THE GNSS ASSIMILATOR: A METHOD FOR UPGRADING EXISTING GNSS USER EQUIPMENT TO IMPROVE ACCURACY, ROBUSTNESS, AND RESISTANCE TO SPOOFING

TODD E. HUMPHREYS
THE UNIVERSITY OF TEXAS AT AUSTIN
BRENT M. LEDVINA
COHERENT NAVIGATION

Abstract. A method is presented for upgrading existing Global Navigation Satellite System (GNSS) user equipment, without requiring hardware or software modifications to the equipment, to improve the equipment's position, velocity, and time (PVT) accuracy, to increase its PVT robustness in weak-signal or jammed environments, and to protect the equipment from counterfeit GNSS signals (GNSS spoofing). The method is embodied in a device, herein termed the GNSS Assimilator or simply the Assimilator, that couples to the radio frequency (RF) input of existing GNSS equipment, such as a GPS receiver. The Assimilator extracts navigation and timing information from RF signals in its environment—including non-GNSS signals—and from direct baseband aiding provided, for example, by an inertial navigation system, a frequency reference, or the GNSS user. The Assimilator optimally fuses the collective navigation and timing information to produce a PVT solution which, by virtue of the diverse navigation and timing sources on which it is based, is highly accurate and inherently robust to GNSS signal obstruction and jamming. The Assimilator embeds the PVT solution in a synthesized set of GNSS signals and injects these into the RF input of a target GNSS receiver for which an accurate and robust PVT solution is desired. The code and carrier phases of the synthesized GNSS signals can be aligned with those of the actual GNSS signals at the input to the target receiver. Such phase alignment implies that the synthesized signals appear exactly as the authentic signals to the target receiver, which enables a user to "hot plug" the Assimilator into a target receiver with no interruption in PVT. Besides improving the PVT accuracy and robustness of the target receiver, the Assimilator also protects the target receiver from GNSS spoofing by continuously scanning incoming GNSS signals for signs of spoofing, and, to the extent possible, eliminating spoofing effects from the GNSS signals it synthesizes.

1. Background

There exist in both military and civil sectors hundreds of thousands of Global Navigation Satellite System (GNSS) receivers that are immediately rendered inoperable by signal obstruction or jamming. A majority of these receivers are also vulnerable to spoofing, a pernicious type of intentional interference whereby a GNSS receiver is fooled into tracking counterfeit GNSS signals. In many cases, the GNSS receivers are coupled to avionics, communication, measurement, or other equipment that depends crucially on the timing signals or navigation data that the GNSS receiver provides. When the steady stream of position, velocity, and time (PVT) data on which this equipment relies is interrupted due to signal obstruction or jamming—or, worse yet, when the PVT data are surreptitiously commandeered by a spoofer—the dependent equipment can cease to function or can malfunction, with potentially disastrous consequences.

Apart from their vulnerability to signal obstruction, jamming, and spoofing, most existing GNSS receivers are incapable of tracking modern GNSS signals and so cannot take advantage of the higher accuracy and availability these signals offer.

Date: November 27, 2009.

The GNSS Assimilator addresses the foregoing shortcomings of existing user GNSS equipment by augmenting, not replacing, the equipment. The augmentation requires no hardware or software modification to the existing equipment—the Assimilator simply attaches to a GNSS receiver's radio frequency (RF) input port and injects a consistent set of synthesized GNSS signals whose implied PVT solution is robust, accurate, and spoof-free.

The Assimilator is a cost-effective alternative to replacing existing user equipment for users who want a PVT solution that is robust against GNSS signal obstruction, jamming, and spoofing, or who want access to the benefits of GNSS modernization.

The following subsections highlight the GNSS Assimilator's application in three focus areas: signal obstruction or jamming, spoofing, and GNSS modernization.

