Crime, GNSS Jamming and Enhanced Loran

Professor David Last

International Loran Association

Portland, Maine

14 October 2009

Since I retired from full-time University life, I have become involved in crime! This has not only been profitable, but I have made new and interesting friends. Curiously, it has also taught me a good deal about the vulnerability of GNSS, and the potential role of eLoran.

I have played a part in developing a new and exciting branch of Forensic Science: the forensics of GPS. There are two principal ways in which this assists law enforcement. Firstly, vehicles satellite navigators (PPT1) – the most numerous of GPS receivers - are packed full of records. They may show where they have been, how they got there, and a great deal more of value to crime investigators.

The destinations stored in car navigators can be extracted and plotted (PPT2). This is now possible with virtually all makes and models, including the ones built into vehicles. The examination must be conducted with great care, maintaining very high forensic standards if the evidence is to stand up in court. And it is essential to preserve evidence, too. So, GPS receivers must be screened from incoming satellite signals whilst they are being examined. This can be really difficult to guarantee, now GPS chips are so remarkably sensitive!

Some car navigators disclose a great deal of information: who owns them; multiple addresses; a *Home Address* plus *Favourites*; those used most *Frequently* or most *Recently*; the language spoken by the user; and whether they travel internationally; even telephone calls made and received. A few car satnavs contain a detailed record, like the one shown in PPT3, containing journeys stretching back over months, each point timed and dated. These can provide compelling evidence of criminal activity.

But really, the most impressive GPS forensic evidence comes from the vehicle tracking systems now fitted to increasing numbers of trucks, trailers, delivery vans and rental cars. You will know the technology shown in PPT4: the vehicle carries a GPS receiver that makes measurements of its location. These are sent at intervals to a Tracking Centre. The communications mostly use the mobile phone data services, GPRS or 3G. At the Tracking Centre the data is stored, processed, and may be displayed on a map. An alarm can be raised if a high-value load deviates from its planned route or if a rental car is about to be exported illegally. Of course, many of these tracking installations are covert, hidden, very difficult to discover.

When the police seize a tracking record, a forensic expert must audit the data in all the ways I have shown in blue in PPT5. These concern the many parts of the system the Tracking Company simply does not control. For example, they do not check the quality and accuracy of GPS at the time and in the place of a crime. They hand over this forensic data to another company, the mobile phone operator. They make processing errors when handling latitude and longitude. Professionals in our business, used to handling high integrity safety-of-life navigation systems, can bring that knowledge and quality to the forensic analysis of tracking records.

It is also necessary to estimate accuracy (PPT6), often in complex situations, such as a GPS receiver with its antenna hidden deep inside a vehicle, maybe behind the dashboard, when the vehicle itself may be surrounded by tall buildings that block and reflect satellite signals. I am asked in court: How accurate is it? This is all a novel and fascinating area of Forensic Science and, as you can see, there is a lot more to it than simply extracting addresses from a TomTom!

And now something our navigation community has long discussed has appeared, and is spreading, in the world of crime. GPS jamming devices, like the one shown in PPT7, are being used by criminals in many countries to overcome tracking systems and so let them steal vehicles and their valuable contents. I examined this device and confirmed that it is a low-power transmitter that can block GPS reception around a vehicle. This kind of jammer is readily available from multiple Internet sources and costs about $150 (PPT8).

Of course, GPS is very easy to jam. As shown in PPT9, the satellites transmit no more power than a car headlight, yet they must illuminate nearly half the earth's surface from 20,000km out in space. The signals that reach a GPS receiver are easily drowned out by even one thousandth of a watt (1mW) of jamming signal radiated close by.

In PPT10 I show the spectrum I measured from the little jammer in PPT7. It is plotted across 100MHz, centred on the GPS L1 frequency. The total power this jammer radiates is only about a tenth of a milliwatt. Yet, that is sufficient to block commercial GPS receivers over a few metres range, which is what the criminals want.

