Secure Tracking for Critical Applications: Communications, GPS and Future Galileo Services

C.Wullems & O.Pozzobon
Qascom S.r.l., Italy

K.Kubik
University of Queensland, Australia

ABSTRACT: Tracking/remote monitoring systems using GNSS are a proven method to enhance the safety and security of personnel and vehicles carrying precious or hazardous cargo. While GNSS tracking appears to mitigate some of these threats, if not adequately secured, it can be a double-edged sword allowing adversaries to obtain sensitive shipment and vehicle position data to better coordinate their attacks, and to provide a false sense of security to monitoring centers. Tracking systems must be designed with the ability to perform route-compliance and thwart attacks ranging from low-level attacks such as the cutting of antenna cables to medium and high-level attacks involving radio jamming and signal / data-level simulation, especially where the goods transported have a potentially high value to terrorists. This paper discusses the use of GNSS in critical tracking applications, addressing the mitigation of GNSS security issues, augmentation systems and communication systems in order to provide highly robust and survivable tracking systems.

BIOGRAPHY: Chris Wullems is the technical director and co-founder of Qascom S.r.l. Italy. He is currently engaged in projects that range from secure tracking for hazardous and safety-critical applications to development of GNSS receiver security technologies. He has been researching signal and data-level security in GNSS and GNSS augmentation systems since 2001. He received his PhD from the Information Security Institute at Queensland University of Technology for his research in these areas.

Professor Kurt Kubik is an emeritus professor at the School of Information Technology & Electrical Engineering at the University of Queensland. His work includes GPS vulnerability analysis, the security of navigation systems, signal propagation modeling and the use of GPS for homeland security applications such as covert tracking and bistatic radar detection. He has been working in Australia since 1988, where he founded the research group working on navigation and location at Queensland University of Technology (QUT). He was program leader for the Cooperative Research Centre for Satellite Systems, Queensland University of Technology, where he managed the Navigation Program of the FEDSAT-1 microsatellite.

Introduction

From the safety of workers to the protection of assets and the transportation of hazardous materials, GPS tracking has increasingly become an important part in providing a safeguard in the presence of adversaries. Vehicle tracking/remote monitoring systems using GPS are a proven method to enhance safety and security. While GPS tracking appears to mitigate some of these threats, if not adequately secured, it can be a double-edged sword allowing adversaries to obtain

sensitive shipment and vehicle position data to better coordinate their attacks, and to provide a false sense of security to monitoring centers.
In this paper we discuss issues we have found pertinent to tracking for critical applications, how we have addressed these issues and how future technologies can further assist in providing enhanced security.

Requirements for Tracking in Critical Applications

The monitoring of assets and vehicles is typically performed by a center equipped to dispatch support personnel and manage crisis situations. Tracking systems can provide near-real-time communications to vehicles, and can be used to monitor vehicle data such as location and vehicle payload information. When emergency or critical messages are received by the monitoring center, an appropriate course of action can be decided, including the notification of necessary emergency responders.
However, there are a number of issues with tracking systems that can pose serious threats to life or financial security if not adequately addressed. Such systems have several points of failure that can be exploited by adversaries, including but not limited to:

- Wireless communication systems, which are potentially vulnerable to signal blockage and jamming;
- Radio-navigation systems (e.g. GPS, DGPS, WAAS), which can fall victim to signal blockage, jamming and signal simulation;
- Onboard vehicle / asset tracking units, which are potentially vulnerable to tampering and unauthorized modification;
- Messaging and data protocols used for communication of monitoring data, which are potentially susceptible to unauthorized modification; and
- Monitoring center information systems, which are potentially vulnerable to wide range of attacks from viruses and Trojans to distributed denial of service.

Tracking systems must be designed with the ability to thwart a variety of attacks ranging from low-level attacks such as the cutting of antenna cables to medium- and high-level attacks involving radio jamming and signal or data-level simulation, especially where the goods transported have a potentially high value to terrorists. A set of high-level requirements for tracking in critical applications is summarized as follows:

- Timely warning of hazardous or emergency situations. Such situations include (but are not limited to) route violation, movement out of a geo-fenced areas, activation of an emergency alarm, and engine failure;
- Tamper-detection and tamper-evidence of the vehicle onboard unit (OBU), such that attempts to tamper with the device are detected and made known to the remote monitoring center, and are physically evident on the OBU. This includes unauthorized access to OBU data and firmware;
- Fault-tolerance and survivability of communications, such that the tracking system is able to function in a timely manner in the presence of attacks, failures or accidents;
- Authentication and association of the party being tracking, the driver and his truck for example;
- Privacy and integrity of communications, such that an unauthorized party cannot obtain information from communications, and modification of messages by an unauthorized party can be detected; and

– Fault-tolerance and survivability of positioning systems such as GPS against signal blockage and intentional disruption.