1.1. **Signal Obstruction or Jamming.** When the signal-to-noise ratio within a GNSS receiver falls below a certain threshold, either because the GNSS signal is obstructed or because a jamming attack is underway, the user is met with a "Need clear view of sky" or similar notice from the receiver. At this point the receiver-produced PVT data either rapidly deteriorate in accuracy or the data stream abruptly halts. Obviously, a better outcome in such weak-signal or jammed environments would be for the receiver-produced PVT data to deteriorate only mildly, if at all. This is what is meant by robust PVT.

When coupled to the GNSS Assimilator, existing GNSS user equipment would be capable of delivering robust PVT. This is because the Assimilator is not limited to deriving PVT information from, for example, GPS signals. Rather, it behaves opportunistically, extracting navigation and timing information from other RF signals in its environment—including those from other GNSS—or from baseband data sources such as an inertial navigation system, an external synchronization signal, or from the user himself.

Some of the additional RF signals available to the Assimilator will be radionavigation signals (e.g., other GNSS or eLoran signals) whose signal-to-noise ratio happens to be higher than those the target receiver is natively capable of tracking, whether because the signals are unobstructed, or intrinsically of higher power, or because their carrier frequency falls outside the jammed frequency range. Yet other available RF signals may not be radionavigation signals as such, but may nonetheless carry implicit navigation or timing data. For instance, it has been shown that television signals [U.S. Patents 7,463,195, 7,372,405, and 7,042,949], cellular telephone signals [U.S. Patents 6,327,473 and 7,053,824], and satellite communication signals [U.S. Patent Applications 20080001819 and 20080062039] can be exploited for navigation and timing.

From available navigation- or time-bearing RF signals, or from baseband data input by the user or by external devices, the Assimilator optimally estimates its PVT state. Consistent with this PVT state, it continuously generates a target-receiver-compliant set of RF GNSS signals and injects this into the target receiver's RF input. To generate the synthesized GNSS signals, the Assimilator employs a GNSS signal simulator whose timing is synchronized to the Assimilator's bank of radionavigation receivers. For embedded applications, the GNSS signal simulator can be implemented together with the Assimilator's other components on a single digital signal processor.

In one embodiment of the Assimilator, the embedded GNSS signal simulator is a special phase-coherent GNSS signal simulator capable of replicating ambient authentic GNSS signals and phase-aligning to these. Such phase alignment implies that the synthesized signals appear exactly as the authentic signals to the target receiver, which means that the Assimilator can be seamlessly "hot plugged" into a target receiver without interrupting or degrading the target receiver's PVT solution.

In a complete GNSS signal blackout, the PVT data produced by the coupled Assimilator and target receiver will eventually degrade, but by leveraging non-GNSS navigation and timing sources, the Assimilator limits this degradation substantially.

1.2. **Spoofing.** All stand-alone commercial civilian GNSS receivers available today are trivial to spoof. One simply attaches a power amplifier and an antenna to a GNSS signal simulator and radiates the RF signal toward the target receiver. A successful attack along these lines was handily demonstrated by researchers at Argonne National Laboratories in 2002 [1]. More recently, successful spoofing attacks against several civil GNSS receivers have been mounted from a powerful yet inexpensive experimental spoofing platform [2–4].

Military-grade GNSS receivers are capable of operating in a spoof-resistant mode in which the receiver tracks an encrypted ranging code whose pattern is unpredictable except to compliant and keyed user equipment. However, in practice, many military personnel fail to maintain the cryptographic keys in their GNSS user equipment or prefer to carry civil GNSS receivers [5], with the result that a large fraction of GNSS receivers in military service are vulnerable to spoofing.

The Assimilator detects the presence of GNSS spoofing by employing detection methods like those described in [2–4] and by validating incoming GNSS signals against other available navigation and timing sources, such as those described in Section 1.1. Once it detects a spoofing attack, the Assimilator alerts the user and excludes the spoofing signals from its internal PVT estimate. The synthesized GNSS signals that the Assimilator continuously sends to the target receiver are accordingly spoof-free, and the target receiver is protected from the spoofing attack.

