produced and used in criminal activity.
Some countries are reporting up to 30 successful jamming attempts per day in shopping mall parking areas on vehicle locking systems and the jamming of wireless alarm systems and GSM Communicators is on the increase.

- The public are often faced with no claims from their insurance companies after a non-forced entry theft from motor vehicles.
- An alarm system can be fully functional during and after a break-in, yet

no signals were received by the Central Station.
- Wireless video systems can malfunction due to Wi-Fi links being blocked during criminal activity due to Wi-Fi jammers being used.

From simple devices such as wireless remote arming keyfobs to sophisticated RF and GSM jamming devices, these products pose a definate threat to any wireless device.

Some of these include:

Wireless Alarm Systems;
GSM Alarm Communcators;
Vehicle Locking Systems;
Cellular phones;
RF Radios Transmitters;
GPS Positioning Systems.
Wireless Video systems.

Commonly Jammed Frequencies

The most commonly jammed frequencies worldwide are the short range open, unlicenced frequencies and particularly in the 400mHz - 433mHz band which is used in many countries.
This frequency, which is considered the most congested and overcrowded frequency in the world, is used in wireless intruder alarm systems, Remote arming keyfobs, Wireless Panic switches, Gate and Garage door automation, Remote controlled cars and Baby monitors.
As this frequency is generally open and unlicenced, it can be used by anyone for anything.

Simple Vehicle Jamming

The simplest and most effective use of jamming is in vehicle locking systems and Wireless intruder alarm systems.
No sophisticated or expensive equipment is required and criminals are using the very same devices we are using in our alarm systems or vehicle locking systems.
By keeping the button continually depressed on a handheld wireless remote or keyfob using the same frequency as the system, it can successfully override the frequency while a vehicle is in the process of being locked. As two of the same frequencies cannot be transmitted at the same time, the person attempting lock their vehicle is under the impression that the vehicle

has been locked, but it hasn't.
It has therefore become important to physically check that our doors are locked. Once the occupant leaves the area, the criminal moves in and opens the vehicle.
Unless a criminal is caught with an (illegal) jamming device or (legal) hand-held transmitter, there is no proof on the part of the occupant that he did in fact lock his vehicle. This type of crime has therefore become an easy risk free target as it is very hard to prove.

Wireless Alarm System Jamming

Wireless Alarm systems have now become vulnerable using the same method as with simple jamming devices.
The criminal depresses the wireless remote button continuously whilst robbing the premises. As there is already one frequency being transmitted, the detectors are unable to transmit information to the control panel using the same frequency.

How does it work?

The explanations of simple jamming outlined above can only be performed using a handheld remote that utilizes a 100% duty cycle. What this means is that the signal is transmitted continuously without interruption for the period that the button is depressed, blocking any signals from other transmitters.
Many lower end devices use a 100% duty cycle and are therefore vulnerable. In better devices a <1% duty cycle is used which means that it stops transmitting after a very short period and the button would then have to be depressed again. These types have not been found to be successful jamming devices.

Alternative Frequency Bands

One of the recent moves to combat jamming in alarm equipment is the introduction of alternative frequncies and to move away from the 400mHz - 433mHz bands and also the use of propriety frequencies.
In Europe, United Kingdom and Africa most manufacturers are now using the 868.600MHz – 868.700MHz which is the CE standard. This is a protected bandwidth referred to as ISM (Industrial, Security, Medical) worldwide. It is recommended by the CE standard for exclusive use by alarms and is not shared by other services and devices. Alarm equipment in this sub-band may only use a maximum of 10mW power with <1% duty cycle and must follow a 25kHz channel spacing.

Other devices in the 868MHz band are allocated in specific sub-bands ranging from 868.000MHz to 869.700MHz but do not share the sub-band and frequencies allocated for alarm use. This is a very important factor to eliminate direct radio frequency interference caused by other equipment in the exclusively allocated alarm bands.
The 433MHz band was in use much earlier in time that the 868MHz band, therefore it is also in much wider use by all sorts of equipment manufacturers. It is generally accepted world-wide (except in the US where mainly 315MHz is in use), that the 433MHz is overcrowded and there is some very low quality hardware available for some equipment on offer (no specific reference to alarm equipment, but all sorts of other equipment in general that share the band).

The 868MHz band suffers from little congestion, partly due to the complicated band-plan and exclusive sub-bands assigned for specific uses, i.e. alarm systems.
The 433MHz band is in use on a shared basis by any type of equipment in use with no restriction on channel spacing or duty cycle. The 868MHz alarm specific sub-band is exclusively regulated world-wide for alarm equipment with a restricted channel spacing and duty cycle.

