

Performance of Optimal INS Monitor Against Jamming Then Spoofing Scenarios

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

BIOGRAPHY

Dr. Birendra Kujur serves as a Senior Research Associate in the Department of Mechanical and Aerospace Engineering at the Illinois Institute of Technology and as a Navigation Engineer at TruNav LLC. He earned both his M.S. and Ph.D. degrees from IIT, following a Bachelor of Science in Mechanical Engineering from Purdue University. His research is centered on advanced navigation technologies, with a particular emphasis on multi-sensor fusion and integrity monitoring. His current work explores the detection and mitigation of GNSS spoofing attacks, the development of robust anti-spoofing methodologies, and satellite fault diagnosis. His contributions aim to enhance the resilience and reliability of navigation systems in safety-critical applications.

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)) under scenarios involving jamming followed by spoofing of Global Navigation Satellite System (GNSS) signals. Previously, we evaluated the monitor's effectiveness against slow spoofing scenarios without prior jamming (Kujur et al. (2024), Kujur et al. (2023), Kujur et al. (2025)). In a more sophisticated attack, a spoofer may deliberately jam GNSS signals and subsequently introduce spoofed signals. This scenario is analogous to GNSS recovery—i.e., reacquisition and validation—after GNSS signals have been excluded due to spoofing detection. Specifically, once spoofing is detected, GNSS signals are rejected for positioning, and after a period of exclusion, they may be reacquired and validated as either authentic or spoofed.

During INS coasting under jamming, IMU calibration degrades. However, even with this degraded calibration, the discrepancy between INS and spoofed GNSS remains sufficient for spoofing detection, even after prolonged jamming periods lasting several minutes. Performance analyses were conducted across various IMU grades. Additionally, we present a preliminary analysis of realistic tracking errors encountered by a spoofer. The results indicate that even with a highly accurate tracking device, the spoofer is unlikely to maintain low centimeter-level tracking error due to large, random positional variations of the aircraft caused by disturbances such as wind gusts. In conclusion, the analysis confirms the monitor's robust capability to detect GNSS spoofing in realistic scenarios involving jamming followed by spoofing.

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 IMU-based GNSS spoofing monitor against worst-case faults was introduced by us (Khanafseh et al. (2014),Tanil et al. (2015b),Tanil et al. (2015a),Tanil et al. (2016a),Tanil et al. (2016b),Tanil et al. (2017),Tanil et al. (2018)). 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 decimeter level tracking error noise with a low probability of missed detection. We also experimentally validated the performance of the optimal monitor with simulated spoofing scenarios (Kujur et al. (2023)), and with live spoofing data (Kujur et al. (2025)).

The performance of the optimal INS monitor demonstrated in our prior work focused on scenarios where spoofing occurred during continuous reception of Global Navigation Satellite System (GNSS) signals. However, in realistic threat environments, a period of jamming—during which GNSS signals are entirely unavailable—may precede the broadcast of false GNSS signals. This paper evaluates the performance of the optimal INS monitor under such jamming-then-spoofing scenarios.

Section II provides background on the design and functionality of the optimal INS monitor. Section III outlines the jamming-then-spoofing scenarios and presents corresponding performance results. Section IV offers a preliminary analysis of realistic spoofer tracking errors, and Section V concludes the study.

II. OPTIMAL INS MONITOR

In this section, we review the optimal INS monitor, as detailed in (Kujur et al. (2024)), along with its predicted analytical performance.