In an alternative embodiment, the Assimilator incorporates a full GPS Selective Ability Anti-Spoofing (SAASM) module, thereby providing military-grade spoofing protection to any target receiver, whether military or civil. This option would be attractive, for example, to military users who demand military-grade security against spoofing but prefer the user-friendly interface of commercial civil user equipment.

In another embodiment, the Assimilator initially acts as a stand-alone spoofing detector, uncoupled from any target receiver. When a spoofing attack is detected, the Assimilator raises an alarm and an unprotected GNSS receiver can then be coupled to the Assimilator for protection against the attack. This embodiment would be attractive to users who are wary of spoofing but who otherwise prefer an untethered GNSS receiver.

1.3. **GNSS Modernization.** Modernized GPS, which offers a 10-fold improvement in civil ranging precision, improved military signal precision and integrity, and greater frequency diversity than legacy GPS, is well underway [6]. Moreover, the Russian GLONASS system is rapidly being replenished and will soon reach full operational capability; the Chinese Beidou/Compass system has an ambitious launch schedule that will populate the constellation within the next few years; and, despite some initial setbacks, the European Galileo system will likely be fully deployed within the next decade.

To directly harness the improved accuracy, availability, and redundancy that these modern GNSS offer, military and civilian GNSS users currently have no option but to declare their existing equipment obsolete and replace it, at significant expense, with newer equipment. The Assimilator changes this situation by delivering the benefits of GNSS modernization through augmentation, rather than replacement, of existing user equipment. The Assimilator can be configured to track all available modern GNSS signals. From these it estimates a highly accurate PVT solution that it embeds in a set of synthesized GNSS signals with which the target GNSS receiver is natively compliant. The synthesized GNSS signals are generated by the signal simulator mentioned in Section 1.1 and injected into the RF input of the target GNSS receiver.

When coupled to a narrowband target GNSS receiver (an L_1 C/A GPS receiver, for example), the Assimilator cannot pass on the full ranging precision of modern wideband civil signals such as the GPS L_5 and the Galileo E_{5a} and E_{5b} signals. Nonetheless, the Assimilator significantly compensates for this limitation by synthesizing GNSS signals whose strong geometry and high signal-to-noise ratio yield a high-precision PVT solution. Furthermore, the Assimilator is able to pass on the improved

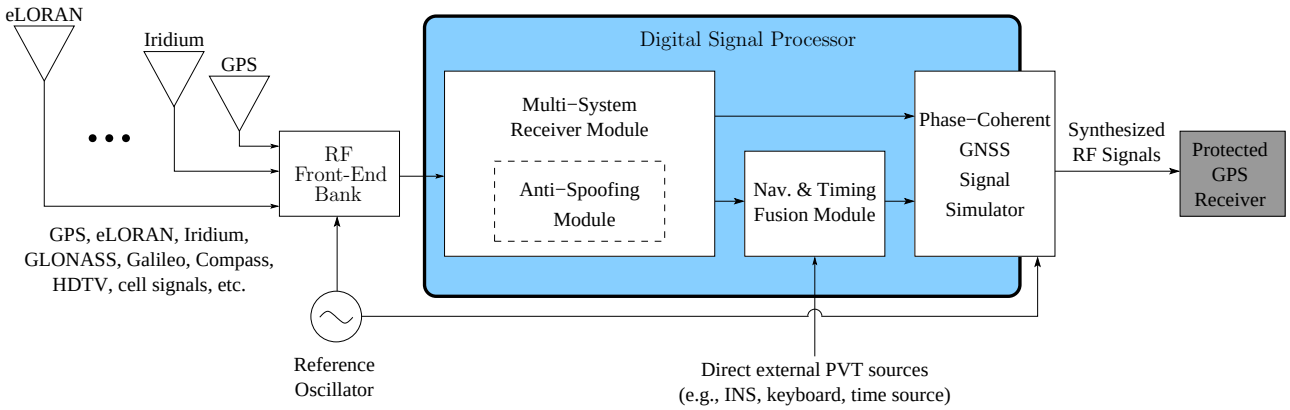

FIGURE 1. Functional block diagram of the GNSS Assimilator.

multipath immunity and orthogonality that modern GNSS signals offer, and, because it tracks signals at multiple GNSS frequencies, it can substantially eliminate ionospheric errors from the GNSS signals it synthesizes. Considering these benefits, one can readily appreciate that the PVT solution of an Assimilator-aided legacy single-frequency narrowband target receiver will be nearly as accurate as that of a modern multi-frequency wideband GNSS receiver.