OBU integrity, communications and positioning functions are two particularly critical areas in which risk mitigation strategies must be put in place. The following two sections discuss these functions in more detail.

Onboard Unit Integrity

Guaranteeing the integrity of an onboard unit (OBU) is one of the more difficult challenges in building secure tracking systems. Above all, OBUs must fulfill two requirements: Availability and survivability in case of fault, and resilience to tampering.
Availability and survivability is about ensuring the system remains operational in all situations. This is particularly import for tracking of hazardous materials. If communications is temporarily impeded, the OBU has sufficient information internally about the route (speeds, dangerous curves in roads, etc), cargo contents and potential dangers along the route to allow the driver to continue movement of the cargo safely. In order to increase the system's ability to survive failures, route, environment and hazard information can be remotely loaded on the OBU before a mission commences, with the option of giving the driver visual indication of contextual route information. If communications are interrupted, the OBU becomes an autonomous system able to take basic actions based on situational awareness. Tamper-resistant memory within the OBU can be used to log any non-compliant activity during the course of a given trip.
Resilience of an OBU to tampering is about ensuring that attempts to defeat or work around the safety and monitoring systems are thwarted. In this case the intent of an adversary is to prevent the OBU from recording position or to inhibit completely positioning and communications functions completely. There are clearly two different types of adversaries: one who is interested to violate route, speed or spatial restrictions to save time, fuel, etc., and one who is interested to hijack the vehicle. The following physical defenses are in protection of the former type of adversary.

Removal or disruption of power supply

The OBU must have an internal auxiliary power supply that can ideally support all functions including communications and positioning for several days, even weeks. At the very least the logging functions of the OBU must be supported. Removal of the power or any disruption of the power supply should be logged in the non-compliance log of the OBU.

Removal of OBU from vehicle

Removal of the OBU is difficult to prevent, however, tamper-evidence seals can provide a deterrent to the first type of adversary. Sensors in the OBU that can detect removal could also be used, with such activity being logged to the non-compliance log.

Removal of GPS and wireless communication system antennas

Removal of antennas can be detected by the OBU and should be logged to the non-compliance log.

Tampering with OBU hardware

Tampering with OBU hardware may be done to disable or defeat route-compliance functionality, or to modify hardware in order to spoof the OBU position, state, etc. Both tamper-detection sensors and tamper-evidence seals can be used as a deterrent. Cryptographic keys should be stored in tamper-resistant memory and ideally in a tamper-resistant module containing both the

cryptographic accelerator and memory for key storage. Tampering attempts should be logged to the non-compliance log.

Tampering with OBU software

Similar to hardware, software modification may be done to defeat route-compliance functionality, or to modify hardware in order to spoof the OBU position, state, etc. Using a methods of authentication of the software and firmware updates can prevent unauthorized modification of software. The OBU compliance-logs should be stored on non-volatile memory in a tamper-resistant way using cryptography to ensure unauthorized modification of the logs is detected.

There is little that can be done if the second type of adversary succeeds to impede communications by cutting antennas for example. The best defenses in this case include hiding of the antennas, mounting of fake antennas and the use of protocol extensions which allow the operations center to know when communications has been disrupted in a timely manner.

Communication Technologies

There are numerous factors that affect the robustness and survivability of communications from the OBU to the operations center for use in critical applications. The following subsections discuss these factors with respect to available technological solutions.

Environment

Environment plays an important part in deciding the type of communication systems to use. In unstable or developing states, terrestrial communications infrastructure such as GSM can suffer from poor coverage and frequent outages. In addition, data communicated over public terrestrial networks such as GSM or VHF radio are more susceptible to interception, whether by rouge employees in public network operators, or adversaries who monitor VHF transmissions directly. Information including position is critical, as interception of this data can result in potential breaches of security and endangerment of life.
As such, maintaining independence from local infrastructure is necessary to ensure that communications are survivable. Even in developed countries, it may not be acceptable to trust public networks in highly-critical situations. Networks can become saturated or are shut-down in emergency situations. Use of cheaper local radio networks has to be balanced with cost of more expensive satellite communications and equipment.

Privacy and Integrity

A typical requirement of tracking systems is for the end-to-end encryption of data from the vehicle (OBU) or asset to the middleware at the monitoring center. The use of encryption protocols can provide security services such as authentication, data integrity, non-repudiation and privacy.
Strong authentication is critical in assuring that a given set of messages originated from an authorized source (the OBU). This effectively prevents adversaries from producing messages without compromising the OBU. In the event an incident arises, it is particularly important that information (tracking data) about the incident remains confidential. Information leaks made by a third-party such as a telecommunications provider can cause safety issues, financial loss, and damage to the victimized company’s reputation.

