GPS Forensics – Crime, Jamming & Spoofing

Professor David Last

Consultant Engineer & Expert Witness

jdl@navaid.demon.co.uk

ABSTRACT. The most widely used of all GPS devices currently are car satellite navigators. When vehicles carrying navigators have been used for criminal purposes, the records they contain may be examined. Such investigations require newly-developed forensic techniques that employ a combination of computer knowledge and navigation expertise. The paper will outline these methods and show examples of the valuable intelligence they can provide for crime investigators.

Of even greater value is the evidence from the GPS-based tracking systems now fitted to many kinds of vehicle. These installations, some of which are covert, provide information on vehicles' movements. The paper will show how tracking records can also be analysed forensically to provide intelligence that is of considerable value in the detection of crime.

While the principal purpose of vehicle tracking systems is generally to provide real-time information that enhances the efficient control of fleets, they also have an important security function. By displaying continuously-updated location information, and identifying vehicles that deviate from planned routes or cross specific boundaries, they play a key role in the protection of assets. These include the vehicles themselves and their high-value contents. Vehicle tracking systems are now among the most important applications of GPS for our society.

The recent appearance of readily availability, low-cost, GPS jamming devices presents a real and immediate threat to all such tracking and security systems. Criminals are now employing jammers that can block both GPS reception and mobile communications. The paper will discuss the implications of this vulnerability of GPS for critical security applications. It will review the degree to which the other global satellite navigation systems (GNSS) now being developed will share that vulnerability.

The paper will also touch on the implications for vehicle security and crime of the development of spoofers for GNSS. It will identify solutions that are not vulnerable to GNSS jamming or spoofing. These alternative technologies promise a degree of protection to vehicle tracking and recovery systems.

KEY WORDS

1. GNSS 2: Forensic science 3: Jamming 4: GPS vulnerability

1. INTRODUCTION. This paper reviews the development of a new and exciting branch of forensic science: the forensics of GPS. It describes the analysis of vehicle satellite navigators, the use of data from GPS tracking systems, and the significance of the appearance among the criminal community of GPS jammers and the prospect of GPS spoofers.

2. ANALYSIS OF VEHICLE SATELLITE NAVIGATORS. Vehicle satellite navigators, still the most numerous of GPS receivers, contain multiple records concerning their users. These 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 (see Figure 1). This is now possible with virtually all makes and models, including the ones built into vehicles. Such examination must be conducted with great care, maintaining very high forensic standards, if the evidence is to survive hostile cross-examination in court. It is essential also to preserve evidence. So, GPS receivers must be screened from incoming satellite signals while they are being examined. This can be remarkably difficult to guarantee, now GPS chips are so very 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 numbers of calls made and received.

A few kinds of car satellite navigator store a record, like the one illustrated in Figure 2, of journeys stretching back over months, each point timed and dated. These can provide compelling evidence of criminal activity. But even where the only information is a simple set of destination addresses (such as in Figure 1a), without dates or times or any certainty that a route was ever planned to them, these locations can be of great significance. In one recent case a bulldozer lay in wait at a point marked and labelled in a TomTom, ready to intercept and smash open a passing cash-in-transit van. In another TomTom a murderer recorded a reminder of where he had buried his victim’s body.

3. TRACKING SYSTEMS. Some of the most powerful GPS forensic evidence comes from the vehicle tracking systems that are now fitted to many trucks, trailers, delivery vans and rental cars. Each vehicle carries a GPS receiver. The location measurements it makes are sent at, typically, one-minute intervals to a Tracking Centre. The communications use the mobile telephone data services, GPRS or 3G. At the Tracking Centre the data is stored, processed, and displayed on a map. An alarm can be raised if a high-value load deviates from its planned route or if a hire car is about to be exported

illegally. Many of these vehicle tracking installations are covert, hidden, and very difficult to discover.

Tracking records may look impressive, but the defence will point out that the forensic trail leading to the records is full of holes. A commercial tracking company will generally not have checked the quality and accuracy of GPS at the time and the place of a crime. They will have handed over this sensitive forensic data to another company, a mobile phone operator, and may well have received it back elsewhere without conducting any quality checks. In addition, tracking companies sometimes make errors when handling latitude, longitude and geodetic datums in calculations.

