The Impact of Uninformed RF Interference on GBAS and Potential Mitigations

Sam Pullen and Grace Gao
Stanford University

Carmen Tedeschi and John Warburton
FAA William J. Hughes Technical Center

ABSTRACT

RF interference (RFI) has been and will continue to be a significant worry for GNSS users. This paper introduces several different types of RFI, categorizes them based upon the intent (if any) of the RFI transmitter, and then examines a relatively new and growing source of RFI: Personal Privacy Devices (PPDs) that aim to prevent people and vehicles from being tracked by GNSS within a limited area. Unfortunately, signals from PPDs are not well-controlled and can interfere with GNSS receivers several hundred meters away. The impact of PPDs on the GBAS reference station site at Newark Airport, New Jersey and the WAAS reference station at Leesburg, Virginia are illustrated. While GBAS ground station monitoring prevents PPDs from posing a significant integrity threat, PPDs can force the sudden loss of service and thus harm continuity and availability. The hardware and software modifications made to the Newark GBAS installation to reduce this impact are described, and the future benefits of more-flexible ground-station siting and GNSS modernization are also identified.

1.0 Introduction and RF Interference Categorization

Because Global Navigation Satellite System (GNSS) signals are very weak when received by user equipment, they are vulnerable to radio frequency interference (RFI). Signals that overlap with GNSS frequencies are likely to come from transmitters much closer than the GNSS satellites. Therefore, these signals can easily "overpower" the GNSS signals and make them unusable. To protect GNSS, existing ITU and FCC regulations prohibit the intentional broadcast of any non-GNSS signals on or near GPS L1/Galileo E1, while lesser protections apply to the GPS L2 and GPS L5/Galileo E5A frequencies. Despite these protections, RFI affecting GNSS is occasionally observed, and its apparent frequency has increased significantly with the number of civil GNSS users.

In order to better understand the many possible sources of RFI and their potential effects on GNSS, this paper suggests a means of classifying RFI affecting GNSS into three categories. These categories are not all-inclusive, nor do their names fit all possibilities, but they help to separate RFI scenarios in a way that makes it easier to forecast impacts and design mitigations.

The first category is *malicious* interference, meaning RFI that is intentionally transmitted to prevent the use of GNSS (or make its use hazardous) for as many users as possible. Coordinated hostile broadcast of RFI, while hopefully very rare, has the potential to make GNSS unusable over large regions and is difficult to defeat. Therefore, it makes sense to provide non-GNSS backup services to support transportation and other critical infrastructure needs [1].

The second category, and the focus of this paper, is *uninformed* interference, which results from the intentional transmission of signals at or near GNSS frequencies but without the desire to cause harm. At first, it may seem that signals deliberately broadcast on or near GNSS frequencies are likely aimed at harming GNSS users, but this is not true of the vast majority of cases, as will be illustrated in the following sections. Personal Privacy Devices, or PPDs, fall into this category and are of particular concern because they have become numerous in the last few years.

The third category is *accidental* interference, which results from unintentional transmissions at or near GNSS frequencies. This usually is due to malfunctions of equipment that is designed to transmit at other frequencies or not to transmit at all. It is less common than uninformed interference both because malfunctions are rare and because they are more rapidly detected now that many GNSS receivers are likely to be in use nearby. On the other hand, accidental interference is more variable because it is not designed to prevent harm to users.

Section 2.0 of this paper provides past and recent examples of accidental and uninformed RFI. Section 3.0 focuses on PPD interference and illustrates the

Figure 1: RF Interferer Location on Stanford Campus

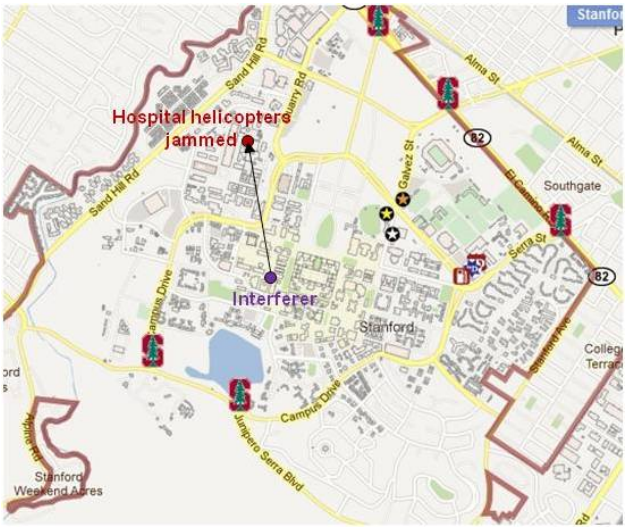

Figure 2: Area at Stanford where GPS was Unusable

characteristics of PPDs. Section 4.0 shows the impact of PPDs on the Wide Area Augmentation System (WAAS) Reference Station (WRS) in Leesburg, Virginia, while Section 5.0 describes their more-severe impact on the Ground Based Augmentation System (GBAS) ground facility at Newark Airport in New Jersey. Section 6.0 describes the GBAS hardware and software modifications being pursued to limit the impact of PPDs at Newark Airport so that acceptable GBAS Category I precision approach service can be provided. Section 7.0 concludes the paper and looks forward to the additional mitigation steps that will be made possible by GNSS modernization.

