Experimental Validation of INS Monitor against GNSS Spoofing

Çağatay Tanıl, Pau Martinez Jimenez, Mihaja Raveloharison, Birendra Kujur,
Samer Khanafseh, and Boris Pervan, *Illinois Institute of Technology*

BIOGRAPHIES

Dr. Çağatay Tanıl received his B.S. and M.S. in Mechanical Engineering from Middle East Technical University, in 2006 and 2009, respectively; and Ph.D. in Aerospace Engineering from Illinois Institute of Technology (IIT) in 2016. His doctoral work, detecting GNSS spoofing attacks using INS coupling, won the 2017 Institute of Navigation (ION) Bradford W. Parkinson Award for excellence in global navigation satellite systems. With more than 12 years of guidance, navigation, and control experience, Dr. Tanil fulfilled many research and development roles such as dynamic modeling and simulation, guidance and control of missiles. From 2006-2013, he worked at leading defense and aerospace companies in Turkey, including Roketsan Missiles Industries, Turkish Aerospace Industries (TAI), and Defense Industries Research and Development Institute (Tubitak-SAGE). Dr. Tanil is currently a Senior Research Associate at IIT and a Research Scientist at TruNav LLC, working on sensor fusion (INS/GNSS) and estimation, fault/spoofing detection, and integrity monitoring for high precision navigation and guidance systems.

Pau Martinez Jimenez is a Research Assistant at the Navigation Laboratory at IIT. He is graduated in a double master's degree program between the Illinois Institute of Technology (IIT) and the Barcelona's superior industrial engineering school (ETSEIB-UPC), received a M.E. in Mechanical and Aerospace Engineering of IIT and a Master in Industrial Engineering with focus in automation and control from the Barcelona Engineering School. He received his B.S. from the Barcelona Engineering School graduating in the top 5 out of 600 students and received 2 special mentions for his academic achievements of the year. He has also worked in the Biomechanics Laboratory at the Barcelona Engineering School implementing exoskeleton systems and test bench design. His current research is focused on inertial navigation systems for GPS spoofing detection.

Mihaja Raveloharison received his Bachelors Degree and a Master degree in mathematics and mechanical Engineering from Enseirb-Matmeca the National Polytechnic Institute of Bordeaux, France in 2016 and 2018, respectively. He obtained his Master of Engineering in Mechanical and Aerospace Engineering from the Illinois Institute of Technology (IIT) in 2018. His work at Navlab during the Spring and Summer of 2018 was focused on an experimental validation of INS Monitor against GNSS spoofing.

Birendra Kujur is a doctoral student in Navigation Lab 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 and Navigation Integrity Monitoring.

Dr. Samer Khanafseh is currently a research assistant professor at Illinois Institute of Technology (IIT), Chicago. 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 of Mechanical and Aerospace Engineering at IIT, where he conducts research on advanced 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 is an Associate Fellow of the AIAA, a Fellow of the Institute of Navigation (ION), and Editor-in-Chief of the ION journal NAVIGATION. He was the recipient of the IIT Sigma Xi Excellence in University

Research Award (2011, 2002), Ralph Barnett Mechanical and Aerospace Dept. Outstanding Teaching Award (2009, 2002), Mechanical and Aerospace Dept. Excellence in Research Award (2007), University Excellence in Teaching Award (2005), IEEE Aerospace and Electronic Systems Society M. Barry Carlton Award (1999), RTCA William E. Jackson Award (1996), Guggenheim Fellowship (Caltech 1987), and Albert J. Zahm Prize in Aeronautics (Notre Dame 1986).

ABSTRACT

Global Navigation Satellite System (GNSS) spoofing attacks are a critical threat to navigation integrity. We previously developed an analytical framework to evaluate the performance of Inertial Navigation System (INS) monitors against spoofing attacks, which is necessary for eventual clarification and certification of the INS monitor. In this paper, we develop and execute an experimental setup to verify the resistance of the monitor against worst-case GNSS spoofing attacks. The test setup includes generation of the worst-case spoofed code and carrier phase GPS signals (using a GNSS simulator) that feed the receiver through a cable without needing to broadcast via transmitter. Using these signals, the miss-detection rates of the Kalman filter innovations-based monitor, has been observed through a tightly-coupled integration of a tactical grade inertial and a standalone GNSS receiver on a static platform. The experimental evaluation technique in this paper is fundamental because it is the first hardware test to quantify spoofing resistance of a widely used IMU with worst-case spoofing signals. We realistically demonstrate that, even if the spoofer tracks the position of the receiver and filters the high-frequency tracking errors, the monitor is still capable of detecting that with low missed detection probability.