But if criminals are to remove a vehicle completely from the radar, they must also jam mobile phones. These could be used to call for assistance and mobile phones too can be tracked, using cell-site analysis. To prevent that, they employ jammers that block not only GPS but also GSM, DCS and 3G mobile phones. In versions for other regions of the world such as the US, these devices jam the local mobile phone bands.

In PPT11 I show the spectra of a typical such device. The GPS jamming signal is centred on 1575.42MHz. Also shown are 900MHz, 1800MHz and 3G jamming signals. Those mobile phone transmissions are carefully tailored to block the base station frequency bands, so the mobiles cannot hear the base stations and so drop off line.

Recently, much more powerful jammers have appeared. These units radiate about 2W, some 20,000 times higher power than that very low-powered jammer. They are more powerful than the jammer used by Sally Basker's team last year to measure the effects on shipping of jamming GPS over a 30km-long sector of the North Sea. Such jammers have substantial ranges.

Returning to the first simple low-power jammer, I show in PPT12 that at the centre of its jamming spectrum is the 2MHz-wide spectrum of civil GPS. But the jammer also neatly covers the military P/Y signal, the yellow block. An interesting question is: why should the designer want to jam the whole military signal? Why not concentrate the power more effectively into the narrow band of the civil signal?

PPT13 shows that the spectrum also encompasses the Galileo signals, the slightly wider band shown in blue. So this device is a Galileo jammer, ready and waiting for Galileo to appear! From PPT14 we can see that its spectrum is not quite wide enough to cover all the GLONASS band, shown in purple. But other jammers, with a little bit wider bandwidth, do jam GLONASS as well.

It is often stated that Galileo will use more than one frequency band, so simply jamming L1 will not work with Galileo. The same is becoming true of GPS. Well, jammers have now appeared that cover L1, L2 and L5. These are the frequency bands in which the world's present and planned GNSS systems operate.

The jammers I have shown are relatively simple and crude devices. But they are highly effective with civil receivers. They are easily available and are certainly being sold and being used by criminals and others. They render our GNSS-based security systems highly vulnerable to attack.

More seriously still, I believe that it is now technically feasible, though not yet within the capabilities of our criminals, to spoof GPS. That will allow the criminals to hi-jack and divert a vehicle whilst the tracking system shows it still following its planned route, so no alarm will be raised. Vehicles will also be able to avoid purely GNSS-based road-user pricing systems.

Let us not be too depressed here – we do have solutions! In many countries there are vehicle tracking systems, like Datatrak, that do not depend on GNSS. There are also stolen vehicle recovery systems, such as Tracker with its LoJack technology in police cars and helicopters. They are immune to GNSS jamming and spoofing. Of course, like all radio systems, they too are jammable. But they are orders of magnitude less vulnerable than GNSS and their jammers are easier to detect; LoJack will even home in on its own jammers! Then, up-market cars with built-in navigators use dead-reckoning to cope with losses of GPS in tunnels and urban canyons. They are immune to jamming, at least for short periods and distances. But they are not immune to spoofing.

And we know that there is a complete alternative navigation technology: Enhanced Loran (eLoran) as shown in PPT15. Built into a GNSS receiver, it can take over seamlessly when GNSS is jammed. It is accurate. It also replaces the exceptionally-precise GPS timing that currently keeps most of our telecommunications systems and the Internet running, and which, of course, is also vulnerable to jamming.

In previous ILA conferences, the threat of intentional GPS jamming has been recognised. We have talked about government tests and terrorists. But what certainly I never foresaw was that an attack would come from the criminal community. Make no mistake: the threat has turned into reality.

So, the legal and forensic aspects of GNSS are growing ever more important and their role more vital, and successful, in reducing crime. But we really must plan our response to the vulnerability of our current and future GNSS-based security systems, which are now under attack. The role of eLoran in providing an alternate to GNSS in facing what has become a real and present danger is now vital.

1700 211009