1. 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,

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

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

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

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 \mathbf{y}_k with respective covariance matrix \mathbf{S}_k at time epoch k is defined as

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

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 error is through a Neyman-Pearson test statistic given as,

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

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

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

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: subscript 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

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

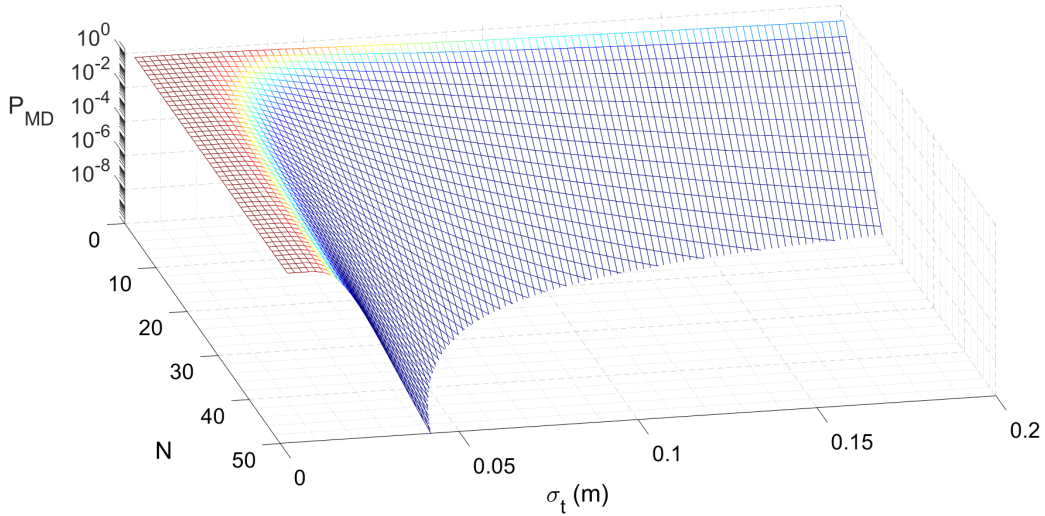


Figure 1: CPI probability of missed detection P_{MD} versus tracking error σ_t and monitor run time N .

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

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

Thus, the missed detection performance of the monitor can be determined since the nominal and spoofed distribution of the test statistic are known as represented in Equations (12) and (14), respectively.

3. Monitor Analytical Performance

In our prior work (Kujur et al. (2024)), we demonstrated the performance of the monitor in detecting spoofing of an en route aircraft. The analytical evaluation was conducted for an aircraft in level cruise flight, equipped with a navigation-grade Inertial Measurement Unit (IMU) and utilizing single-frequency GPS measurements. Satellite, atmospheric, and environmental errors in the GPS signals were compensated using error models integrated into the KF. To simulate spoofed measurements, tracking errors were modeled as WGN and added to authentic GPS data. Our results showed that the monitor's performance is strongly influenced by the accuracy of carrier phase measurements and the velocity random walk (VRW) characteristic of the IMU.

Figure 1 illustrates the missed detection probability as a function of tracking error and monitor run time. For a given scenario and missed detection requirement—along with knowledge of the spoofer's minimum tracking error magnitude—the required run time for the monitor can be determined. This analysis corresponds to a situation in which the user receiver is deceived into switching from authentic to spoofed measurements during the tracking phase. Since it is generally easier to trick a receiver during the acquisition phase, a spoofer may choose to first jam authentic GNSS signals and then broadcast a higher-power spoofed signal. In the next section, we evaluate the performance of the optimal INS monitor under such jamming-then-spoofing scenarios.

III. JAMMING THEN SPOOFING SCENARIOS

Spoofing of GNSS signals can be preceded by a jamming period. A spoofer may first jam GNSS signals and then transmit higher-power spoofed signals. After such a jamming period, the receiver is more likely to lock onto the stronger spoofed signals. While a jamming event raises suspicion of potential spoofing, a dedicated spoofing detection test is required to validate the integrity of incoming signals post-jamming. Spoofing after jamming a target user is generally easier than spoofing during continuous signal reception. However, from a detection standpoint, jamming-then-spoofing scenarios are intuitively more difficult to detect. Additionally, the INS-only coasting solution experiences drift proportional to the duration of the jamming period, further degrading the overall navigation performance.

