A RFI Testbed for Examining GNSS Integrity in the Various Environments

Yu-Hsuan Chen, Zixi Liu, Juan Blanch, Sherman Lo, Todd Walter
Stanford University

Biographies

Yu-Hsuan Chen is a research engineer in GPS laboratory at Stanford University. He received his Ph.D. in electrical engineering from National Cheng Kung University in 2011.

Zixi Liu is a Ph.D. candidate at the GPS laboratory at Stanford University. She received her B.Sc. degree from Purdue University in 2018 and her M. Sc. degree from Stanford University in 2020.

Juan Blanch is a senior research engineer at the GPS laboratory at Stanford University

Sherman Lo is a senior research engineer at the Stanford GPS Laboratory and the executive director of the Stanford Center for Position Navigation and Time. He received his Ph.D. in Aeronautics and Astronautics from Stanford University in 2002. He has and continues to work on navigation robustness and safety, often supporting the FAA. He has conducted research on Loran, alternative navigation, SBAS, ARAIM, GNSS for railways and automobile. He also works on spoof and interference mitigation for navigation. He has published over 100 research papers and articles. He was awarded the ION Early Achievement Award.

Todd Walter is a Professor of Research and director of the GPS laboratory at Stanford University.

Abstract

A testbed is built for examining the GNSS integrity under RFI for aviation environment. The combination of hardware and software enables us to simulate the RFI and GNSS environment on the aircraft in the laboratory. Considering existing different jamming types and power level effect on the GNSS integrity, several jamming type data sets are pre-generated and jamming power is adjustable by setting the transmitter gain. The receivers collect the raw measurements needed for protection level computation or output built-in protection level. The algorithm to compute the protection level is the multiple hypothesis solution separation algorithm (MHSS). Then, convert the protection level to Navigation Integrity Category (NIC) which is a field in Automatic Dependent Surveillance-Broadcast (ADS-B). Three receivers from surveying to consumer grade are tested for examining different responses of receiver brands.

1. INTRODUCTION

In the safety of life applications of GNSS, integrity is the crucial measure of how much we can trust the GNSS Position, Velocity and Time (PVT). Integrity is originated from aviation and is the key to validate the GNSS performance whether achieving the requirement of different flight phases. Then, the pilot uses this information to determine which mode is safe to proceed. Automatic Dependent Surveillance-Broadcast (ADS-B) system on the aircraft broadcasts airborne navigation integrity category (NIC) which specifies the containment radius that the current reported aircraft position is guaranteed to be within. Other aircraft and air traffic control use NIC as a parameter to determine whether reported position is within acceptable level. Beyond the aviation, for the autonomous vehicles and drones, integrity ensures the autonomous maneuver decisions within safety zone. For the marine application, Automatic identification system (AIS) provides accuracy flag and RAIM-flag indicating the reported vessel position whether use the Receiver Autonomous Integrity Monitoring (RAIM) to protect reported position accuracy.

Radio frequency Interference (RFI) is harmful to GNSS and is the most likely factor to degrade integrity other than satellite and constellation faults Rothmaier et al., (2019). The growing dependence of critical infrastructure and safety of life applications

relying on GNSS makes detection of RFI important. To locate the interference source usually needs a dedicated equipment and closed to impacted area of RFI. However, integrity information is widely and publicly available through ADS-B and AIS messages in the air. Researchers have been examining crowdsourced integrity information from ADS-B and AIS to RFI localization which is not limited by equipment and geolocation Liu et al., (2022). But the relationship between received power level of RFI and integrity information needs to be investigated and it is the only measurement of overall localization research. Other usage of this relationship is to learn how powerful RFI being experienced just using integrity information.

In this paper, a testbed is built for examining the variation of protection level under RFI. To simulate real-world situation, real open-sky signal is repeated in the anechoic chamber. At the same time, jammer signal is generated by a transmitter and connected to another antenna in the chamber. On the receiving side, an aviation antenna is setup to export signal to out-of-chamber receivers. The receivers collect the raw measurements needed for protection level calculation. For the RFI, the power level is altered and measured by a power meter to ensure the exact power level is received. RFI types have different effect on the response of receivers. Two common types of RFI are generated including wideband additive white Gaussian Noise (AWGN) and chirp and pulsed chip.

For the protection level calculation, the multiple hypothesis solution separation algorithm (MHSS) is developed to consider the threat model and probability of individual faults and provides more precise protection level. This algorithm is examined in the testbed. The results of relation between received power of RFI and protection level are provided in terms of different RFI power level and types, receivers variation.

2. TESTBED DESCIRPTION

The built testbed to examine the GNSS integrity is set up in the laboratory shown in Figure 1. Below are the details of hardware and software.