Navigation professionals, used to high integrity safety-of-life systems, can bring that knowledge and quality level to the forensic analysis of tracking records. They can audit these systems in the ways shown in blue in Figure 3, checking for errors and eliminating them. They can then present the data in court and defend it in cross-examination. And, of course, they may also be able explain to a jury in simple language how GPS works – a challenge to anyone's teaching skills!

It also helps to take a common-sense look at tracking records: in high-quality data like that shown in Figure 4, the fixes from a moving vehicle (the red bulls-eyes) lie close to roads, not in the middle of fields. As here, they may even be biased to the side of the carriageway on which vehicles drive in that country. Stationary vehicles remain in a small area. If these elements are pointed out simply and carefully to a jury, tracking evidence can be compelling.

4. GPS TRACKING ACCURACY. Defences also, quite rightly, question the accuracy of GPS. A recent case turned on the certainty with which it could be shown that a group of accused could not have been some130 metres away from where GPS tracking data put them when they were reconnoitring the scene of a future crime. Engineers tend to quote GPS accuracy in statistical terms, for example stating that "95% of measurements fall within 5 metres of the true position", as if the spread were always Gaussian. But is this approach valid for a covert GPS tracker installed deep inside, or even underneath, a vehicle? And what about a city centre where tall buildings block and reflect satellite signals? There is almost nothing in the GPS literature about GPS accuracy in such places in language that would be acceptable to a court.

Figure 5 shows the results of a recent analysis of tracking data; the conclusions are dramatic in their simplicity. A cheap GPS receiver operating in open country, installed on the roof of a car – a perfect site and a perfect installation – produced fixes of which 95% fell within 2 metres of the true position (left-hand example). There was not a single error of more than about 3 metres in many hours of records. When the receiver was then mounted under a corner of the vehicle, it still recorded continuously. The Gaussian

spread increased so that 95% of readings now fell within some 4 metres; but there were still no gross errors (centre example). Then the receiver was taken to the urban canyons of Canary Wharf in London's Dockland (right-hand example) - and multipath errors of more than 300 metres appeared.

These experiments demonstrate some simple rules about GPS tracking systems. Firstly, the kind of receiver does not matter: even very low-cost civil GPS receivers now perform superbly well. Secondly, how the receiver is installed in the vehicle hardly matters either: if it tracks continuously, those tracks will be good. Thirdly: what does cause gross errors is simply multipath. The key factor is the location of the vehicle. So one of the skills of a GPS forensic expert must be to bring to the analysis of crime scenes an understanding of radio propagation.

5. GPS & MOBILE PHONE JAMMING. A new factor has appeared in GPS Forensics: GPS jamming devices are now in the hands of criminals in the UK. They employ them to defeat tracking systems and so steal vehicles and their valuable contents. Figure 6 shows a jammer: a low-power radio transmitter that can drown out GPS reception over a range of tens of metres. This particular model also jams the mobile telephone bands. It blocks the data channel of any tracking system and it disables mobiles that could be used to call for assistance or themselves be tracked using cell-site analysis. A GPS jammer can also disrupt many communications systems, including the Tetra Airwave system employed by the emergency services. It transmits only a thousandth of the power of a mobile phone. Jammers are readily available from Internet sources and cost just tens of pounds. Their implications for GPS-based security systems are very serious.

GPS is very easy to jam since its satellites transmit no more power than a car headlight, yet must illuminate nearly half the earth's surface from 20,000km out in space. A jammer nearby easily deafens a satellite navigator on a vehicle, straining to hear those tiny signals. GPS jammer technology is advancing rapidly. Jammers some 2000 times more powerful than the one in Figure 6, but still transmitting only a couple of watts, can affect GPS across a city if deployed correctly. Such jammers will defeat GPS-based road-user pricing systems; and jammers ten times more powerful than that are now on the market.

The significance of the three-band GPS jammer advertised as in Figure 7 is that its manufacturer has already provided for the next generation of GPS and for Europe's coming Galileo satellite system. GPS, Galileo, the Chinese, Japanese and Russian satellite navigation systems plus their augmentations all use essentially the same technology and the same frequency bands. So, switching from GPS to one of the others will not protect against jamming.

6. SPOOFING. More serious than jammers are the ‘spoofers’ for civil GPS, which have recently been demonstrated. Spoofing is transmitting fake GPS signals; the receiver locks onto them and the spoofer then controls the receiver. Spoofers will allow 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. There is as yet no evidence that criminals have access to spoofers. But there are already low-cost GPS generators with programmable scenarios, into which tracks can be entered using Google Earth. So, spoofing is not far away.

