Experimental Validation of Optimal INS Monitor against GNSS Spoofer Tracking Error Detection

Birendra Kujur
MMAE Department
Illinois Institute of Technology
Chicago, USA
bkujur@hawk.iit.edu

Samer Khanafseh
MMAE Department
Illinois Institute of Technology
Chicago, USA
khansam1@hawk.iit.edu

Boris Pervan
MMAE Department
Illinois Institute of Technology
Chicago, USA
pervan@iit.edu

***Abstract*—In this paper, we demonstrate the performance of the proposed optimal Inertial Navigation System (INS) monitor [19] using experimental setup that includes Global Navigation Satellite System (GNSS) spoofing scenarios using state-of-the-art GNSS spoofing software Skydel and real IMU data. Skydel is a software-based simulation platform which can generate GNSS radio frequency (RF) signals that can be fed into a receiver, using a Universal Software Radio Peripheral (USRP). The experimental setup includes GNSS, and Inertial Measurement Unit (IMU), dynamic data collection unit in a ground vehicle, which is used to generate the test trajectory for Skydel. Skydel is then used to generate authentic and spoofed signals which are then collected using a GNSS receiver. Along with the previously collected IMU data, the authentic and spoofed signals are used to validate the optimal INS monitor. A spoofer's uncertainty of user position (or position tracking error) is modeled as white Gaussian noise and added to the replica of authentic signal to form the spoofed signal. We show that the monitor is able to detect spoofer's tracking error even at decimeter level magnitudes. As a result, the conducted experiments demonstrate the monitor ability in detecting realistic GNSS spoofing events even with minimal tracking errors.**

***Index Terms*—GNSS spoofing, INS, spoofer tracking error**

I. Introduction

The civil infrastructure of safety critical fields such as aviation, maritime and terrestrial navigation rely on GNSS. This brings a major responsibility to ensure absolute GNSS integrity. The civil GNSS signal structure is publicly known and vulnerable to spoofing attacks, which endangers public safety [1]. Spoofing attacks consist of intentional jamming of the authentic radio-frequency signals and feeding a pre-determined faulty signal to the user. The fault can be injected to cause gradual position or time offsets. Potential detection techniques include signal processing techniques, cryptographic authentication [2], spoofing discrimination using spatial processing by antenna arrays, and automatic gain control schemes [3], [4], GNSS signal direction of arrival comparison [5], code and phase rate consistency checks [6], high-frequency antenna motion [7], and signal power monitoring techniques [8]. Some of these methods are indeed effective but they have various computational, logistical and physical limitations. Augmenting data from auxiliary sensors such as Inertial Measurement Units (IMU), barometric altimeters, and independent radar sensors to discriminate spoofing has also been proposed [9], [10].

The first stochastic description and quantification of the performance of IMU-based GNSS spoofing monitor against worst-case faults was introduced by us [11-17]. We specifically investigated anti-spoofing solutions utilizing IMUs, since all modern vehicles are equipped with them, thereby requiring minimal additional cost or system modification. An IMU is immune to external interference, which makes it the best candidate for counter measure against GNSS spoofing attacks. INS, when used in the navigation solution in various integration schemes with GNSS (such as uncoupled, loosely-, tightly-, or ultra-tightly coupled), provides redundancy to the system, which is a direct means of resisting spoofing attacks.

To specifically address the most difficult to detect scenario where a spoofer replicates the authentic GNSS signal with only additive errors due to the spoofer's uncertainty and latency in knowledge of the target's position, we developed an optimal INS monitor [19]. The monitor accumulates the spoofer's target tracking errors over time to detect the anomalous temporal structure of the spoofed measurements. We provided an analytical method for determining the length of the monitor window that would ensure detection of tracking error with a given missed detection probability. We evaluated the performance of the monitor with tracking errors modeled as both white and colored Gaussian noise and showed detectability of decimeter level tracking error noise with low probability of missed detection.

This work experimentally validates the analytical performance shown in our prior work [19]. In section II we review the optimal INS monitor and the predicted analytical performance. The experimental setup and the spoofing scenario utilized for this work is described in section III. The monitor performance with this experimental setup is shown in section IV. Finally, we conclude this work in section V.

II. Optimal INS Monitor

In this section we review the optimal INS monitor and its predicted analytical performance.

