Reliability and Availability of GPS Measures in Airport Landing Systems

V. Barrile, M. Cacciola, and F. Cotroneo
University "Mediterranea" of Reggio Calabria, Italy

Abstract—In the last decades, the modern airports have considerably increased the traffic to manage. Consequently, the requirement of technological solutions in order to control vehicles and airplanes in relevancy areas (such as parking area, taxiways and runways) is increased. Among various considered solutions, the more efficient ones use Global Positioning System receivers to establish location of moving objects into the airport. Thanks to this solution, it is possible to increase both the efficiency in runway usage and the safety in ground movements. Nevertheless navigational systems like Galileo or GLONASS cannot be considered as "high availability systems". For examples, positioning service can be interrupted by unintentional radiofrequency interferences, or terrorist attacks through techniques known as "antenna jamming" and "code contamination". In this paper, these problems are analyzed in the context of airplane ground control, and a secure system is suggested. Especially, technical solutions are adopted in navigational routines using Global Positioning System receivers, in order to improve reliability and security, and above all to guarantee a narrow range of variation for positioning for the whole necessary time.

1. Introduction

The most critical phase in a flight is surely the landing; therefore it is necessary to increase the safety of the aerial transportations, above all civil ones, by usage of some tools which aids the pilot during the landing phase, especially in condition of low visibility. The landing instrumentation used to assist pilots or integrated in an automatic landing systems offers different performances (precision, reliability, low latency of calculation) which are compatible with specific climatic conditions. Just to be able to well classify the different levels of risk, the International Civil Aviation Organization (ICAO) defines three categories of visibility for landing civil aircraft [1]:

1. Category I—Decision Height not lower than 200 ft and Runway Visual Range (RVR) not less than 1800 ft with appropriate runway lighting; Decision Height (DH) is the height above the runway at which the landing must be aborted if the runway is not in sight;
2. Category II—DH not lower than 100 ft and RVR not less than 1200 ft; the pilot must see the runway above the DH or abort the landing,
3. Category III - This category is subdivided into:
   - IIIA: DH lower than 100 ft and RVR not less than 700 ft;
   - IIIB: DH lower than 50 ft and RVR not less than 150 ft;
   - IIIC: Zero visibility, no DH or RVR limits.

In comparison to the traditional systems for landing assistance (i. e., Instrument Landing Systems, INS, and the Microwave Landing Systems), Satellite Landing Systems (and particularly the Global Positioning System, GPS) seem to answer in a more suitable way to the requisite of precision and inexpensiveness for all the categories of employment mentioned above. Nevertheless the GPS technology has some problems related to the nature of the used signal and to the data transmission protocol from satellites to receiver. In fact, GPS receivers are susceptible to attacks exploiting interference techniques on the spread-spectrum signals (i. e., jamming), such as Denial of Service (DoS) attacks; their purpose is to make unusable a determined service, i. e., GPS service, for a particular time interval. Moreover, a hacker can modify the C/A and P codes so that the position calculated by the receiver is not correct (spoofing attack). Therefore, it is necessary to integrate the GPS system with other devices in order to eliminate these problems, which constitute an enormous limit for the adoption of the Global Position System during the landing phase. In this paper, an hybrid GPS/INS navigational system is proposed in order to avoid spoofing and jamming attacks, and to increase the precision of GPS positioning. In section 2,

jamming attacks and our GPS/INS solution approach are described; subsequently, section 3 gives a panorama of spoofing attacks and analyses our mixed protocol to avoid "code contamination"; finally, at section 4, some conclusions are pointed out.

2. Jamming Attacks and Proposed Solution Approach

The GPS signal has low power and is vulnerable to interference. The dangerous means of interference go from cheap, expendable, low-power jammers which can be widely distributed across an area of conflict, to medium and high-power ground and air-based jammers which can deny usage of GPS over hundreds of miles. The interruption of GPS positioning service by a jamming attack is particularly simple to be caused during landing phase of an airplane: in fact it is sufficient to send an interference signal on a defined location and in a defined temporal window. Since a landing assistance tool must have as principal characteristic a high availability degree for the whole period of employment, a low cost solution to the jamming vulnerability has been integrated into the GPS, the so called Inertial Navigation System (INS) [3].