As such, there is a requirement for flexible and bandwidth efficient security protocols that can traverse different types of networks with different communication paradigms.

Redundancy

For certain types of critical applications, reliance on a single communication technology is insufficient. In addition to GSM and other terrestrial radio networks, there are a number of satellite-based communication solutions that can be used in a multi-modal solution.
Multi-modal solutions typically use a combination of either GSM and satellite communications (SATCOM) or VHF and SATCOM. Combined with sophisticated algorithms, the multi-modal devices provide communication redundancy and cost optimization, resulting in lower operating costs than a SATCOM-only solution, and higher reliability than a VHF- or GSM-only solution. Through the use of specialized protocols, even intentional disruption of communications (such as disconnection of OBU antennas) can be detected by the operations center in near-real-time.

Satellite Communications Providers

Each candidate SATCOM provider reviewed in this section has characteristics that make it well suited to particular applications and geographical regions. Although both Geostationary (GEO) and Low-Earth Orbit (LEO) commercial satellite communication providers are available, only LEO satellite systems will be discussed. LEO satellite systems (up to 1,500km in altitude) offer the following advantages over GEO systems (orbit of an altitude of 35,800km) for tracking applications:

- LEO systems provide better quality of service to low-powered mobile user equipment;
- LEO systems can make use of low-cost portable, omni-directional antennas instead of bulky expensive directional antennas used with GEO systems; and
- LEO systems offer better survivability due to constellation rotation if a satellite fails. GEO satellite failure could result in regional system outage.

Tables 1-3 summarize operational characteristics of the various SATCOM systems that have been considered.

Orbcomm

Orbcomm is packet-switched two-way satellite communication system with a space segment consisting of a constellation of 63 LEO satellites and a ground segment consisting of a number of Gateway Earth Stations (GES) and Gateway Control Centers (GCC) located throughout the world. The Orbcomm system operates in the VHF part of the spectrum between 137-150Mhz. All communications within the Orbcomm system must pass through a gateway (a GES and GCC). Orbcomm provides four data service elements (ORBCOMM Global, 1999): Data Reports of 6 bytes (subscriber originated), Commands of 5 bytes (subscriber terminated), Messages of about 100 bytes and GlobalGrams, which are packets that are sent or received when the visible satellite does not have access to an Orbcomm gateway.
A GlobalGram packet is stored in satellite memory until the satellite can establish contact with a gateway. In the case of a subscriber-terminated packet, the packet is received from the gateway and stored in memory until contact with the subscriber is possible, and the subscriber requests it. Inherit in this type of store-and-forward functionality is the high latency of communications, which is unacceptable for some critical applications.

When data are sent as a Message, the subscriber and gateway must both be in line-of-sight of a satellite, resulting in lower latency communications. The suitability of this system for critical applications depends on the region and availability of a gateway. Figure 1 illustrates the global coverage of the Orbcomm satellite constellation.

Table 1. Orbcomm Characteristics

Type	Data only.
Coverage	Approx 84.6 percent actual coverage using Globalgram mode (store and forward); significantly less coverage using gateway mode, as a given satellite must have line of sight to both user equipment and a gateway.
Bandwidth	2.4 Kbps uplink; 4.8 Kbps downlink
Pros	Low cost hardware. Low cost data service.
Cons	Occasional coverage holes, which can be severe depending on geographical region and messaging mode. High latency in GlobalGram mode.