I. INTRODUCTION

This paper develops a state-of-the-art experimental test setup to demonstrate the feasibility and performance of Inertial Navigation System (INS) monitors to detect worst-case GNSS signal spoofing. The monitor uses Kalman filter (KF) innovation sequence obtained from a tightly coupled integration of a tactical-grade Inertial Measurement Unit (IMU) and a standalone GNSS receiver.

With its accurate, continuous, and global capabilities, GNSS offers seamless satellite navigation that meets the most stringent requirements for aviation users. Space-based positioning and navigation especially when used in differential, enables three-dimensional position determination for aircraft en route, approach, and landing, existing or near-future unmanned aerial vehicles (UAVs or drones) operated by postal services, police departments and others for surveillance purposes. Also many strategic infrastructures such as offshore oil drilling, surveying, electric power grids or communications networks heavily rely on GNSS for localization, navigation, and time synchronization. However, civil use of GNSS is vulnerable to intentional spoofing and the threat of spoofing is likely to increase. Therefore, there is an emerging need for mitigations to these vulnerabilities by proof-of-concept techniques.

A spoofing attack happens when a counterfeit signal is deliberately broadcast to a user receiver, potentially resulting in incorrect position estimates. It is rarely observed, but the methods of how to spoof are known and its consequences have been demonstrated to be dangerous [1]. Numerous anti-spoofing techniques have been developed in the last decade, and the strengths and vulnerabilities of these existing methods have been discussed in [2]. These include cryptographic authentication techniques employing modified GNSS navigation data [3], spoofing discrimination using spatial processing by antenna arrays and automatic gain control schemes [4] [5], GNSS signal direction of arrival comparison [6], code and phase rate consistency checks [7], high-frequency antenna motion [8], and signal power monitoring techniques [9]. Some of these methods are indeed effective but they have some computational, logistical and physical limitations. Augmenting data from auxiliary sensors such as Inertial Measurement Units (IMU), baro-altimeters, and independent radar sensors to discriminate spoofing has also been proposed in [10] [11].

The first thorough description and quantification of integrity performance of the inertial aided fault monitoring was introduced by our prior work in [14]. There, inertial sensors are investigated as a direct means of detecting GNSS spoofing attacks since they are integrated with GNSS receivers to support essentially all aerospace, terrestrial, and maritime navigation applications, and therefore do not require additional cost or modification to existing positioning systems. The basis for the detector is a coupled integration of GNSS measurements and INS kinematic models using a Kalman filter (KF) estimator. The redundancy required for detection is provided through INS measurements using the KF innovations sequence for spoofing detection, which is highly sensitive to slowly growing faults. Using this

detector it is possible to analytically determine the worst-case sequence of spoofed GNSS measurements that is, the spoofed GNSS signal profile that maximizes integrity risk. The methodology allows for the quantification of the monitor performance against the most sophisticated spoofers, capable of tracking and estimating the receiver position.

Using this technique, it was shown that if the spoofer knows the exact position of the receiver, it might eventually cause errors large enough to exceed hazard safety limits without being detected [18]. However, in reality, the users actual position will always deviate from the prescribed position assumed by the spoofer due to natural disturbances. For aircraft applications, these may include wind gusts, autopilots control actions, or lowering landing gear. These high-frequency accelerations, which are unknown to the spoofer in an open-loop attack, where spoofer assumes a nominal trajectory, would enhance detection the capability of the INS monitor [17]. Our most recent work [18] investigated potential closed-loop attack scenarios where the spoofer is capable of tracking real-time position of the receiver and broadcasting worst-case sequence of spoofed signals. The covariance analysis results showed that the closed loop spoofing is still easily detectible by the INS monitor, with high integrity, unless the spoofers position tracking devices have unrealistic, near-perfect accuracy, and no time delays. The performance of the monitor were also compared in different INS/GNSS integration schemes. It was evident that the tightly-coupled detector is superior to detectors in loosely-coupled and uncoupled (solution separation between INS and GNSS) integrations. The reason is that the tightly-coupled one monitors the discrepancies in measurement domain whereas others monitors discrepancies in position domain, therefore is highly sensitive to additional small (even millimeter level) high frequency variations or biases (due to tracking errors) on the carrier phase measurements.