The jamming-then-spoofing detection scenario is also analogous to GNSS signal recovery. A user may voluntarily reject GNSS signals—whether due to suspected spoofing or other reasons. When the user later chooses to resume GNSS usage, it becomes

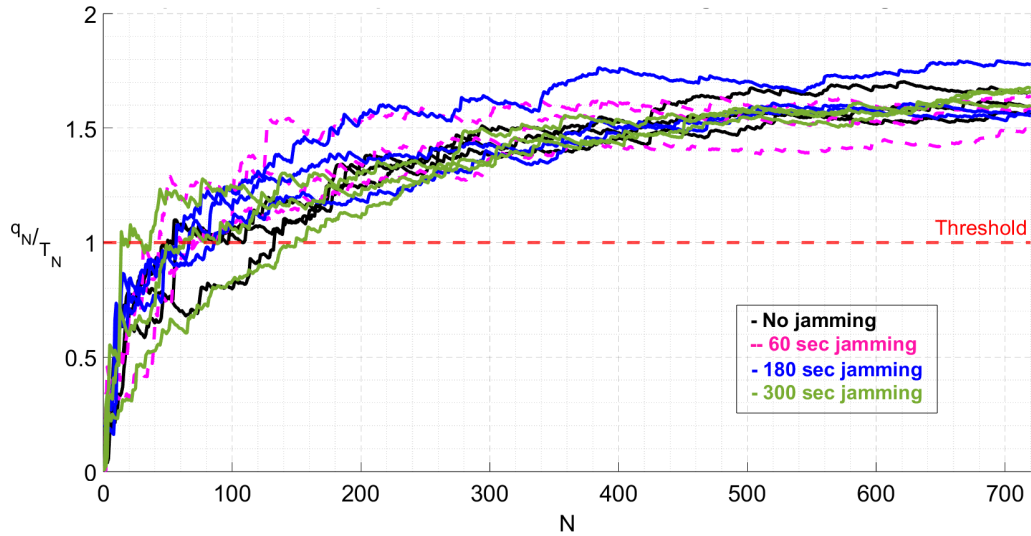


Figure 2: Monitor performance against spoofing after various jamming periods with navigation grade IMU and WGN tracking error of standard deviation 2 cm.

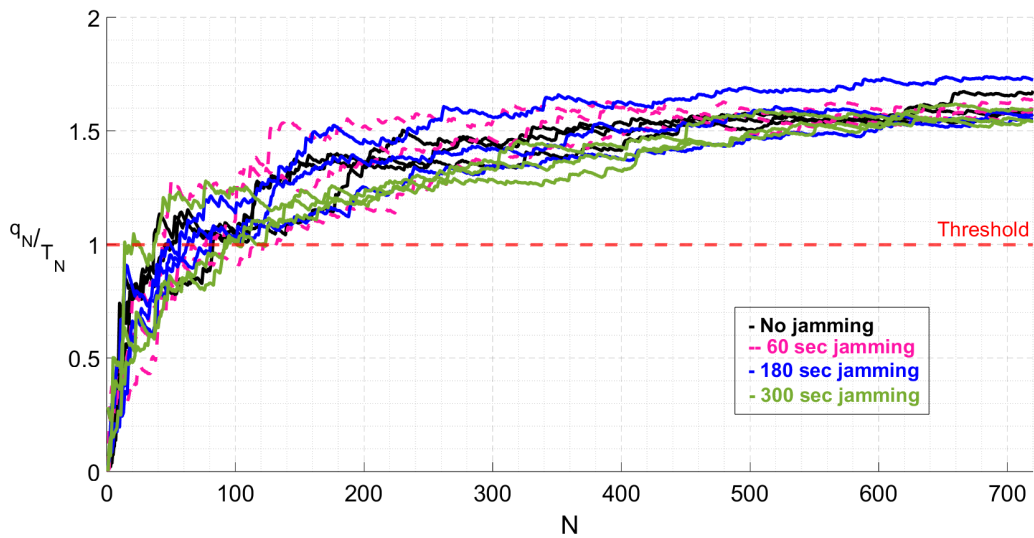


Figure 3: Monitor performance against spoofing after various jamming periods with automotive grade IMU and WGN tracking error of standard deviation 2 cm.

essential to validate the authenticity of the recovered signals, particularly in spoofing-prone environments.