A. Kalman Filter State Model

The navigation architecture considered in this work is a tightly-coupled GNSS/INS Kalman filter (KF) which provides navigation solution using IMU and GNSS measurements. The dynamics of the system is represented with the process model,

$$\mathbf{x}_{k+1} = \mathbf{\Phi}_k \mathbf{x}_k + \mathbf{\Gamma}_{w_k} \mathbf{w}_k, \tag{1}$$

where $\mathbf{x}_k$ is the state vector, $\mathbf{\Phi}_k$ is the state transition matrix, $\mathbf{\Gamma}_{w_k}$ is the process noise model matrix, and $\mathbf{w}_k$ is the additive white process noise with a respective covariance matrix $\mathbf{Q}_k$. The measurement model is

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \boldsymbol{\nu}_k, \tag{2}$$

where $\mathbf{H}_k$ is the observation matrix and $\boldsymbol{\nu}_k$ is the measurement noise with a respective covariance matrix $\mathbf{V}_k$. The innovation vector $\boldsymbol{\gamma}_k$ with respective covariance matrix $\mathbf{S}_k$ at time epoch k is defined as

$$\boldsymbol{\gamma}_k = \mathbf{z}_k - \mathbf{H}_k \overline{\mathbf{x}}_k \tag{3}$$

where, $\overline{\mathbf{x}}$ is the state vector estimate prior to the measurement update at time epoch k.

B. Cumulative Position Domain Innovation Monitor

We choose the most difficult to detect spoofing scenario where the spoofer replicates the authentic signals with only additive noise. This additive noise represents the uncertainty of user position due to limitations of methods and devices used to track the user position. In our prior work [19], we showed that the spoofer's tracking error of target position would first appear in the innovations. The general detection principle is to accumulate these tracking errors over time (say period N) to detect spoofing. If the spoofer has tracking error in an arbitrary spatial direction represented by unit vector $\mathbf{u}$, we derived that the optimal test statistic to observe these tracking error is through a Neyman-Pearson test statistic given as,

$$q_{N} = \sum_{k=1}^{N} (\gamma_k^u)^T \gamma_k^u, \tag{4}$$

where we define the γ_k^u as the *scalar* projection of the innovation vector and is represented as

$$\gamma_k^u = \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} \gamma_k, \tag{5}$$

It can be interpreted as a weighted projection of the innovation vector into the position domain direction $\mathbf{u}$—i.e., the tracking error direction under consideration. Thus, we define γ_k^u as the position domain innovation.

Under spoof-free conditions, the scalar position domain innovation in Eq. (5) is Normally distributed as

$$\gamma_k^u \sim \mathcal{N}(0, \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} \mathbf{H}_k \mathbf{u}). \tag{6}$$

To simplify the notation, we define the variance as

$$\sigma^2_{\gamma_k^u} = \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} \mathbf{H}_k \mathbf{u}. \tag{7}$$

For the spoofed case, we model the tracking error ν_k^t as white Gaussian noise (WGN) distributed as $\mathcal{N}(0, \sigma_t^2)$, where σ_t^2 is the *unknown* variance of the tracking error. This tracking error appears in the test statistic as (Note: subscript s is used to represent spoofed case.)

$$\gamma_k^{us} = \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} (\gamma_k + \mathbf{H}_k \nu_k^t) = \gamma_k^u + \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} \mathbf{H}_k \mathbf{u} \nu_k^t. \tag{8}$$

Thus, under spoofed conditions, the position domain innovation has the following Normal distribution:

$$\gamma_k^{us} \sim \mathcal{N}(0, \sigma^2_{\gamma_k^u} + \sigma^4_{\gamma_k^u} \sigma_t^2), \tag{9}$$

For notational simplicity, we also define,

$$\sigma^2_{\Delta\gamma_k^{us}} = \sigma^4_{\gamma_k^u} \sigma_t^2. \tag{10}$$

For a period of accumulation N, our optimal Cumulative position-domain innovation (CPI) test statistic (in the unspoofed case) is

$$q_{N} = \sum_{k=1}^{N} \left(\frac{\gamma_k^u}{\sigma_{\gamma_k^u}} \right)^2 \tag{11}$$

The test statistic in the unspoofed case q_{N} is Gamma distributed as follows,

$$q_{N} \sim \Gamma\left(\sum_{k=1}^{N} \frac{1}{2}, 2 \right) = \Gamma\left(\frac{N}{2}, 2 \right). \tag{12}$$

