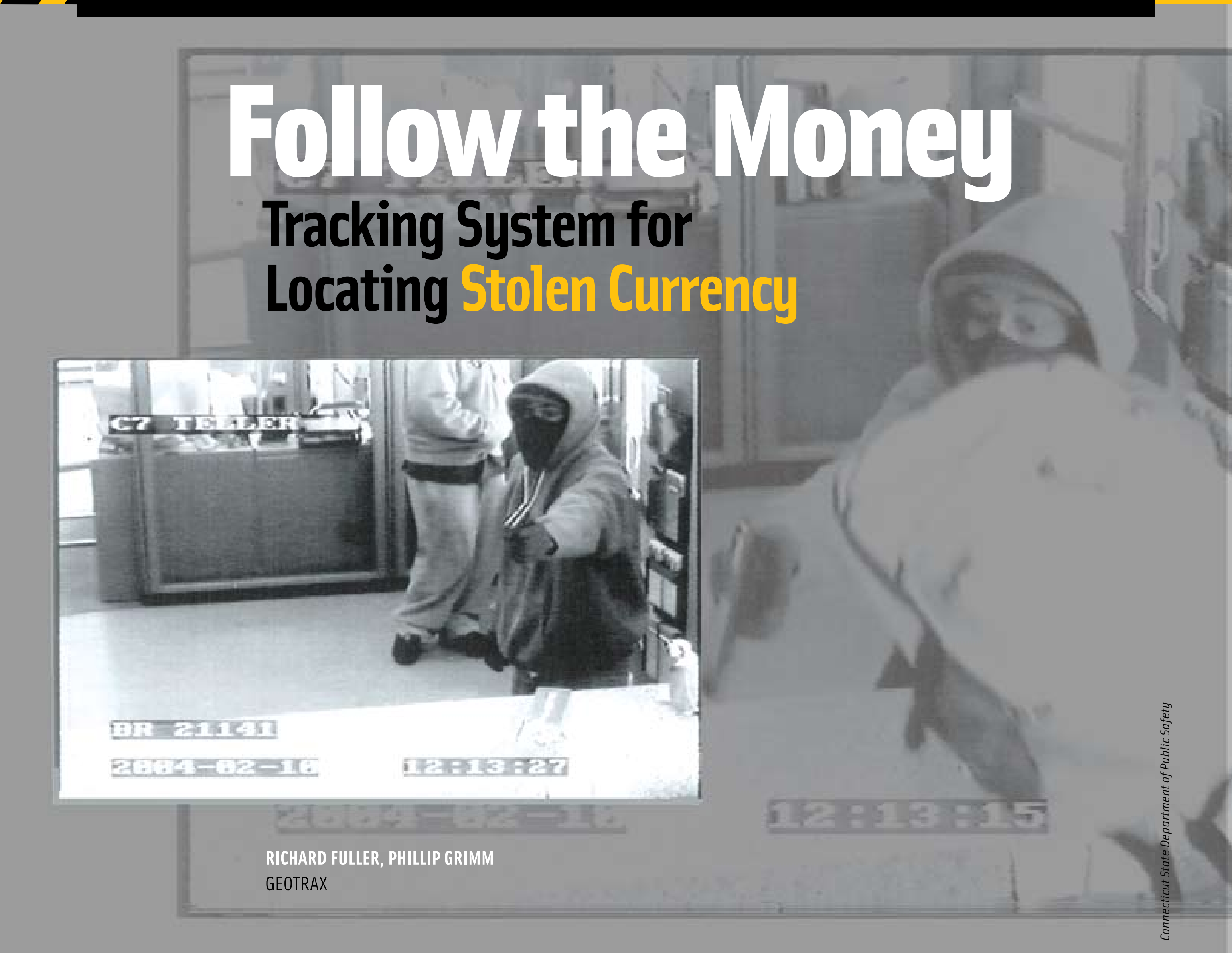
POLICE LINE DO NOT CROSS P

Follow the Money

Tracking System for Locating Stolen Currency



Connecticut State Department of Public Safety

RICHARD FULLER, PHILLIP GRIMM
GEOTRAX

Bank robberies have a long and infamous history in the United States – more than two centuries' worth, in fact. About 10,000 take place in the country each year with a total of nearly $100 million stolen. Only slightly more than half of these bank robberies end in an arrest, and the money is not always recovered. Now an Arizona company has developed a covert tracking device hidden in packets of cash that incorporates GPS, radiobeacon technology, and a cellular modem. The results: a 73 percent recovery rate in more than 30 robberies in which the system was deployed.

Bank robbery in the United States is nearly as old as the country itself. According to Ron Avery, writing for ushistory.org, the first such robbery occurred in 1798 with the loss of the then-enormous sum of $162,821.

The concentration of generally unidentifiable and readily convertible cash forms an irresistible temptation to both the novice and hardened criminal. As legendary robber Willie Sutton explained when asked why he robbed banks, "That's where the money is."

Coupled with the banking industry's policy directing employees to cooperate with a robber's instructions (to help protect both the teller and customers from harm), that simple and sublime logic establishes bank robbery as one of the most profitable theft scenarios. According to a 2002 special report by the U.S. Federal Bureau of Investigation (FBI), a total of $469,815,218.10 was reported stolen in U.S. bank robberies between 1996 and 2000.

According to a recent FBI report, bank robberies made up only 2.4 percent of total crime incidents in 2004, but that percentage still represented more than 9,600 bank robberies. Furthermore, the average loss per bank robbery was $4,221, which was more than three times the average for all robberies that year.

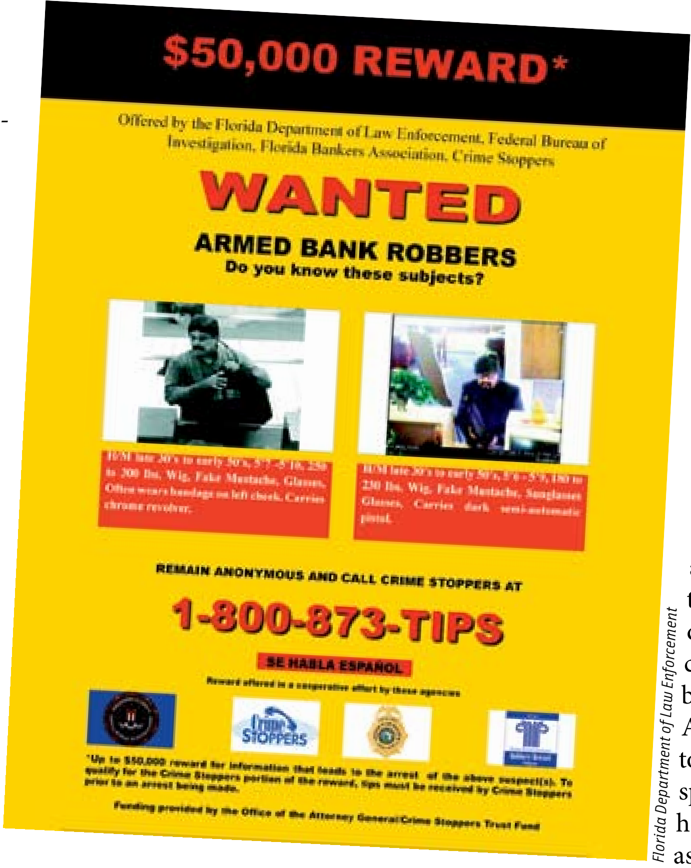
However, cooperation does not imply that banks are simply abandoning their responsibility for protecting their customers' capital. Quite the opposite; the banking industry has employed numerous techniques over its history, employing technology, psychology, and common sense to minimize opportunities of robbers and maximize their chance at recovering stolen cash.