Once GNSS signals are reacquired following a jamming period, it is critical for the user to verify whether the incoming signals are authentic or spoofed. From the spoofer’s perspective, the broadcast spoofed signals post-jamming must closely resemble authentic signals, as the spoofer is unaware of any additional spoofing detection mechanisms the user may be employing—such as altitude validation using a barometric altimeter.

To investigate this, we simulate an en-route aircraft scenario in straight and level flight (SLF). The spoofer first jams the authentic GNSS signals for a defined duration, then transmits higher-power spoofed signals, which the user’s receiver subsequently locks onto. These spoofed signals are modeled as authentic signals with additive user tracking errors.

After the jamming period, the aircraft relies solely on spoofed signals from six GPS satellites, supplemented by its onboard IMU. An optimal INS monitor is initiated immediately upon signal reacquisition. For analysis, we simulate varying jamming

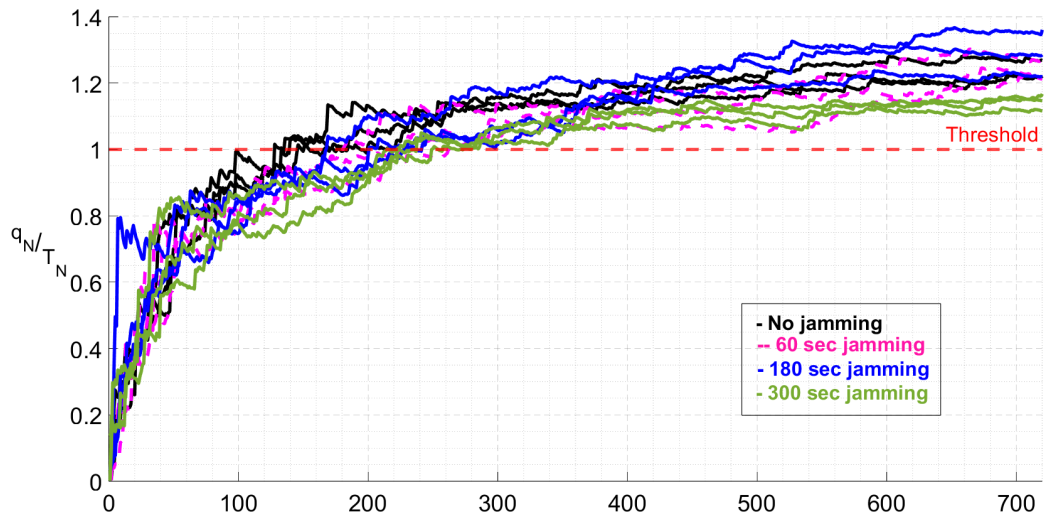


Figure 4: Monitor performance against spoofing after various jamming periods with navigation grade IMU and colored tracking error of standard deviation 7 cm and time constant 10 seconds.