In the spoofed case, with the tracking error embedded in the test statistic, we have

$$q_{N}^{s} = \sum_{k=1}^{N} \left(\frac{\gamma_k^{us}}{\sigma_{\gamma^u}} \right)^2 \sim \Gamma\left(\sum_{k=1}^{N} \frac{1}{2}, 2 \left(1 + \frac{\sigma^2_{\Delta\gamma^{us}}}{\sigma^2_{\gamma^u}} \right) \right). \tag{13}$$

Defining the ratio $\Omega = (\sigma_{\Delta\gamma^{us}} / \sigma_{\gamma^u})^2$ the above equation can be re-written as

$$q_{N}^{s} \sim \Gamma\left(\frac{N}{2}, 2\left(1 + \Omega\right) \right). \tag{14}$$

C. Monitor Analytical Performance

In our prior work [19], we showed the performance of the monitor against spoofing of an en route aircraft. The analytical performance evaluation was done for an aircraft cruising at level flight, equipped with a navigation grade IMU, and utilizing single frequency GPS measurements. All the satellite, atmospheric, and environmental errors in the GPS measurements were compensated using error models in the KF. The IMU measurement rate was 4 Hz whereas the GPS measurement rate was 2 Hz. Tracking errors were modeled as WGN and added to authentic GPS measurements to generate spoofed measurements. We showed that performance of the monitor is dependent on the carrier phase measurement accuracy and velocity random walk (VRW) of the IMU.

Figure 1 illustrates the missed detection probability as a function of tracking error and monitor run time. Thus, for a given scenario, and missed detection requirement with knowledge of spoofer's minimum tracking error magnitude, the run time for the monitor can be determined.

In this work, we aim to validate this optimal detection method with experimental results which includes real IMU and GPS measurements. We choose dynamic scenario of a ground vehicle to analyze the experimental performance of the monitor.

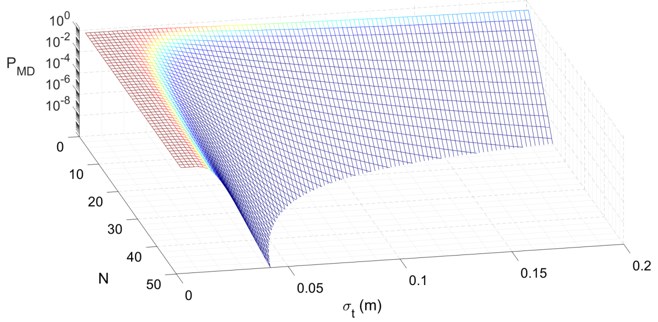

Fig. 1. CPI probability of missed detection P_{MD} versus tracking error σ_t and monitor run time N.

III. Experimental Setup

The experimental setup for this work includes the software platform Skydel and and the hardware comprised of GNSS/INS board and USRP.

a) Skydel GNSS Simulation Software: Skydel is a software-based GNSS simulation platform which offers multi-constellation/multi-frequency signal generation from user-defined scripts, and integrated spoofing and interference generations. Skydel is used to create GNSS/RF signals digitally, and software-defined radios (SDR) to output RF. Figure 2 illustrates how Skydel is used for reproducing live sky conditions with an active antenna. We choose Skydel to generate spoofed measurements instead of digitally adding tracking error noise to collected GPS measurements, as this closely mimics the actual spoofing process of having tracking errors embedded into digital signals before transmitted as RF.

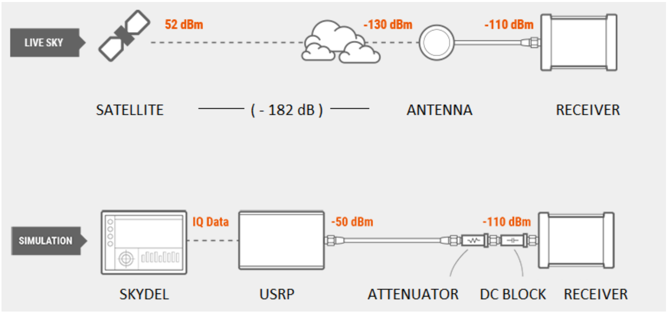

Fig. 2. Illustration of Skydel reproducing live sky conditions with an active antenna [21].

b) Hardware: The GNSS/INS board used for this experimental setup is AsteRx-i3 S Pro+ from Septentrio. This GNSS/INS board is equipped with an industrial grade IMU, ELLIPSE2-I-G4-A3, from SBG systems. Figure 3 shows the GNSS/INS board used to collect experimental data. The ELLIPSE2-I-G4-A3 IMU specifications are listed in Table I. The Ettus X300 USRP is used to transmit RF signals to the GNSS receiver.