RF Jamming Detection

Several alarm panel manufacturers have the ability to detect radio frequency interference. However, it is pointless unless we can do something with the jamming signal.
This detection is typically called "RF Jamming Detection" and a variety of options are generally available, normally including the transmission of an "RF Jamming" signal to a control room if connected by a suitable connection like telephone line monitoring or a transmitter able to send all signals produced via Contact ID or SIA formats.
The "RF Jamming" signal is normally processed as an emergency signal equal to the "Burglary" signal status.
Some alarm panels have the ability for the "RF Jamming" signal to trigger a locally connected bell/siren, if programmed during installation.
Some alarm panels have limited programmable outputs and use them all for direct long-range radio triggers to transmit Burglary, Panic, Duress, etc. signals and therefore does not have spare outputs for the "RF Jamming signal"
On detection of a real interference signal detected, a warning can be sounded or sent to the control room, but it cannot be counteracted in any way.
The question still remains as to what action to take on receipt of a jamming

signal and whether central station operators are sufficiently trained to deal with these signals.
At this point in time we have not been able to identify any systems being jammed on this (868) frequency which is a reflection of the lack of successful jamming attempts during tests done this far and NOT a claim that it can't be jammed. It is only a matter of time before these frequencies are intercepted but,as mentioned before, it would have to operate on a 100% duty cycle to be successful. With the right equipment and power levels, any radio-based system can be jammed. The question is, what type of equipment is generally available (although illegal) to the general public or criminals to carry out such an act.

To jam an 868MHz device, a purpose-built jammer must be used and must have enough radiating power and high enough sweep frequency to effectively saturate the alarm panel receiver and preventing the alarm panel from receiving and decoding any signal from an attached detector. Such jammers are highly illegal but can still be sourced on the internet; therefore it is theoretically possible but unlikely as a general threat.

Spread Spectrum

Spread spectrum differs from a classical narrow-band or broadband system in that the signal energy is spread over a much wider frequency range, reducing the power spectral density of the signal and providing several advantages:

- Low Probability of Interception, meaning that it is harder to detect the RF signal;
- Higher tolerance to narrow-band noise sources i.e. Better penetration (distance);
- Spread-spectrum signals are highly resistant to narrowband interference;
- Spread-spectrum transmissions can share a frequency band with many types of conventional transmissions with minimal interference.
- Spread Spectrum is highly immune to jamming but NOT impossible to jam. However the equipment required must be highly sophisticated.

The use of anti-jamming techniques is not available in the 433MHz band. In the 868MHz band manufacturers have access to two versions of improving data transfer, **Frequency-hopping spread-spectrum (FHSS)** and **Direct-sequence spread-spectrum (DSSS)**. Some alarm equipment

manufacturers already make use of these technologies for wireless equipment in their range of products.

GSM/GPRS Jamming

The jamming of GSM alarm communicators is increasing, with numerous jamming devices flooding the market. These devices are a lot more sophisticated and are available in ranges from 50m - 500m and can sweep multiple frequencies.
Newer devices can jam up to 14 bands as illustrated below.
As you can see, these jammers cover most of the frequencies used in the intruder alarm industry.

1.CDMA 800:850 to 894MHz
2.GSM 900:925 to 960MHz
3.DCS/PCS 1805 to 1990MHz
4.3G:2110 to 2170MHz
5.GPSL1:1570 to 1580MHz
6.GPSL2-L5:1170 to 1230MHz
7.WIFI 2.4G:2400 to 2500MHz
8.VHF:135 to 174MHz
9.UHF:400-470MHz
10.4G Wimax:2345 to 2400MHz(American standard) or 2620 to 2690MHz(European standard)
11.4G LTE:725 to 770MHz(American standard) or 790 to 826MHz(European standard)
12.Lojack:167-175MHz
13.315MHz
14.433MHz

The most effective method to combat GSM jamming is the use of Dual Communication to the Central Station using two different technologies.

Solutions and Recommendations

There are many effective ways that we can reduce the possibility of jamming.
Each technology improves resistance to jamming and the more features combined, the higher the immunity:

What to look for in new equipment:

- Frequency hopping communication from detectors to panel
- 2-way communication between the panel and all the peripherals.
- 868MHz is generally better than 433MHz (cleaner band)
- Unique, licensed frequency for detectors and peripherals, (away from the open bands)
- Device networking forming mini-repeaters (mesh networks)
- Only use remotes/keyfobs that utilize a <1% duty cycle.

Installations

- Jamming detection should be turned on in the control panel during installation and activate a local bell/siren.
- The use of Dual monitoring of signals to a Central Station using two different technologies.
- It is recommended that no more than 70% of the spread risk be covered by wireless equipment in alarm systems. 30% should be hard-wired.
- The control panel and receivers/repeaters should be protected by a hard-wired PIR detector.