This article describes a system using GPS- and radiobeacon-based positioning, which our company has developed for tracking stolen currency and aiding in its recovery. Since its first field installation in 2003, this system has been deployed in more than 30 robberies with a recovery rate of better than 73 percent — a figure substantially better than the 57.7 percent cited by the FBI as the average "clearance rate" of bank robberies resulting in arrest. This application requires a high-sensitivity device capable of operating inside vehicles under car seats or in a glove box, inside homes or building, and other urban environments.

We will discuss the technology incorporated into the tracking device as well as its design and development and use by law enforcement agencies. The article will also provide a summary of the success of our law-enforcement partners in using this system to apprehend suspects and describe some of the more interesting recovery episodes.

The Security Challenge

Over the years, banks have employed a variety of systems and methods in an effort to protect their cash. According to an 2001 article authored by Wells Fargo Bank in the *Bankers Hotline*, the banking industry and law enforcement agencies have used nine primary methods to prevent robberies and apprehend robbers: training, surveillance cameras, reward programs, unarmed guards, police tellers, off-duty police officers, bulletproof "bandit barriers," bait money, and explosive devices and tracking systems. Our approach, of course, falls into the last category.



$50,000 REWARD*

Offered by the Florida Department of Law Enforcement, Federal Bureau of Investigation, Florida Bankers Association, Crime Stoppers

WANTED

ARMED BANK ROBBERS

Do you know these subjects?

H/M late 30's to early 50's, 5'7"-5'10, 250 to 300 lbs. Wig, Fake Mustache, Glasses. Often wears bandage on left cheek. Carries chrome revolver.

H/M late 20's to early 30's, 5'6"-5'9, 180 to 230 lbs. Wig, Fake Mustache, Sunglasses Glasses. Carries dark semi-automatic pistol.

REMAIN ANONYMOUS AND CALL CRIME STOPPERS AT

1-800-873-TIPS

SE HABLA ESPAÑOL

Reward offered in a cooperative effort by these agencies

*Up to $50,000 reward for information that leads to the arrest of the above suspect(s). To qualify for the Crime Stoppers portion of the reward, tips must be received by Crime Stoppers prior to an arrest being made.

Funding provided by the Office of the Attorney General/Crime Stoppers Trust Fund

Florida Department of Law Enforcement

The experience with dye pack technology bears a little further discussion here because its use has some common features with tracking systems such as ours. Banks employ these types of devices both for apprehension (and recovery) as well as prevention, when word is leaked of their use in a particular area. Of course, in the latter case, training is critical because many bank robbers present instructions to not pass "bait money or dye packs" as knowledge of these methods have become better known.

Dye packs stain stolen currency by exploding a colored substance, usually a powder, that covers the cash and makes it obvious that the bills have been involved in a robbery. In some devices, tear-gas is included in the dye to not only make the presence of the stolen currency but also show a colored cloud for searching by law-enforcement.

A dye pack consists of a hollowed-out stack of real bills with chemicals and electronics inside, usually with one or two bills stuck on the top and bottom of the stack. The dye pack sits idle in "safe mode" on a magnetic plate while in the teller drawer. When a robbery occurs, the teller is supposed to subtly slip the device in with other money. Removing the device from the magnetic plate does not cause the dye to be released; it is simply armed at that point.

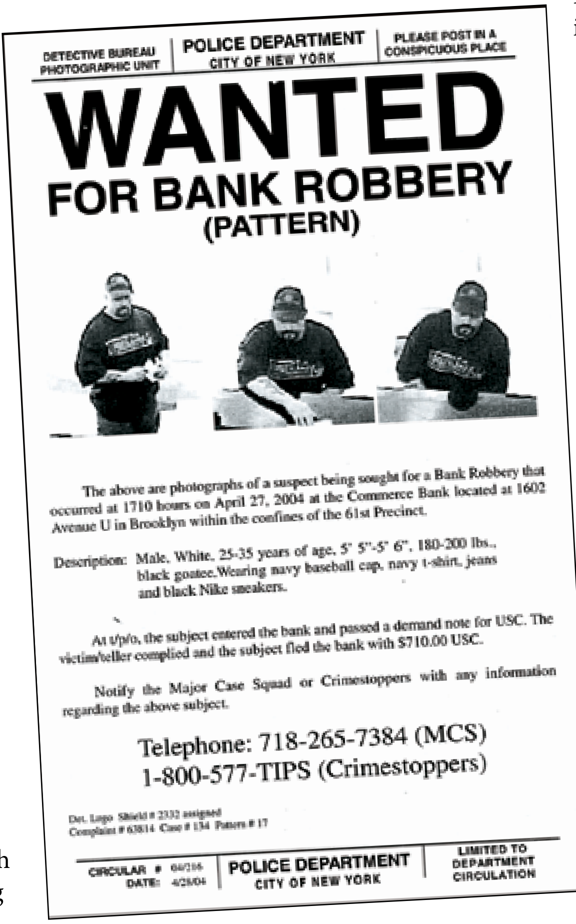
As the bank robber passes a radio activation field near the front door, a timer in the dye pack is activated. Delayed release of the dye allows time for the bank robber to get some distance from the bank before the money is stained. In many cases the hands and/or clothing of the bank robber are stained making identification easier.

Initially these devices had rigid construction that made them harder to conceal. However, evolution in electronics has enabled design of flexible versions for the explosive device and even the chemical pouches, thus allowing them to be passed during a robbery with low chance of detection by the robber (who is often an "amateur"). Although a potentially useful tool, this type of device requires special handling and some banks have not adopted this technology as a result. Nonetheless, the dye pack is reportedly used in more than 75 percent of banks in the United States, and has helped recover substantial amounts of stolen money and apprehend perpetrators.

Another common in-drawer cash protection system employed by banks is the miniature RF beacon. As in the case of the dye pack, the device sits idle in the teller drawer until activated by being lifted off of a magnetic plate. This RF signal activates a network of stations located throughout a city and along likely escape routes of a robber, which localizes the transmitter to the closest station. Police personnel can also be equipped with receivers to determine proximity, range, and direction to the stolen currency pack.

Although the beacon transmitter can be extremely small, one of the most significant limitations to this technology is the requirement for beacon receiver stations to be placed around the area of operation. If a beacon device should get outside of the network of stations, however, it can no longer be tracked effectively. To cover the whole lower 48 states of the US, assuming a five-mile radius of receiver coverage, would take a minimum of 40,000 stations (excluding line-of-sight issues that would substantially increase the number of stations).

These considerations almost certainly make it financially impossible to place receiving stations throughout the country for a single application. Therefore, RF beacon technology practically provides only a local solution, leaving the system vulnerable to coverage gaps.



DETECTIVE BUREAU
PHOTOGRAPHIC UNIT

POLICE DEPARTMENT
CITY OF NEW YORK

PLEASE POST IN A
CONSPICUOUS PLACE

WANTED
FOR BANK ROBBERY
(PATTERN)

The above are photographs of a suspect being sought for a Bank Robbery that occurred at 1710 hours on April 27, 2004 at the Commerce Bank located at 1602 Avenue U in Brooklyn within the confines of the 61st Precinct.

Description: Male, White, 25-35 years of age, 5' 5"-5' 6", 180-200 lbs., black goatee.Wearing navy baseball cap, navy t-shirt, jeans and black Nike sneakers.

At t/p/o, the subject entered the bank and passed a demand note for USC. The victim/teller complied and the subject fled the bank with $710.00 USC.