2.1 Hardware

The hardware consists of an anechoic chamber, transmitter/receivers and a personal computer (PC). To avoid radiating the jammer signals to outside world, an anechoic chamber is used to place all the antennas including 1) helical antenna 2) marine antenna 3) aviation antenna. Antennas are connected to SMA connectors on the back panel and extended to outside facility.

2.1.1 Antennas

Helical antenna

A wideband L1/L2/L5 helical antenna is connected to a Trimble Zephyr Geodetic 2 antenna located on building roof. The open sky signal from the antenna is repeated and rebroadcasted by the helical antenna.

Marine antenna

A L1 marine antenna is a passive helical antenna connected to the outside transmitter, Universal Software Radio Peripheral (USRP). This antenna serves as RFI source.

Aviation antenna

A L1 aviation antenna is an active antenna connected to the outside splitter/receivers. This antenna serves as receiving antenna simulating the receiving environment on the aircraft.

2.1.2 Transmitter

A USRP B200mini-i transmits the jamming signal by playing pre-generated jamming data sets.

2.1.3 Splitter and Receivers

The signal from the received antenna firstly is split into 4 branches. Three branches are connected to three GNSS receivers listed as below.

Trimble BX940

BX940 is a survey-graded receiver supporting L1/L2/L5 bands.

Septentrio mosaic-X5

Mosaic-X5 is a consumer-graded receiver supporting L1/L2/L5 bands.

u-blox F9P

F9P is a consumer-graded receiver supporting L1/L2 bands.

2.1.4 Spectrum analyzer

A spectrum analyzer is connected the fourth branch of splitter and used to measure jamming power out of receiving antenna. The power measurement from the analyzer is the same as three receivers seen.

2.1.5 PC

A PC is used to send the jamming Intermediate Frequency (IF) data to the USRP and upconvert to Radio Frequency (RF) signal. Second use of PC is to run receiver PC applications.

