GPS Forensics, Crime, and Jamming

By David Last

The most widely used of all GPS devices are in-car navigators. When vehicles carrying navigators are used for criminal purposes, records contained in the devices may be examined. Such investigations rely on newly developed forensic techniques that employ a combination of computer expertise and navigation knowledge, yielding valuable data for crime investigators.

Evidence from GPS-based tracking systems now fitted to a wide range of vehicles can be of even greater value. These installations, many of them covert, provide a history of vehicle movements. Forensic analysis of such records can provide evidence of considerable value in the detection of crime.

Criminals use jammers to overcome tracking systems and steal vehicles.

Whilst the principal purpose of vehicle tracking systems is generally to provide real-time information for efficient fleet control, they also serve an important security function. By continuously displaying up-to-date location information and identifying vehicles that deviate from planned routes or cross specific boundaries, they help protect assets that include the vehicles themselves and their high-value contents. Vehicle tracking systems now constitute one of the most important GPS applications for our society.

The recent appearance of readily available, low-cost GPS jamming devices presents a real and immediate threat to all such tracking and security systems. Criminals now employ jammers that can block both GPS reception and GSM in Europe, and U.S. and other mobile phone systems throughout the world, rendering vulnerable the use of GPS in critical security applications. Other global satellite navigation systems (GNSS) in development will likely share that vulnerability. While not yet deployed for criminal purposes, spoofers that mimic GNSS signals will pose an even greater threat to vehicle security than jammers.

Alternative technologies, including enhanced Loran (eLoran), for vehicle navigation and tracking are not vulnerable to these threats, and promise a degree of protection to vehicle tracking and recovery systems. These solutions will likely play an increasing role as GNSS jamming and spoofing activity increases.

Vehicle Navigators

Vehicle navigators often contain large numbers of records created by their users. These may show where they have been, how they got there, and a great deal more of value to investigators.

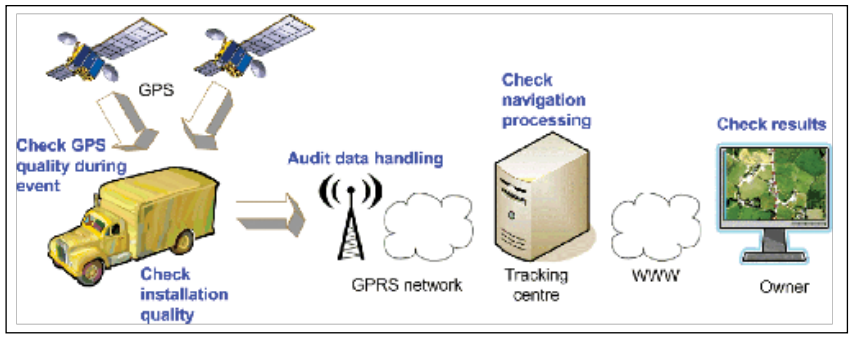
The destinations stored in car navigators can be extracted, listed, and plotted. It is now possible to do this for virtually all makes and models of device, whether after-market installations or built-in by the manufacturer. Such examinations must be conducted with great care, to maintain very high forensic standards so the evidence will stand up in court. It is also essential to preserve that evidence. This requires screening receivers from incoming satellite signals during the examination; this can be very difficult to achieve given the exceptionally high sensitivity of current GPS receivers!

Some car navigators disclose a great deal of information: who owns them; multiple addresses; a home address plus favorite addresses; destinations visited most frequently or most recently; the language spoken by the user, and other preferences; whether the user travels abroad; and occasionally telephone calls made and received. Some units even contain a detailed record of journeys stretching back over months, each point timed and dated (see **FIGURE 1**). These can provide compelling evidence of criminal activity.

Tracking systems

Probably the most impressive forensic evidence involving GPS comes from the tracking systems now fitted to increasing numbers of trucks, trailers, delivery vans, and rental cars. Each vehicle carries a receiver that records its location and sends it at intervals to a tracking

▲ **FIGURE 1** Detailed tracks of routes travelled by a vehicle, each point dated and timed



▲ **FIGURE 2** Vehicle tracking system with checks (in blue) to establish quality of evidence

center via mobile phone data services. The tracking center may store, process, and display the data on a map, and raise an alarm if a high-value cargo deviates from its planned route or if a rental car is about to be exported illegally. Many of these tracking installations are covert and very difficult to discover.

When the police seize a tracking record, a forensic expert must audit the data in various ways, shown in blue in **FIGURE 2**. These focus on the many parts of the system the tracking company does not control. Tracking companies generally do not check the quality and accuracy of GPS at the time, and in the place, of a crime. A navigation professional, accustomed to dealing with high-integrity safety-of-life systems, can bring valuable experience to examining tracking records.

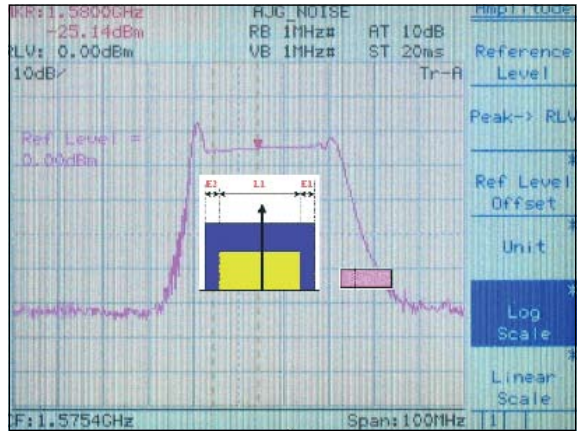
It is also often necessary to estimate the accuracy of GPS fixes. Doing so may require analysis of complex situations. An example would be the GPS receiver in a covert tracking system, with its antenna hidden deep inside the vehicle, perhaps behind the dashboard. The vehicle itself might be surrounded by tall buildings that block and reflect satellite signals. This is a novel and fascinating area where navigation and forensic science meet!