Notify the Major Case Squad or Crimestoppers with any information regarding the above subject.

Telephone: 718-265-7384 (MCS)
1-800-577-TIPS (Crimestoppers)

Det. Lugo Shield # 2332 assigned
Complaint # 63814 Case # 134 Pattern # 17

CIRCULAR # 04/216
DATE: 4/28/04

POLICE DEPARTMENT
CITY OF NEW YORK

LIMITED TO
DEPARTMENT
CIRCULATION

New York City Police Department

GPS Tracking

GeoTrax was formed in late 2002 with the goal, among others, of developing a cash tracker that would overcome the technical and operational limitations of the covert systems used at the time. Consequently, our solution would have to provide a success rate that met or exceeded current systems but without the drawbacks, such as dangerous chemicals or limited coverage.

A couple of significant FBI statistics provided additional guidance to our design of the tracking system. The first is the distinction between "amateur" and "professional" bank robbers. A landmark study by Dr. Yoshio Akiyama written in 1983 discovered that, over a 10-year period, an overwhelming percentage of bank robberies was conducted by individuals without a prior criminal record. It was as if the individual was acting on an impulse as compared to a well-thought-out plan. Obviously, relative inexperience is a factor that can be accounted for in the design of a bank cash protection system.

Another relevant data point from the FBI is the distribution robberies by population. One would expect that cities, with their dense population of both people and financial institutions would be prime areas for bank robberies. However, statistics show little variation by population density in a region for bank robberies. This means that even suburban and rural areas need protection the same as large banks in urban centers.

The system would also require near-real-time position reporting to enable pursuit by law enforcement officers. Latencies of a minute or more could introduce enough target uncertainty in a chase to confuse the pursuers. Tests conducted in trials indicated that the system needed an update rate of 15 seconds or less.

This provided an extremely short interval in which to send location information to some central location then disseminate it to the police in the field. Communication channels would have to be chosen to ensure that a controllable (or at least reliable) latency could be maintained.

In developing the system we had to assume that, given enough time, even an "amateur" thief would detect the smallest device embedded in currency. So, the overall design of the device would have to help prevent its obvious detection within the first 5 to 10 minutes after a robbery, especially in the case of a single perpetrator who may not have time to inspect the stolen cash. This 5-10 minute period is the crucial response time for the police to isolate the location of the criminal. Therefore, precise location as soon as a minute or two after activation is necessary to support effective response by the law enforcement community.

Keep in mind that placing a tracking device employing GPS in a potentially challenging environment — an unknown enclosure, possibly next to the human body, in an unknown orientation — was virtually impossible with off-the-shelf GPS technology in 2002. This would prove to be a critical hurdle in bringing this solution to market. Table 1 presents a list of the requirements that Geotrax thought the tracking device would face.

Another aspect of system design would have to deal with location uncertainty. Even the most sensitive autonomous GPS receiver operating at optimal accuracy could produce enough positioning ambiguity to hinder recovery of the tracking pack. To illustrate, consider a scenario in which the police determine that a GPS tracking device is operating in the southeast corner of a parking lot. The pack is somewhere within a 20-meter radius of a given point. Within that radius there are 10 cars; which one do they search? They do not necessarily have "probable cause" to search them all and in some jurisdictions may prefer to get a warrant for a specific car before proceeding.

As a result of such considerations, early in the design process GeoTrax decided to add an RF direction-finding beacon to the tracking device to help law enforcement with the isolation of the pack in such situations.

Based on these observations, plus feedback from marketing partners and potential customers, high-level performance requirements were developed to meet the needs of the banks and law-enforcement agencies. These system requirements are summarized in Table 2.

Item	Performance Goal
Device Size	Small enough to be completely concealed in a bundle of cash
Device Weight	Match currency stack within 20 grams
Device Flexibility	Must bend at two internal junctions by at least 20°
Reporting Period	Less than 10 seconds to support 15-second mapping intervals
Wireless Data Link	Digital wireless modem (to meet reporting period)
Reporting Coverage	Must support the populated regions of the US with high reliability
Battery Capacity	Must support wireless modem. Available LiIon capacities ~750 mAh
Battery Life	45-minutes after activation. 18-month shelf life. (4 hours on full charge)
Battery Voltage	3.2-4.2V (operational)
Device Battery Charging	In-field technician-serviceable battery charging
RF Beacon Transmit Power	Sufficient for open-air 150m operation
Configurability	Over-the-air operating configuration
GPS Capability	High sensitivity GPS tracking and advanced location algorithms allow GPS locations to be obtained in non-open sky environments include – for example, in car trunk or glove box, under car seat, in homes and other buildings, as well as many urban environments

TABLE 1. Device requirements.

The following section will address how GeoTrax made certain technical choices to meet these performance requirements.

Systems Analysis and Alternatives

One of the first technical decisions to be made related to the wireless data telemetry solution. Multiple options existed

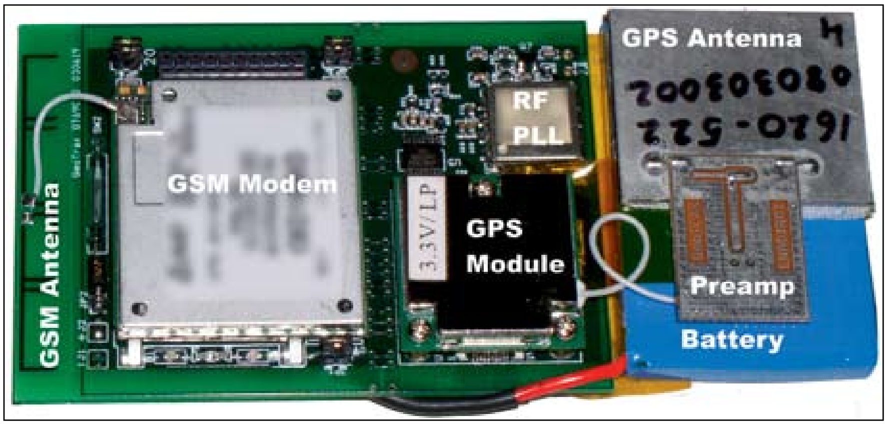


FIGURE 1 The currency tracking device

in late 2002 for data telemetry. Control-channel modems offered the best coverage in the United States (and selected coverage internationally).

These solutions offered relatively inexpensive data rates, mid-level modem costs, and nearly complete coverage in the lower 48 states. The downside was the relatively large size of the modems compared to their corresponding cellular counterparts. This, in fact, proved to be a prohibitive factor given the goal of enclosing the modem in a package that would be hard for an inexperienced thief to detect. Additionally the data payload for these services was limited to a several bytes of data at a time and even the fastest update rates were a minute or longer.

As a result, we quickly focused on cellular modems after these limitations become clear. Several models met the strict size requirements; so, the main choice was between the two major competing digital wireless standards at the time: CDMA and GSM.

The advantages of CDMA included excellent coverage in the United States, built-in high-sensitivity GPS, and existing deployment of packetized data connections (that is, mobile Internet, referred to as 1XRTT for CDMA). But CDMA had a downside as well: available modems were slightly larger than their GSM counterparts and coverage in western Europe was non-existent. Moreover, access to high-sensitivity GPS required carrier commercial service, which had not been rolled out at that point.

In comparison, GSM modems had some of the smallest-volume dimensions and were readily available and supported in many countries, including North America and all of western Europe. On the negative side, coverage for GSM at the time was a smaller footprint than for CDMA, modems with built-in GPS or assisted-GPS were not then available, and packetized data for the GSM network (GPRS for GSM) was only partially implemented in the United States.

