

Performance of Optimal INS Monitor Against Live Spoofing

Birendra Kujur, Samer Khanafseh, Boris Pervan, *Illinois Institute of Technology*

BIOGRAPHY

Birendra Kujur is currently a PhD candidate in Mechanical and Aerospace Engineering at Illinois Institute of Technology. He received his Bachelor of Science in Mechanical Engineering from Purdue University in 2014. His research interests include multi-sensor navigation systems, navigation integrity monitoring, detecting GNSS spoofing attacks, and developing anti-spoofing solution.

Dr. Samer Khanafseh is currently a research associate professor at Illinois Institute of Technology (IIT), Chicago, and the principal of TruNav LLC. He received his MSc and PhD degrees in Aerospace Engineering from IIT in 2003 and 2008, respectively. Dr. Khanafseh has been involved in several aviation applications such as Autonomous Airborne Refueling (AAR) of unmanned air vehicles, autonomous shipboard landing for NUCAS and JPALS programs and Ground Based Augmentation System (GBAS). His research interests are focused on high accuracy and high integrity navigation algorithms, cycle ambiguity resolution, high integrity applications, fault monitoring and robust estimation techniques. He was the recipient of the 2011 Institute of Navigation Early Achievement Award for his outstanding contributions to the integrity of carrier phase navigation systems.

Dr. Boris Pervan is a Professor and Frank Gunsaulus Faculty Fellow in Mechanical and Aerospace Engineering at the Illinois Institute of Technology (IIT), where he conducts research on high integrity navigation systems. Prior to joining the faculty at IIT, he was a spacecraft mission analyst at Hughes Aircraft Company (now Boeing) and a postdoctoral research associate at Stanford University. Prof. Pervan received his B.S. from the University of Notre Dame, M.S. from the California Institute of Technology, and Ph.D. from Stanford University. He has received the Samuel M. Burka and Johannes Kepler Awards from the Institute of Navigation (ION), IIT Sigma Xi Excellence in University Research Award (twice), IIT University Excellence in Teaching Award, IEEE Aerospace and Electronic Systems Society M. Barry Carlton Award, RTCA William E. Jackson Award, Guggenheim Fellowship (Caltech), and the Albert J. Zahm Prize in Aeronautics (Notre Dame). He is a Fellow of the ION and former Editor-in-Chief of the ION journal NAVIGATION.

ABSTRACT

In this paper, we demonstrate the performance of the proposed optimal Inertial Navigation System (INS) monitor (Kujur et al. (2024)) against live spoofing with multiple Global Navigation Satellite System (GNSS) spoofing scenarios. We evaluate the monitor performance for a live spoofing event where an aircraft was subjected to live GNSS spoofed signals using onboard equipment during its flight with different spoofed trajectories such as step, ramp, and accelerating position offsets. The spoofing signals were generated and broadcast on a single frequency GPS constellation while spoof-free GNSS signals were acquired using other constellations. Spoofed GPS signals, spoof-free GNSS signals, and Inertial Measurement Unit (IMU) dynamic data was collected. Results show that the optimal INS monitor can detect spoofing even at sub-decimeter level magnitudes within minutes. As a result, the conducted experiment demonstrates the monitor's ability to detect realistic GNSS spoofing events even with minimal position offsets, thereby validating the performance of the monitor.

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 (Humphreys et al. (2008)). Spoofing attacks consist of intentional jamming of the authentic radio-frequency signals and feeding a predetermined 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 (Wesson et al. (2011)), spoofing discrimination using spatial processing by antenna arrays, and automatic gain control schemes (Akos (2012)), (Nielsen et al. (2014)), GNSS signal direction of arrival comparison (Meurer et al. (2012)), code and phase rate consistency checks (Moshavi (1996)), high-frequency antenna motion (Psiaki et al. (2013)), and signal power monitoring techniques (Jafarnia-Jahromi et al. (2012)). 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 (Swaszek et al.

(2016)), (Kerns et al. (2014)).

The first stochastic description and quantification of the performance of an IMU-based GNSS spoofing monitor against worst-case faults was introduced by us (Khanafseh et al. (2014); Kujur et al. (2019); Tanil et al. (2016a, 2018, 2015a,b, 2016b, 2017)). 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 (Kujur et al. (2024)). 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 centimeter level tracking error noise with a low probability of missed detection (10^{-7}) and false alarm (10^{-5}). We also experimentally validated the performance of the optimal monitor with simulated spoofing scenarios (Kujur et al. (2023)).

This work validates the realistic application of the optimal INS monitor against live spoofing. In Section II we review the optimal INS monitor and the predicted analytical performance. The live spoofing scenarios are described in Section III and the monitor performance against these different live spoofing scenarios is presented in Section IV. Finally, we conclude this work in Section V.

II. OPTIMAL INS MONITOR

1. Kalman Filter State Model

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

$$\mathbf{x}_{k+1} = \Phi_k \mathbf{x}_k + \Gamma_{w_k} \mathbf{w}_k, \quad (1)$$

where \mathbf{x}_k is the state vector, Φ_k is the state transition matrix, Γ_{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

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{v}_k, \quad (2)$$

where \mathbf{H}_k is the observation matrix and \mathbf{v}_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

$$\boldsymbol{\gamma}_k = \mathbf{z}_k - \mathbf{H}_k \bar{\mathbf{x}}_k \quad (3)$$

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

2. 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 (Kujur et al. (2024)), 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 errors is through a Neyman-Pearson test statistic given as,

$$q_N = \sum_{k=1}^N (\boldsymbol{\gamma}_k^\mu)^T \boldsymbol{\gamma}_k^\mu, \quad (4)$$

where we define $\boldsymbol{\gamma}_k^\mu$ as the *scalar* projection of the innovation vector represented as

$$\boldsymbol{\gamma}_k^\mu = \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} \boldsymbol{\gamma}_k, \quad (5)$$

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^μ as the position domain innovation.