6. MITIGATING JAMMING & SPOOFING. What are the options for mitigating jamming and spoofing? Ofcom are improving their techniques for detecting jammers and attempting to prohibit their sale and use by force of law. There are vehicle tracking systems such as Datatrak and stolen vehicle recovery systems like Tracker with its LoJack technology in police cars and helicopters; neither of those uses GPS. Of course, all radio systems are jammable - it is a matter of degree. But those two are much harder to jam than GPS, without drawing attention to one’s self. Indeed, Tracker/LoJack can even home in on the jammer! There are asset recovery products in which a cellular system locates the vehicle. And many cars with built-in satellite navigators employ have dead-reckoning, using wheel rotation counters and heading sensors, to cope with the temporary loss of GPS signals in tunnels. These let the driver carry on navigating, navigating out from the last GPS fix, at least for short periods and over limited areas. But they cannot measure positions, so it is essential that GPS should return eventually.

There are also alternative location technologies: at sea a backup system for GPS called ‘Enhanced Loran’ (eLoran) is being developed. ELoran uses completely different technology from GPS. Built into a satellite navigator, it can take over seamlessly when GPS is jammed. As an important bonus, it also replaces the precise GPS timing that keeps telecommunications systems and the Internet running.

7. CONCLUSIONS. The legal and forensic aspects of GPS are growing ever more important and their role more vital and more successful in helping detect crime. I anticipate that GPS evidence will increasingly be presented, challenged and defended in the courts. It will have to become established via test cases, just as radar speed traps and mobile phone tracing did. But even before that, navigation professionals must plan their response to the vulnerability of current GPS-based security systems, which are now under attack.

FIGURES

Location	Latitude	Longitude
Home	51.66855	-3.90383
A56 Chester Road, Manchester	53.46023	-2.29038
Cemetery Road, Sheffield	53.37154	-1.47992
Coed Y Maes, Bangor (Gwynedd)	53.21327	-4.15964
Nun's Road, Chester	53.18913	-2.89714
Unnamed road, Strelley	52.97967	-1.2392
Unnamed road, Shrewsbury	52.74558	-2.73656
Granby Avenue, Kitts Green	52.47246	-1.77225
A38 Bath Road, Broomhall (Worcester)	52.15934	-2.21467
77 Ty Glas Avenue, Cardiff	51.52687	-3.19156
Limekiln Close, Stoke Gifford	51.50885	-2.54866

(a)

(b)