To overcome the limitations of coverage and the lack of packetized data, GeoTrax decided to use the GSM Short-Message-Service (SMS) for data communication. This option provided coverage that actually somewhat exceeded voice coverage. (Informal company tests verified that two-way SMS was often possible when a voice call would not complete or stay connected). SMS also offered a data solution for which several wireless data aggregators could provide service to our company. However, this still left the problem of getting access to a high-sensitivity GPS solution.

Finding a GPS solution. In 2002 a number of enhanced-sensitivity GPS chipsets were under development. Available research indicated that real-world degradation of signals could easily be 15 dB and as much as 50 dB over traditional line-of-sight GPS applications. Given the nature of how the mobile device would be used operationally in this application, obtaining the highest sensitivity GPS solution available would be critical.

One strong option of interest was only available at the time as a chipset, not a receiver module. Selecting that option would have required development of a dedicated board to support the chipset's operation. Due to time constraints in reaching the marketplace, we decided to use an off-the-shelf technology— module plus firmware — that appeared to be the only commercially available solution in module form supporting enhanced sensitivity GPS.

During our evaluation we estimated that GPS sensitivity was at least 10 dB over "traditional" receivers (including the selected module without the firmware). This was confirmed by simulator and indoor testing performed by the University of Calgary with a development kit based on the same technology (See the article by Gerard Lachapelle et al cited in the Additional Resources section at the end of this article.) We enhanced the receiver functionality by incorporating our own patented antenna design that minimized the effect of placing the device in close proximity to the human body. (See the article by R. Fuller et al cited in Additional Resources.)

Finding a beacon. The next aspect of the design involved

Item	Performance Goal
Application Environment	Potential for hosting on a variety of law-enforcement computers (no O/S dependence) – led to browser-based approach
Web Application	Secure web application to provide basic mapping of current device location for law enforcement and bank security personnel
Mapping Update	Must update at less than 15 second intervals
Mapping Coverage Area	Coverage of the continental United States (Canada and Western Europe desirable for expanded markets)
Location Determination Capability	Primarily GPS with cell-based location as a backup. Back-up cell-based location automatically provided in cases where GPS coverage not available
Alert Capability	Email, IM, pager and SMS alert capability

TABLE 2. System requirements.

selecting an RF beacon, embedding it into the device, and identifying the associated RF beacon receiver. As with the GPS solution, market considerations demanded a solution that offered minimum development time.

A directional receiver was located through a U.S. company that specializes in designing and manufacturing directional receivers for various applications. The receiver can be selected to any of three 40-kHz-wide channels that down-selects the frequency into an audible tone and an LED readout of power. The receiver has a fold-away pistol-grip handle, weighs less than 15 ounces, and stores away with the dimensions of 6.8 × 3.8 × 1.4 inches. For convenience of field replacement, the receiver uses eight standard alkaline type-AA batteries for power.

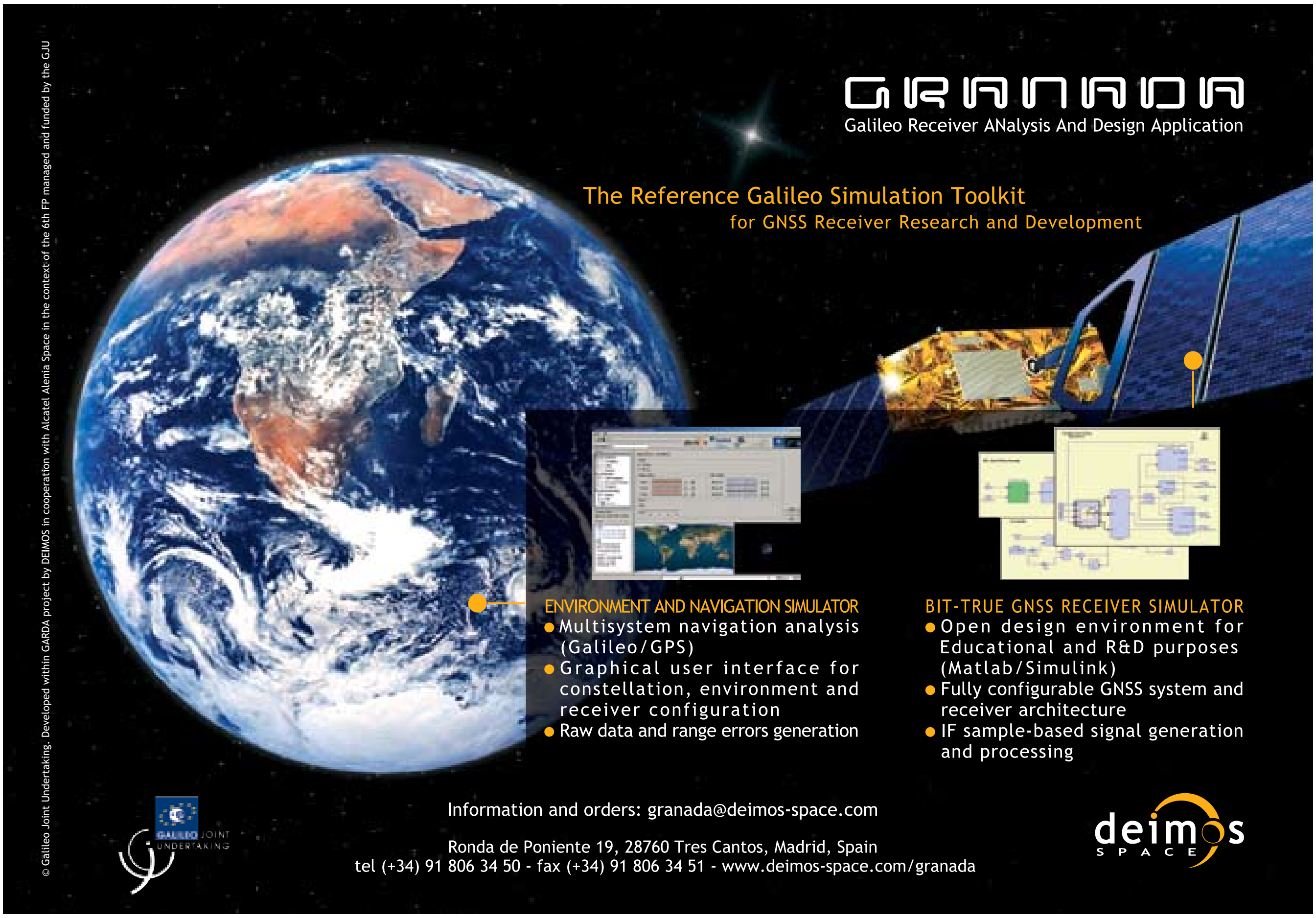
The beacon transmitter embedded in the tracking device uses a frequency synthesizer chosen to create a stable low-noise signal that could supply a pure carrier tone necessary for beacon reception. The synthesizer is combined with a high quality reference oscillator and loop filter that provide the feedback tuning voltage for a voltage controlled oscillator. This oscillator generates a signal from a low phase-noise, local oscillator that is connected, unamplified, to a loop antenna embedded in the device.

All three of these three subsystems; cellular, GPS, and RF beacon are combined with a battery-power system for delivery of operational power and charging. These subsystems are mounted on three rigid boards with wire interconnects that allow for the flexibility required in the design.

Figure 1 shows the device with all of its components mounted on a single board. The major electronic systems are the GSM modem, the GSM antenna, the GPS module, the GPS preamp, the GPS antenna, the RF beacon phase-locked loop (PLL), the RF beacon antenna, and the power system (battery). The GSM modem serves not only for communications, but also for the main application processor. It has an application layer that can be modified by the developer, which proved useful in minimizing parts count and integration issues.