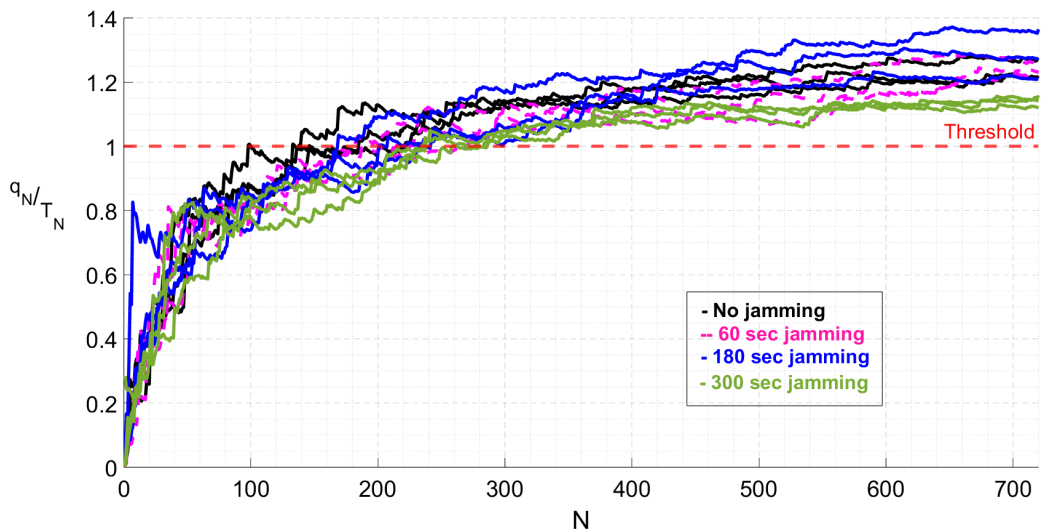


Figure 5: Monitor performance against spoofing after various jamming periods with automotive grade IMU and colored tracking error of standard deviation 7 cm and time constant 10 seconds.

durations to assess their impact on monitor performance and compare the results to a baseline scenario without jamming.

Figure 2 illustrates the performance of the optimal INS monitor under varying jamming durations—specifically, 0 (no jamming), 60, 180, and 300 seconds—prior to spoofing. The results correspond to a navigation-grade IMU, with the y-axis representing the normalized test statistic; detection is triggered when the trace crosses the threshold value of 1. The spoofing signal tracking error is modeled as white Gaussian noise (WGN) with a standard deviation of 2 cm. For comparison, Figure 3 presents the corresponding results for an automotive-grade IMU.

Figures 4 and 5 illustrate the performance of the optimal INS monitor under varying jamming durations prior to spoofing, in the presence of colored noise tracking errors in the spoofed signals. The results are shown for navigation-grade and automotive-grade IMUs, respectively. The colored noise tracking error is modeled as first order Gauss-Markov process with a time constant of 10 seconds and a standard deviation of 7 cm.

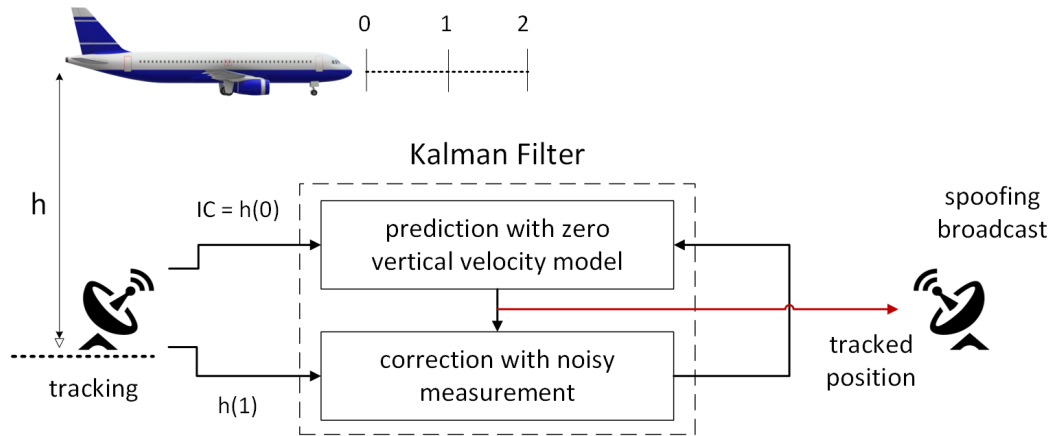


Figure 6: Spoofer's tracking method with Kalman filter for aircraft vertical position during straight level flight.