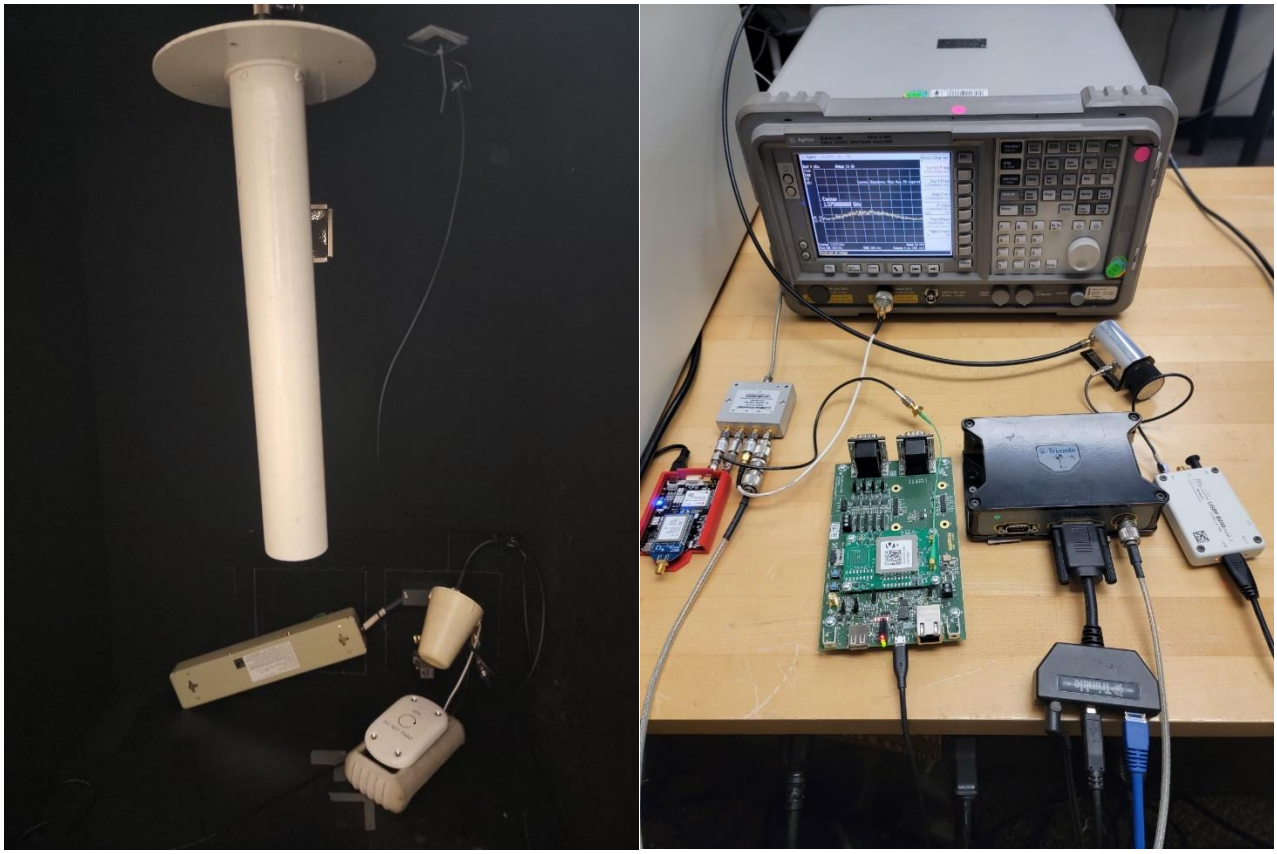

Figure 1 *Testing facility (Left) antennas inside anechoic chamber (Right) receivers, spectrum analyzer and USRP*

2.2 Software

The software consists of jamming datasets generator, USRP Hardware Driver (UHD) and receiver PC applications. All three software are run on the PC.

2.2.1 Jamming datasets generator

The jamming dataset is pre-generated to a file by a program jamming generator and specifying the jammer type, bandwidth, frequency and length.

2.2.2 UHD

The driver controls the USRP from streaming the jamming dataset to setting the RF transmitting gain. The gain setting is the way to adjust the jamming power.

2.2.3 Receiver PC applications

The applications collect logging data from receivers including measurement, ephemeris and receiver status.

3. JAMMING SIGNAL

The jamming signal broadcasted in the chamber has two jamming types, chirp and noise. Each jamming signal is illustrated below.

3.1 Chirp jamming signal

Chirp signal is a swept frequency continuous wave, and its phase is also continuous. We specify the swept frequency range 40 MHz and sweeping period of 10 seconds to sweep full band. Chirp jamming signal is common seen in the personal privacy device. Figure 3 is the signal spectrum of chirp jamming signal.

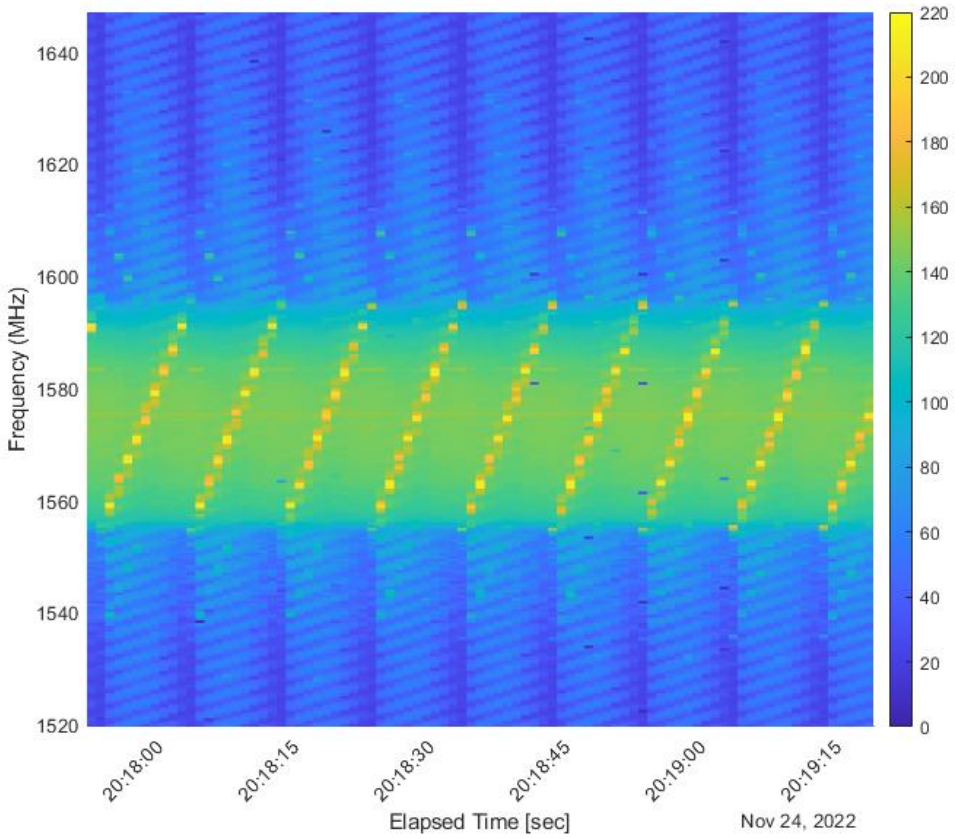

Figure 2 *Spectrum of Chirp jamming signal with swept frequency range 40 MHz wide which is plotted using 200msec data*

3.2 Noise jamming signal

Noise signal is a broadband signal or named as Additive White Gaussian Noise (AWGN). We specify the bandwidth of noise 40 MHz and a fixed seed to generate the random signal. Noise jammer is common seen in the military high-power jammer. Figure 4 is the signal spectrum of noise jamming signal.