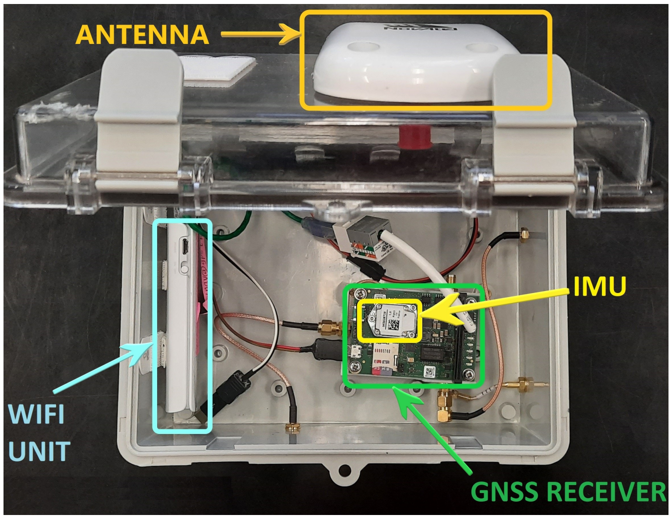

Fig. 3. GNSS/INS board for experimental data collection.

TABLE I
IMU specifications for ELLIPSE2-I-G4-A3

	Accelerometers	***Gyroscopes***
Bias stability	± 5 mg	± 0.2 deg/s
Random walk	57 μg /$\sqrt{\text{Hz}}$	0.15 deg/$\sqrt{\text{hr}}$
Bias in-run instability	14 μg	7 deg/hr
Bias time constant	3600 s	3600 s

Figure 4 illustrates the block diagram for the experimental setup. GNSS and IMU data is collected using the GNSS/INS board. This data is used to generate a trajectory which is then used in Skydel to generate both authentic and spoofed GNSS signals. The spoofed signals here refer to signals generated using the authentic trajectory with additive tracking error noise. This method of generating spoofed signals mimics the spoofer's process of generating GNSS signals. These GNSS signals are fed into the USRP digitally to generate RF signals which are collected using a GNSS receiver. Together with IMU measurements previously collected, the GNSS measurements obtained from the GNSS receiver are fed into the KF to obtain navigation solution. The optimal INS monitor uses the output from the KF (specifically the innovations) to detect spoofing.

IV. Monitor Performance

A dynamic scenario with an automotive vehicle is considered to evaluate the monitor performance. Dynamic GNSS/INS data is collected using a vehicle driving around Illinois Tech's campus. Figure 5 shows the trajectory of the vehicle along which GNSS/IMU data is collected. The data is collected with an IMU measurement rate of 100 Hz and GNSS measurement rate of 2 Hz. Skydel is used to generate GPS L1 C/A signals for this given trajectory and tracking error as WGN is added to the trajectory itself mimicking how tracking error would appear in spoofed signals. For simplicity, GPS measurements without ionospheric and tropospheric errors are generated using Skydel.

We choose a dynamic section as shown in Figure 6 within this trajectory where GPS signals switch from authentic to spoofed. Also, the monitor starts monitoring for spoofing as

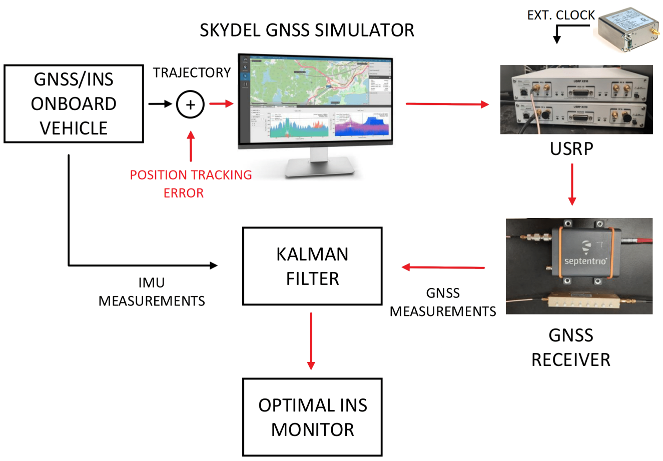

Fig. 4. Illustration of experimental setup block diagram.