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

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

To simplify the notation, we define the variance as

$$\sigma_{\gamma_k^\mu}^2 = \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} \mathbf{H}_k \mathbf{u}. \quad (7)$$

For the spoofed case, we model the tracking error v_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: superscript s is used to represent spoofed case:)

$$\gamma_k^{\mu s} = \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} (\gamma_k + \mathbf{H}_k v_k^t) = \gamma_k^\mu + \mathbf{u}^T \mathbf{H}_k^T \mathbf{S}_k^{-1} \mathbf{H}_k \mathbf{u} v_k^t. \quad (8)$$

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

$$\gamma_k^{\mu s} \sim \mathcal{N}(0, \sigma_{\gamma_k^\mu}^2 + \sigma_{\gamma_k^\mu}^4 \sigma_T^2), \quad (9)$$

For notational simplicity, we also define,

$$\sigma_{\Delta \gamma_k^{\mu s}}^2 = \sigma_{\gamma_k^\mu}^4 \sigma_T^2. \quad (10)$$

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

$$q_N = \sum_{k=1}^N \left(\frac{\gamma_k^\mu}{\sigma_{\gamma_k^\mu}} \right)^2 \quad (11)$$

The test statistic in the unspoofed case q_N is Gamma distributed as follows,

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

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

$$q_N^s = \sum_{k=1}^N \left(\frac{\gamma_k^{\mu s}}{\sigma_{\gamma_k^\mu}} \right)^2 \sim \Gamma \left(\sum_{k=1}^N \frac{1}{2}, 2 \left(1 + \frac{\sigma_{\Delta \gamma_k^{\mu s}}^2}{\sigma_{\gamma_k^\mu}^2} \right) \right). \quad (13)$$

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

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

3. Monitor Analytical Performance

In our prior work (Kujur et al. (2024)), we also 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.

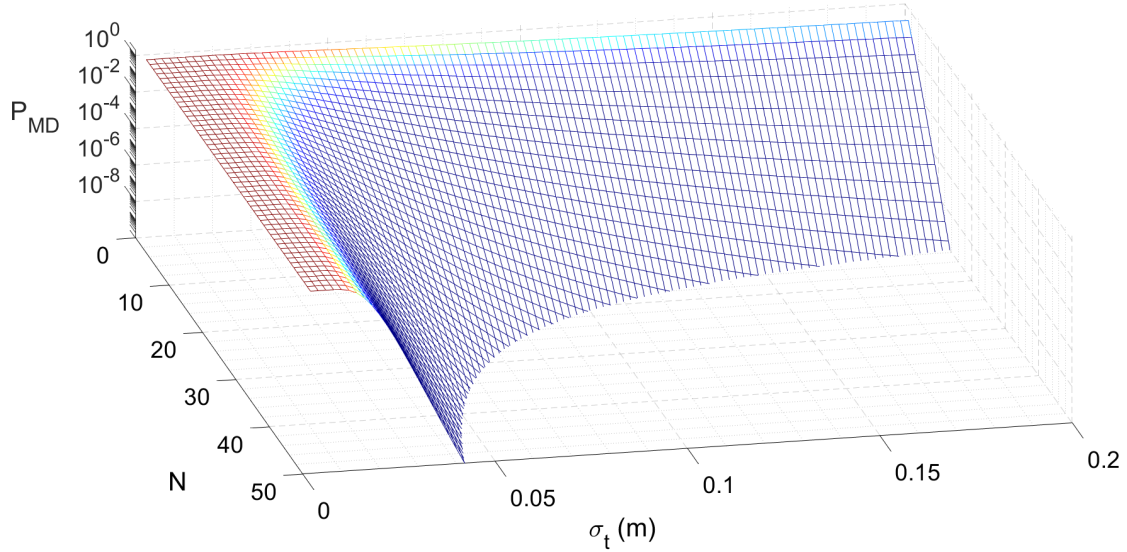


Figure 1: CPI probability of missed detection P_{MD} versus tracking error σ_t and monitor run time N .

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. After analytical simulation results and experimental validation of the monitor, the next step was to test the monitor against live spoofing to validate realistic performance. In the next section we provide details of the different live spoofing scenarios used for monitor validation.

III. LIVE SPOOFING SCENARIOS

An aircraft was subjected to live spoofing using on-board equipment during different phases of its flight. For this spoofing event it was known which sections of flight were spoofed as well as the spoofing profiles injected. A single GPS L1 frequency signal was spoofed with different three-dimensional spoofing profiles. The spoofed GPS L1 signal and other GNSS signals along with a near navigation grade IMU (FOG and MEMS accelerometer) measurements were collected.