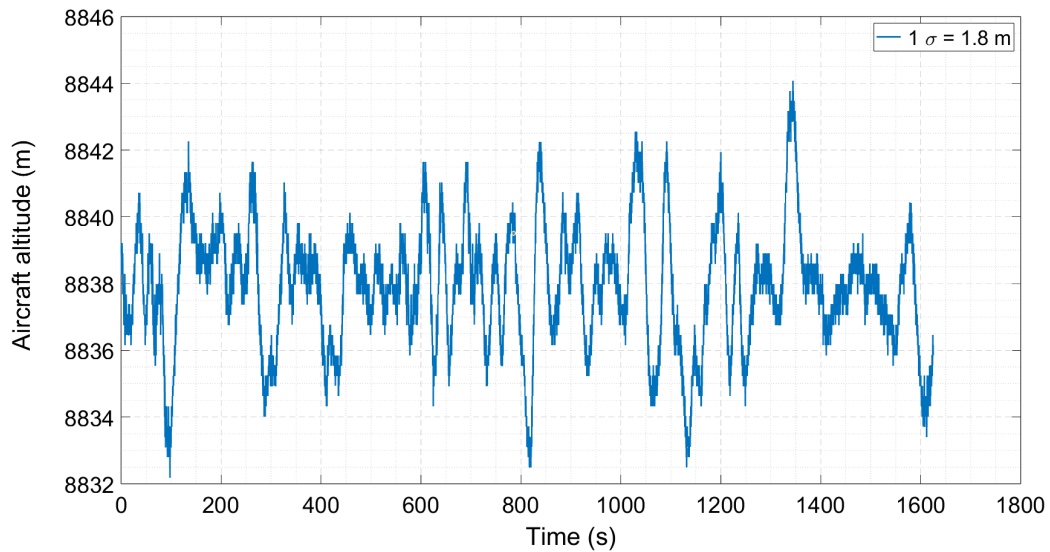


Figure 7: Aircraft vertical position variation during straight level flight.

The results clearly indicate that the jamming duration has a negligible impact on the performance of the optimal INS monitor. The IMU remains uncompromised regardless of whether the spoofing signal tracking error is modeled as WGN or colored noise. Notably, the monitor's performance does not degrade even when using a lower-grade automotive IMU.

This robustness can be attributed to the fundamental detection mechanism of the monitor, which compares the relative smoothness between the carrier-phase-derived navigation solution and the IMU-based solution. For short durations, the IMU solution closely replicates the motion captured by the precise carrier phase, enabling the monitor to detect even subtle discrepancies between the two.

IV. REALISTIC SPOOFER TRACKING ERROR

The optimal INS monitor has demonstrated robustness across various spoofing scenarios, including cases where the spoofer first jams authentic GNSS signals before initiating spoofing. It can be inferred that the monitor's performance is primarily a function of the spoofer's tracking error, which must be constrained to low centimeter-level magnitudes to result in missed detection.

This raises a critical question: what level of tracking error is realistically achievable by a spoofer in real-world conditions? To explore this, we conduct a preliminary analysis simulating a spoofer attempting to track an aircraft's vertical position during SLF. Figure 6 illustrates a plausible method a spoofer might employ, using external tracking devices such as radar or lidar to