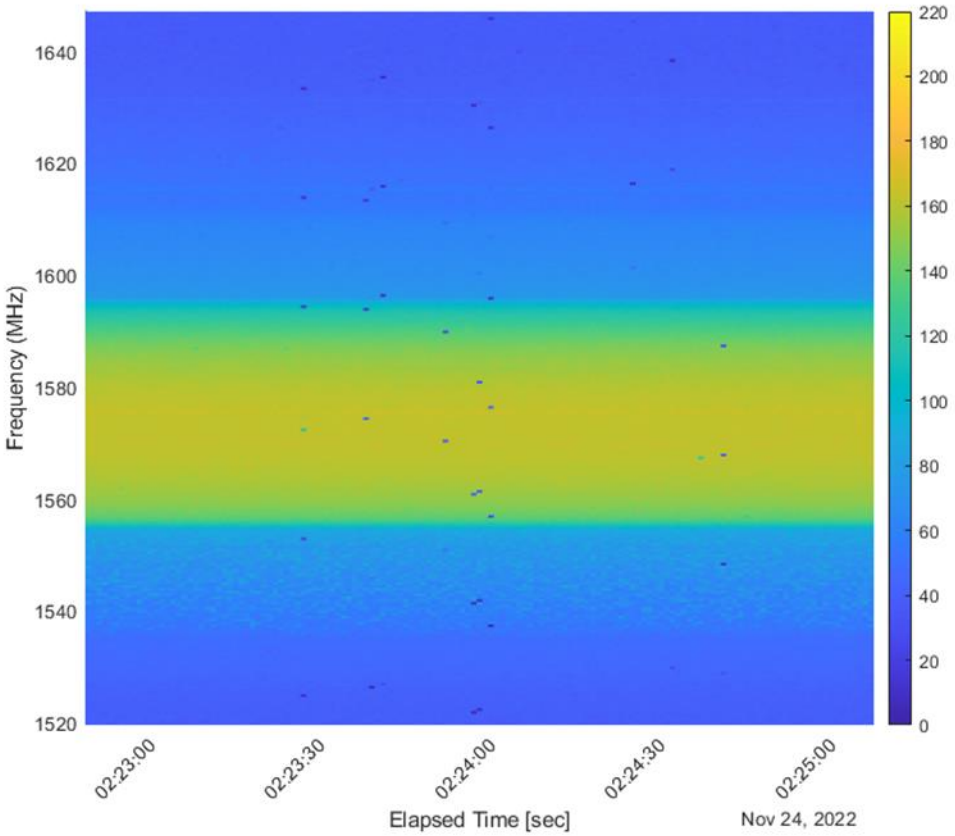

Figure 3 *Spectrum of Chirp jamming signal with 40 MHz bandwidth which is plotted using 200msec data*

4. PROTECTION LEVEL AND NIC

One of metric of GNSS integrity is protection level which describes the maximum position error with specified confident. The horizontal protection level is equivalent to the other metric Containment Radius (Rc) in the aviation field. Automatic Dependent Surveillance-Broadcast (ADS-B) broadcasts airborne navigation integrity category (NIC) field specifying the containment radius of reported aircraft position. Table 1 lists the relation between NIC and containment radius.

TABLET 1 *NIC versus Containment Radius*

NIC	Containment Radius
0	$R_c \geq 37.04$ km (or Unknown)
1	$R_c < 37.04$ km (20 NM)
2	$R_c < 14.816$ km (8 NM)
3	$R_c < 7.408$ km (4 NM)
4	$R_c < 3.704$ km (2 NM)
5	$R_c < 1852$ m (1 NM)
6	$R_c < 1111.2$ m (0.6 NM)
	$R_c < 926$ m (0.5 NM)
	$R_c < 555.6$ m (0.3 NM)
7	$R_c < 370.4$ m (0.2 NM)
8	$R_c < 185.2$ m (0.1 NM)
9	$R_c < 75$ m
10	$R_c < 25$ m
11	$R_c < 7.5$ m

The GNSS receiver uses Receiver Autonomous Integrity Monitoring (RAIM) to calculate the protection level. FAA certified receiver should use WAAS correction and provide GPS-only solutions. In the testbed, two approaches to get the protection level are 1) adopting the protection level outputting from receiver 2) computing protection level by multiple hypothesis solution separation algorithm (MHSS) ARAIM in Blanch et al., (2015). Table 2 lists the parameters used for MFSS.