INS is accomplished by an Inertial Measurement Unit (IMU) which integrates the output of a set of sensors in order to compute position, velocity, and attitude. Sensors used are gyros and accelerometers. Gyros determine angular velocity respect to inertial space, while accelerometers evaluate linear acceleration respect to an inertial frame. Integration is a simple process; difficulties are due to various encountered coordinate frames, sensor errors, and system noise. INS suffers of drift velocity errors constantly accumulated during time; therefore, an INS which operates during an appreciable length of time must be updated periodically with new positioning information. This can be accomplished by using an external navigation reference, such as GPS. An integrated GPS/INS system has advantages in terms of output rate, reliability, and accuracy. In fact:

- it is autonomous and does not rely on any other external aids or visibility conditions, and maintains the availability of navigation solution during GPS outages caused by interference, jamming, and so on;
- an optimal mixing of INS and GPS informations reduces the effect of GPS errors; therefore GPS accuracy is improved by integrated solutions;
- INS provides the full navigation state without differentiation (6 degrees of freedom, 3 translational and 3 rotational); GPS signals could be used to determine accelerations by differentiation or attitude by techniques;
- INS provides the navigation solution in real time (i.e., without latency) at rates higher than one achievable from a GPS receiver.

The integration between the two navigation systems with complementary characteristics is possible thanks to the use of a Kalman Filter. Kalman Filter is a recursive algorithm designed to compute corrections to a system based on external measurements. The corrections are weighted according to the filter's actual estimate of the system error statistics. The derivations of the filter equations require some knowledge of linear algebra and stochastic processes. The filter equations can be unwieldy in an algebraic point of view. Fortunately, the operation of the filter can be understood in fairly simple terms. All that is required is an understanding of various common statistical measures. Kalman filtering is an extremely effective and versatile procedure for combining noisy sensor outputs to estimate the state of a system with uncertain dynamics. Kalman Filter exploits a powerful synergism between the Global Positioning System (GPS) and Inertial Navigation System (INS). This synergism is possible, in part, because the INS and GPS have very complementary error characteristics. Short-term position errors of INS are relatively small, but they have an unbounded degradation on time. GPS position errors, on the other hand, are not so good on short term, but they do not degrade with time. The Kalman filter is able to take advantage of these characteristics in order to provide a common, integrated navigation implementation with better performances than both GPS and INS ones. Kalman filter is able to combine a GPS system, having position uncertainty in the order of tens of meters, with INS system, having position uncertainty which degrades at kilometers per hour (INS); the achieved results is the so called Differential GPS (DGPS) system having position uncertainties in the order of centimeters up to meters. A key role performed by the Kalman filter is the statistical combination of GPS and INS information in order to track drifting parameters of the sensors in the INS. Therefore, the INS can provide enhanced inertial navigation accuracy during GPS signal losses; then, the improved position and velocity estimated by INS can be used to make faster the reacquisition of GPS signal.

Our proposed system uses the DGPS, because in case of jamming the initial state of INS has to be the most exact as possible. In Figure 1, a block model of the general system GPS/INS for landing help is illustrated.