The integrity risk methodology developed in the prior work focused on the analytical evaluation of the monitors performance against worst-case spoofing fault sequence, which is necessary for eventual clarification and certification of the INS monitor. However, experimental validation is equally important because it will prove that the system can actually be implemented and used in aviation, and other terrestrial and maritime navigation applications. A recent study [19] experimentally tested MEMS- and tactical-grade inertials on a moving car to investigate the minimum sensor requirements for GNSS spoofing protection. It compared the snapshot residual-based monitor performance in a tightly coupled INS/GNSS integration. More recent experimental studies in [20], [21], and [22] demonstrated the feasibility of GNSS spoofing detection in both vehicular and aviation applications using low-cost accelerometers that were not coupled to GNSS receivers. Both used solution separation based monitors that simply check the consistency of raw IMU measurements with the second time-difference of GNSS measurements directly at the acceleration level. Even though their preliminary results are promising, their approach to compute missed detection rates are based on specific types of fault profiles, such as ramp or quadratic types, which do not necessarily represent the worst-case fault profiles, therefore do not guarantee the protection levels.

In response, this paper develops and explains an experimental test setup that generates worst-case spoofed code and carrier phase GPS signals (using a GNSS simulator–Spectracom GSG 6) that feed the receiver through a cable without needing to broadcast via transmitter. Using these signals, the performance of the Inertial Aided Anti-Spoofing Monitor (IASM) that is based on KF innovation sequence, has been tested with a tightly-coupled integration of a tactical grade inertial (STIM300) and a standalone GNSS receiver (AsterX-m UAS) on a static platform. This approach is easier than testing the monitor performance on a moving platform because it eliminates the need of additional hardware for real-time position tracking and platform controller and their potential complications. Yet it is more conservative because unlike moving scenarios the monitor on a static platform does not leverage from disturbances on the vehicle motion that may not be captured in the spoofed signals. The spoofed RF signals are directly transmitted to the receiver coupled to the inertial for position estimation and fault monitoring. This closed-loop mechanism allows for direct testing the INS monitor performance under the worst-case spoofing attacks. The experimental evaluation technique in this paper is fundamental because it is the first experimental study to quantify spoofing resistance of a widely used tactical-grade IMU under a worst-case GNSS spoofing attack.

Sect. II reviews the analytical aspects of KF innovations-based monitor, the worst-case fault sequence optimization, and integrity risk evaluation technique. Sect. IV presents the hardware prototype of Inertial Aided Anti-Spoofing Monitor (IASM), the experimental setup and validation approaches for spoofing scenarios. Appendix. A discusses the signal characterization techniques and results for GPS and INS data collected from GNSS simulator and STIM300, respectively. Performance test results are given in Sect. V. In this section, we verify that the missed-detection rates obtained from hardware tests, are considerably consistent with the integrity risk results obtained from covariance

analysis. We demonstrate and describe the characteristic behavior of the worst-case fault that can be injected to a specific INS/GPS navigation system and its difference from the conventional fault profiles (constant jerk, acceleration, velocity, or biases). The experiments also address the effect of high and low frequency (white and colored noise) errors that may appear on the spoofed signals due to remote tracking and smoothing. We demonstrate that realistically, even if spoofer implements a smoothing filter to reduce the high frequency components of tracking errors, the monitor is able to detect that with low missed detection probability.

II. Inertial Aided Anti Spoofing Monitor

GNSS and INS can be coupled using a variety of integration schemes. These can range from the simple loosely coupled integration, to the complex ultra-tightly coupled mode in which the INS directly aids the GNSS tracking loops [23]. This experimental validation in this work is performed for a nominal tightly-coupled integration. There are two main reasons for that: 1) it is a widely used implementation for integrated GNSS/INS systems providing superior estimation performance to loosely-coupled systems but without the excessive cost and complexity associated with ultra-tight systems, 2) Using other integration schemes (loosely-coupled and uncoupled) for spoofing detection have been investigated and analyzed in our previous work [18], the covariance results have shown that tightly-coupled integration is superior to lower level integrations in terms of spoofing detection performance.

A. A Review of Kalman Filter Innovation Sequence Monitor

In a typical INS/GNSS tightly-coupled mechanization, the Kalman filter time update equation can be written as [18]:

$$\overline{\mathbf{x}}_k = \mathbf{\Phi}_{k-1}\,\hat{\mathbf{x}}_{k-1} + \mathbf{\Gamma}_{k-1}\,\tilde{\mathbf{u}}_{k-1} \tag{1}$$

where $\mathbf{\Phi}_k$ is the state transition matrix of the process model, $\tilde{\mathbf{u}}_k$ is IMU measurements, $\mathbf{\Gamma}_k$ is IMU input coefficient matrix, and $\overline{\mathbf{x}}_k$ $(m \times 1)$ is the a priori estimate of $\mathbf{x}$ at time epoch k.