2.0 Examples of RF Interference to GPS

Figures 1 and 2 show an instance of RF interference to GPS that occurred at Stanford University in 1999. At the time, construction was occurring in the Engineering section of the Stanford campus. A camera had been

Figure 3: RF Interference at Moss Landing Harbor [2]

installed on the Durand Building with a good view of the construction site, and an attached datalink transmitted digital pictures of the site to the construction headquarters trailer to allow progress to be monitored. This proceeded without incident until, for some reason, the datalink transitioned from its primary frequency of 1530 MHz to its secondary one of 1570 MHz, which is very close to the GPS L1 frequency of 1575.45 MHz. The GPS lab at Stanford discovered that GPS was suddenly "gone" – we could not acquire or track any signals. We also discovered that other GPS users in the area were affected, including the helicopters that transported severe cases to Stanford Hospital. This made it clear that the outage zone had a radius of at least 1 km. The cause was not immediately evident, but the use of directional antennas and signal analyzers allowed us to track down the offending device and (manually) remove its power source, after which GPS became usable again.

Once the offending data transmitter was discovered, Todd Walter of Stanford communicated with the device's designers, who knew that their secondary transmission frequency was close to GPS L1 but thought that such transmissions were legal as long as they remained below a certain power level. In other words, they had no intention of interfering with GPS and had no idea that they were capable of doing so. In any case, this company's understanding was incorrect: no intentional transmissions (regardless of power level) are allowed this close to L1. At this time, the civil use of GPS was relatively new, and it is not surprising that the regulations protecting it were not well understood. Uninformed interference due to misunderstandings of this sort should be less likely now that GNSS is well-established.

Figure 3 shows another, well-known RFI incident from 2001 that was previously described in [2]. This was an example of accidental interference caused by amplifiers attached to UHF/VHF antennas for receiving over-the-air

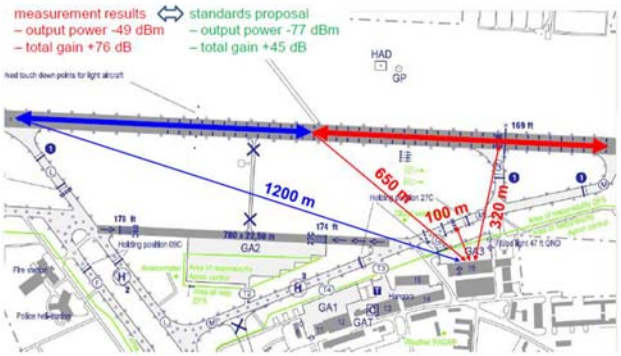

Figure 4: RFI Generated by GPS Repeater at German Airport [3]

TV signals. Due to an unknown defect, these amplifiers were spewing signals into the GPS L1 band, making it impossible to track GPS L1 throughout Moss Landing Harbor in Central California. At least one boat reported the unavailability of GPS in the harbor, but no action was taken until the differential base station at the nearby branch of the Monterey Bay Aquarium Research Institute (MBARI) did a careful study and demonstrated the degree of GPS signal degradation. Once the problem was recognized, it took several months to completely remove the interference because multiple boats docked in the harbor were equipped with the same model and batch of faulty amplifier. Again, because the interference was due to a defective electrical component, no signal transmission near L1 was ever intended, making this an "accidental" event. If something like it happened today, it would probably not take long to indentify the existence of a problem, although tracking down multiple defective components might still take time.

Figure 4 shows a more-recent example of uninformed RF interference generated by a device known as a "GNSS repeater" that was deliberately re-broadcasting GPS signals [3]. This device receives GNSS signals from an antenna with good sky visibility and re-transmits them to nearby users who could not otherwise receive them. In Figure 4, the repeater was installed in an aircraft hangar to re-broadcast live GPS signals inside the hangar. GPS-equipped aircraft inside the hangar, which cannot ordinarily receive GPS signals at adequate signal strengths, instead receive the "repeated" signals and thus can confirm the functionality of their equipment without having to leave the hangar.

The problem with signal repeaters like this one is that they can "leak" unwanted signal power outside the intended area of use. In this case, the problem was exacerbated by the fact that the re-transmission power of the repeater device was variable and could be increased to achieve better performance inside the hangar. The resulting GPS-like signal leakage outside the hangar was reported by several aircraft and, when investigated by the German DFS (the German Air Traffic Control and Air Navigation Services provider), was determined to exceed recommended limits by almost 30 dB (–77 dBm max. recommended vs. –49 dBm actually measured). The presence of repeated GPS signals this much stronger than those received over the air could result in denial of GPS usage or, what is worse, the application of the repeated signals in place of the actual signals from the sky, resulting in potentially very large user errors. Potentially large GPS navigation errors were noticed by at least one pilot who originally reported the problem [3].

Further investigation by DFS has determined that the same type of repeater has been installed in hangers at many German airports. In most cases, significant RF interference from these devices has not been reported, most likely because the problem shown in Figure 4 occurred due to the repeater in question being set to transmit at much too high a power level. However, flight tests conducted by DLR (the German Aerospace Center) at Braunschweig Airport in Germany discovered poor GPS performance when in the vicinity of a hangar known to be equipped with a repeater of this type [4]. Further investigation is needed to confirm that the repeater is the source of these problems.