Figure 1: (a) addresses of destinations listed, (b) addresses plotted

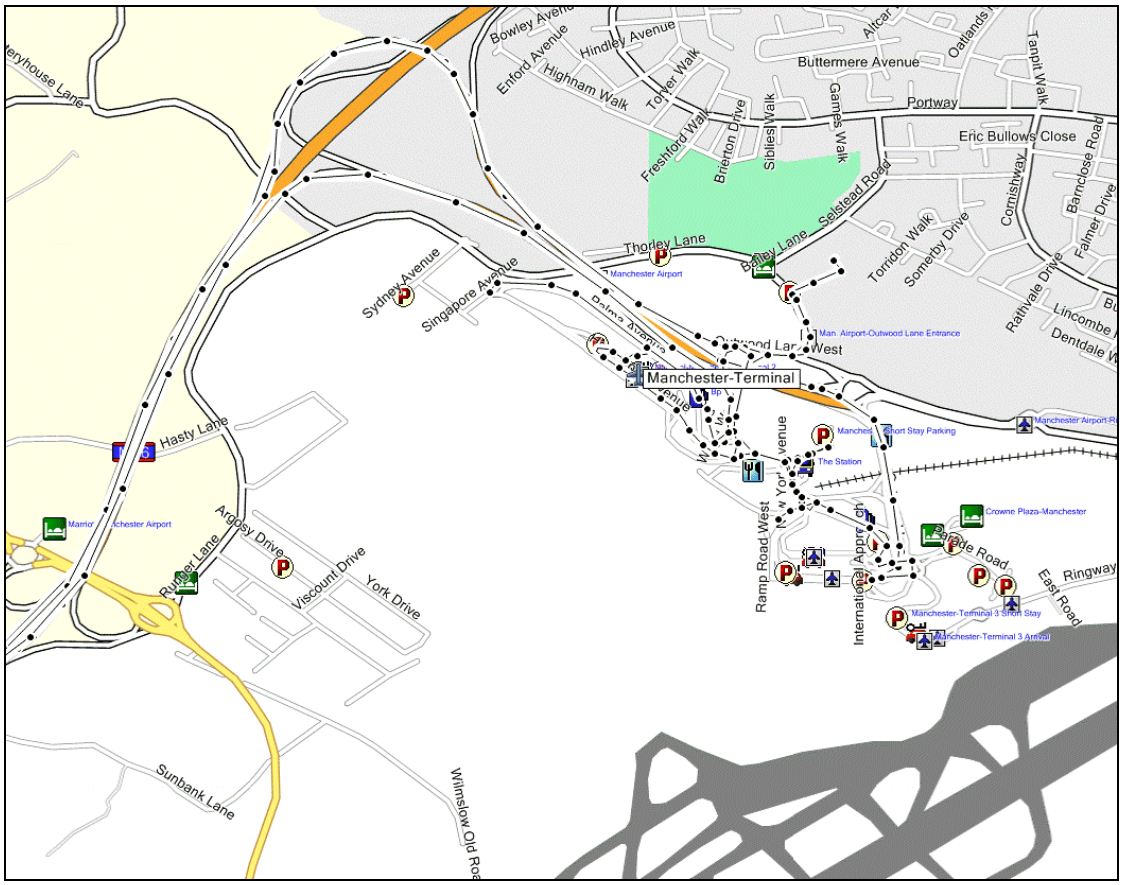

Figure 2: Detailed tracks of routes travelled by a vehicle, each point dated and timed

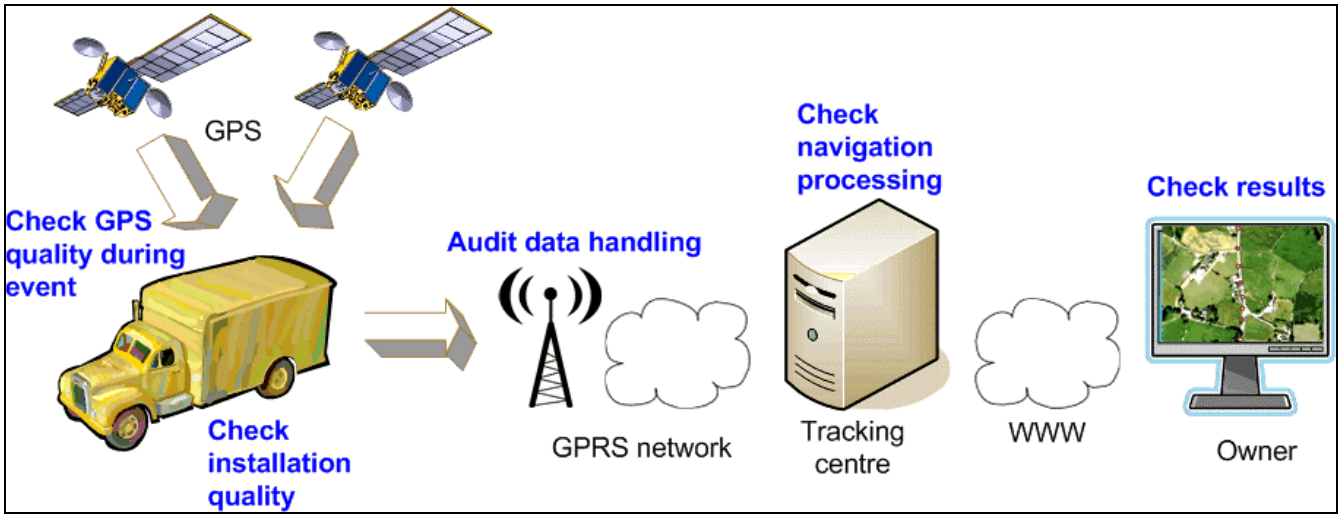

Figure 3: Vehicle tracking system with checks (in blue) to establish quality of evidence