To achieve ultimate compactness the GSM and RF beacon antennas can be directly integrated into the main board. (The RF beacon antenna is the thin trace on the outside of the board.) Doing the same with the GPS antenna would have been physically prohibitive and costly; so, it is either glued or taped to the battery during manufacturing.

One of the advantages of working with distinctly independent modules with very different operating characteristics was that RF interference (RFI) and electromagnetic interference (EMI) were relatively easy to deal with. The RF beacon operates at 216 or 219 MHz, and the Federal Communications Commission places strict requirements



on out-of-band emissions, which limits interference on other modules. Similarly, the GSM modem was designed for operation at 1900/1800 & 800 MHz, well clear of the RF beacon at 216/219 and the GPS receiver at 1575 MHz. The most important design characteristic was isolating the modules on the supply lines so that their individual digital processors did not created unwanted noise going into the other modules.

The final design has a mass of 48 grams, which is within the tolerances of the currency volume it displaced. The module's dimensions are 104 (length) × 48 (width) × 12.5 (depth). The depth was slightly outside of design specs, but foam of slightly lower height was used to accommodate it. The added 4 millimeters along the length was accommodated by sliding the GSM antenna into the edge of the currency.

This device sits completely inactive when in a teller drawer, with the power held low by the magnetic reed switch (shown between the GSM modem and the GSM antenna). When outside of the magnetic plate's field the device turns on.

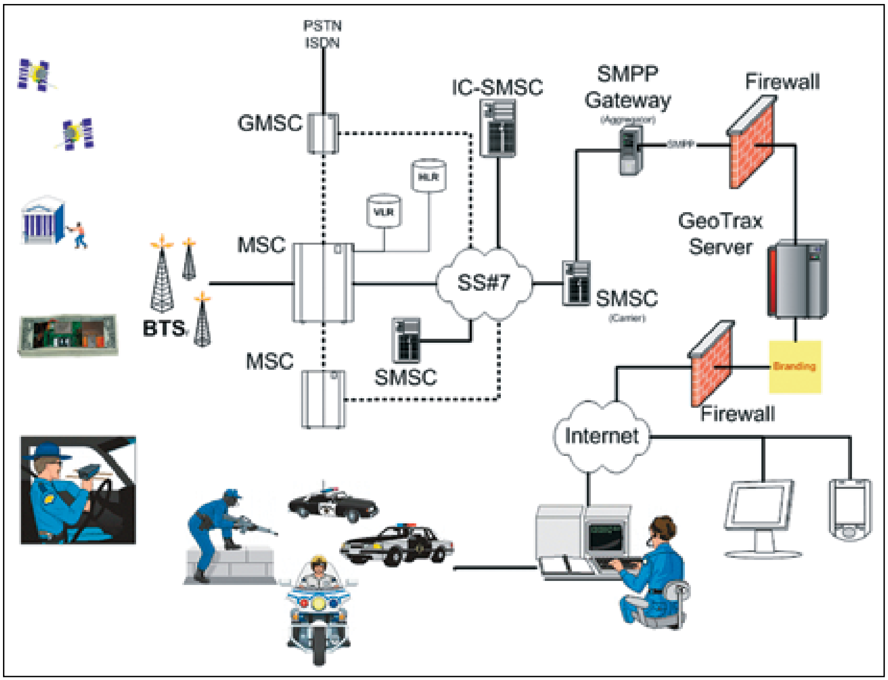


FIGURE 2 System Architecture: BTS, Base Transceiver Station; MSC, Mobile Switching Center; GMSC, Gateway Mobile Switching Center; SMSC, Short Message Service Center; IC-SMSC, Inter-carrier SMSC; SMPP Gateway, Short Message Peer-to-Peer Protocol; SS#7, Signaling System 7.

System Architecture

The network design was just as critical. Information from an active device needed to be received, processed, recorded (for later retrieval), and disseminated in the fastest and most reliable fashion. Because different security and law-enforcement agencies would have different computing and communications systems, we decided to use a secure Web link to deliver streaming notification and mapping (with updates of 15 seconds or faster) to the police forces to ensure maximum compatibility.

Due to the high-reliability requirements placed on this system, we decided that the mapping software needed to reside behind the firewall under our administration (as compared to using a web-based service). In addition to the map rendering, one of the most critical features offered by the software is the use of reverse-geocoding to provide an approximate location based on the last known GPS location. Although some smoothing of GPS data takes place, no map matching or other corrections are made to the data or the map.

The reason for this is that many times the activated device winds up well away from a street or intersection. Many times a stolen pack is located in a large parking lot or inside a residence or, in one instance, taken to a creek 200 meters from a residence and discarded. Having a map-matching algorithm would in many cases give the pursuers the false sense that the device never left the road.

However, because GPS locations are not perfect, we did our best to ascribe an uncertainty value to the locations generated by the unit, both in dimensions shown with the text summary (e.g., "GPS Location, Uncertainty 25 meters") and graphically by an ellipse that shows the uncertainty as a shaded region centered on the most likely location.

One of the most important design considerations from the outset was the notification of the users that a pack had gone active in their jurisdiction. We established an alert methodology that allows any number of devices to receive an alert (e-mail, IM, pager, SMS, etc.), and each user can control how they are alerted. They may chose to receive an e-mail and a page, or only an SMS, or all of the above (or no alerting if they so chose). The website itself has an audible alert that turns on when a device that the user is assigned to goes active. A high-level system diagram is show in Figure 2.

The overall operational scenario is depicted in Figure 3: during a robbery the tracking device is activated in the same manner as a dye pack or simple beacon tracking device. This activation sends a notification to the appropriate security personnel and police in that area, indicating that they have an active tracking device in their jurisdiction.

A police dispatcher (bottom right in figure) views the near-real-time location of the device and routes police to the specific area. The police also transport the handheld beacon tracker to the area where the robber has fled to help isolate the precise location in a building or parking lot, if necessary. Once the suspect is identified, the police move in and make the arrest.