3.0 Personal Privacy Device (PPD) Characteristics

With the examples from Section 2.0 as background, it is time to examine the most prevalent current sources of RF interference to GNSS in the U.S., which are known as "Personal Privacy Devices" or PPDs. This name comes from the fact that the primary market for these devices consists of people who fear being tracked or monitored by GNSS in their vehicles. Freight and delivery trucks, in particular, are now commonly tracked and dispatched by their headquarters using GNSS. This has significantly changed the working environment of truck drivers over the last decade, and some drivers resent the resulting loss of independence. Because of the general fear of governmental or corporate surveillance and loss of privacy in the 21st Century, ordinary citizens may be moved to take special measures to attempt to protect themselves without understanding the consequences.

The ready availability of inexpensive, mobile GNSS RFI transmitters on the Internet makes it easy for drivers to translate their worries about privacy into action. As noted earlier, GNSS signals are very weak when received by users and can easily be overwhelmed by a device transmitting at nearby frequencies that is much closer to the receiving antenna. For vehicles equipped with GNSS receivers, a small, low-power device can easily transmit enough power to "jam" the GNSS receiver and make it unusable. Unfortunately, as in the case of the GNSS repeater example described above, the zone of effectiveness of such jammers can easily extend far

Figure 5: PPDs Tested in FAF Study [5]

beyond the vehicle to other users that depend on GNSS for safety-critical applications. PPDs violate the frequency protections established for GNSS and are illegal almost everywhere, but enforcement is difficult, and penalties in the U.S. are limited in most cases to confiscation of the device.

Recently, several organizations have acquired and tested PPDs under controlled laboratory conditions to better understand their behavior and their potential impact on GNSS receivers. The results of these studies have been published in several recent papers [5,6,7]. Figure 5 shows the PPDs tested by the study conducted by the University of Federal Armed Forces (FAF), Munich, Germany [5]. These are very small devices, and some are clearly designed to fit into "cigarette lighter" power sources in automobiles. Note that the second one from the right does not use an external antenna so as to better camouflage itself as a mobile phone.

Figures 6 and 7 show two signal outputs from the PPDs shown in Figure 5. Figure 6 shows the very-narrow-band spectrum generated by two of the cigarette-lighter-type PPDs. These devices transmit a signal at a single frequency very close to L1 that changes slowly with the temperature of the device. The bandwidth of this signal is so narrow (less than 1 kHz) that it can be modeled as "tone" or "CW-like" interference which is significantly attenuated by the spread-spectrum nature of GNSS codes. However, GPS L1 C/A-code has a short period of 1 ms and contains spectral lines or "teeth" of 100-Hz width spaced 1 kHz apart. Because the center frequencies of these lines move as the satellite doppler frequency offset changes, it is likely that the CW-like signal shown in Figure 6 will overlap with the spectral lines of one or more satellites at a time and greatly limit the usefulness of C/A code [8].

Figure 7 shows the pattern of broadband interference that is generated by most PPDs. In this case, the bandwidth of the jamming signal is about 12 MHz, with the center frequency being very close to L1. As shown in [5], this spectrum is created by varying the frequency of a CW-like signal very rapidly. For example, the PPD shown in Figure 7 changes its frequency linearly from about L1 – 6

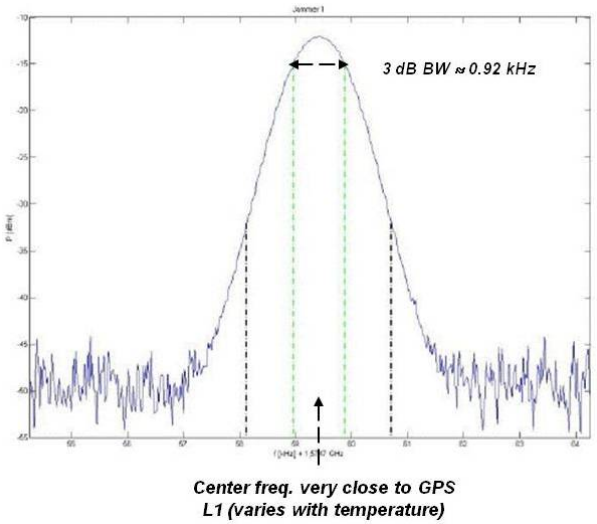

Figure 6: Spectrum of CW-Like PPD [5]

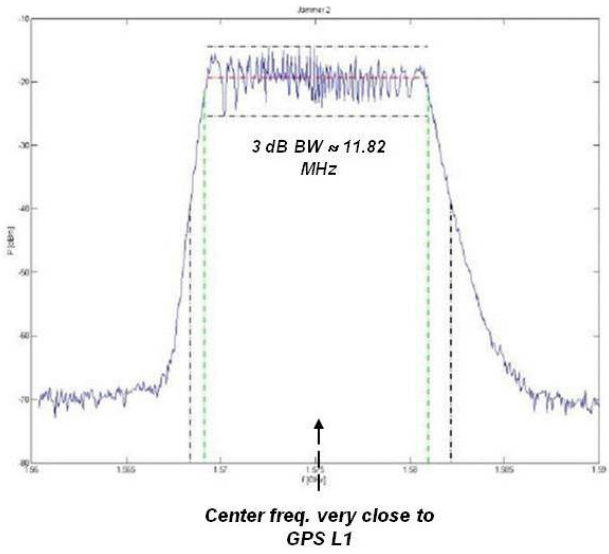

Figure 7: Spectrum of Broadband PPD [5]

MHz to L1 + 6 MHz in a period of about 12 µs (~ 1 MHz / µs), after which the pattern repeats. This generates the effect of broadband interference with simple RF design and components.