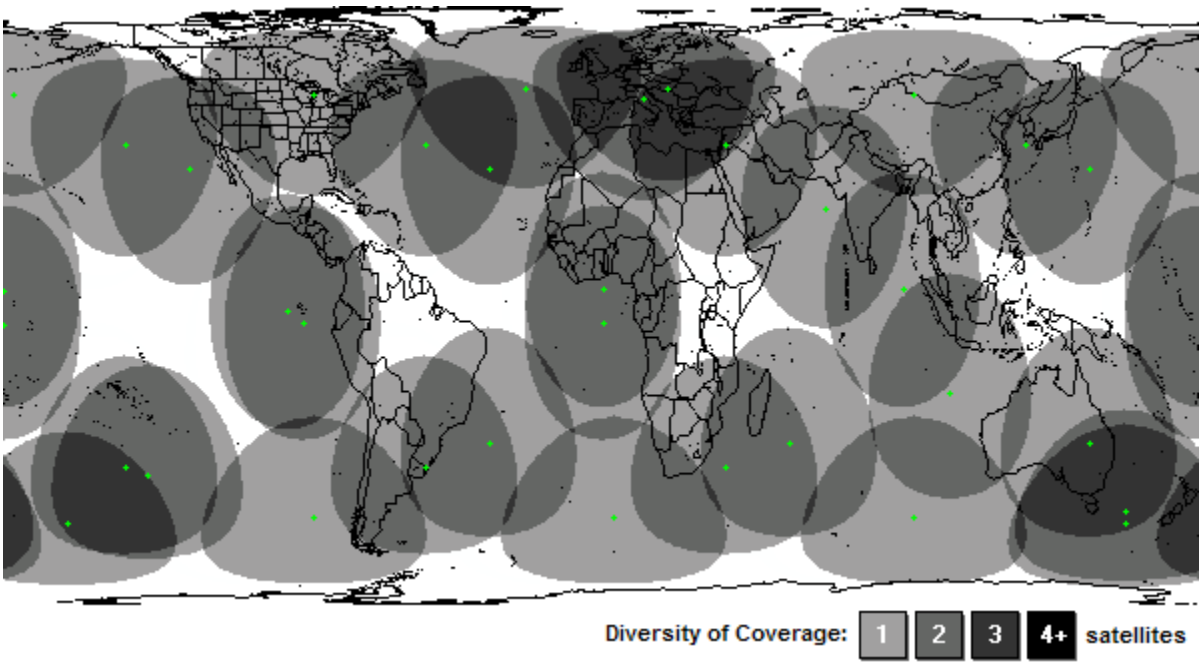

Figure 1: Orbcomm Satellite Constellation Global Coverage
(Source: Frame from a SaVi simulation (Worfolk and Thurman, 2006))

Globalstar

Globalstar is a LEO satellite network providing both voice and data services. The system consists of a space segment of 48 satellites, a ground segment comprising multiple gateways and ground operations control centers. Path diversity, in which calls are routed through as many as four satellites, is responsible for the high level of reliability, reducing the likelihood of a call being dropped. Globalstar supports voice and a number of data services including short message (SMS), asynchronous data and packet data services. Figure 2 illustrates the global coverage of the Globalstar satellite constellation. Although the coverage illustrated appears to be quasi-complete, it is in fact limited to where user-equipment has line-of-sight of both a satellite and a gateway[1].

[1] Refer to http://www.globalstareurope.com for a map of the effective coverage of Globalstar.

Table 2. Globalstar Characteristics

Type	Voice / Data.
Coverage	Approx 96.4 percent actual satellite coverage; however, effective coverage is much lower as a given satellite must have line-of-sight to both user equipment and a gateway. No coverage at poles.
Bandwidth	Full-duplex 9.6 Kbps.
Pros	High reliability. Relatively high data rate.
Cons	Lower effective coverage.

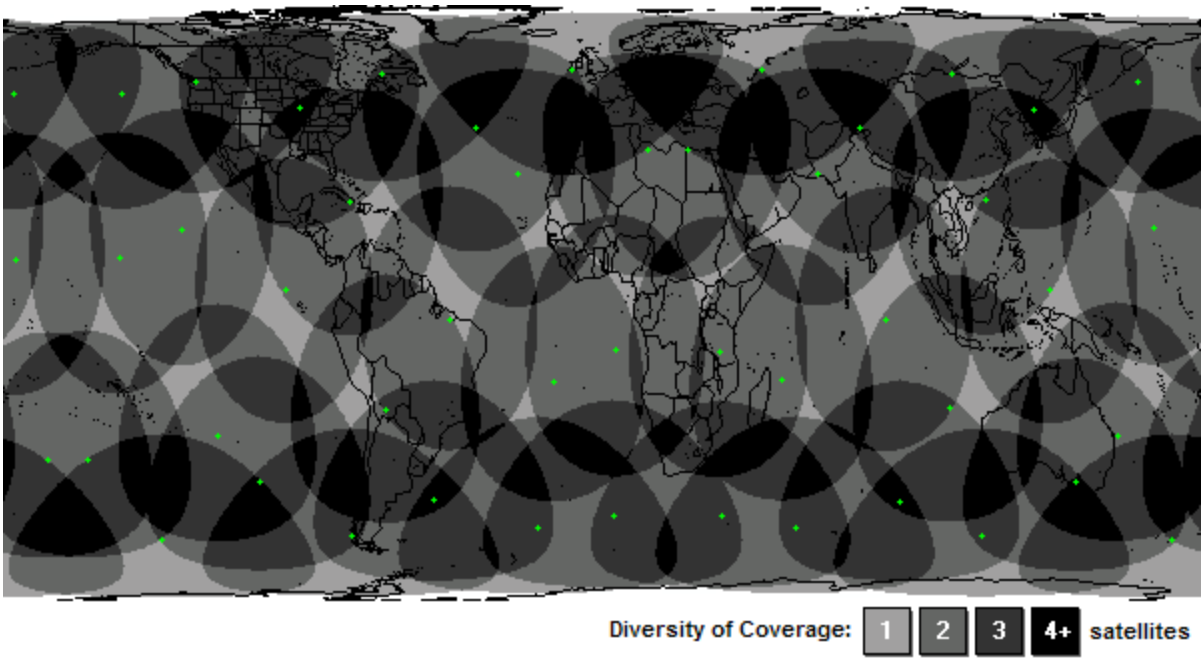

Figure 2. Globalstar satellite constellation global coverage
(Source: Frame from a SaVi simulation (Worfolk and Thurman, 2006))