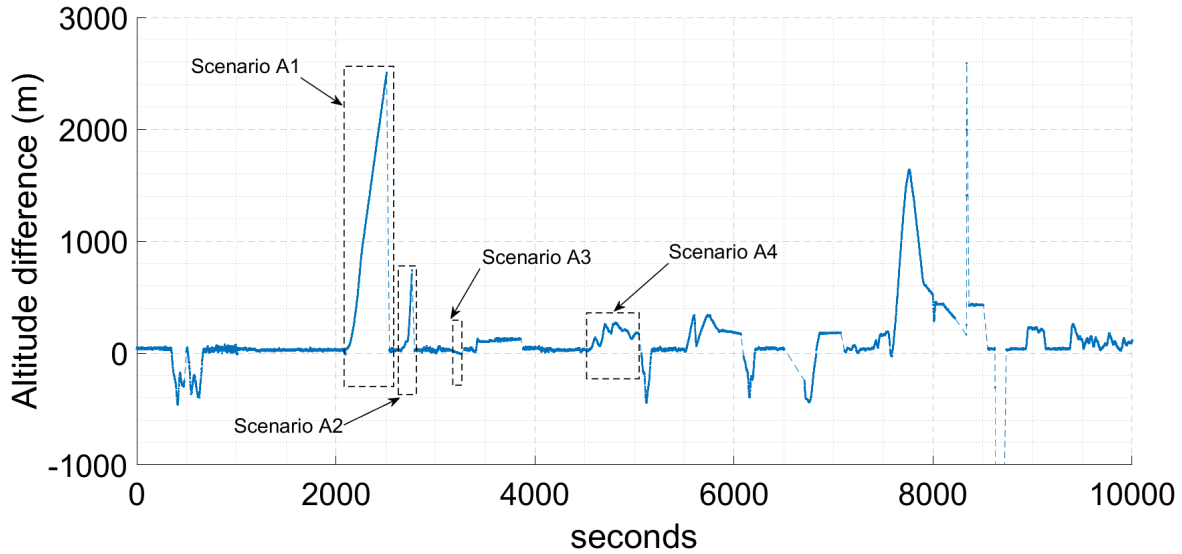


Figure 2: Difference in altitude position estimates between authentic and spoofed GNSS signals showing spoofed scenarios.

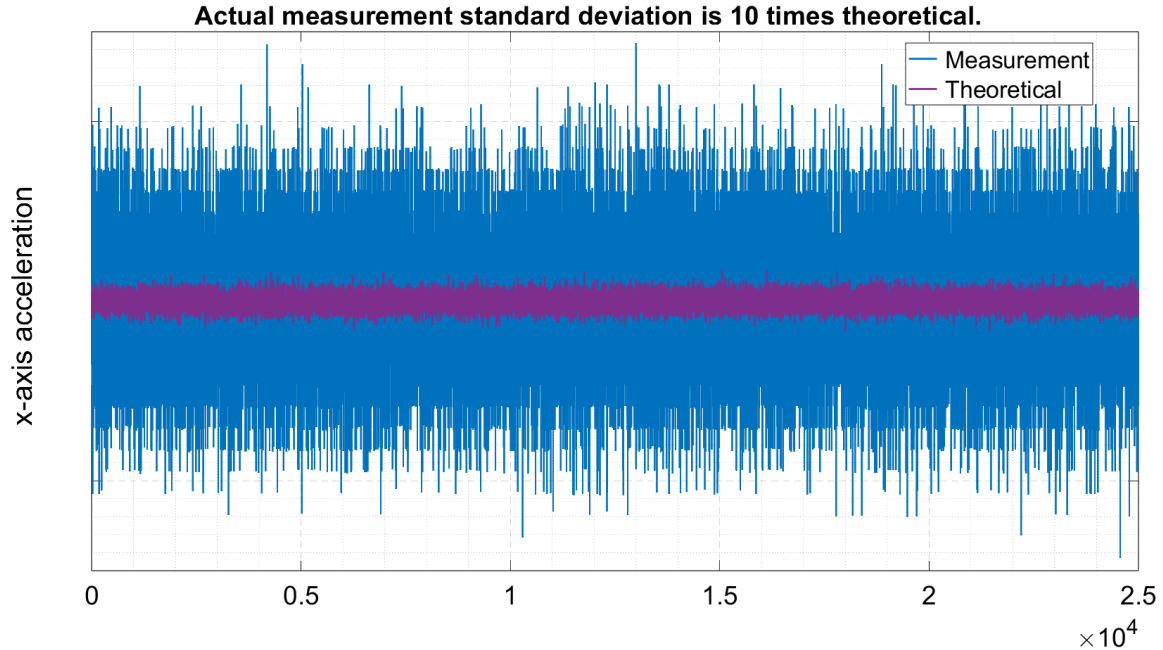


Figure 3: IMU performance degradation due to vibration noise.

Figure 2 shows the difference in vertical position estimates due to authentic and spoofed signals. For this validation work we only observe for discrepancies in the vertical direction. The figure illustrates the different vertical spoofing profiles injected along the spoofed sections during the flight. A total of four spoofing scenarios labeled A1 through A4 with profiles such as ramp, acceleration, oscillation, etc., are illustrated in Figure 2.

The measurement data set that captured the spoofed scenarios along with the IMU data was fed into a tightly-coupled Kalman filter. The optimal monitor sequential window implementation as described in our work (Kujur et al. (2024)) was utilized. The advantage of the optimal INS monitor to detect spoofing at a very early stage of spoofing (even before position offsets) relies on carrier phase measurement accuracy and short term IMU performance. If the IMU performance is degraded due to an external nuisance such as vibration, the monitor performance is degraded as well. The IMU used for this validation was an external IMU and not the avionics navigation grade IMU used for aircraft navigation. This external IMU was not isolated for vibration and was simply strapped to the aircraft frame. This caused the IMU to experience large magnitudes of vibration causing performance degradation. Figure 3 shows the IMU x-acceleration measurements compared to the theoretical sample measurements when the aircraft was stationary. It was observed that the standard deviation of the IMU measurements were 10 to 20 times larger than predicted by specifications. This caused the IMU noise error model standard deviations to be inflated resulting in an increased threshold for the optimal INS monitor. One of the drawbacks of a noisy IMU is that if the tracking error is small enough it cannot be distinguished from IMU noise. This caused detection performance degradation for the monitor. Thus, in this work, the monitor relied on a mix of tracking errors and position offsets to detect spoofing. In the next section we present the detection results for each of the spoofing scenarios.