TABLET 2 *MHSS ARAIM parameters*

Name	Description	Value
$PHMI_{VERT}$	integrity budget for the vertical component	2×10^{-8}
$PHMI_{HOR}$	integrity budget for the horizontal component	9.8×10^{-8}
P_{FA_VERT}	continuity budget allocated to the vertical mode	1×10^{-8}
P_{FA_HOR}	continuity budget allocated to the horizontal mode	5×10^{-7}
TOL_{PL}	tolerance for the computation of the Protection Level	5×10^{-2}
P_{EMT}	probability used for the 10^{-5} calculation of the Effective Monitor Threshold	1×10^{-7}
P_{THRES}	threshold for the integrity risk coming from unmonitored faults	9×10^{-8}
F_C	threshold used for fault consolidation	0.01

5. TESTING SCENARIOS

We conducted two experiments on November 8th and 24th, 2022 with different RFI profiles. The details of experiments are described below.

5.1 Increasing received jammer power by steps

The experiment on November 8th, the noise jammer is transmitted. The received power is gradually increased from -92.5 dBW to -77.5 dBW by 0.5 dB step. For each power level, data is collected for 2 minutes. The protection level is computed by MHSS ARAIM using three receivers' L1 GPS-only measurements. The attempt of this experiment is to see how the NIC response when received jamming power increases and different receivers' reaction.

5.2 Increasing and then decreasing received jammer power by steps

The experiment on November 24th, both chirp and noise jammers are transmitted. The protection level is adopted from the Septentrio mosaic-X5 receiver built-in RAIM and using multi-constellations GPS+Galileo+GLONASS+BeiDou L1. The attempt of this experiment is to see NIC change when an aircraft flying over a RFI source.

5.2.1 Chirp jammer scenario

The received power is gradually increased from -100 dBW to -85 dBW by 0.5 dB step and then decreased from -85 dBW to -100 dBW. For each power level, data is collected for 1 minute.

5.2.2 Noise jammer scenario

The received power is gradually increased from -98 dBW to -85 dBW by 0.5 dB step and then decreased from -85 dBW to -95 dBW. For each power level, data is collected for 1 minute.

6. TESTING RESULTS

The testing results of scenarios described in section 5 are shown and discussed in this section.

6.1 Increasing received jammer power by steps

Figures 4,5 and 6 are NIC versus received jamming power from Trimble BX940, Septentrio mosaic-X5 and u-blox F9P receivers. For each figure, on the top plot, x-axis is jamming received power (Pr) and y-axis is NIC. The black curve represents the mode or most frequent NIC given Pr. The number on the plot representing percentage of corresponding NIC values been observed among all measurements at each given Pr. On the bottom plot, x-axis is NIC, and y-axis is Pr. The black curve represents the mode or most frequent Pr given NIC. The legend represents total number of samples for each NIC.

From the results, the NICs remain between 7 and 9 for Pr < -86.5 dBW. From Pr=-86 dBW, F9P's NIC drops to 6, but other two receivers remain NIC=7. Pr=-84.5 dBW is an outlier for both of BX940 and mosaic-X5. Pr=-84 dBW is the power level with drastic change of NIC for F9P. For the BX940 and mosaic-X5, Pr = -82.5 is the power level with drastic change of NIC. The NIC becomes 0 mostly when Pr > -83.5 dBW for F9P, -82 dBW for BX940 and -81.5 dBW for mosaic-X5. To conclude, there is a certain power level of RFI leading NIC change drastically. Also, F9P is about 2dB less tolerable than other receivers