Iridium

Iridium is a LEO satellite network with a constellation of 66 satellites, three terrestrial gateways and a satellite network operations center. It is the only service with 100 percent complete coverage including oceans, airways and Polar regions (See Figure 3). Unlike Globalstar and Orbcomm, which are both based on bent-pipe technology, Iridium employs an intra-satellite link architecture such that the satellites are able to communicate both with gateways and between themselves, alleviating the need for regional gateways. The intra-satellite link architecture additionally supports end-to-end communications between two users after initial call set-up, without passing though ground stations. This facilitates global coverage with low signal latency. Iridium supports voice and numerous types of data services. Among the data services, there are short message (SMS), dial-up data, direct Internet, router-based unrestricted digital interworking connectivity solution (RUCIDS) and short burst data (SBD) services. The Iridium network additionally supports the same security algorithms for authentication and encryption that GSM does. (Iridium Satellite LLC, 2003)

Table 3. Iridium Characteristics

Type	Voice / Data.

Coverage	100 percent.
Bandwidth	Full-duplex 2.4 Kbps (up to 8 Kbs with data compression).
Pros	100 percent coverage. Low signal latency. Lower-cost hardware due to low power requirement.
Cons	Relatively low bandwidth.

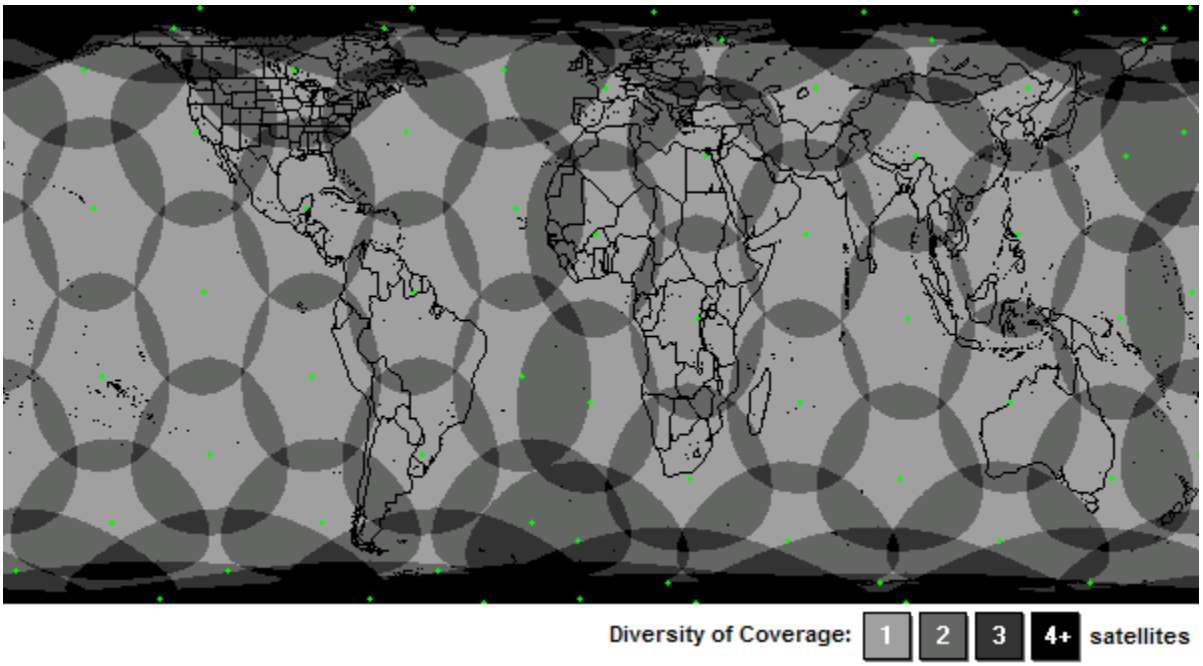

Figure 3. Iridium satellite constellation global coverage
(Source: Frame from a SaVi simulation (Worfolk and Thurman, 2006))

Integration of Communication Technologies

A flexible architecture has been developed to support the requirements of companies seeking a robust tracking solution. The tracking system is developed around a middleware platform, which provides secure end-to-end communications with onboard units (OBUs) and exposes access to OBU functions and its geographical database through web services.
Multi-modal communications is achieved by algorithms that are located both on the OBU and the middleware, ensuring data received is consistent. Algorithms that detect the performance of a given data channel are used in order to route data based on channel performance and message priority. While the middleware can support any number of different communication protocols and paradigms, the OBUs were developed with two modes of operation: SMS and packet mode.