Augmentation with the Assimilator is cost-effective in every case where the Assimilator itself is less expensive than replacing existing user equipment with a new model as capable as the Assimilator-receiver pair.

2. DETAILED DESCRIPTION

The GNSS Assimilator, a functional block diagram of which is shown in Figure 1, is a device with one or more RF input ports and one RF output port. Antennas connected to the RF input ports receive navigation- or time-bearing RF signals present in the Assimilator's environment. Another input is available for receiving external PVT information provided at baseband such as inertial measurements, a time synchronization pulse, or PVT input from a user. The Assimilator's RF output port is connected to the RF input of an existing GNSS receiver (the target receiver). By extracting navigation and timing information from the incoming RF signals and from the baseband PVT input, and by incorporating an anti-spoofing module (described in Section 2.1), the GNSS Assimilator provides robust and accurate PVT and spoofing protection for the target receiver.

The Assimilator comprises:

(1) A digital signal processor on which the multi-system receiver module, the navigation and timing fusion module, and the digital processing component of the embedded GNSS signal simulator are all implemented. (The embedded GNSS signal simulator is depicted in Fig. 1 as residing partly outside the digital signal processor because it includes an external RF upconversion component.)
(2) A bank of RF front ends that filters, mixes, and digitizes electromagnetic navigation- or time-bearing signals in the vicinity of the Assimilator, including, but not limited to
   (a) GPS signals
   (b) Galileo signals
   (c) GLONASS signals
   (d) Beidou/Compass signals
   (e) SBAS signals (e.g., WAAS, EGNOS)

(f) Loran signals
(g) eLoran signals
(h) Iridium signals
(i) HDTV signals
(j) Cellular telephone signals
(k) WiFi signals
(l) NIST timing signals

The output of the RF front-end bank is a stream of digital data samples that is routed to the multi-system receiver module. For synchronization, the RF front-end bank and the embedded GNSS signal simulator are tied to the same reference oscillator.

(3) A multi-system receiver module 5 capable of processing and extracting navigation and timing data from a diverse set of RF signals whose combined digitized data are output by the RF front-end bank. GNSS carrier and code phase measurements and GNSS carrier frequency measurements produced by the multi-system receiver module are routed to the embedded signal simulator for phase alignment of the synthesized GNSS signals. The multi-system receiver module is a software radio based on techniques such as those described in U.S. Patents 7,010,060 and 7,305,021 and in [7].
(4) The anti-spoofing module described in Section 2.1 as a subcomponent of the multi-system receiver module.
(5) An input for receiving external baseband PVT information 16 (external PVT input). This input may come, for example, from an inertial navigation system, an external clock, or a keyboard.
(6) A navigation and timing fusion module that employs optimal estimation techniques to combine the PVT data from the external PVT input with navigation and timing observables extracted from the signals in item 2 to produce a robust PVT solution that serves as an input to the embedded GNSS signal simulator described in Section 2.2.
(7) The embedded GNSS signal simulator described in Section 2.2.

The following subsections provide further details on the anti-spoofing module and the embedded signal simulator.

2.1. **Anti-Spoofing Module.** The anti-spoofing module continuously analyzes the data stream entering the Assimilator to detect spoofing signatures. If a spoofing attack is detected, the anti-spoofing module asserts an indicator. The anti-spoofing module employs one or more of the following techniques to detect the presence of spoofing:

(1) The data bit latency defense [3].
(2) The vestigial signal defense [3].
(3) The multi-antenna angle-of-arrival defense [4].
(4) A civil GPS cryptographic defense that requires changes to the broadcast GPS signals or the wide-area augmentation signals (WAAS) (e.g., [8, 9]).
(5) A civil GPS cryptographic defense that does not require changes to the broadcast GPS signal nor to WAAS [10].
(6) A cryptographic defense based on incorporating a SAASM-type (i.e., military-grade) GPS receiver into the anti-spoofing module.