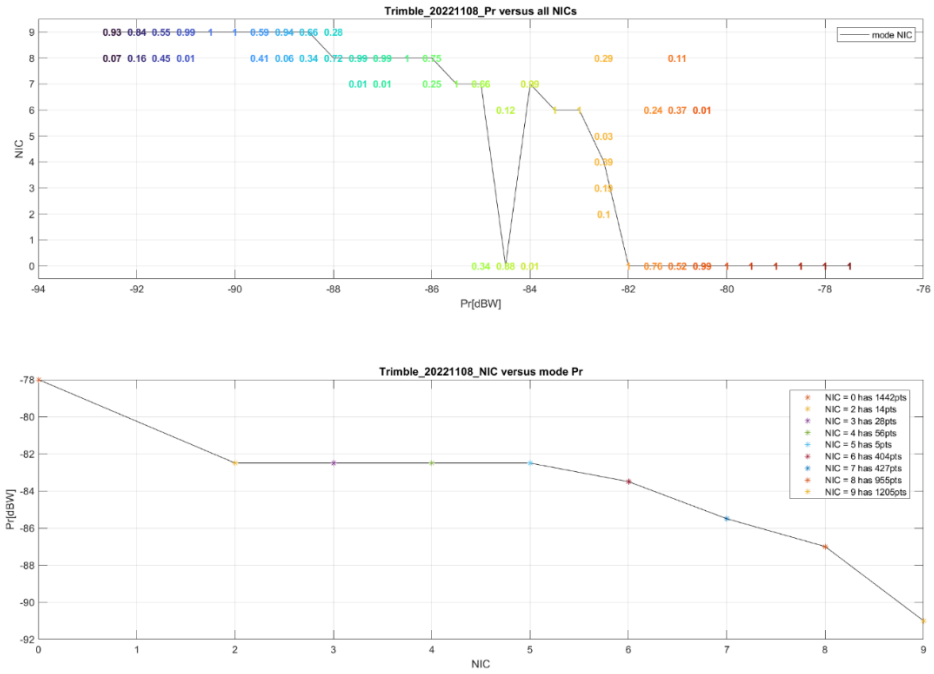

Figure 4 *NIC versus received jamming power of noise type jammer 40 MHz bandwidth from Trimble BX940 receiver*

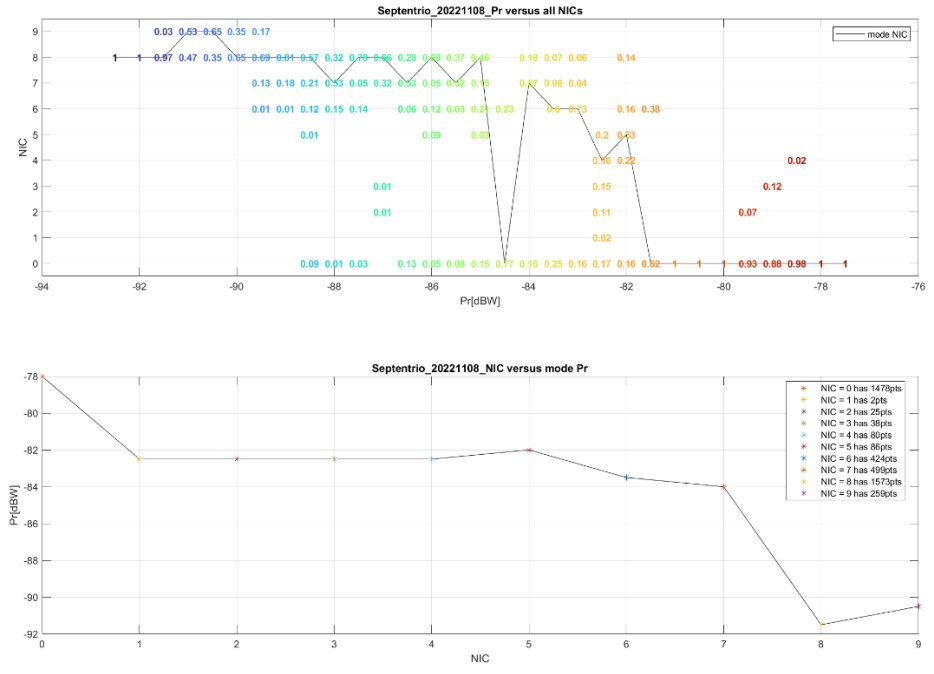

Figure 5 *NIC versus received jamming power of noise type jammer 40 MHz bandwidth from Septentrio mosaic-X5 receiver*

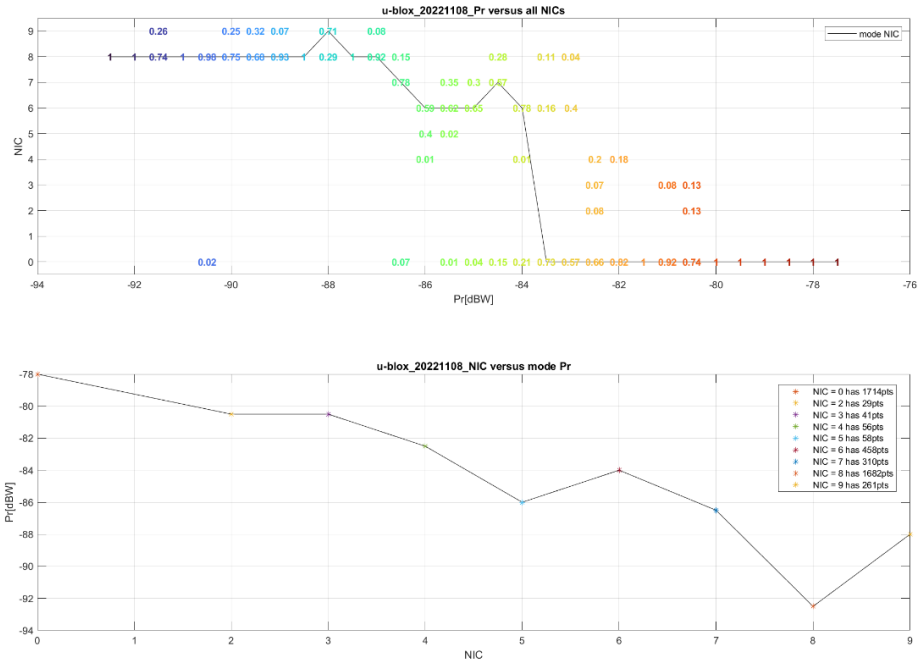

Figure 6 *NIC versus received jamming power of noise type jammer 40 MHz bandwidth from Trimble u-blox F9P receiver*