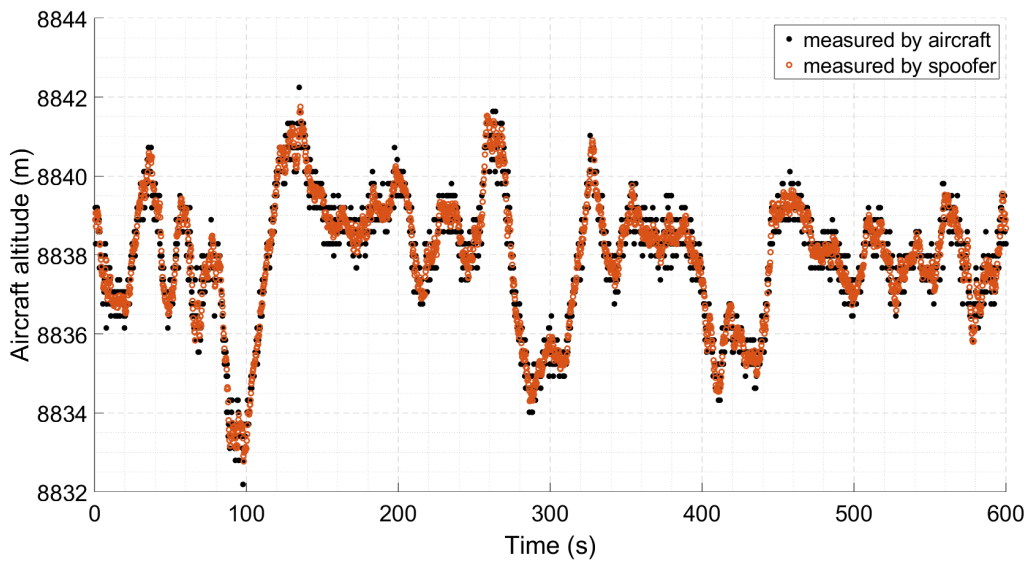


Figure 8: Aircraft vertical position measured by aircraft versus spoofer's prediction.

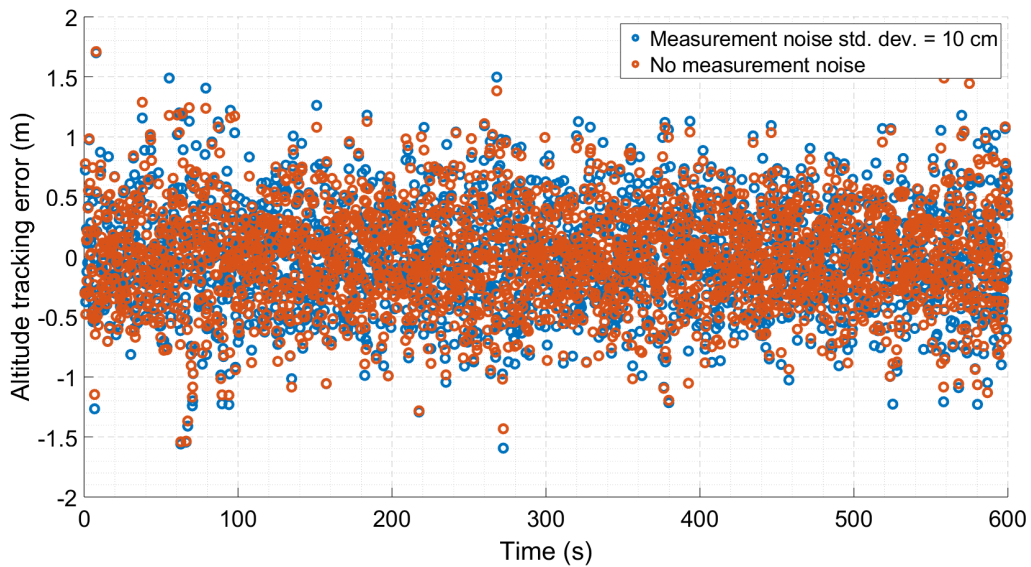


Figure 9: Spoofer's tracking error of aircraft with and without measurement noise results in a standard deviation of 0.42 m.

measure the aircraft's vertical position. These measurements are inherently noisy.

To estimate the aircraft's position, the spoofer may implement an object tracking filter, such as a Kalman filter, configured with a simple zero vertical velocity prediction model. This model uses the most recent measurement to predict the aircraft's future position, assuming negligible process noise. However, the spoofer faces a fundamental limitation: spoofed measurements can only be generated using data available up to the last measurement epoch. Once a new noisy measurement is received, the spoofer can update the predicted state.

Consequently, the spoofer's tracking error magnitude is directly influenced by the latency in generating spoofed measurements. This latency-driven prediction gap introduces a realistic constraint on the spoofer's ability to maintain low tracking error, thereby reinforcing the effectiveness of the INS monitor.