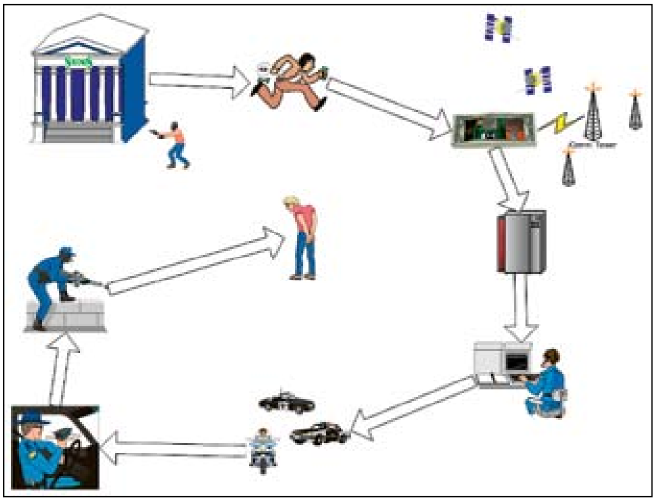


FIGURE 3 Operational Scenario: Bank Robbery

Subsystems

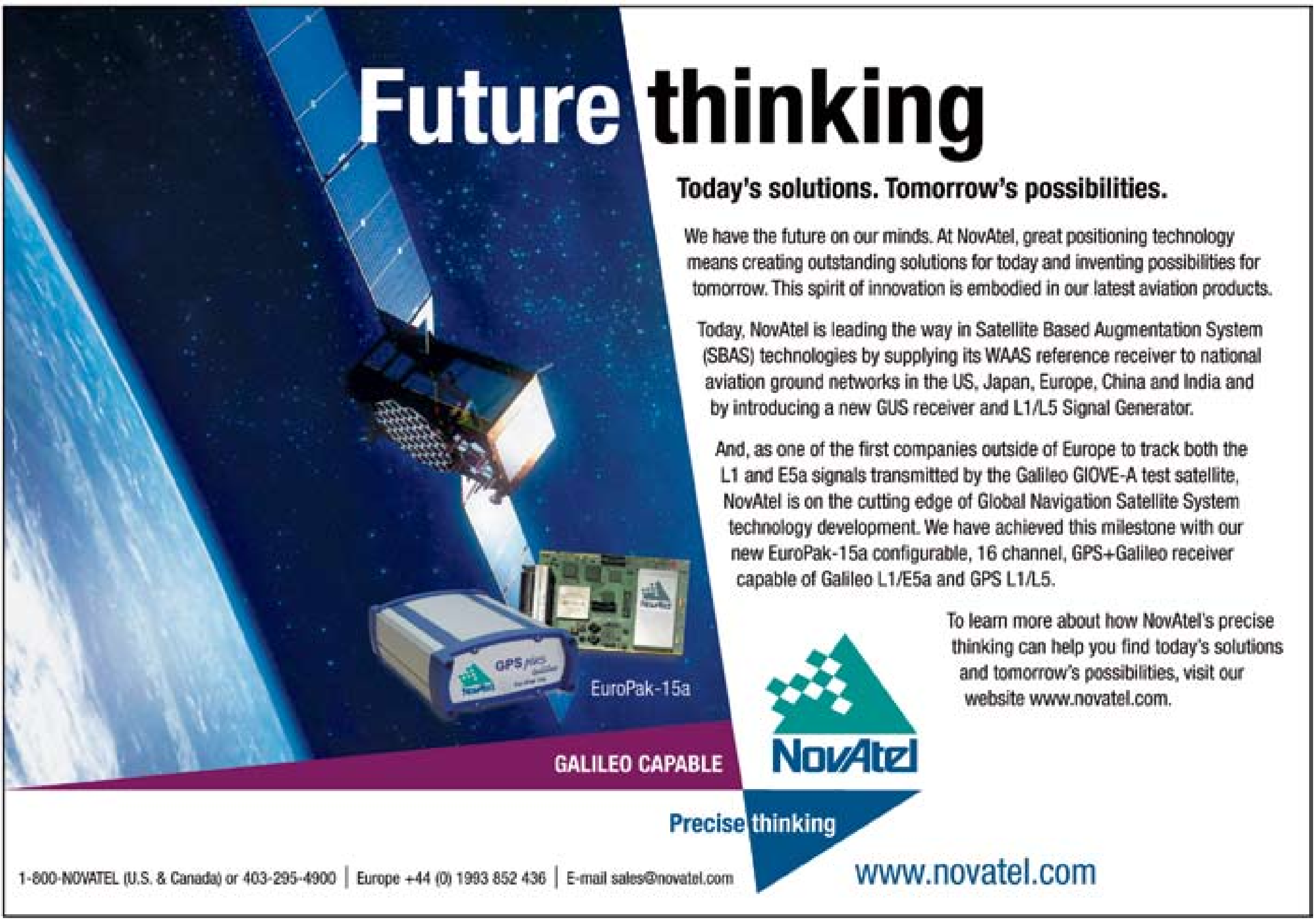
As mentioned in the previous section, we selected GSM as the data transport system. GSM has its foundations in Europe. Throughout the 1980s, a number of incompatible analog voice networks had been developed and deployed by different European countries. The United Kingdom had the Total Access Communications System (TACS), Scandinavia had NMT, and Germany had C-Netz.

The original GSM system designers wanted to create an all-digital, truly portable standard that would work across national boundaries but still allow for network carriers to have a national origin (i.e., the home network). In 1989, a standards organization, the European Telecommunication Standards Institute or ETSI, was established with the charter to oversee the committees charged with defining GSM.

By 1992 the first networks were operational. In 1994, data transmission capabilities, including the Short Messaging Service (SMS), were completed. The adoption rate for GSM has been phenomenal. GSM offers support in almost every country and a total subscriber base of approximately 1.5 billion worldwide.

Choices for the GSM modem included the PCS frequency band in the United States and Canada (1900 MHz) and DCS (1800 MHz) and E-GSM (900 MHz) for use in Europe (and many other roaming countries). We optimized the design of our embedded cellular antenna for operation at the 1900 MHz band, but it also supports 1800MHz and 900 MHz to a lesser extent.

High-Sensitivity GPS. The high-sensitivity GPS chipset, combined with the antenna and an extremely low noise-figure in the RF front end of the receiver led to system performance that was sufficient to meet the tracking goals spelled out in Table 1.



RF Beacon Usage. The RF beacon tracking device is approximately 6.8 × 3.1 × 1.4 inches with a fold-away pistol grip (see accompanying photo). It has an LED bar to aid tracking (red light flashes on right showing signal strength). An attenuator switch helps reduce swamping and assures accurate close-in tracking. The effective range in operational scenarios has varied between 100 and 200 meters and has aided in the isolation of stolen currency to a car and inside the wall of a house.

The beacon receiver has two indicators, an LED panel and a signal tone. The received signal levels are indicated by both the number of LEDs that light up as well as the clarity and volume of the audible tone. By turning 360 degrees in a horizontal plane a user can find the most likely direction of the transmitter (the direction with the maximum tone/most LEDs). As a receiver gets closer to the transmitter, the tone volume increases.

The maximum range is approximately 200 meters, depending on the obstructions between the transmitter and receiver. The direction to the transmitter can usually be determined quite clearly between 100 down to one or two meters.

Battery Life: Operational and Storage. Battery life is particularly important for this application, both during storage and activation. As mentioned previously, the battery selected uses LiIon chemistry. Multiple tests were run to estimate the battery life of the device with the selected battery. Because of the unit's design as a standalone device, we decided not to outfit it with any special instrumentation for battery-life tests, as these could affect the operation of the device.

We designed the tracking device to monitor voltage while the unit is active. Although voltage alone is not completely sufficient to characterize battery life (both voltage and current, with temperature, are preferred), we used a process that measures the total life of the battery in each battery cycle from full charge to completely empty in order to estimate the components of battery drain.

RF Beacon handheld receiver

The battery capacity of the tracking device was a known quantity of 750 milliamp-hours (mAh), as specified by the manufacturer. We measured battery drain against the parameters of SMS usage (in mAh/SMS), GPS usage (in mAh/min of GPS operation), RF beacon (in mAh/min of RF beacon usage), and modem (in mAh/min of modem usage).

GeoTrax engineers conducted tests in which varying levels of each of these parameters were used. For example, one test would have GPS on 100 percent of the time and the RF beacon on 50 percent, while sending an SMS twice each minute. Another test would have the GPS on 100 percent of the time and the RF beacon on 20 percent of the time, with an SMS message at a rate of 10 per minute — and so on. Twenty-five different cases were conducted varying the RF beacon duty cycle, GPS duty cycle, and SMS update rate parameters.