Figure 8 shows a table summarizing the characteristics of the PPDs tested and reported in [5]. The CW-type interferer shown in Figure 6 is designated as “Class I” in this table, while different varieties of Broadband interferers are divided into Classes II, III, and IV (Interferer No. 2 of Class II is the one shown in Figure 7). What is most notable is that, within this set of seven devices, the peak power varies by almost 20 dB. The two CW-like Class-I devices (Nos. 1 and 4) are very similar except that their peak power differs by 13.5 dB. While all of these PPDs are likely to make GNSS L1 signals unusable within the 5 – 10 m radius needed to “protect” a

No.	Class	Center frequency	Bandwidth	P_{Peak} [dBm]
1	I	1.5747594 GHz	0.92 kHz	-12.1 dBm
2	II	1.57507 GHz	11.82 MHz	-14.4 dBm
3	II	1.58824 GHz	44.9 MHz	-9.6 dBm
4	I	1.5744400 GHz	0.92 kHz	-25.6 dBm
5	III	1.57130 GHz	10.02 MHz	-19.3 dBm
6	IV	1.57317 GHz (1.57723 GHz)	11.31 MHz (– 19.43 MHz)	-9.5 dBm
7	II	1.57194 GHz	10.72 MHz	-30.8 dBm

Figure 8: PPD Characteristics from FAF Study [5]

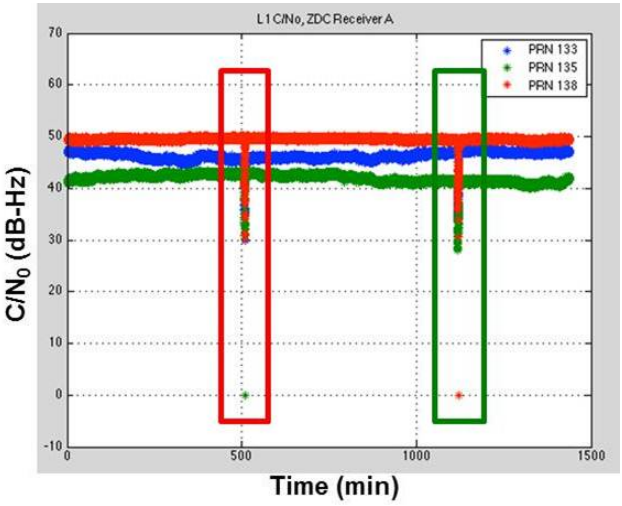

Figure 9: PPDs Observed at Leesburg WRS

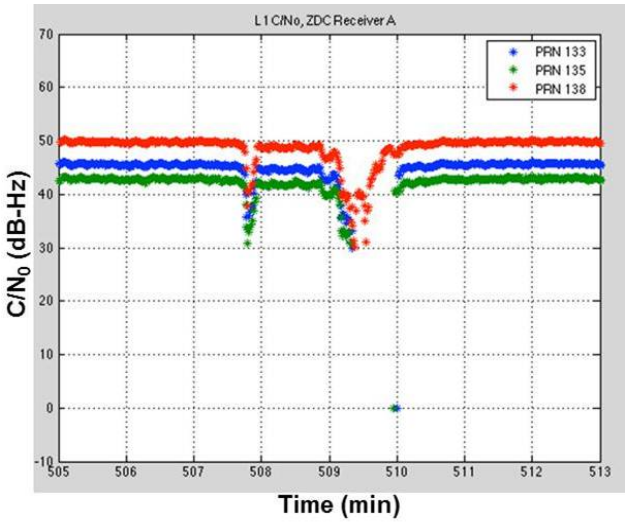

Figure 10: Zoom-in on Earlier PPD at Leesburg WRS

vehicle, some of them have enough additional power to jam L1 for tens to several hundreds of meters away.

The fact that PPDs make GNSS unusable well beyond the zone that they are intended to protect is not surprising for several reasons. First, PPDs tend to be advertised based on power output, similar to mobile-phone jammers that are likely produced by the same people. To buyers and,

Figure 11: Map of Vicinity of Leesburg WRS Site

possibly, sellers, it might not be obvious that jamming areas beyond the vehicle to be protected is not desirable because it increases the chance of detection. Second, because PPDs are illegal and are made and sold cheaply, quality control in manufacturing is not to be expected. In addition, many buyers of these devices do not understand that they work by interfering with GNSS for everyone nearby. In other words, even though PPD users are doing so deliberately, many (if not most) do not realize that other GNSS users may suffer.

4.0 Impact of PPD RFI on WAAS Reference Station

Vehicles with PPDs have been observed to interfere with both GBAS and Space Based Augmentation System (SBAS) reference receivers in the Eastern U.S. Looking at SBAS first using data provided by Zeta Corporation, interference affecting the WRS at Leesburg, Virginia (denoted as ZDC) has been identified. Figures 9 and 10 show received signal-to-noise (C/N_0) ratios from the three Geostationary (GEO) satellites used by WAAS on April 9, 2011. Each WRS has three reference receivers with antennas spaced a few tens of meters apart. These plots show the results from receiver A, as the results from receivers B and C are very similar.