6.2 Increasing and then decreasing received jammer power by steps

Figures 7 and 9 show the NIC versus received jamming power, x-axis is received jamming power and y-axis is NIC. The black curve represents the mode or most frequent NIC given Pr. The number on the plot on representing probability of NIC given Pr. Figure 8 and 10 show the number of satellites (NrSV) versus received jamming power, x-axis is received jamming power and y-axis is the number of satellites. The black curve represents the mode or most frequent NrSV at each given Pr. The number on the plot represents probability of NrSV given Pr. Pr=-inf is when the RFI is off for comparing with and without RFI. When the RFI is on in the weakest power level, half of satellites are affected and lose lock.

6.2.1 Chirp jammer scenario

From the Pr=-91 dBW, NIC drops to 6. Pr = -90 dBW, NIC starts drastically changing. The NIC becomes 0 mostly when Pr > -88.5 dBW.

6.2.2 Noise jammer scenario

From the Pr=-85 dBW, NIC drops to 6. Pr = -83 dBW, NIC starts drastically changing. The NIC becomes 0 mostly when Pr > -82.5 dBW.

To conclude, chirp jammer impacts NIC at lower power level than noise jammer and both of NIC and NrSV has a lot of variation. It is likely due to swept mechanism of chirp signal. Also, the NIC response is asymmetric respect to lowest power level for the chirp jammer. For the noise, the result somehow matches first experiment with only 1 dB difference. Also, the NIC and NrSV have less variation for the noise jammer. In addition, the NIC value drops significantly once the jamming power reaches certain power level. This indicates a discrete or stairstep behavior of how protection level reacts during jamming. The receiver is able to either provide reliable position information or output a non-trustworthy warning of the result. There is no intermediate reaction.

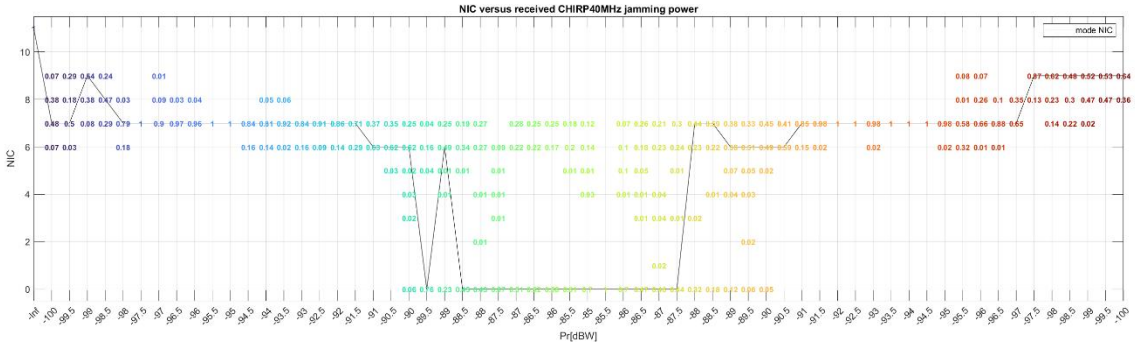

Figure 7 *NIC versus received jamming power of Chirp jammer 40 MHz swept range*

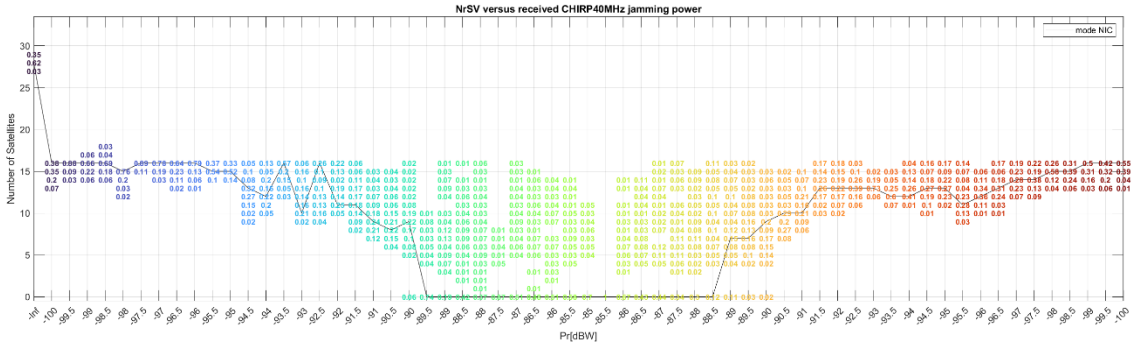

Figure 8 *Number of satellites versus received jamming power of Chirp jammer 40 MHz swept range*