SMS Mode

SMS mode can operate with both GSM and Iridium, as illustrated in Figure 4 and Figure 5. GSM is used in preference to Iridium to reduce communication costs. Where General Packet-Radio Service (GPRS) is not supported, SMS mode is used with GSM. An SMSC gateway facilitates access to the messages from the middleware. Where there is no GSM coverage, or the SMS Internet gateway is offline, point-to-point Iridium SMS messages provide complete independence from terrestrial infrastructure. High-priority and emergency messages can be configured to use Iridium messaging by default.

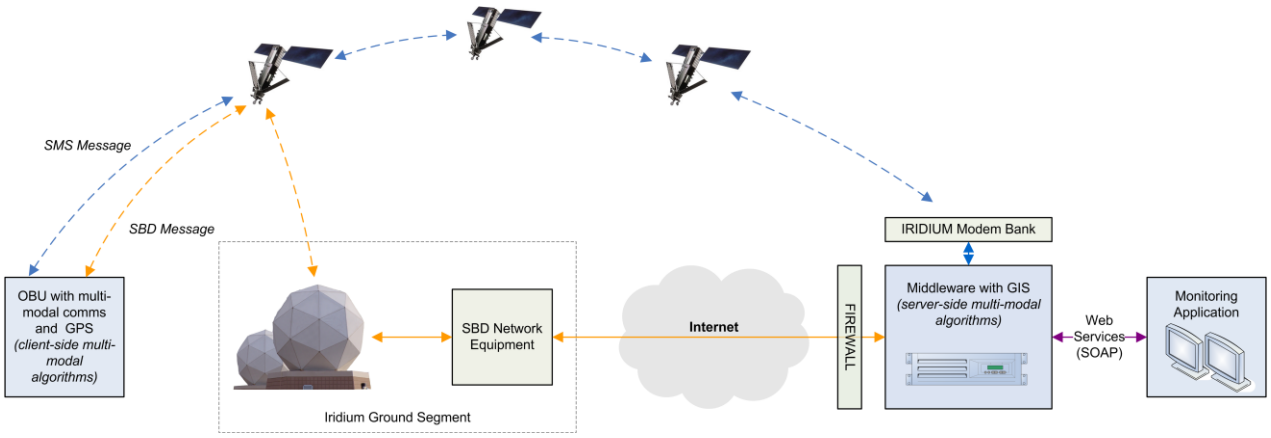

Figure 4: Tracking with Iridium

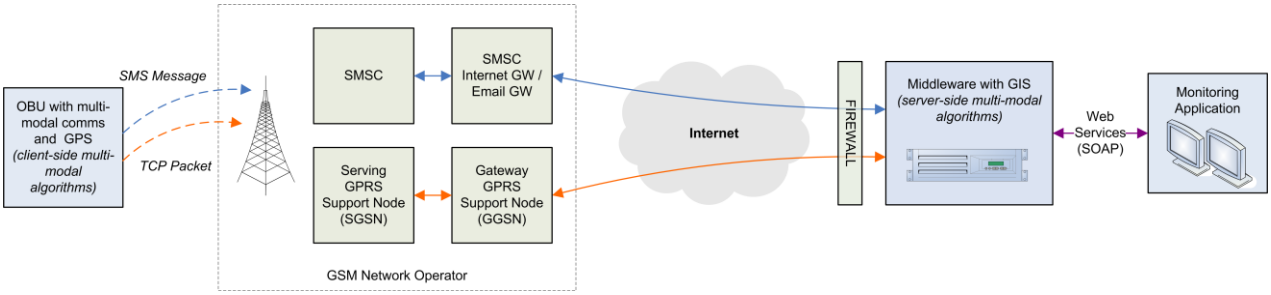

Figure 5. Tracking with GSM

Packet Mode

Packet mode provides lower-cost messaging via GSM GPRS or Iridium SBD service. Messages from both services are accessed via the Internet, and represent the mode of communications used for the majority of communications.

In addition to data services, Iridium and GSM both offer push-to-talk voice capability for communication with a person or driver in an emergency situation. Both technologies support the use of voice and data services simultaneously.