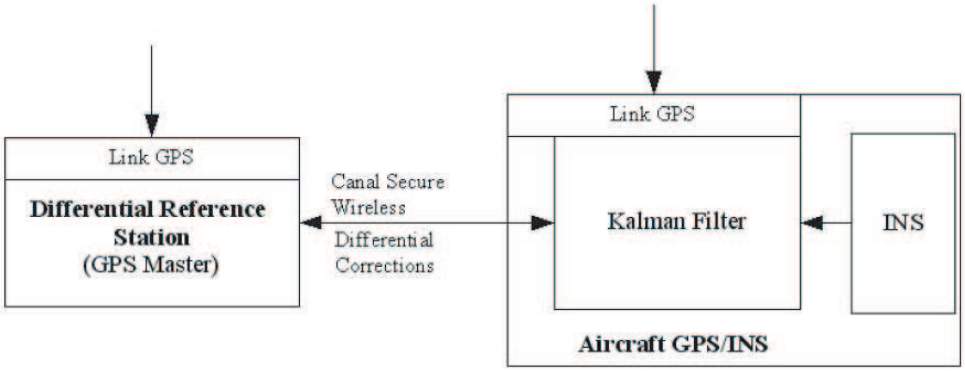

Figure 1: Integrated GPS/INS system for secure landing: it use modality of DGPS, GPS Master on the runway airport and rover over aircraft. The communication link for security is a Wireless LAN.

The master station calculates corrections to the pseudoranges of code and phase and sends them to the rover station; it applies corrections to its observations before the calculation of the position. These operations must be performed in real time, trying to minimize the latency of the whole system. The calculation of the corrections in master station uses the following equations:

$$P_m^j = \rho_m^j + E^j + c(\Delta T_m - \Delta t') + I + T \quad (1)$$

$$\Phi_m^j = \rho_m^j + E^j + c(\Delta T_m - \Delta t') - I + T + \lambda N_m^j \quad (2)$$

where P_m^j and Φ_m^j are the pseudoranges of code and phase, ρ_m^j is the master-satellite distance, E^j is ephemeris error, ΔT_m and $\Delta t'$ are respectively clock errors of master and satellite, I and T are ionospheric and tropospheric delays and λN_m^j is the phase ambiguity. By positions of j^{th} satellite from the ephemeris and master station, it is possible to calculate the master-satellite distance except than ephemeris error: $\rho_m^j + E^j$. Subtracting this quantity from P_m^j and Φ_m^j, the following equations of corrections are obtained:

$$\delta P_m^j(t_i) = P_m^j - \rho_m^j - E^j = c(\Delta T_m - \Delta t') + I + T \quad (3)$$

$$\delta \Phi_m^j(t_i) = \Phi_m^j - \rho_m^j - E^j = c(\Delta T_m - \Delta t') - I + T + \lambda N_m^j \quad (4)$$

The master station also calculates the variation of corrections for each epoch:

$$\delta \widetilde{P}_m^j(t_i) = (\delta P_m^j(t_i) - \delta P_m^j(t_{i-1}))/\Delta t \quad (5)$$

$$\delta \widetilde{\Phi}_m^j(t_i) = (\delta \Phi_m^j(t_i) - \delta \Phi_m^j(t_{i-1}))/\Delta t \quad (6)$$

The main calculation is the orbit determinations, which are normally drawn by the ephemeris broadcast both in the master and in the rover. Nevertheless, it is rather expensive, if it has to be repeated each second; while it is possible to calculate more quickly the orbits using the ephemeris in SP3 format. In conclusion, using DGPS with the master station on runway and a rover on airplane, and providing airplane with the typical INS instrumentation (accelerometer, gyroscope), a GPS/INS navigation system guarantees good performances in case of jamming attack. In fact, position and speed informations retrieved by INS are satisfactory to complete the landing, while GPS stops the increasing of position error calculated by INS.

3. Spoofing Attacks and Proposed Solution

The spoofing attacks are more difficulties to be realized in comparison to jamming, but at the same time they are more dangerous. In this case, in fact, the hacker replaces actual GPS data with ones compatible with the standard GPS format, inducing the pilot to consider a wrong position of airplane. Proposed solution is based on a verification system for the trajectory suggested by the system GPS/INS to the pilot. Particularly, a software/hardware computation system is placed into the control-tower; it esteems the values of parameters retrieved by GPS/INS navigation system in the following sampling instant by means of actual measures; if a strong discrepancy is obtained, the control-tower communicates to use only INS system and to disable GPS only for a few seconds, in order to avoid contemporaneous jamming attacks. An exhaustive description of system control operations can only be obtained by analyzing the timing of events which interest the airplane during the

phase of landing. In Figure 2 three operational phases are underlined, during which the modules are employed to anti-spoofing control and the control-tower develops the respective assignments.