The measurement update gives the a posteriori estimate $\hat{\mathbf{x}}_k$ as

$$\hat{\mathbf{x}}_k = \overline{\mathbf{x}}_k + \mathbf{L}_k\big(\mathbf{z}_k - \mathbf{H}_k\,\overline{\mathbf{x}}_k\big) \tag{2}$$

where $\mathbf{L}_k$ and $\mathbf{H}_k$ are the optimal Kalman gain and observation matrices at time epoch k.

Based on the Kalman filter estimator defined in (1) and (2), we implement a detector that utilizes the Kalman filter innovation sequence from the INS/GNSS integration [18]. The detector is simple, efficient, and can directly be implemented on top of tightly-coupled INS/GNSS integrations without requiring any modification to the existing navigation system.

The innovation vector $\boldsymbol{\gamma}$ at time epoch k is defined as

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

A cumulative test statistic q_k is defined as the sum of squares of the normalized innovation vectors over time as

$$q_k = \sum_{i=1}^{k} \boldsymbol{\gamma}_i^T\,\mathbf{S}_i^{-1}\,\boldsymbol{\gamma}_i \tag{4}$$

where $\mathbf{S}_i$ is innovation vector covariance matrix at time epoch i.

The monitor simply checks whether the test statistic q_k is smaller than a pre-defined threshold T_k^2 as

$$q_k \gtrless T_k^2 \tag{5}$$

Let n be the number of measurements for each GNSS measurement update; under fault free conditions, the test statistic q_k at the k^{th} GNSS measurement update is chi-square distributed with kn degrees of freedom. For a given continuity requirement, the threshold T_k^2 is determined from the inverse chi-square cumulative distribution function. The INS monitor alarms for a fault if $q_k > T_k^2$. Under faulted conditions, q_k is non-centrally chi-square distributed with a non-centrality parameter λ_k^2,

$$\lambda_k^2 = \sum_{i=1}^{k} \mathbb{E}[\boldsymbol{\gamma}_i]^T\,\mathbf{S}_i^{-1}\,\mathbb{E}[\boldsymbol{\gamma}_i] \tag{6}$$

which is used to evaluate the probability of missed detection.

B. Monitor Evaluation under Worst Case Spoofing Measurement Faults

In this section, we summarize the methodology [18] to obtain an analytical expression of the worst-case measurement fault that maximizes the integrity risk of the innovation sequence monitor. The worst-case evaluation approach used here assumes a worst-case spoofing attack where the attacker is capable of real-time tracking and spoofing the receiver position. Furthermore, it conservatively assumes that the attacker have the knowledge of error models used in onboard estimator and detector.

Under fault hypothesis, the measurement vector $\mathbf{z}_k$ in (2) can be replaced by $\mathbf{z}_k + \mathbf{f}_k$ where $\mathbf{f}_k$ is a full-set $(n \times 1)$ non-zero fault vector. Using (1) and (2) one can express the expected values of estimation error, $\tilde{\mathbf{x}} = \hat{\mathbf{x}} - \mathbf{x}$, and innovation as a function of $\mathbf{f}_k$ as

$$\mathbb{E}[\tilde{\mathbf{x}}_k] = \big(\mathbf{I} - \mathbf{L}_k\mathbf{H}_k\big)\mathbf{\Phi}_k\mathbb{E}[\tilde{\mathbf{x}}_{k-1}] + \mathbf{L}_k\mathbf{f}_k \tag{7}$$

$$\mathbb{E}[\boldsymbol{\gamma}_k] = -\mathbf{H}_k\mathbf{\Phi}_k\mathbb{E}[\tilde{\mathbf{x}}_{k-1}] + \mathbf{f}_k \tag{8}$$

where it was shown $\mathbb{E}[\tilde{\mathbf{x}}_i\boldsymbol{\gamma}_j^T] = 0$ and $\mathbb{E}[\boldsymbol{\gamma}_i\boldsymbol{\gamma}_j^T] = 0$ for all $i \geq j$ in [18].

In this work, integrity risk, the probability that the state estimate error exceeds an alert limit without being detected (i.e., $q < T^2$), is used as a metric to quantify the performance of the innovation sequence monitor. Conservatively assuming a prior spoofing fault probability of 100%, for a given $\mathbf{f}_k$ the integrity risk at time epoch k is expressed in terms of the test statistic q_k and the estimate error ε_k as