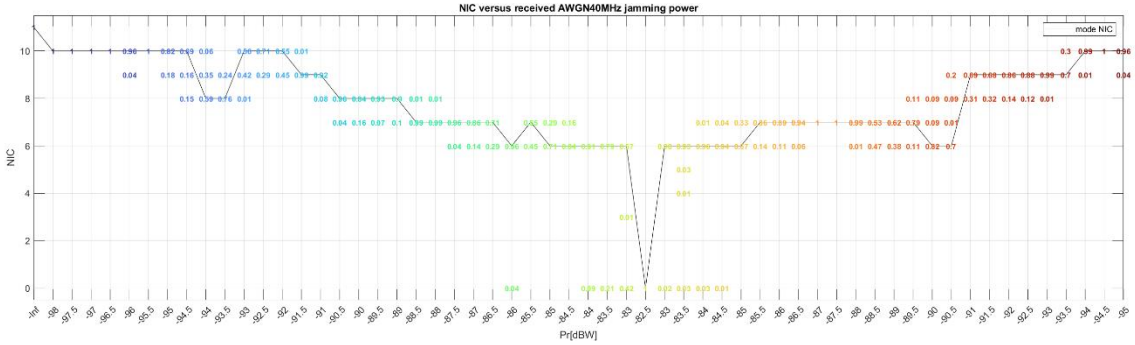

Figure 9 *NIC versus received jamming power of Noise jammer 40 MHz bandwidth*

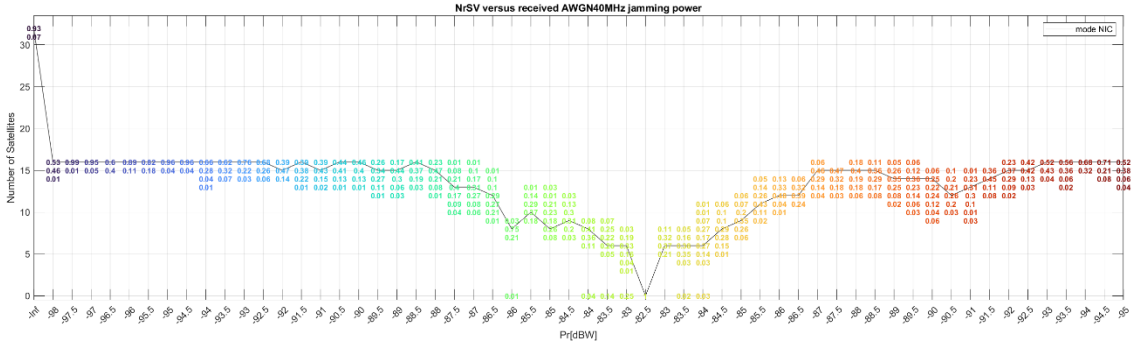

Figure 10 *Number of satellites versus received jamming power of Noise jammer 40 MHz bandwidth*

7. CONCLUSION

The two experiments are conducted in the built testbed. The result reveals how protection level reacts during different types of jamming, power level and receivers. Also, there is a non-linear and discrete relationship between received jamming power and NIC. When using the NIC from ADS-B as jamming measurement, need to take the factors previously described into account.

In the next step, we would like to extend our testing from aviation to marine and autonomous driving. Identify how integrity level indicators from AIS would react under different jamming scenarios. Compare results from different protection level calculation algorithms.

ACKNOWLEDGMENTS

We gratefully acknowledge the support of the FAA Satellite Navigation Team for funding this work under Memorandum of Agreement #: 693KA8-22-N-00015. We also acknowledge Professor Dennis M. Akos for providing Septentrio mosaic-X5 receiver and Mr. Stuart Riley, Dr. David De Lorenzo from Trimble for providing the Trimble BX-940 receiver.

REFERENCES

Blanch, J., Walter, T., Enge, P., Lee, Y., Pervan, B., Rippl, M., Spletter, A., Kropp, V. (2015). Baseline Advanced RAIM User Algorithm and Possible Improvements, *IEEE Transactions on Aerospace and Electronic Systems*, *Volume 51, No. 1, January 2015.*

Rothmaier, F., Chen, Y-H., Lo, S. (2019). Improvements to steady state spoof detection with experimental validation using a dual polarization antenna. *Proc. of the 32nd International Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2019), Miami, FL,* 967-983. https://doi.org/10.33012/2019.16989

Liu, Z., Lo, Sherman, Walter, T., and Blanch, J. (2022). Real-time Detection and Localization of GNSS Interference Source Published in *Proceedings of the 35th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2022), Denver, CO.*