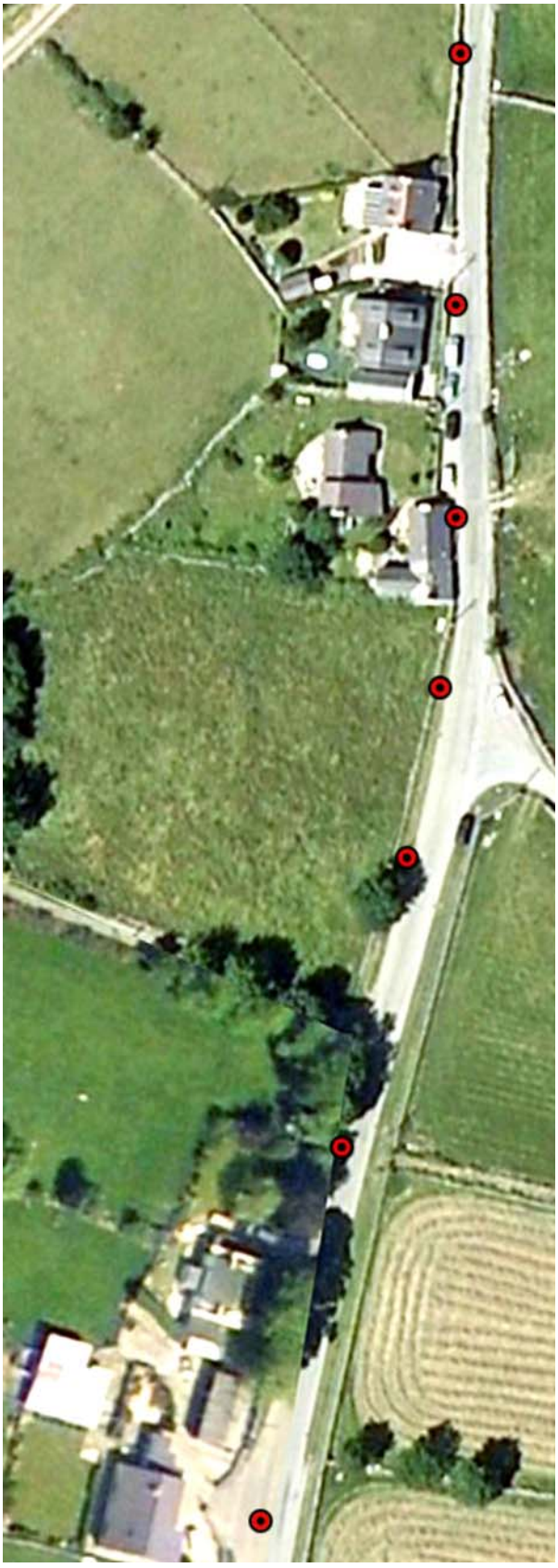

Figure 4: High quality tracking data: vehicle's fixes lie close to roads (Record: www.tdl.ltd.uk)