The plot in Figure 9 covers the entire day (1440 minutes) of April 9 and shows two similar events where C/N_0 drops significantly on all three GEO satellites. This disruption appears and then quickly goes away, which is suggestive of a PPD in a vehicle rather than RFI from a fixed location. Figure 10 shows an 8-minute "zoomed-in" window focused on the earlier event on April 9 and shows that the RFI event was brief but actually occurred in two stages, one between t = 507 – 508 min and another shortly after between t = 509 – 510 min.

Figure 11 shows a map of the roads near the Leesburg WRS. Vehicles traveling along the two main roads adjacent to the WRS (i.e., from Route 7 to Highway 15, or vice versa) would approach within 200 meters of the WRS antennas at two different points but be significantly further away in between those points. In addition, variations in ground cover between the roads and the

Figure 12: Overview Map of Newark Airport

Figure 13: LGF Site at Newark Airport

WRS can make a significant difference. Observations made over several months by Zeta Corp. confirmed that the RFI shown in Figures 9 and 10 was due to a PPD-equipped vehicle that passed by the Leesburg WRS on a regular basis in the morning and afternoon [7]. The regularity of the driver's schedule allowed him to be eventually pulled over and his PPD confiscated.

The significance of RFI due to PPDs (and RFI in general) to WAAS and SBAS is relatively limited because SBAS networks include many widely-spread reference stations and are usually robust to temporary losses of individual reference stations. The same is not true of GBAS, where all reference receivers serving a given airport are located within the property of that airport and, in the Honeywell SLS-4000 configuration, have antennas that are typically sited within 100 – 200 meters apart. Therefore, a single powerful interferer can temporarily deny GBAS service for an entire airport. The impact of PPDs on the GBAS installation at Newark Airport (EWR) in New Jersey (near New York City) is described in the next section.

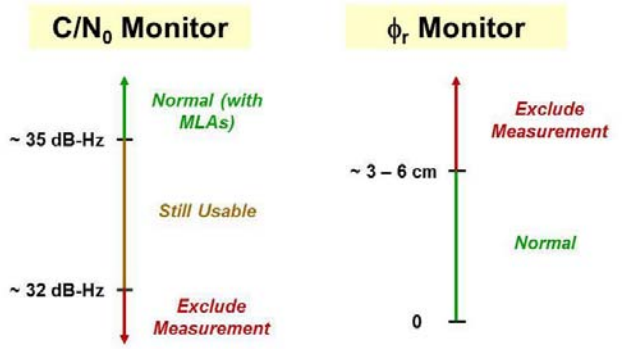

Figure 14: LGF Integrity Monitors that Detect RFI

5.0 Impact of PPD RFI on GBAS at Newark Airport

Figure 12 shows a map of Newark Airport and the surrounding area. While Newark is one of the busiest airports on the East Coast, it is shoehorned into a relatively small physical area, which made finding a good site for the GBAS ground station a challenge. The U.S. version of GBAS is known as the Local Area Augmentation System, or LAAS, and the ground-station component of LAAS is known as the LAAS Ground Facility (LGF). Several sites for the LGF at Newark were considered, but the only one that met the requirements established at the time of siting (in 2008 – 2009) was the one shown in Figure 12 [9].

As detailed in Figure 13, the LGF site at Newark consists of four reference receiver antennas arrayed approximately in a line with separations of about 100 meters. All four antennas are within 200 meters of heavy traffic (over 100,000 vehicles per day) along the New Jersey Turnpike (I-95). The proximity of I-95 was not thought to be a problem prior to installation, but during testing after installation in late 2009, the system went into "alarm" mode, requiring system shutdown and loss of service [10]. Investigation revealed that, as shown in the previous section, multiple reference receivers suffered large drops in C/N_0 on GPS L1 C/A code on multiple satellites, making them unusable. Further work by the FAA and Zeta Corp. confirmed that these events were due to RFI coming from the direction of I-95 and were due to PPDs on vehicles passing by [7]. Prior to the software and site modifications described in Section 6.0, PPD interference was observed as often as several times per day. It remains there today, but the mitigations applied thus far have reduced the frequency of PPDs strong enough to affect the LGF to several per week on average [9,10].

Figure 14 shows a graphical representation of two of the key integrity monitor algorithms within the LGF that detect the presence of RFI when it occurs [11]. Because the algorithms needed to protect the integrity of GBAS are very sensitive, they almost always detect RFI before its impact is evident in terms of loss of satellite tracking.