IV. RESULTS

Figures 4, 6, 8, and 10 show the details for spoofing scenarios A1, A2, A3, and A4, respectively. These figures illustrate the time spoofing was initiated and the respective spoofing profiles. Figures 5, 7, 9, and 11 show the detection results for scenarios A1, A2, A3, and A4, respectively. The test statistic from Equation (11) after being normalized with the threshold is shown for each of the scenarios along with the spoofing profiles. Detection occurs once the normalized test statistic exceeds the normalized threshold value of 1. For all the detection results a monitor window was assumed to start before the spoofing.

The first scenario A1 starts once the aircraft is in its straight and level flight. As illustrated in Figure 4, a ramp-like short spoofing profile is injected that grows to 40 m offset in around 10 seconds and then after a sudden jump the spoofing proceeds with very slow acceleration profile. Figure 5 shows the detection result where spoofing is detected in the initial short ramp-like profile before the sudden jump in less than 10 seconds. This spoofing profile was the most aggressive compared to the others.

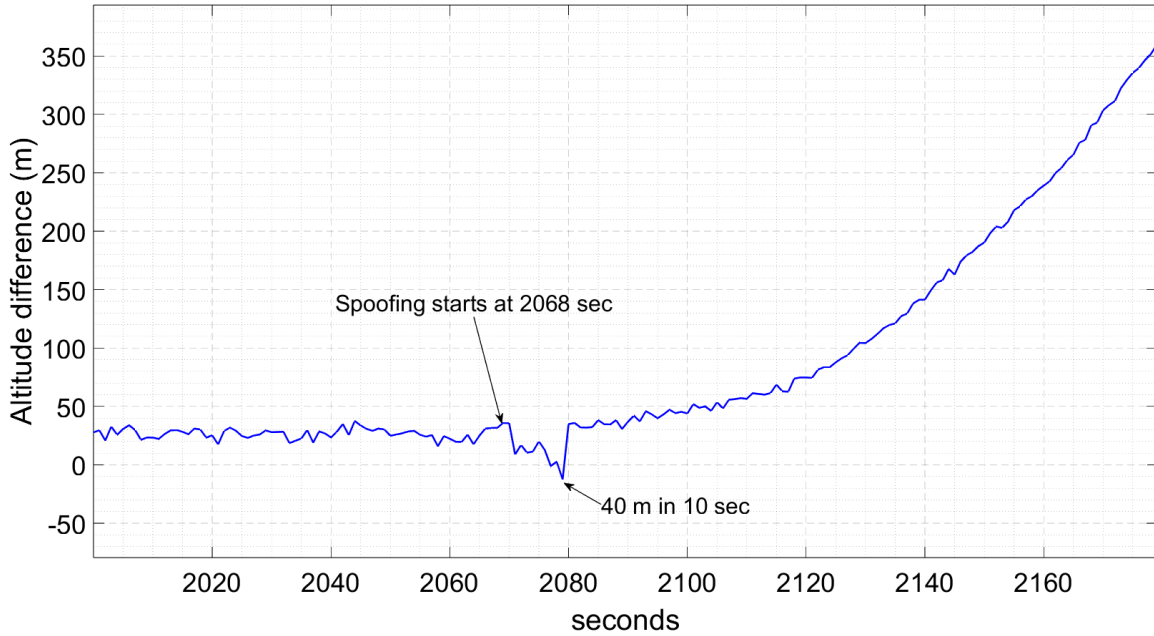


Figure 4: Spoofing scenario A1.

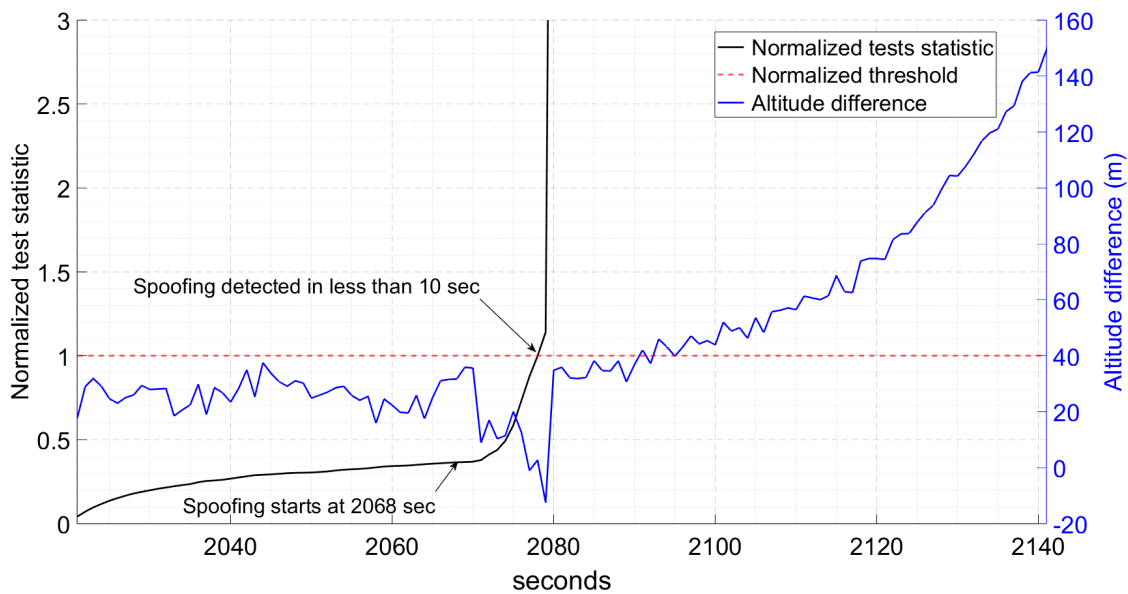


Figure 5: Detection result for scenario A1.