2.2. **Embedded GNSS Signal Simulator.** The embedded GNSS signal simulator is a GNSS signal simulator whose digital signal processing component can be implemented along with the multi-system receiver module and the navigation and timing fusion module on a single digital signal processing

platform. The simulator generates multiple GNSS signals whose implied navigation and timing solution is consistent with a commanded position, velocity, and time. This is the operation of a standard GNSS signal simulator [U.S. Patent 5,093,800].

In one embodiment of the Assimilator, the embedded GNSS signal simulator is a specialized phase-coherent GNSS signal simulator. This type of simulator generates multiple GNSS signals that, if broadcast from the location of the simulator's radio frequency output, would have carrier and code phases that are aligned with the carrier and code phases of the corresponding authentic GNSS signals at an arbitrary nearby location specified by the user. This specialized phase-coherent capability would enable the user to "hot plug" the Assimilator into a target receiver. In other words, the Assimilator could be coupled a target receiver that is already tracking or was recently tracking GNSS signals without interrupting or degrading the target receiver's PVT solution.

3. Comparison with Alternative Methods

The GNSS Assimilator will be compared with alternative methods in each of the following focus areas: signal obstruction or jamming, spoofing, and GNSS modernization.

3.1. **Signal Obstruction or Jamming.** There are many techniques for improving a GNSS receiver's immunity to jamming and its ability to track obstructed (weak) GNSS signals. A common goal of these techniques is to extend the interval of time over which the GNSS receiver is able to perform coherent or non-coherent integration [11]. Accordingly, there are techniques designed to stabilize the receiver's reference clock, either by improved oscillator technology or by exploiting an external aiding signal (e.g., U.S. Patents 7,239,857, 7,155,183, and 7,010,307); techniques for eliminating the phase ambiguity caused by the navigation data modulation, whether by internal prediction of the data bits or by external data bit aiding (e.g., U.S. Patents 6,327,473 and 7,053,824); techniques for incorporating data from inertial measurement units (e.g., [12]); techniques for implementing parallel correlation banks to reduce acquisition time (e.g., U.S. Patents 6,704,348 and 6,606,346); and systems that implement a combination of these techniques (e.g., U.S. Patent Applications 20080001819 and 20080062039).

A key characteristic of these techniques is that they must be built into GNSS user equipment at the time of manufacture or they require a specialized coupling between the receiver and external aiding sensors or signals. In contrast, the GNSS Assimilator can be used to upgrade any existing GNSS receiver because it couples to the target receiver through the receiver's standard RF input. No special connectors or interface protocols are required. All of the tight integration with external aiding sensors and signals happens within the Assimilator itself, upstream from the target receiver. Thus, any existing GNSS receiver can, without any hardware or software modification, be upgraded with weak-signal-tracking capability and reduced susceptibility to jamming.

Another distinction between the GNSS Assimilator and standard weak-signal-tracking and jamming-robust-tracking techniques is that the Assimilator enables the target receiver to continue operating even in the absence of GNSS signals. This is because the Assimilator can synthesize GNSS signals from any source of PVT information, including non-GNSS RF signals (e.g., eLoran & Iridium). The Assimilator extracts navigation and timing estimates from these "signals of opportunity" and can therefore withstand a complete blackout of all standard GNSS signals. This ability to synthesize GNSS signals on the basis of external non-GNSS PVT information, and then to phase-synchronize the synthesized signals with GNSS signals when they become available, is unique to the Assimilator.