GPS Jamming

The use of GPS jammers, long foreseen in navigation circles, has become a reality as criminals employ them to overcome tracking systems and steal vehicles. These low-powered transmitters (see **PHOTO**), readily available over the Internet for as little as $150, can block GPS reception in a vehicle's vicinity.

GNSS satellites transmit no more power than a car headlight, yet must illuminate nearly half the Earth's surface

▲ **LOW-POWER** GPS jammer



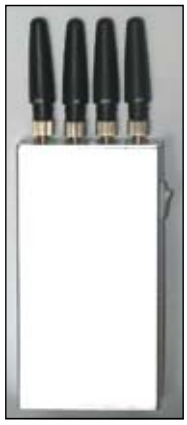
▲ **FIGURE 3** Signal spectrum radiated by low-power jammer

DAVID LAST is the immediate past-president of the Royal Institute of Navigation, a consultant and expert witness on radio-navigation and communications systems to companies, governmental and international organizations, and criminal investigators.

ADVISORS UPDATE

PASCAL CAMPAGNE, CEO of France Developpement Conseil and a founder of the ORganisation of European GNSS equipment and services INdustry (OREGIN), has merged the latter entity with Galileo Services, another non-profit consortium of companies covering GNSS applications and services. The new body totals more than 200 members, both small and large enterprises, spanning the value chain and all application domains.

Pascal Campagne



▲ **JAMMER** for GPS, GSM (900MHz), DCS (1800MHz) and 3G mobile bands

▲ **HIGH-POWER** jammer for GPS and mobile phone bands

▲ **L1 AND L2** jammer

from 20,000 kilometers above it. Signals reaching a receiver are easily swamped by even a thousandth of a watt of jamming signal radiated near by.

FIGURE 3 shows the spectrum of the signal radiated by the low-power jammer in the photo above it, plotted across a 100MHz frequency range centred on the GPS L1 frequency at 1575.42MHz. The total power this jammer radiates is only about one tenth of a milliwatt, yet that is sufficient to block commercial GPS receivers over a few meters range — all the criminals need.

GPS/Phone Jammers

If a vehicle is to be completely screened from electronic tracking, not only must GPS be disabled in its vicinity, so must mobile phones as well. If not, they can be used to call for assistance; they can also be tracked using cell-site analysis methods. To prevent that, a jammer (see adjacent **PHOTO**) can block not only GPS reception but also that of all the mobile phone bands used in the area. The spectra of the jamming signals radiated by this device are designed to cover the frequency bands in which European 900MHz, 1800MHz, and 3G base stations transmit, so preventing mobiles from receiving them and establishing communications.

Recently, much more powerful jammers have appeared on the market (see adjacent **PHOTO**). These radiate approximately 2W on each frequency, a power level some 20,000 times greater than the low-power jammer — and more powerful than the transmitter employed recently in official UK tests of effects on shipping of jamming GPS over a sector of the North Sea up to 30 kilometers from the jammer. A 2W jammer could interfere over a substantial area.

Other GNSS

The spectrum in Figure 3 of the jamming signal of the simple low-power device extends from approximately 1563MHz to 1600MHz. Towards the center of this band is the civil GPS signal, approximately 2MHz wide. The jammer also covers the 20MHz-wide military P/Y signal, the yellow block. The slightly wider blue block represents L1 signals planned for Galileo, so this device would serve as a Galileo jammer, too. Its spectrum covers only the low end of the (purple) GLONASS bands, but other similar devices on the market jam that as well.

It is often argued that, since Galileo will use more than one frequency band, simply jamming L1 would not prevent Galileo reception. However, the bottom **PHOTO** shows a jammer that has recently come onto the market, with two transmissions: one covering L1, the other, at a higher power, covering the L2 band. Adding L5 would be trivial. These are the frequency bands in which present and planned GNSS operate.

The jammers presented here are relatively simple and crude, but highly effective in preventing the operation of civil GPS receivers. They are readily available and are certainly being sold and being used. They render our GNSS-based security systems vulnerable to attack.

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

Mitigation

All is not lost! In many countries, vehicle tracking systems such as Datatrak are deployed that do not depend on GNSS. There are also vehicle recovery systems such as Tracker with its LoJack technology installed in police cars and helicopters. These systems are immune to GNSS jamming and spoofing. Of course, like all radio systems, they can be jammed. But they are orders of magnitude less vulnerable than GNSS, and jammers that targeted them would be easier to detect.

Dead-reckoning can also mitigate GNSS jamming. Many cars with built-in navigators carry heading sensors and wheel-rotation counters to cope with loss of GPS in tunnels and urban canyons. They are immune to jamming, at least for short periods and distances. But they would not necessarily be immune to GNSS spoofing.

Enhanced Loran, or eLoran, offers a complete alternative navigation technology. Built into a GNSS receiver, it can take over seamlessly when GNSS is jammed, and replace precise GPS timing that currently keeps most of our telecommunications systems and the Internet running. There is currently great interest in this cost-effective insurance policy worldwide.

Conclusions

Legal and forensic aspects of GNSS grow ever more important, and their role more vital and successful in reducing crime. We must plan our responses to the vulnerability of our current and future GNSS-based security systems, which are now under attack. We must recognize these threats and encourage open and full discussion of them and of solutions to the dangers they pose.