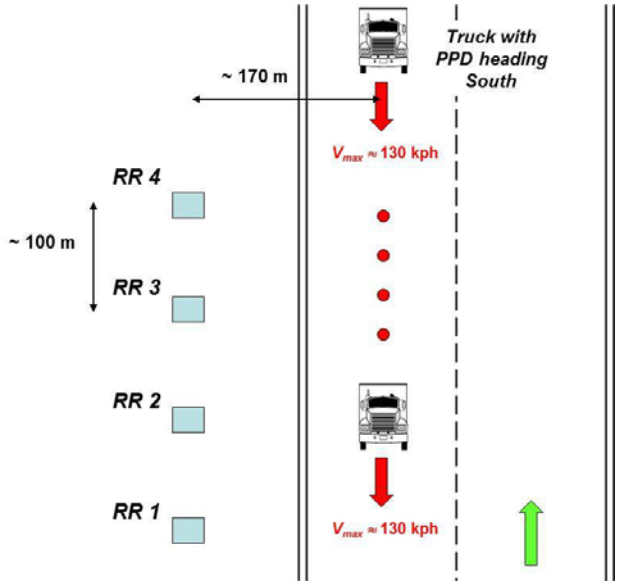

Figure 15: Typical PPD Interference Scenario

Fortunately, the quality of measurements provided by the multipath-limiting antennas used by the LGF is sufficient to allow these monitors to cleanly separate nominal conditions from those which are unacceptably degraded by RFI. The real-time signal-strength (C/N_0) monitor shown in Figure 14 is a good example. Nominal measurements, meaning those affected by RFI within tolerable limits (i.e., the RF interference mask specified in Appendix D of [12]), almost always give C/N_0 measurements of at least 35 dB-Hz, even for low-elevation satellites. The highest level for which hazardous errors are possible (under very conservative assumptions) is around 32 dB-Hz. Thus, placing a C/N_0 threshold slightly above 32 dB-Hz insures detection before any hazard can occur while making "false" detections under nominal conditions very rare. A similar situation applies to the carrier-phase residuals monitor also shown in Figure 14.

Figure 15 shows a simplified diagram of a typical PPD interference scenario at Newark. In this example, a truck equipped with a powerful PPD is traveling southbound on I-95 at full freeway speed (meaning that traffic is light) and is approaching the northernmost of the four LGF receiver antennas (RR 4). Once the truck gets close enough to RR 4, measurements on most satellites tracked by RR 4 will become unusable due to detection by one or more monitor algorithms or simply loss of receiver tracking. Because the RR antennas are only separated by 100 meters from one to the next, a PPD powerful enough to "jam" one RR could easily jam two RRs (e.g., RRs 4 and 3) once it reaches the proper position on the road. Given sufficient additional power, all four RRs could be jammed and become unusable at the same time. The more likely event is that, as the truck moves southward and proceeds to jam RRs 3, 2, and 1 in succession, the northern RRs become free of jamming and are able to track satellites again. The recovered measurements of affected receivers are not immediately usable to form broadcast pseudorange corrections, as both their carrier-smoothing filters and the filters used in their integrity-monitor algorithms must be restarted and allowed to re-converge. However, if enough usable measurements remain present throughout the pass-by of the PPD, GBAS can still provide uninterrupted full-integrity service.

One thing to note about the potential threat of PPDs to GBAS (and SBAS) is that it is mostly focused on the threat to ground-station reference receivers as opposed to receivers on aircraft in flight. The geometry at Newark is such that PPDs on I-95 are much closer to the GBAS reference receivers than they could be to approaching aircraft. The worst-case scenario for PPDs affecting aircraft would be a high-traffic highway running underneath the decision-height location of a precision approach. For Category I approaches down to a 200-foot decision height, it is theoretically possible for a PPD to be only 200 ft (61 meters) below an aircraft. However, the GNSS antenna used by the aircraft would be on the top of the fuselage and would enjoy significant (perhaps ~ 10 dB) resistance to signals coming from below the aircraft. In addition, unlike reference-receiver antennas, approaching aircraft are moving rapidly and would be exposed to nearby PPD interference for a very brief period during an approach. While no instances of PPD interference to aircraft receivers are known, further study is recommended to confirm that the threat is as small as it appears to be.

Because no precautions against PPDs had been taken in the original LGF design and siting at Newark, the frequent presence of PPD interference caused the LGF to interrupt service multiple times per week. Some of these interruptions generated alarms which required manual intervention to re-start the system. The overall effect was that the availability and continuity requirements for Category I precision approaches could not be met (although integrity was protected by the monitor alerts and shutdown procedures). Once the PPD threat was better understood, a series of software and hardware modifications was undertaken to allow Category I service to be provided at Newark despite the presence of PPDs. The next section describes how this is being done and suggests future modifications.

6.0 GBAS Software and Hardware Mitigations

Significant changes to the software of the Honeywell SLS-4000 LGF design have been made in response to the PPD threat at Newark. As noted above, the original software, known as "Block 0," protected against potential hazards from RFI by detecting and excluding the affected measurements. The modifications that led to the current "Block 1" software at Newark were intended to retain this

Figure 16: Adjusting the Height of RR 2 Antenna

protection while reducing the rate of system shutdowns and alarms that led to lengthy periods out of service.

As shown in the example in Figure 15, a powerful PPD interferer can jam more than one reference receiver at a time. In the Block-0 software, the loss of measurements from more than one receiver led to system shutdown, meaning (at a minimum) the broadcast of empty pseudorange correction measurements, making the system unusable by aircraft for some time. The most important change in the Block 1 software is briefly allowing the loss of two reference receivers while still providing corrections and usable service. This means that the integrity monitor algorithms, which previously assumed that measurements from at least three receivers would always be available, had to be reconsidered from the standpoint of meeting all requirements with only two receivers for a short period (note that only a period of several minutes is required because, in most cases, the PPD will have "moved on down the road" by then). This is a significant challenge because relatively little performance margin exists for some of the monitors. Versions of the Block 1 software have been in use at Newark for some time and have shown significant progress in reducing the impact of PPDs on system availability and continuity. The potential integrity impacts of the Block 1 changes remain under review as of the time of this writing.