3.2. **Spoofing.** Although there exist several civil anti-spoofing techniques [2–4, 8, 9, 13], no civil GPS receivers of which the authors are aware are currently equipped with these techniques or with any deliberate defenses against spoofing, and no manufacturer has disclosed plans to incorporate civil GPS spoofing defenses in the future. The Galileo system's proposed public regulated service would provide

a civil spoofing defense, but the service is years away at best and may never materialize if it becomes clear that users would rather accept the risks of the unencrypted but free GPS and Galileo signals than pay a premium for the public regulated service. Meanwhile, as far as the authors are aware, there are no proposals for retrofitting existing GNSS user equipment with anti-spoofing technology besides the proposed Assimilator.

GPS military receivers with SAASM technology are of course protected against spoofing, but these receivers are not necessarily designed to detect the presence of spoofing. Hence, the Assimilator's spoofing detection capability may be of value even to military users.

3.3. **GNSS Modernization.** The vast majority of existing civil GNSS receivers are consumer-grade single-frequency GPS receivers. The next largest class of civil receivers are survey-grade dual-frequency codeless or semi-codeless tracking GPS receivers. The hardware in these receivers cannot be practically modified to track modernized GNSS signals, leaving consumers who wish to exploit the improved accuracy, availability, and redundancy of modern GNSS no option but to declare their existing equipment obsolete and replace it with a newer model. Likewise, existing military GPS receivers, such as the popular DAGR, are incapable of tracking the modernized GPS military signals and would be impractical to retrofit for this purpose. The DAGR's manufacturer will no doubt recommend that military customers wishing to track modernized GPS signals replace the DAGR with modernized user equipment, at considerable expense to the military customer.

The Assimilator changes this situation by delivering the benefits of GNSS modernization through augmentation, rather than replacement, of existing user equipment—both commercial and military. The augmentation requires no hardware or software changes to the existing equipment, and is cost-effective in every case where the Assimilator is less expensive than replacing existing user equipment with a new model as capable as the Assimilator-receiver pair.

References

[1] J. S. Warner and R. G. Johnston, "A simple demonstration that the Global Positioning System (GPS) is vulnerable to spoofing," *Journal of Security Administration*, 2003.

[2] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat," *GPS World*, vol. 20, no. 1, pp. 28–38, Jan. 2009.

[3] ——, "Assessing the spoofing threat: development of a portable GPS civilian spoofer," in *Proceedings of ION GNSS 2008*. Savannah, GA: Institute of Navigation, 2008.

[4] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, vol. 4, no. 2, pp. 40–46, April 2009.

[5] D. Jewell, "DAGR, GAO furors," *GPS World*, vol. 20, no. 7, pp. 8–10, July 2009.

[6] T. E. Humphreys, L. Young, and T. Pany, "Considerations for future IGS receivers," in *Position Paper of the 2008 IGS Workshop*, 2008.

[7] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, and P. M. Kintner, Jr., "GNSS receiver implementation on a DSP: Status, challenges, and prospects," in *Proceedings of ION GNSS 2006*. Fort Worth, TX: Institute of Navigation, 2006.

[8] L. Scott, "Location Assurance," *GPS World*, vol. 18, no. 7, pp. 14–18, 2007.

[9] ——, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proc. ION GPS/GNSS 2003*. Portland, Oregon: Institute of Navigation, 2003, pp. 1542–1552.

[10] M. L. Psiaki, "Spoofing detection for civilian GNSS signals via aiding from encrypted signals," in *Accepted as an alternate paper at ION/GNSS 2009*. Savannah, GA: Institute of Navigation, sep 22-25 2009.

[11] A. J. Van Dierendonck, *Global Positioning System: Theory and Applications*. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1996, ch. 8: GPS Receivers, pp. 329–407.

[12] D. Gebre-Egziabher, "Design and performance analysis of a low-cost aided dead reckoning navigator," Ph.D. dissertation, Stanford University, Department of Aeronautics and Astronautics, 2001.

[13] "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," John A. Volpe National Transportation Systems Center, Tech. Rep., 2001.

E-mail address: todd.humphreys@mail.utexas.edu