Secure GNSS Technologies

There are two types of disruption that can affect the integrity of a Global Navigation Satellite System (GNSS) system: unintentional and intentional. The former is caused by signal interference in space or on the ground, transmission errors and hardware failures. Unintentional disruptions (excluding unintentional jamming) of GNSS can be mitigated by a myriad of systems, including space-based augmentation systems (WAAS, EGNOS); ground-based augmentation systems (DGPS, marine radio beacons); and a number of privately operated services providing improved accuracy and integrity. GPS augmentation systems can be used to provide integrity and availability to civilian GPS. WAAS and EGNOS both provide ranging signals that can be used by a GPS receiver as if there were a part of the GPS constellation. WAAS notifies all users within 6 seconds of a problem with any satellite in the GPS

constellation, including the WAAS signal itself. This type of integrity indicates malfunctions and physical disturbances. It provides information on the health of the satellite constellation and augmentation system, but does not provide cryptographic integrity or authentication of the data source.
Intentional disruption, however, cannot be effectively mitigated by existing augmentation systems. Intentional disruption can represent a real threat against safety-critical applications such as hazardous-materials tracking. This imminent threat in the civilian domain by terrorists, hackers and adversaries engaging in telecommunication warfare has generated the demand for GNSS technologies able to prevent or provide mitigation strategies against intentional disruption. Refer to (John A. Volpe National Transportation Systems Center, 2001) for detailed information on GPS vulnerabilities in the transportation infrastructure. Intentional disturbances range from GPS jamming to spoofing of the GPS signal and GPS augmentation data.
GPS Course Acquisition (C/A) code transmitted on the L1 frequency is very weak (typically -130dBm at the antenna) and as such, relatively easy to jam. GPS jammers generate noise on the L1 band and corrupt the original signal, causing errors in acquisition and tracking. It is well known that a 1-watt (cellular phone-size) jammer can be built from readily available schematics, and can prevent a good quality civilian receiver from acquiring the C/A code from distances as far as 60 km. This is a significant threat for critical tracking applications; however anti-jamming antennas are typically too expensive for tracking applications. If sufficiently critical, anti-jam antennas should be considered.
GPS spoofing is significantly more difficult than jamming and has the intent cause a GPS receiver to lock on to signal(s) that appear legitimate in order to mislead the targeted user. (John A. Volpe National Transportation Systems Center, 2001) notes that at present there are no practical mitigation methods available for spoofing attacks, and that a few potentially effective techniques would be too expensive for civilian applications, in particular intelligent transportation systems. It is additionally noted that until civilian solutions are available, training of users and operators of intelligent transportation systems about GPS disruption, detection and alternative providers is crucial to minimizing the impact of GPS degradation or disruption.
A number of simple navigation checks such as the following, can be performed using commercial-off-the-shelf receivers and could provide effective mitigation to short-term disruption:

- Continuity checking of time and position;
- Use of a trusted clock to detect time drift associated with spoofing;
- Use of navigation sensors such as inertial measurement units (IMUs) to detect anomalies; and Validation of the navigation solution, checking for large residual errors.

The use of inertial measurement units (IMUs) integrated with GPS is recommended, not only for detecting anomalies, but as a redundancy measure in case the GPS signal becomes temporarily unavailable for short time periods.

Next-Generation GNSS

The modernization of GPS and the development of the new Galileo satellite navigation system will provide a number of new civil services over multiple frequencies with improved accuracy, integrity and security. These new services will act as an enabler for systems that provide certified levels of security and integrity.
The risk of Jamming can be decreased through the use of these services, as the likelihood of signals on different frequencies of both GPS and Galileo being simultaneously jammed is reduced, however, not impossible. In addition the use of multiple GNSS provides improved mitigation against control-segment problems.

The next-generation GPS will provide new civilian services on the L2 and L5 frequency bands. Galileo will provide four navigation services on the L1, E5 and E6 bands, three of which are for civilian use. The Open Service (OS) will be accessible to all users without a usage fee. The Safety of Life service will provide the same position and timing accuracy as the OS with the broadcast of integrity information and guaranteed service levels. The Commercial Service (CS) will provide higher performance than that of the OS and a limited data broadcasting capability for market applications for a fee. Access to CS data will be controlled through the use of Navigation Data Encryption (NDE). Encrypted CS data will be present in the E1-B, E5b and E6-B signal data channels. Access to the E6 signal (with the exception of the E6-A) channel will be controlled through the use of Spreading Code Encryption (SCE). The Public Regulated Service (PRS) will provide position and timing to governmental applications. Access to the PRS will be restricted through the use of SCE.
Table 4 lists the security services projected to be included on each signal in Galileo. To date there is no indication that any security services will be provided to civilian users. (Refer to the OS Interface Control Document (European Space Agency, 2006) for details of the Galileo signals and services)