The next scenario A2 is also a ramp-like spoofing profile as illustrated in Figure 6 that grows slowly to around 70 m offset in 45 seconds. After a pause the spoofing profile further accelerates to 700 m. Figure 7 shows the detection result for this scenario. Even though the spoofing profile is ramping at a slower rate than scenario A1, it is still detected within 11 seconds.

Figure 8 illustrates scenario A3 where spoofing causes a very slow ramp profile but for extended duration, where the ramp causes an offset of 35 m in 120 seconds. This profile is indeed slow, but due to accumulation of errors over the extended time, detection was possible. Figure 9 shows the result for this scenario where detection occurs in 40 seconds, which given the rate of fault injected is about 11 meters.

The next scenario A4 is a wave-like spoofing profile as illustrated in Figure 10. Figure 11 shows the detection result for this

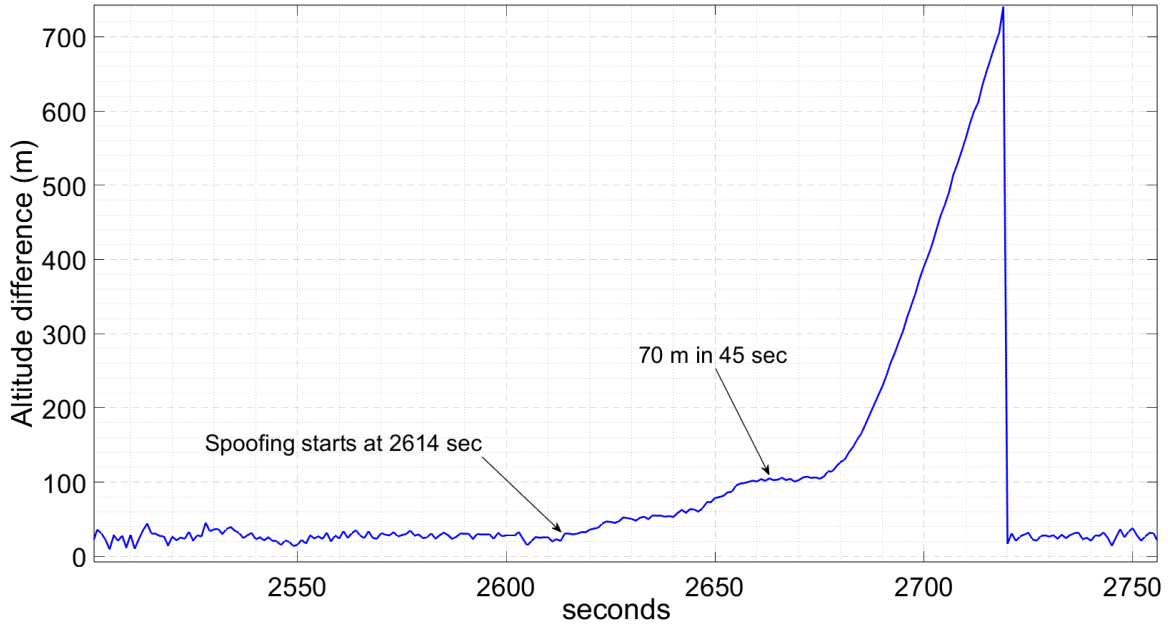


Figure 6: Spoofing scenario A2.

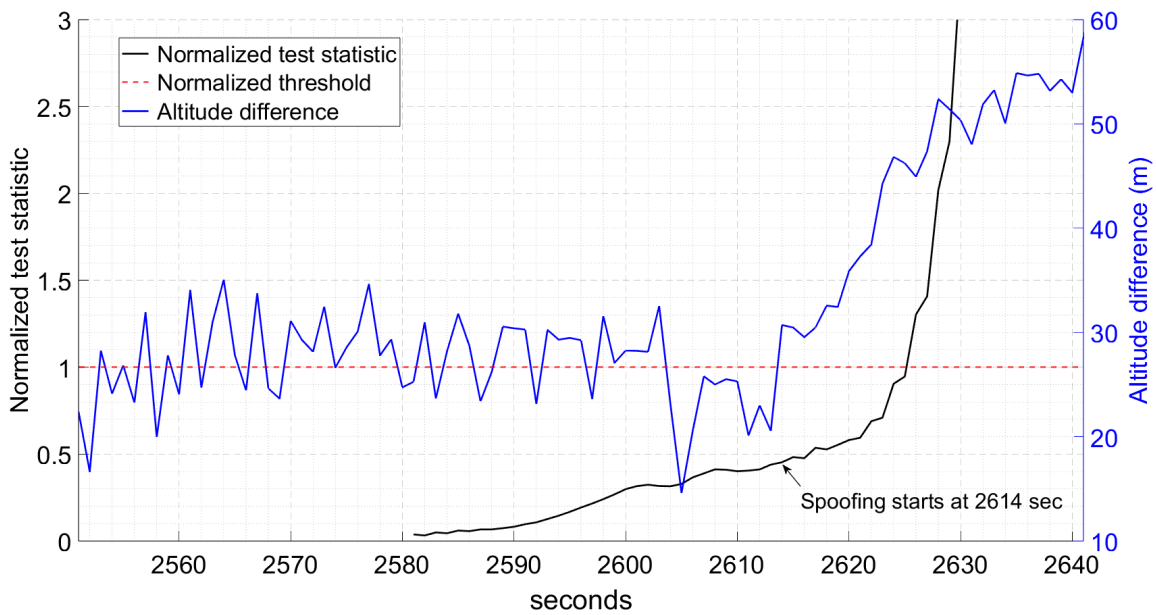


Figure 7: Detection result for scenario A2.

scenario. Due to continuous increase in position offset the test statistic also increases respectively causing detection within 25 seconds.