We utilize data from (Matthews (2012)) corresponding to a large aircraft undergoing SLF while experiencing typical atmospheric

disturbances. Figure 7 illustrates the vertical position variation during the SLF segment, sampled at 4 Hz. The standard deviation of this variation is 1.8 meters, consistent with fluctuations caused by wind gusts and other environmental factors.

For our analysis, we assume the spoofer requires 0.25 seconds to generate and broadcast spoofed measurements. The resulting tracking error arises from the aircraft's random vertical motion during this latency window. Figure ?? compares the aircraft's measured vertical position—obtained via onboard sensors—with the predicted position estimated by the spoofer. The tracking error is defined as the difference between these two datasets.

Figure 9 presents this tracking error under two conditions. In the first case, the spoofer's measurements are corrupted by additive WGN with a standard deviation of 10 cm, resulting in a tracking error with a standard deviation of 0.42 meters. In the second case, we assume perfect measurements for the spoofer, yet the tracking error standard deviation remains at 0.42 meters. This outcome indicates that even with ideal measurements, the spoofer cannot achieve centimeter-level tracking accuracy due to the aircraft's unpredictable vertical motion—even over a short latency duration of 0.25 seconds.

V. CONCLUSION

To evaluate the performance of the optimal INS monitor under realistic operational conditions—such as jamming preceding spoofing or the validation of recovered GNSS signals following exclusion—comprehensive simulation results are presented. These results demonstrate that the monitor reliably detects spoofing even after extended jamming durations lasting several minutes, with no observable degradation in performance. Analyses are conducted for both navigation-grade and automotive-grade IMUs, confirming consistent robustness across sensor classes.

Additionally, a preliminary assessment is performed on a simplified spoofer tracking strategy employing a Kalman filter. Even with accurate measurements, the spoofer's tracking errors are significantly affected by large, random vertical displacements of the aircraft, driven by environmental disturbances such as wind gusts. These findings underscore the inherent limitations faced by spoofers and affirm the effectiveness of the optimal INS monitor across a broad spectrum of realistic spoofing scenarios.

VI. ACKNOWLEDGMENT

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) and the Federal Aviation Administration (MOA 693KA8-21-T-00027). Any opinions, findings, conclusions or recommendations expressed in this document are those of the authors and do not necessarily reflect the views 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.
- 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.
- Jafarinia-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.
- 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.
- 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.
- 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)*, pages 592–596.
- Kujur, B., Khanafseh, S., and Pervan, B. (2024). Optimal INS Monitor against GNSS Spoofer Tracking Error Detection. *Journal of the Institute of Navigation*, 71(1).
- Kujur, B., Khanafseh, S., and Pervan, B. (2025). Performance of Optimal INS Monitor Against Live Spoofing. In *Proceedings of the 2025 International Technical Meeting of The Institute of Navigation*, pages 579–589.

Matthews, B. (2012). Flight data for tail 687. NASA DASHlink Dataset retrieved from: <https://c3.ndc.nasa.gov/dashlink/resources/664/>.

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.

Nielsen, J., Broumandan, A., and Lachapelle, G. (2014). GNSS Spoofing Detection for Single Antenna Handheld Receivers. *Navigation*, 58(4):335–344.

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.

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.

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.

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.

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.

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.

APPENDIX

A. IMU specifications

Table 1: Specifications for navigation and automotive IMU grades

Parameter	Navigation	Automotive	Unit
Velocity random walk	1.43×10^{-2}	0.18	m/s/ \sqrt{h}
Accelerometer bias instability	1×10^{-2}	4×10^{-2}	mg
Accelerometer bias repeatability	2.5×10^{-2}	1.5	mg
Accelerometer bias time constant	3600	3600	s
Angular random walk	1×10^{-3}	0.2	deg/ \sqrt{h}
Gyroscope bias instability	3.5×10^{-3}	7	deg/h
Gyroscope bias repeatability	3×10^{-3}	120	deg/h
Gyroscope time constant	3600	3600	s