Results were calculated using a least-squares fit to the following equation:

Uc*Sm*t + Bc*Bd*t + Gc*Gd*t + Mc*t = Tc

where:

t=	Uptime
Uc=	Capacity/SMS [mAh/SMS]
Sm=	SMS/min
Bc=	Capacity/minute for beacon [mAh/min]
Bd=	Beacon duty cycle
Gc=	Capacity/minute for GPS [mAh/min]
Gd=	GPS duty cycle
Mc=	Capacity/minute for modem [mAh/min]
Tc=	Total capacity

The least-squares fit produced the following estimates for the drain parameters for the device:

Uc=	0.084407	mAh/SMS
Bc=	0.288682	mAh/min
Gc=	1.509625	mAh/min
Mc=	0.794321	mAh/min

This allowed us to form a predictive model of battery life for the device for various operational scenarios. Generally speaking, the device is run at 20 percent duty cycle for the beacon, 100 percent duty cycle for GPS, and 10 SMS per minute. Our model predicted a total battery life in this case of 234.0 minutes, which is only 6.3 percent less than the actual, average measured time of 249.7 minutes in that configuration. Although these calculations are somewhat crude, this model has provided a serviceable estimate for total battery life of the device.

Storage life is also a great concern as the unit will sit idle for many months (up to 18 months is expected) and must have enough reserve capacity after sitting idle to run for at least 45 minutes. Various reports indicated that the self-discharge rate of a lithium-ion battery could be as high as 10 percent (that is, remaining capacity can decrease by as much as 10 percent per month). This would produce a shelf life of only about 15 months, assuming a remaining 45 minutes of operating reserve capacity.

We used fielded devices to gain insight into the actual self-discharge rate of the batteries. When each device was installed in a bank branch, its battery level was recorded. Over time, either robberies or false alarms were triggered that reported the battery voltage to our server. Those measurements were collected over the first year of operation.

From this data (22 test cases), estimates of the battery self-discharge rate ranged from less than 1 percent to as high as 6.5 percent. The average was 1.9 percent. Adding in the standard deviation of 2.3 percent gives a conservative estimate of 4.2 percent for the self-discharge rate of the battery. Combining this rate with the existing battery-life model resulted in an estimate of 39 months of standby time while inactive — far in excess of the design goal of 18 months.

The accompanying photo shows the integrated device enclosed in a money packet.

When the locksmith found the device while counting the money in the restaurant, he had just happened to dump the device in the truck of a person who could later identify him with the cash.

Operational Field Experience

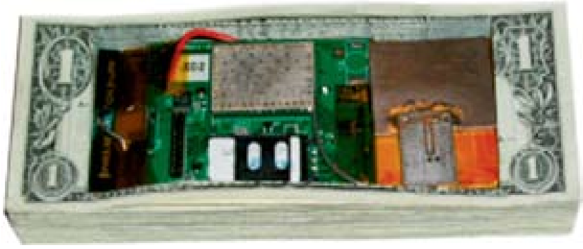
We launched the GeoTrax currency tracking system in the spring of 2003. To date the system has performed well. Through the first 25 activations, police made 23 arrests — a 92 percent arrest rate. Since then, our channel partner for banking institutions and currency recovery, 3SI Security Systems (www.3sisecurity.com), has reported a 71 percent arrest rate. Note that these numbers are substantially higher than the reported FBI clearance rate for bank robberies of 57.7 percent cited earlier.

In addition to the technology used in the device, this high success rate probably benefited from our making the activation of the device the same as other cash protection systems, which reduced the potential for confusion about the system operation. Of course, false alarms are triggered on occasion, many times by new or temporary tellers.

One order of cash to go. One of the most interesting robberies encountered so far is the first recorded by the system. In July 2003, a bank's branch manager had left for the day when the alarm went off, indicating that a pack was active. However, all of the tellers at the branch reported that they had not activated a unit.

The police responded. In the course of the investigation, tellers began to check individual units to determine if one of them had been inadvertently activated. While this was taking place, the device that had triggered the alarm and was being monitored by police seemed to "shuffle" around the bank.

This pack appeared to be moving in a random pattern, which was thought could possibly be "noise" in the GPS measurements — the apparent "jumping" from one position fix to another that reflects the error in autonomous receiver operation. (We should point out that, despite the puzzling behavior, the tracking device was generating GPS positions inside the bank building.)



Tracking device enclosed in currency.

Once all the teller drawers had been checked, investigating officers decided that a device in the vault drawer had been accidentally activated, a drawer for which the branch manager kept the only key. After about 30 minutes, the location of the device moved outside of the bank.

Because the police had been on-scene throughout, it seemed unlikely that a device could have made it out of the branch at that time. The alarm was turned off and the event treated as an accidental activation of the vault pack.

When the branch manager returned to work the next morning, she discovered that the entire vault drawer had been emptied (along with the device). Soon after that discovery, the manager of a local McDonald's restaurant turned in the tracking pack, which he had found in the bed of his pickup truck. Upon learning the time frame of the alert from the tracking device, the manager recalled that a man with a toolbox had come into his restaurant about the time in question and counted a large amount of cash at a table.

It turned out this customer was the locksmith whom the bank manager had let into the vault before leaving for the day. This locksmith removed the lock from the vault drawer and emptied the entire contents, including the tracker into his toolbox. He finished his work in the vault and walked the device right past the police in his toolbox.

When the locksmith found the device while counting the money in the restaurant, he had just happened to dump the device in the truck of a person who could later identify him with the cash. This, plus security surveillance in the bank lobby placing him there at the time of the robbery led police to make the arrest.

Case closed in 20 minutes. One of the more violent robberies in which a GeoTrax device has been involved occurred in a case where three robbers entered a bank branch in a "take-over" style attack. Because they went behind the teller line, they had direct access to the cash. The robbers cleaned out all of the teller drawers and the vault.

While removing the cash, unknown to them they also took three tracking devices that were hidden with the currency. The devices automatically sent location information to police. During their flight, they switched vehicles more than once. Police closed in and captured all three within 20 minutes. More than $20,000 was recovered along with weapons and bulletproof vests. It turned out that the gang had been responsible for several other robberies as well.

The tell-tale cash. In another interesting case, a bank was robbed and a device covertly handed over to the thief. Police were notified and dispatch directed response to the area. The pack tracked for approximately five minutes with good GPS

Mr. Robber's Wild Ride

Just the facts: Suspect robs a bank and flees on foot.

Police notified immediately and dispatched to scene.

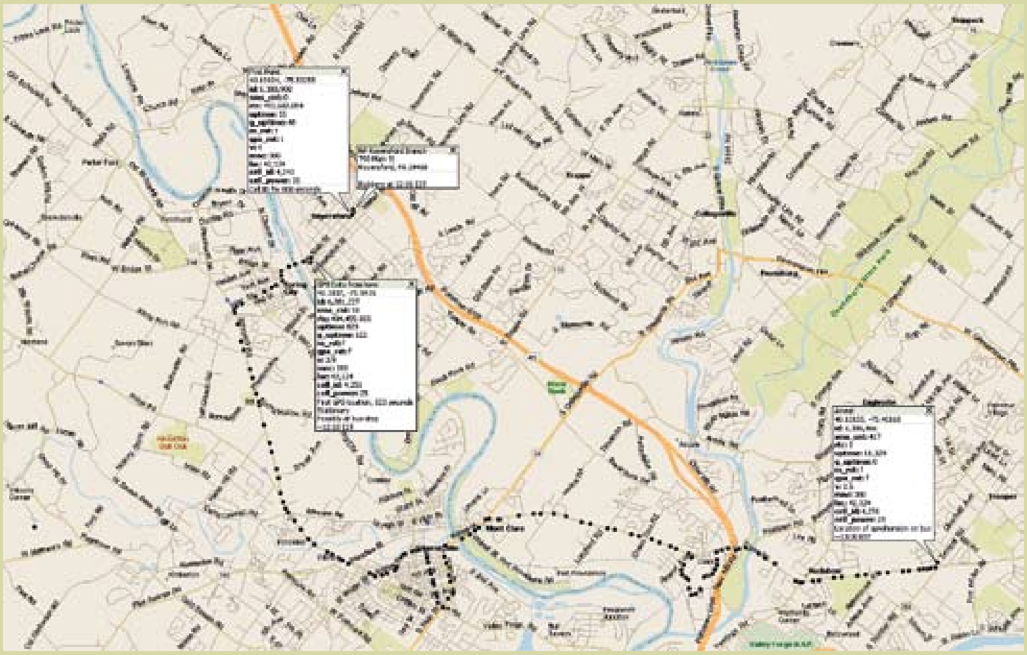
Suspect goes back to his apartment where he finds the cash tracker.