Several hardware improvements have also been implemented at Newark. Figure 16 shows the results of adjusting the height of the antenna connected to RR 2, which originally had the highest occurrence of PPD-driven measurement losses [9]. At first, it was thought that raising the antenna would reduce the impact of RFI from PPDs by taking advantage of the gain pattern of the antenna, which is designed to reject multipath coming from the ground. However, when this was tried, it was found that the impact got worse, as the "shielding" effect of nearby obstructions was lost. Therefore, it made sense to try lowering the antenna height, as shown in Figure 16, and this was successful in reducing the impact of RFI on

Figure 17: Example Newark Antenna Reconfiguration with Greater Separations

RR 2 to about the same level as that on the other three reference receivers. In addition, the metal fence near RR 2 visible in Figure 16 has been augmented by the addition of ½-inch wire mesh in an attempt to "break up" arriving RFI signals and further enhance the obstructions separating RR 2 from the freeway.

The example in Figure 15 also demonstrates the disadvantage of having all four reference receiver antennas so close together and therefore vulnerable to PPD RFI at the same time. The FAA is conducting tests in which RR 1 and its antenna are temporarily moved about 500 meters further south, away from the other three antennas, to see how much benefit is obtained. Figure 17 shows one of several proposed configurations in which two pairs of antennas are separated from each other by ~ 500 meters, while each pair is separated by ~ 200 meters. This setup makes it less likely that two reference receivers will be jammed at the same time by a single PPD, and much less likely that more than two receivers will be affected. Separations larger than 100 meters are also preferred because of the proposed addition of carrier-phase-based monitoring of ionospheric spatial gradient anomalies for GBAS ground stations supporting Category III precision approaches and landings [13]. While the SLS-4000 is limited in the receiver spacing that it can support, future GBAS ground-station designs may support much larger separations (1 km or more), which would almost ensure that a single PPD could not affect more than one reference receiver at a time.

As noted above, Newark Airport is limited by the fact that few (if any) usable reference receiver sites exist outside of the zone close to I-95. However, an obvious lesson from the Newark experience with PPDs is to stay away from busy roads to the extent possible. Figure 18 shows how this lesson has been applied at Houston George Bush Airport (IAH), where much more open space is present. The reference-receiver site selected at Houston is more than 1 km away from the nearest road with any significant

Figure 18: Reference Receiver Siting at Houston/George Bush Airport

level of traffic (FM 1960). While PPD interference has been observed at other locations on the airport that are close to the roads feeding into the airport from the southern direction (e.g., John F. Kennedy Blvd.), the LGF receiver site is sufficiently isolated that very little (if any) PPD interference is expected to be strong enough to reach it and cause a noticeable impact.

7.0 Summary and Potential of GNSS Modernization

This paper has examined several past instances of accidental and uninformed RF interference to GNSS before focusing on the growing threat of interference from Personal Privacy Devices, or PPDs. These small, inexpensive GNSS jammers are illegal to use but are readily available on the Internet and offer those worried about being tracked by their companies or the government with a sense of privacy. Recent GPS L1 C/A-code measurements and anecdotal observations suggest that PPDs are now sufficiently common as to present a significant threat to safety-critical GNSS users that must operate in proximity to busy roadways.

The impact of PPDs on the GBAS ground system at Newark Airport has been described in detail. Because severe siting constraints at Newark required that the reference-receiver antennas be placed near and parallel to a very busy freeway, severe and frequent RFI from PPDs was noticed almost immediately after site installation. In protecting the integrity of the received measurements, the ground station shut down too often and stayed offline too long to meet its availability and continuity requirements. Once the characteristics and impact of PPDs were better understood, a series of hardware and software

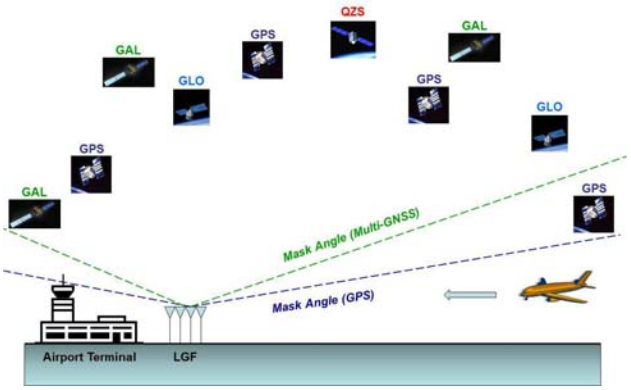

Figure 19: Higher Mask Angle and Increased Low-Elevation Signal Rejection for Future GNSS

modifications were implemented to allow the ground station to continue operating under a greater range of RFI conditions while still meeting the integrity requirements. Testing and evaluation of these modifications continues as of the time of writing of this paper. If all goes well, the upgraded "Block 1" software and the hardware and siting modifications at Newark will be approved to support Category I precision approach operations later in 2012.