Table 4. Galileo Signals

Signal	Channel	Type	SCE	NMA	NDE	Service
E2-L1-E1	$E2\text{-}L1\text{-}E1_B$	Data	No	No	CS data	OS / SoL / CS
E2-L1-E1	$E2\text{-}L1\text{-}E1_C$	Pilot	No	--	--	OS / SoL / CS
E5a	$E5a_I$	Data	No	No	No	OS / SoL
E5a	$E5a_Q$	Pilot	No	--	--	OS / SoL
E5b	$E5b_I$	Data	No	No	CS data	OS / SoL / CS
E5b	$E5b_Q$	Pilot	No	--	--	OS / SoL / CS
E6	$E6_B$	Data	Yes	No	Yes	CS
E6	$E6_C$	Pilot	Yes	--	--	CS

While the Galileo high-level mission definition (European Space Agency, 2002) and design consolidation (Galilei Consortium, 2003) indicated that NMA may be incorporated into the OS, the first public draft version of the OS Interface Control Document (ICD) (European Space Agency, 2006) does not include provision for such a service.
While the details of the CS are yet to be publicly released, the CS could be potentially useful for tracking in critical applications. The CS could be used to mitigate the risk of spoofing and provide high quality of service and integrity guarantees. A CS receiver, being a multi-frequency receiver, would also have a level of immunity to non-intentional jamming.

GNSS Security Services

GNSS security services can be used for a wide range of purposes, including cryptographic signal validation, which provides strong integrity and quality of service guarantees to applications. Security services for GNSS can be categorized into the following three classes (Wullems et al., 2005):

Navigation Data Authentication and Cryptographic Integrity Protection Mechanisms

Navigation Message Authentication (NMA) is a mechanism designed to overcome spoofing and to provide increased safety and service guarantees. An NMA scheme would add authentication messages to the navigation message stream, both authenticating the source and providing cryptographic integrity protection of the navigation data.
Should an adversary attempt to generate or change the navigation data, a receiver would be able to detect the activity. An adversary would not be able to simulate the authentication message, as he would not have the keys required to generate them.

Signal Access Control Mechanisms

A signal access control mechanism facilitates restriction of access to the signal from unauthorized users. GPS and Galileo signals use Direct Sequence Spread Spectrum (DSSS) and Code-Division Multiple Access (CDMA). Access to the signal can be restricted through Spreading Code Encryption (SCE), in which the spreading code is protected using cryptography. Only users with the appropriate cryptographic keys are able to generate/obtain the secret spreading code which then allows de-spreading of the signal.

SCE in combination with NMA, provides the best protection against spoofing. SCE alone can provide protection from spoofers so far as the keys or cryptographic algorithms used to decrypt/generate the spreading code are secure. A spoofer with access to the spreading code, either legitimately or illegitimately could potentially spoof other users of the signal.

Navigation Data Access Control Mechanisms

A navigation data access control mechanism facilitates restriction of access to parts or all of a navigation data stream modulated over a given signal through encryption. Navigation Data Encryption (NDE) can be used to support various value-added services.

Conclusion

Secure tracking serves to improve safety by enforcing route compliance and providing protection from theft. This paper has addresses a number of requirements for secure tracking systems from onboard unit integrity to wireless communication systems and global satellite navigation systems. Wireless communication systems and GPS represent the most significant points of failure in tracking systems. While there are numerous options for wireless communications systems (many networks, terrestrial and satellite-based) and a certain level of maturity for communications security, GPS does not offer the same guarantees or cost-effective backup solutions, and is perhaps destined to become more vulnerable to attacks that it's communications counterparts. It is nearly certain that Galileo will have a big impact, on both performance and security in this arena.

We predict that the future of GNSS security will most likely be analogous to trends seen in IT security. As IT technologies grew, the number of attacks and sophistication of these attacks increased at alarming rates. GPS analysts have been led to believe that an increase of attacked (such as spoofing) is improbable due to their inherent complexity. However, the rapid growth of GNSS applications in recent years and the future projected growth will likely increase the number of applications where security exploits could result in financial reward, risk to life, or cause financial damage. In addition, the cost of equipment that can be used to mount attacks has dropped significantly and will most likely continue to reduce. This combination of effects will inevitably result the increase of attacks against GNSS dependant applications in the future.

References

ORBCOMM Global, L. P. 1999. ORBCOMM System Overview.

John A. Volpe National Transportation Systems Center 2001. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System.

European Space Agency 2002. GALILEO Mission High Level Definition.

Galilei Consortium 2003. The Galilei Project: GALILEO Design Consolidation.

Iridium Satellite LLC 2003. Iridium Satellite Data Services White Paper.

Wullems, C., Pozzobon, O. and Kubik, K. 2005. Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems. European Navigation Conference (ENC-GNSS 2005) Vol. Munich, Germany.

Worfolk, P. and Thurman, R. 2006. SaVi - Satellite Constellation Visualization. The Geometry Center, University of Minnesota, http://savi.sf.net/.
European Space Agency 2006. Galileo Open Service - Signal in Space Interface Control Document (OS SIS ICD/D0).