He decides to change clothes and make an escape.

Takes the money AND cash tracker with him, presumably intending to dump the tracker.

Over the next hour-and-a-half Geotrax staff "rejoice" about 10 times as the pack appears to stop moving, indicating a recovery.

However, nine times tracker begins moving again.



Police eventually eliminate all other vehicles being tracked: except for a bus in which they find the cash and tracking device.

The halts in the tracker's progress apparently represented stops made by the bus.

positions; then the GPS signals began to diminish. The pack began registering as stationary.

After another few minutes, the device switched over to cell-only location. The pack remained stationary for the next 3-1/2 hours. The police took two handheld beacon receivers to the area of the last accurate GPS location and searched for the device. As they had been trained, the officers worked the units in tandem and separately, eventually narrowing the search to one house.

Once inside the building and using the handheld units, police eventually were able to locate the signal coming from behind a paneled wall. Apparently the robber had left a wall unfinished in his house and sealed the cash (and cash tracker) into the wall after the robbery. When crime scene investigators arrived, they uncovered the device, stolen cash, and a weapon.

Typically, police and GeoTrax follow the progress of the tracker in real time on a digital map display, with dispatchers directing police officers in the field accordingly. See the sidebar titled, "Mr.. Robber's Wild Ride," for another example of a successful pursuit.

Conclusion

For years, both bank security professionals and law enforcement agencies have employed various techniques to help deter — and if not deter, apprehend — people who steal from banks. As our current success rate and anecdotes indicate, this GPS-based tracking device is a tool that can be used to help solve crimes and perhaps minimize repeat offenders. Our system, designed from scratch, represents a unique demonstration of tracking capability in extremely difficult environments to address a difficult problem for the banking community and law enforcement.

Acknowledgments

This article is based in part on a paper presented at the Institute of Navigation ION GNSS 2006 conference. The authors would like to acknowledge 3SI Security Systems for their work with the banking and law enforcement communities. Additionally, the authors would like to recognize the following team members without whose tireless dedication this system would not have been possible: Konstantin Gromov, Timothy Pfafman, Jonathan Nichols, Roger Hayward, Glenn Karlberg, and Fernando Saldain.

Manufacturers

The GeoTrax currency tracking system uses the SiRFStarII/LP with XTrac firmware, from **SiRF Technology**, San Jose, California. An alternative option of particular interest was the GPS technology from **Global Locate**, San Jose, California, which was only available as a chipset in 2002. The University of Calgary's testing of the SiRFStarII/LP pseudorange measurement noise versus signal power used a Spirent STR6560 hardware GPS signal simulator from **Spirent Communications**, Paignton, Devon, England, and Yorba Linda, California, USA. The beacon receiver was a model TRX-3S from **Wildlife Materials** of Carbondale, Illinois. The mapping software was the Enterprise Advantage System provided by **MapQuest, Inc.**, Denver, Colorado, USA, and map database came from **Tele Atlas**, Gent, Belgium. Model 053048AH batteries were supplied by **Shenzhen Full-Join Technology Co. Ltd.** Shenzhen, Guangdong, China. The GSM modem was model EN2001 from **Voxson Ltd.**, Brisbane, Australia.

Additional Resources

[1] Akiyama, Y., "Crime Indicators System, Fourth Semiannual Briefing on Crime", Federal Bureau of Investigation, 1983

[2] Allen, M. F., "Electronic Detection and Tracing Means," U.S. Patent Number 3618059

[3] Avery, R., "America's First Bank Robbery", <http://www.ushistory.org/carpentershall/history/robbery.htm>, 1995.

[4] Bergveld, H. J., and W. S. Kruijt and P. H. L. Notten, *Battery Management Systems: Design by Modeling*, Kluwer Academic Publishers, 2002

[5] Buchman, I., *Batteries in a Portable World: Second Edition*, Cadex Electronics Inc., 2001

[6] Culpepper, J. W., and H. A. Currie, and W. F. Heathcock, "Beacon tracking system", U.S. Patent Number 4021807

[7] Enge P., and R. Fan, A. Tiwari, Chou A., Mann W., Sahai A., Stone J., Van Roy B., "Improving GPS Coverage and Continuity: Indoors and Downtown", *Proceedings of ION-GPS 2001*, Institute of Navigation, September 2001

[8] Federal Bureau of Investigation, Department of Justice, "Bank Robbery in the United States: Special Report, Crime in the United States 2002," 2002

[9] Federal Bureau of Investigation, U.S. Department of Justice, "Crime in the United States 2004, Uniform Crime Reports," Washington, D.C., 20535

[10] Fuller R., and R. Hayward, N. Marshall, and J. Glissman, J., "An Antenna Design Utilizing a Cavity Architecture for Global Positioning System (GPS) Applications," U.S. Patent Number 6720923

[11] http://money.howstuffworks.com/question671.htm

[12] Keniston, S. E., "Bendable currency security dye pack", U.S. Patent Number 5196828 and U.S. Patent Number 5485143

[13] Lachapelle G., and H. Kuusniemi, D. T. H. Dao, G. MacGougan, and M. E. Cannon, "HSGPS Signal Analysis and Performance under Various Indoor Conditions," *Proceedings of ION GPS/GNSS 2003*, September 2003

[14] Ma, C., G. Jee, G. MacGougan, G. Lachapelle, S. Bloebaum, G. Cox, L. Garin, and J. Shewfelt, J., "GPS Signal Degradation Modeling," *Proceedings of ION GPS 2001*, Institute of Navigation, September 2001

[15] Peterson, B., Bruckner, D., Heye, S., "Measuring GPS Signals Indoors", *Proceedings of ION GPS 2001*, Institute of Navigation, September 2001

[16] van Diggelen, F., "Global Locate Indoor GPS Chipset & Services", *Proceedings of ION-GPS 2001*, Institute of Navigation, September 2001

[17] Wipprecht, B., "Bank Robberies 2001 - Part II", *Bankers' Hotline*, Vol. 12, No. 8, 10/02

Authors

Richard Fuller co-founded GeoTrax in 2002 and serves multiple roles as project manager and technical lead. He has presented numerous talks and papers and been involved in establishing several patents in GPS and its applications, among them the GPS Tensor, an innovative space receiver design. Prior to forming GeoTrax, Fuller studied the U.S. Federal Aviation Administration's GPS Wide Area Augmentation System at Stanford University. Fuller earned Ph.D. and master's degrees from Stanford University in aeronautics and astronautics engineering and a bachelor's degree in aerospace engineering from Boston University.

Phillip Grimm is co-chief executive officer and founding member of GeoTrax LLC. Functioning in various management positions, he has directed the affairs of the finance and accounting, sales and marketing, operations, IT, and engineering departments for Motorola, Bowmar Instrument Corporation, Harman International, and Group Bull Information Systems. Grimm is a graduate of Brigham Young University with a B.S. in finance and accounting and a minor in economics. IG