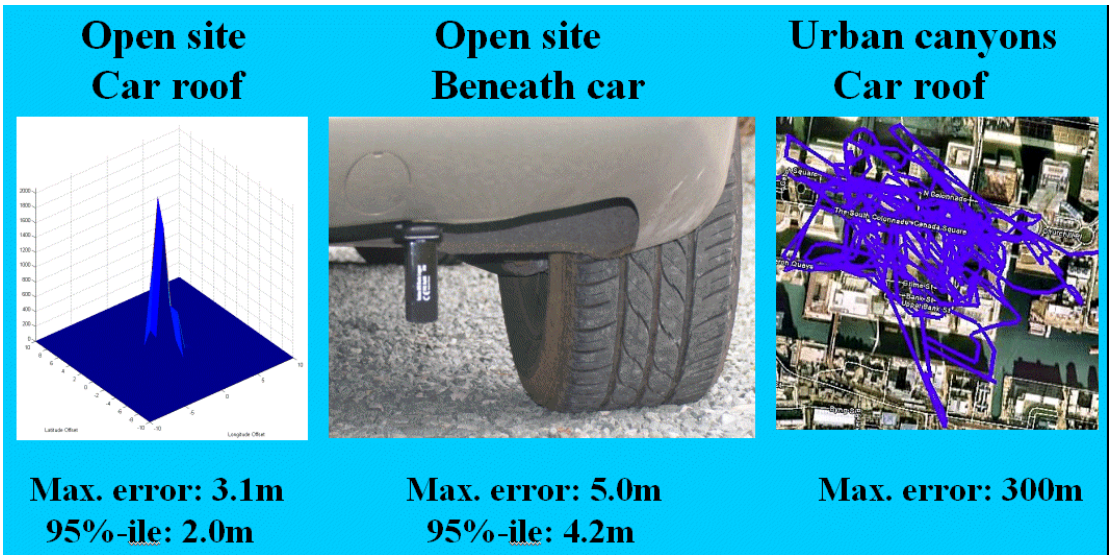

Figure 5: Examples of GPS accuracy

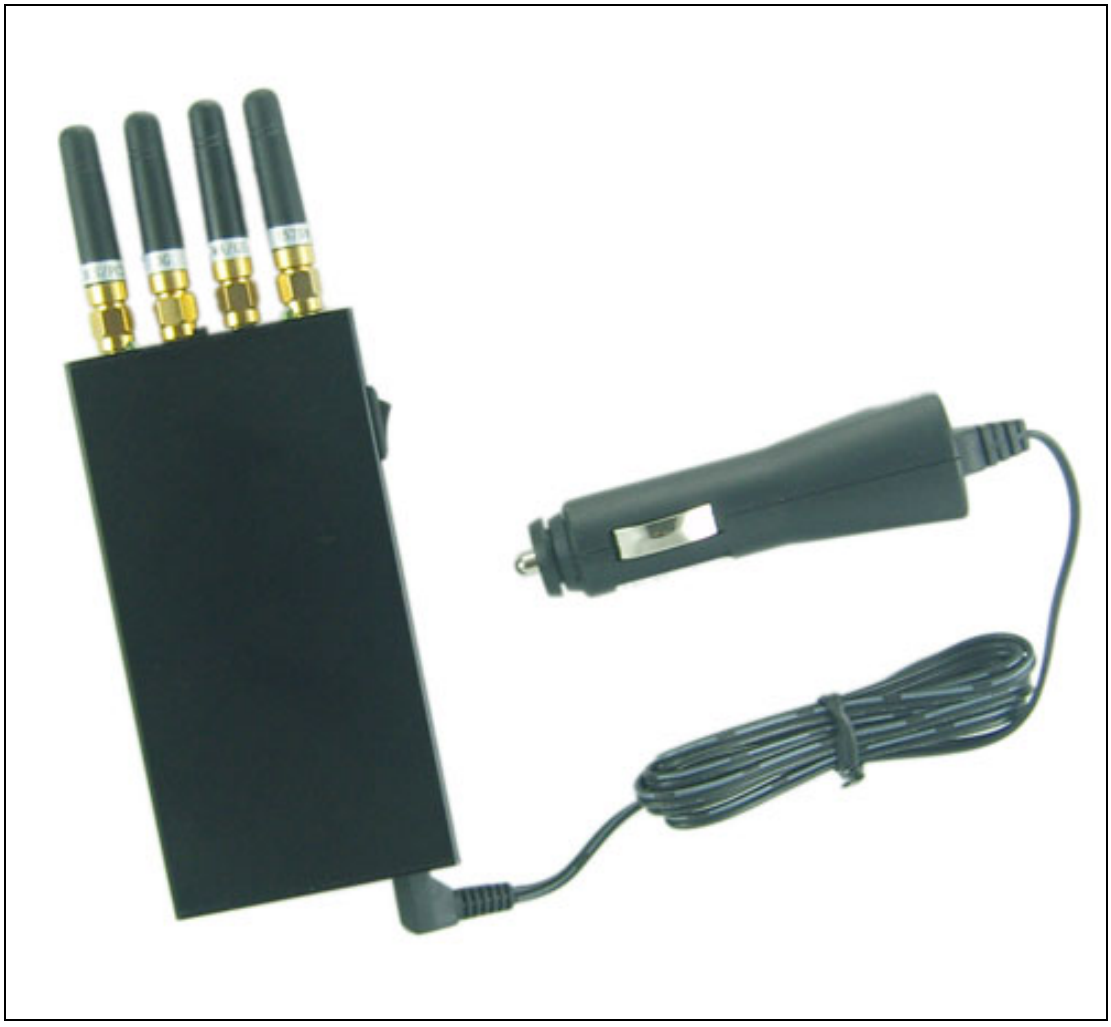

Figure 6: Jammer for GPS plus the mobile telephone bands (Picture: www.tayx.co.uk)

Figure 7: Jammer for the L1, L2 and L5 frequency bands (Picture: www.jammer-store.com)