Scenarios where the spoofing profile was a sudden jump were not included in the results as they can be detected instantly. Although easily detectable, this kind of spoofing can cause major problems for flight management systems (FMS) which use GPS for positioning and time synchronization. For example, due to a sudden jump in position, alert systems such as the Terrain Avoidance and Warning System (TAWS) could be triggered.

A major takeaway from this live spoofing validation was the limitation of the IMU and therefore the monitor to detect spoofing in the presence of vibration noise. In order to achieve predicted performance of the monitor it is therefore necessary to isolate

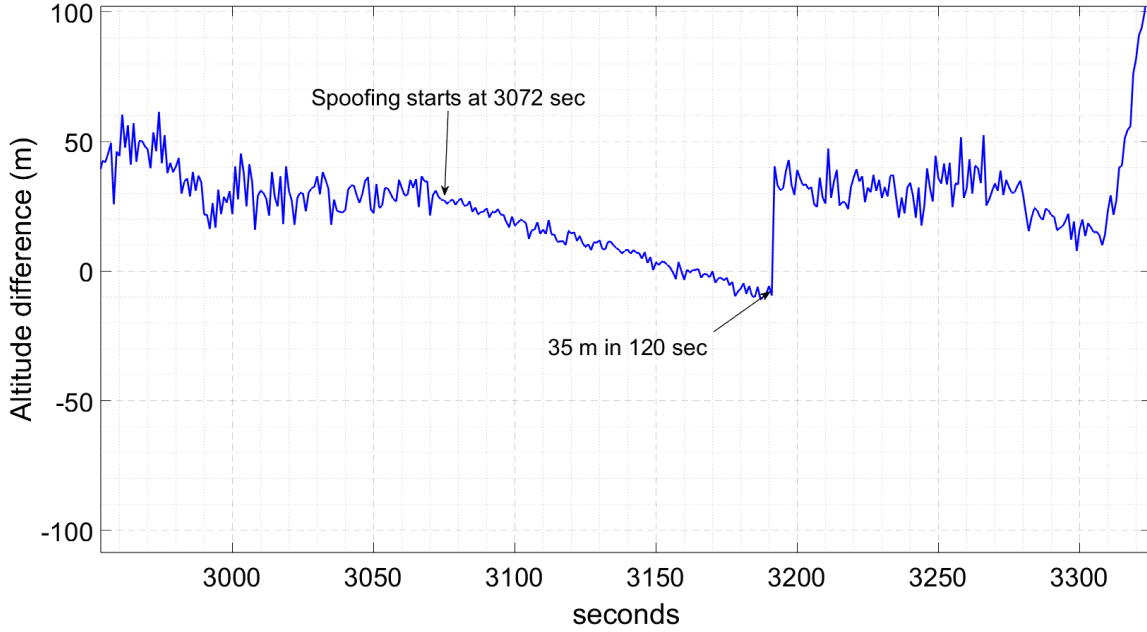


Figure 8: Spoofing scenario A3.

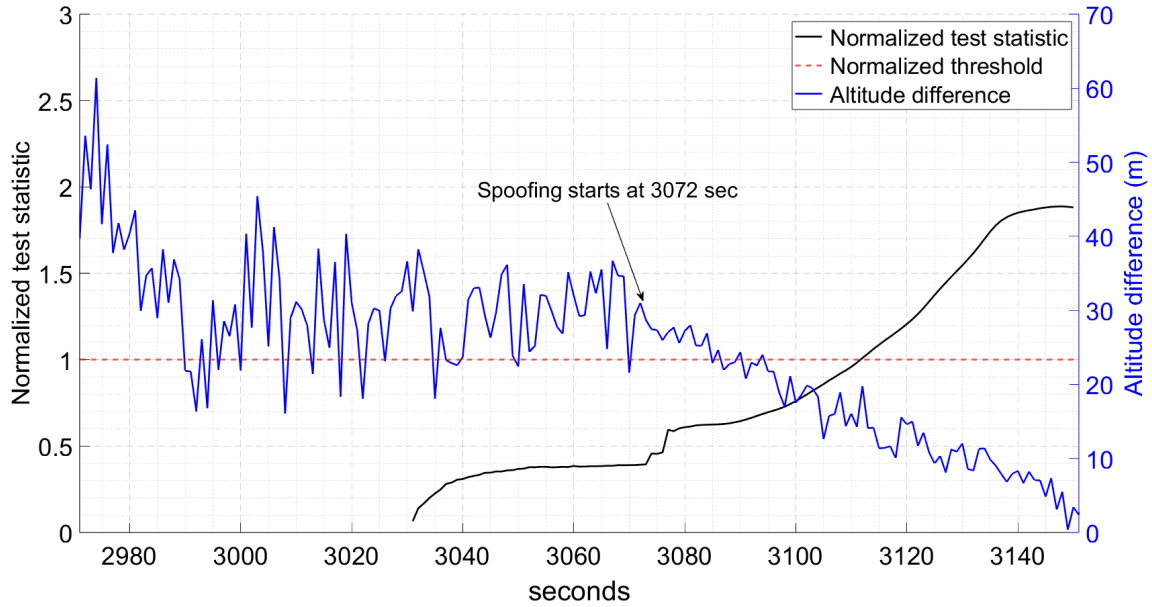


Figure 9: Detection result for scenario A3.

the vibrations affecting the IMU as much as possible.