soon as spoofed signals are substituted. In our prior work [19], we explain in detail the architecture of using windows of optimal INS monitors to ensure that start of INS monitor is always coincident to spoofing onset. We added centimeter level tracking errors in the z-position (down) direction. Figure 7 shows the monitor performance for tracking error standard deviations of 5 and 10 centimeters. A false alarm rate of 10^{-5} was used to determine the threshold which is shown as normalized value of 1 in Figure 7. It can be seen that for both these tracking error magnitudes detection occurs within 30 seconds. As expected, a larger tracking error will result in faster detection as shown in Figure 7.

Future work includes sensitivity analysis of the monitor to error models utilized in the KF and also evaluating monitor performance with live spoofing data.

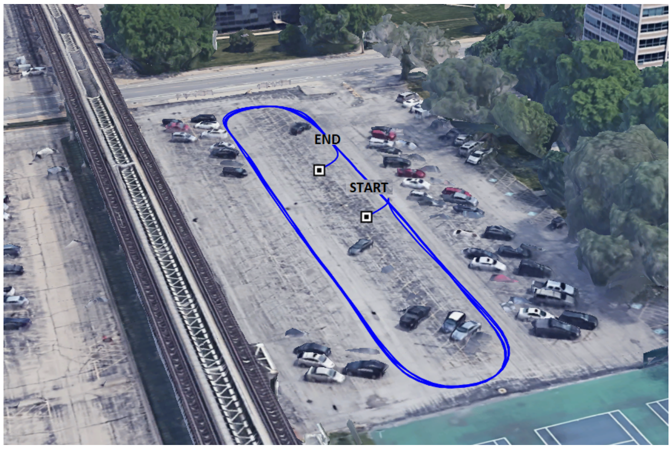

Fig. 5. Illustration of trajectory used for experimental validation.

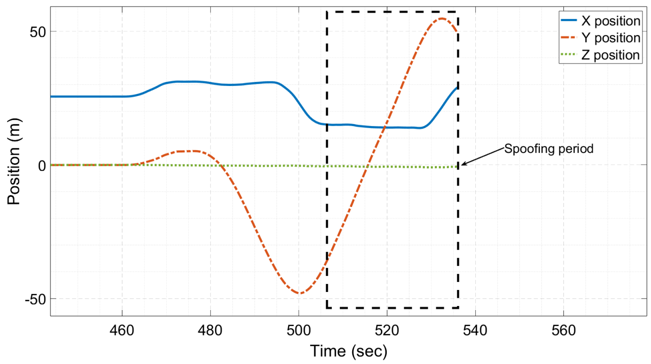

Fig. 6. Illustration of trajectory section where tracking error was introduced to mimic spoofed signals.

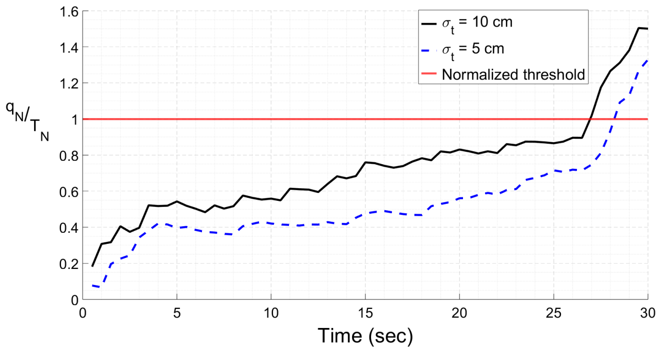

Fig. 7. Monitor performance in dynamic scenario for different tracking errors.

V. Conclusion

To validate the optimal INS monitor, real dynamic data using GNSS receiver and IMU are collected with a ground vehicle driving around Illinois Tech's campus. This data is used to generate a trajectory using the Skydel software. Skydel software is then used to generate authentic and spoofed GNSS signals along the desired trajectory. The simulated spoofed GNSS signals mimics the authentic signals but with additive tracking error noise. The Skydel output is then fed into a USRP, which provides the RF data to a commercial GNSS receiver through an RF cable. These GNSS signals along with the previously collected IMU data are then used in the tightly-coupled KF through which optimal INS monitor's performance is evaluated. Experimental results validate the detection methodology of the optimal INS monitor. The optimal INS monitor can detect spoofing even with decimeter level tracking error in less than 30 seconds.