While many approaches to mitigating PPDs are possible within the framework of today's GNSS, a future of multiple interoperable GNSS constellations offers significant further benefits, as illustrated in Figure 19. One reason that GBAS and other systems are vulnerable to RFI coming from sources on the ground is that it is necessary to track low-elevation GNSS satellites in order to obtain a high probability of "good" positioning geometry (e.g., low PDOP). GBAS, for example, is required to provide corrections for satellites at elevation angles of 5 degrees or above in order to maximize the usable GPS satellite geometry at the aircraft. Reliably tracking GPS satellites at 5 degrees requires antenna gain patterns that are at least somewhat receptive to interference coming from the vicinity of 0 degrees. However, in a future with multiple interoperable GNSS constellations, a much higher effective mask angle (perhaps as high as 15 – 20 degrees) could be applied, as low-elevation satellites would not be necessary to achieve good positioning geometry. Allowing reference-receiver antennas to reject signals below 10 degrees would greatly add to the resistance of GBAS ground stations to RF interference of all types and reduce the need for siting antennas far apart and away from roads.

ACKNOWLEDGMENTS

The authors would like to thank the FAA Satellite Navigation Program Office and the FAA William J. Hughes Technical Center for their support of Stanford University's research on LAAS and WAAS. However, the opinions expressed here are solely those of the

authors. The authors would like to thank Todd Walter, Sherman Lo, and others at the Stanford GNSS laboratory for sharing their thoughts and recollections regarding past examples of RF interference. They would like to thank Karl Shallberg and Joe Grabowski of Zeta Corporation for providing WAAS Reference Station data from the ZDC site and explaining features of the results. They would like to thank Kim Class, Mike Meyer, Mike Meemken, and their colleagues at Honeywell for their data and observations of the impact of PPDs on the SLS-4000 installation at Newark airport. They would also like to thank Winfried Dunkel of DFS and Michael Felux and his colleagues at DLR for their information regarding interference generated by GNSS repeaters at German airports.

REFERENCES

[1] *Vulnerability Assessment of the Transportation Infrastructure Relying Upon the Global Positioning System: Final Report*. Volpe Systems Center, U.S. Dept. of Transportation, Aug. 29, 2001. http://preview.tinyurl.com/VolpeRFI

[2] W.R. Vincent, *et al*, "The Hunt for RFI," *GPS World*, Jan. 2003. http://preview.tinyurl.com/HuntRFI

[3] W. Dunkel, O. Weber, F. Butsch, "GNSS Interference Detection with GIMOS," 11th Int'l. GBAS Working Group Meeting (I-GWG-11), Osaka, Japan, Feb. 24, 2011. http://preview.tinyurl.com/DFS-main

[4] M. Felux, T. Dautermann, B. Belabbas, "Towards Full GAST-D Capability - Flight testing DLR´s Experimental GBAS-station," *Proceedings of ION ITM 2012*, Newport Beach, CA, Jan. 30-Feb. 1, 2012. http://www.ion.org

[5] T. Kraus, R. Bauernfeind, B. Eissfeller, "Survey of In-Car Jammers - Analysis and Modeling of the RF Signals and IF Samples (Suitable for Active Signal Cancelation)," *Proceedings of ION GNSS 2011*, Portland, OR., Sept. 20-23, 2011, pp. 430-435. http://www.ion.org/search/view_abstract.cfm?jp=p&idno=9605

[6] R.H. Mitch, R.C. Dougherty, *et al*, "Signal Characteristics of Civil GPS Jammers," *Proceedings of ION GNSS 2011*, Portland, OR, Sept. 20-23, 2011, pp. 1907-1919. http://www.ion.org/search/view_abstract.cfm?jp=p&idno=9740

[7] J. Grabowski, "Field Observations of Personal Privacy Devices," *Proceedings of ION ITM 2012*, Newport Beach, CA, Jan. 30-Feb. 1, 2012. http://www.ion.org

[8] P. Misra, P. Enge, *Global Positioning System: Signals, Measurements, and Performance*. Lincoln, MA: Ganga-Jamuna Press, 2nd Edition, 2006, Sections 9.7 and 13.1. http://www.gpstextbook.com/

[9] C. Tedeschi, "The Newark Liberty International Airport (EWR) GBAS Experience," 12th Int'l. GBAS Working Group Meeting (I-GWG-12), Atlantic City, NJ, Nov. 17, 2011. http://laas.tc.faa.gov/

[10] J. Warburton, C. Tedeschi, "GPS Privacy Jammers and RFI at Newark: Navigation Team AJP-652 Results," 12th Int'l. GBAS Working Group Meeting (I-GWG-12), Atlantic City, NJ, Nov. 17, 2011. http://preview.tinyurl.com/FAA-RFI

[11] G. Xie, *Optimal On-Airport Monitoring of the Integrity of GPS-Based Landing Systems*. Ph.D. Dissertation, Stanford University, Dept. of Aero/Astronautics, March 2004. http://preview.tinyurl.com/GXie-Thesis

[12] *Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment*. Washington, D.C., RTCA SC-159, WG-4, DO-253C, Dec. 16, 2008. http://www.rtca.org

[13] S. Khanafseh, F. Yang, *et al*, "Carrier Phase Ionospheric Gradient Ground Monitor for GBAS with Experimental Validation," *Proceedings of ION GNSS 2010*, Portland, OR, Sept. 21-24, 2010, pp. 2603-2610. http://ion.org/search/view_abstract.cfm?jp=p&idno=9368