V. CONCLUSION

To validate the monitor performance under realistic spoofing scenarios, GNSS measurements and IMU data for an aircraft under live spoofing are collected. These spoofed GNSS measurements along with the IMU data are then used in the tightly coupled Kalman filter through which the optimal monitor's performance is evaluated. Results show that the monitor can detect spoofing in less than 40 seconds for different spoofing profiles. Although limited in performance due to effects of aircraft vibration on the IMU, this work demonstrates that the optimal INS monitor can successfully detect realistic spoofing in real-life environments.

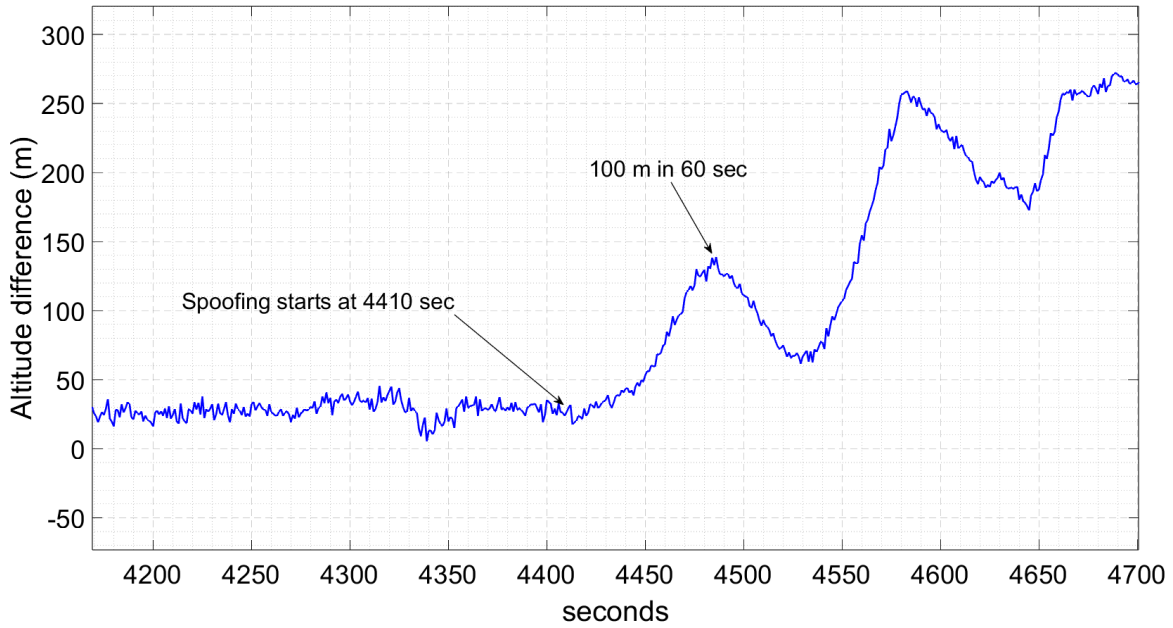


Figure 10: Spoofing scenario A4.

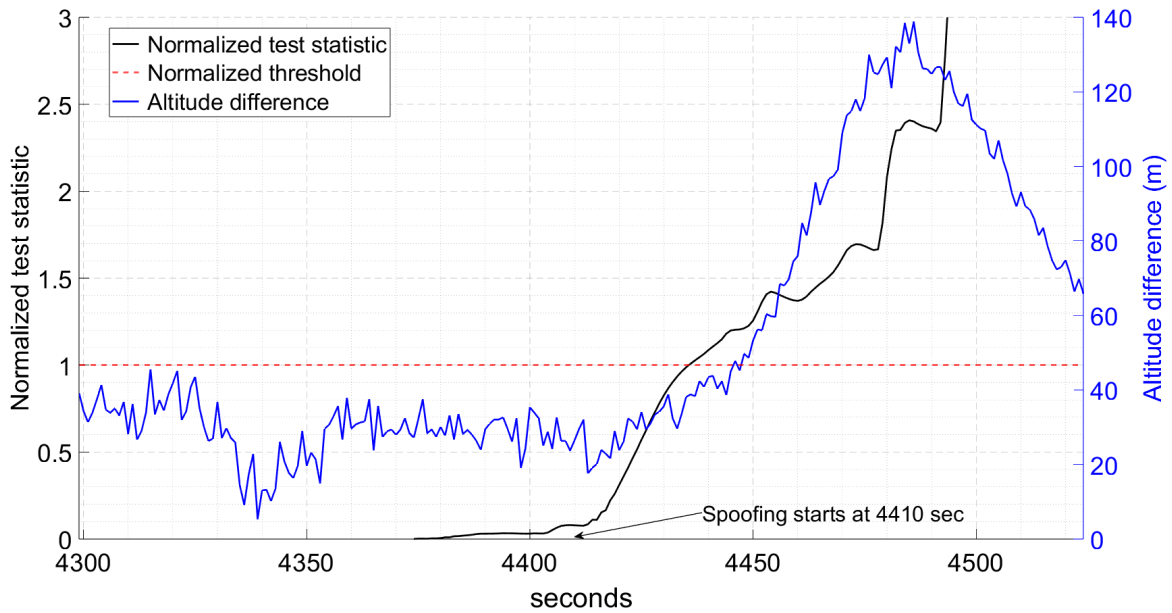


Figure 11: Detection result for scenario A4.