VI. Acknowledgment

We would like to thank Orolia (Safran) for the donation of Skydel simulation software to Navigation and Guidance Lab, Department of Mechanical, Materials and Aerospace Engineering at Illinois Institute of Technology.

References

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, and B. W. O'Hanlon, "Assessing the spoofing threat: development of a portable GPS civilian spoofer," in Proc. IEEE/ION PLANS, Savannah, GA, 2008, pp. 2314–2325.

[2] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "A proposed navigation message authentication implementation for civil GPS anti-spoofing," in Proc. IEEE/ION PLANS, Portland, OR, 2011, pp. 3129-3140.

[3] D. M. Akos, “Who’s afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC),” Navigation, vol. 59, no. 4, pp. 281–290, Winter. 2012.

[4] J. Nielsen, A. Broumandan, and G. Lachapelle, “Spoofing detection and mitigation with a moving handheld receiver,” GPS World, vol. 21, no. 9, pp. 27–33, Sep. 2010.

[5] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hattich, “Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM,” in Proc. ION GNSS+, Nashville, TN, 2012, pp. 3007–3016.

[6] S. Moshavi, “Multi-user detection for DS-CDMA communications,” IEEE Communications Magazine, vol. 34, no. 10, pp. 124–135, Oct. 1996.

[7] M. L. Psiaki, S. P. Powell, and B. W. O’Hanlon, “GNSS spoofing detection using high-frequency antenna motion and carrier-phase data,” in Proc. ION GNSS+, Nashville, TN, 2013, pp. 2949–2991.

[8] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables,” International Journal of Satellite Communications and Networking, vol. 30, no. 4, pp. 181–191, Jul. 2012.

[9] P. F. Swaszek, R. J. Hartnett, and K. C. Seals, “GNSS spoof detection using independent range information,” in Proc. ION ITM, Monterey, CA, 2016, pp. 739–747.

[10] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, “Unmanned aircraft capture and control via GPS spoofing,” Journal of Field Robotics, vol. 31, no. 4, pp. 617–636, 2014.

[11] S. Khanafseh, et. al., ““GPS Spoofing Detection Using RAIM with INS Coupling,” in Proc. ION PLANS Conference, Monterey, CA, 2014.

[12] C. Tanil, S. Khanafseh, and B. Pervan, “Impact of Wind Gust on Detectability of GPS Spoofing Attack Using RAIM with INS Coupling,” in Proc. IEEE/ION PNT Conference, Honolulu, HI, 2015, pp. 1232–1239.

[13] C. Tanil, S. Khanafseh, and B. Pervan, “GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory,” in Proc. ION GNSS+, Tampa, FL, 2015, pp. 3345–3357.

[14] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, “Kalman filter-based Innovation monitor to detect GNSS spoofers capable of tracking aircraft position,” in Proc. IEEE/ION PLANS, Savannah, GA, 2016, pp. 1027–1034.

[15] C. Tanil, S. Khanafseh, and B. Pervan, “An Innovation monitor against GNSS Spoofing Attacks during GBAS and SBAS- assisted Aircraft Landing Approaches,” in Proc. ION GNSS+, Portland, OR, 2016.

[16] C. Tanil, S. Khanafseh, and B. Pervan, “Detecting Global Navigation Satellite System spoofing using inertial sensing of aircraft disturbance,” Journal of Guidance, Control, and Dynamics, vol. 40, no. 8, pp. 2006–2016, 2017.

[17] C. Tanil, S. Khanafseh, M. Joerger, B. Pervan, “An Innovation monitor to Detect GNSS Spoofers Capable of Tracking Aircraft Position,” IEEE Transactions on Aerospace and Electronics, vol. 54, no. 1, pp. 131–143, Feb 2018.

[18] C. Tanil, P. M. Jimenez, M. Raveloharison, B. Kujur, S. Khanafseh, B. Pervan, “Experimental Validation of INS Monitor against GNSS Spoofing,” in Proc. ION GNSS+, Miami, FL, Sep 2018.

[19] B. Kujur, S. Khanafseh, and B. Pervan, “Optimal INS Monitor for GNSS Spoofer Tracking Error Detection,” Navigation (Under review).

[20] ”Orolia Skydel User Manual,” orolia.com. https://www.orolia.com/manuals/skydel/ (accessed Jan. 9, 2023).