The transmission protocol communicates the coordinates at regular time intervals. In fact, the airplane communicates its position in the WGS84 reference system at time t_i, together with the instantaneous speed. Subsequently, the control-tower esteems the value of airplane coordinates at time t_{i+1}. When the new coordinates will be received from the tower, a comparison will be made with the coordinates previously esteemed, in order to discover a spoofing attack: in this case it will be communicated to the airplane to use only the INS system. Obviously, the communication channel between control-tower and airplane must be secure; indeed, it is possible to use a wireless link similar to 802.11 b protocol or superior both for data control's communication between control-tower and airplane and for DGPS data correction's communication. Even if this technology suffers of a particular type of vulnerability, the so called "man in middle", this attack is a lot difficult to effect within the times characterizing the landing phase.

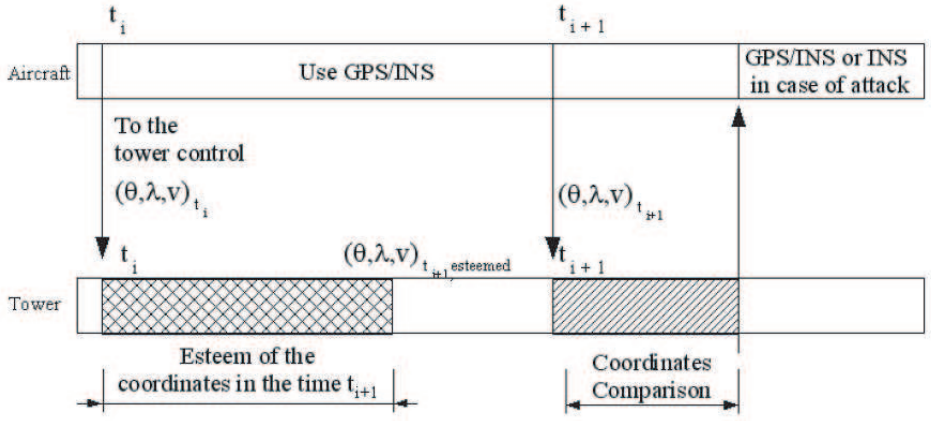

Figure 2: The aircraft communicates own coordinates to the tower in order to verify the presence of a spoofing attack.

4. Conclusions

The safety of flights is a "must" above all for civil transportation. The most dangerous phase of flight is surely the landing phase, in which the navigation systems can be subjected to jamming or spoofing attacks. In this paper, GPS and INS has been analysed; they have complementary characteristics. GPS provides an estimate of position and velocity with bounded estimation error, but it suffers of problems related to signal format and data transmission protocol. GPS uses a space-to-earth signal and the power of received signal is −160 dBW. The low power level makes GPS highly susceptible to interference and a pilot may experience short-term loss of GPS signal during the landing phase. On the other hand, INS is not dependent on the external field, but it suffers of drift velocity errors constantly accumulated during time. Therefore, the integration of these two systems is a reliable tool for helping pilots in the landing phase, above all in countries with an high risk of terrorist attacks. In this paper, a so defined GPS/INS landing-aid system has been proposed in order to avoid the jamming problem. Moreover, an infrastructure between control-tower and airplanes (based at least on 802.11 b communication protocol) has been considered in order to ensure a complete reliability of our hybrid GPS/INS system and have a secure navigational system, verifying and avoiding the presence of possible spoofing attacks.

REFERENCES

1. *Federal Aviation Administrator: Advisor Circular 120-29, Advisor Circular 120-28c.*
2. Brown, A., D. Reynolds, and D. Robert, "Jammer and interference location system-design and initial test results," *Proceedings of the ION 55th Annual Meeting*, 1999.
3. Stovall, S. H., *Basic Inertial Navigation*, Naval Air Warfare Center Weapons Division, California, USA, 1997.
4. Grewal, M. S., L. R. Weill., and A. P. Andrews, *Global Positioning Systems, Inertial Navigation, and Integration*, Wiley, Canada, 2001.