VI. ACKNOWLEDGEMENT

This article is based on work supported by the Center for Assured and Resilient Navigation in Advanced Transportation Systems (CARNATIONS) under the US Department of Transportation (USDOT)'s University Transportation Center (UTC) program (Grant No. 69A3552348324). Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the view of the sponsors.

REFERENCES

- Akos, D. M. (2012). Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *Navigation*, 59(4):281–290. <https://doi.org/10.1002/navi.19>.
- Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., and Kintner Jr., P. M. (2008). Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, pages 2314–2325.
- Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., , and Lachapelle, G. (2012). GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements. *International Journal of Satellite, Communications and Networking*, 30(4):181–191. <https://doi.org/10.1002/sat.1012>.
- Kerns, A. J., Shepard, D. P., Bhatti, J. A., and Humpherys, T. E. (2014). Unmanned Aircraft Capture and Control via GPS Spoofing. *Journal of Field, Robotics*, 31(4):617–636. <https://doi.org/10.1002/rob.21513>.
- Khanafseh, S., Roshan, N., Langel, S., Chan, F., Joerger, M., and Pervan, B. (2014). GPS spoofing detection using RAIM with INS coupling. In *2014 IEEE/ION Position, Location and Navigation Symposium (PLANS) 2014*, pages 1232–1239. <https://doi.org/10.1109/PLANS.2014.6851498>.
- Kujur, B., Khanafseh, S., and Pervan, B. (2023). Experimental Validation of Optimal INS Monitor against GNSS Spoofer Tracking Error Detection. In *2023 IEEE/ION Position, Location and Navigation Symposium (PLANS) 2023*, pages 592–596. <https://doi.org/10.1109/PLANS53410.2023.10140096>.
- Kujur, B., Khanafseh, S., and Pervan, B. (2024). Optimal INS Monitor for GNSS Spoofer Tracking Error Detection. *NAVIGATION: Journal of the Institute of Navigation*, 71(1). <https://navi.ion.org/content/71/1/navi.629>.
- Kujur, B., Tanil, C., Khanafseh, S., and Pervan, B. (2019). Sensitivity of Innovation Monitors to Uncertainty in Error Modeling. In *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, pages 3266–3274. <https://doi.org/10.33012/2019.17066>.
- Meurer, M., Konovaltsev, A., Cuntz, M., and Hattich, C. (2012). Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation using Direction Assisted Multiple Hypotheses RAIM. In *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, pages 3007–3016.
- Moshavi, S. (1996). Multi-user detection for DS-CDMA communications. *IEEE Communications Magazine*, 34(10):124–136. <https://doi.org/10.1109/35.544334>.
- Nielsen, J., Broumandan, A., and Lachapelle, G. (2014). GNSS Spoofing Detection for Single Antenna Handheld Receivers. *Navigation*, 58(4):335–344. <https://doi.org/10.1002/j.2161-4296.2011.tb02590.x>.
- Psiaki, M. L., Powell, S. P., and O'Hanlon, B. W. (2013). GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data. In *Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013)*, pages 2949–2991.
- Swaszek, P. F., Hartnett, R. J., and Seals, K. C. (2016). GNSS Spoof Detection using Independent Range Information. In *Proceedings of the 2016 International Technical Meeting of The Institute of Navigation*, pages 739–747. <https://doi.org/10.33012/2016.13457>.
- Tanil, C., Khanafseh, S., Joerger, M., and Pervan, B. (2016a). Kalman filter-based INS monitor to detect GNSS spoofers capable of tracking aircraft position. In *2016 IEEE/ION Position, Location and Navigation Symposium (PLANS) 2016*, pages 1027–1034. <https://doi.org/10.1109/PLANS.2016.7479805>.
- Tanil, C., Khanafseh, S., Joerger, M., and Pervan, B. (2018). An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position. *IEEE Transactions on Aerospace and Electronic Systems*, 54(1):131–143. <https://doi.org/10.1109/TAES.2017.2739924>.
- Tanil, C., Khanafseh, S., and Pervan, B. (2015a). GNSS Spoofing Attack Detection using Aircraft Autopilot Response to Deceptive Trajectory. In *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015)*, pages 3345–3357.
- Tanil, C., Khanafseh, S., and Pervan, B. (2015b). Impact of Wind Gusts on Detectability of GPS Spoofing Attacks Using RAIM with INS Coupling. In *Proceedings of the ION 2015 Pacific PNT Meeting*, pages 674–686.
- Tanil, C., Khanafseh, S., and Pervan, B. (2016b). An INS Monitor against GNSS Spoofing Attacks during GBAS and SBAS-assisted Aircraft Landing Approaches. In *Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016)*, pages 2981–2990. <https://doi.org/10.33012/2016.14779>.

- Tanil, C., Khanafseh, S., and Pervan, B. (2017). Detecting Global Navigation Satellite System Spoofing Using Inertial Sensing of Aircraft Disturbance. *Journal of Guidance, Control and Dynamics*, 40(8):2006–2016. <https://doi.org/10.2514/1.G002547>.
- Wesson, K. D., Rothlisberger, M. P., and Humphreys, T. (2011). A Proposed Navigation Message Authentication Implementation for Civil GPS Anti-Spoofing. In *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, pages 3129–3140.