$$I_{r_k} = \Pr\left(|\varepsilon_k| > \ell, q_k < T_k^2\right) \tag{9}$$

where ℓ is the vertical alert limit, and T_k^2 is pre-defined threshold for detection which is the same as that in (5). The error associated with the state of interest (e.g., altitude for aircraft approach, or cross track position for ground navigation), ε_k, can be extracted from $\tilde{\mathbf{x}}_k$ using the row transformation vector $\mathbf{T}_\varepsilon$ as $\varepsilon_k = \mathbf{T}_\varepsilon\tilde{\mathbf{x}}_k$. Since $\mathbb{E}[\tilde{\mathbf{x}}_i\boldsymbol{\gamma}_j^T] = 0$, the cumulative test statistic q_k obtained from $\boldsymbol{\gamma}_{1:k}$ and the error state of interest ε_k obtained from $\tilde{\mathbf{x}}$ will be statistically independent. As a result, the integrity risk I_{r_k} can be written as a product of two probabilities

$$I_{r_k} = \Pr\left(|\varepsilon_k| > \ell\right)\, \Pr\left(q_k < T_k^2\right) \tag{10}$$

Because all GNSS measurements may be impacted by the spoofing attack, it is assumed that all GNSS measurements are faulty during the attack period and that the IMU measurements are the fault-free sources of redundancy in the monitor. If a spoofing attack is not detected instantaneously, it may impact the INS error state estimates through the tightly coupled mechanism, which can degrade subsequent detection ability. Therefore, a smart spoofer may select a fault profile $\mathbf{f}_{1:k}$ with smaller faults at the beginning and gradually increasing over time, thereby corrupting INS calibration, leading to a lower probability of detection.

Using (7)-(10), a worst-case fault that maximizes integrity risk for a Kalman filter estimator was previously derived in [18]. First, it was shown that the worst-case direction of fault sequence vector $\mathbf{f}_{w_{1:k}}$, that maximizes the failure mode slope ρ_k^2, the ratio $\mathbb{E}[\varepsilon_k]^2/\lambda_k^2$, is

$$\mathbf{f}_{w_{1:k}} = \mathbf{B}_{1:k}^{-1}\mathbf{S}_{1:k}\mathbf{B}_{1:k}^{-\intercal}\mathbf{A}_{1:k}^{\intercal}\mathbf{T}_\varepsilon^{\intercal} \tag{11}$$

where $\mathbf{S}_{1:k}$ is a $(nk \times nk)$ block diagonal matrix containing innovation covariances of past and current time epoch in its diagonal blocks. $\mathbf{A}_{1:k}$ and $\mathbf{B}_{1:k}$ are $(m \times mk)$ and $(mk \times mk)$, respectively, which can be obtained using Kalman filter parameter history as follows:

Let

$$\mathbf{C}_{ij} = \begin{cases} \Big(\prod_{t=j}^{i+1}\big(\mathbf{I} - \mathbf{L}_t\mathbf{H}_t\big)\mathbf{\Phi}_t\Big)\mathbf{L}_i & \text{if } i < j \\ \mathbf{L}_i & \text{if } i = j \end{cases} \tag{12}$$

then

$$\mathbf{A}_{1:k} = \begin{bmatrix}\mathbf{C}_{1k} & \mathbf{C}_{2k} & \dots & \mathbf{C}_{kk}\end{bmatrix} \tag{13}$$

for $k \geq 1$, and

$$\mathbf{B}_{1:k} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{0} \\ -\mathbf{H}_2\mathbf{\Phi}_2\mathbf{C}_{11} & \mathbf{I} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{0} \\ -\mathbf{H}_3\mathbf{\Phi}_3\mathbf{C}_{12} & -\mathbf{H}_3\mathbf{\Phi}_3\mathbf{C}_{22} & \mathbf{I} & \dots & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & & \mathbf{I} & \mathbf{0} \\ -\mathbf{H}_k\mathbf{\Phi}_k\mathbf{C}_{(k-1)1} & -\mathbf{H}_k\mathbf{\Phi}_k\mathbf{C}_{(k-1)2} & \dots & \dots & -\mathbf{H}_k\mathbf{\Phi}_k\mathbf{C}_{(k-1)(k-1)} & \mathbf{I} \end{bmatrix} \tag{14}$$

where note that $\mathbf{B}_{1:1} = \mathbf{I}$.

Then, the magnitude of the worst-case fault is determined through a one dimensional search to maximize $I_{r_k}(\alpha)$ in (10).

III. Closed Loop Tracking and Spoofing

Advanced forms of GNSS spoofing methods have been investigated in response to efforts to mitigate signal spoofing. In this paper, we assume self-consistent spoofing attacks that defeats various defense strategies that have been developed [2]. There, the spoofer tracks the target antenna position based on which it generates a replica of authentic signal for each receiver channel with a higher power than the authentic signals. After capturing the target receiver's carrier- and code-phase tracking loops, the spoofer adjusts its spoofing signals to induce a worst-case position offset (fault) that is slowly increasing in an optimal sense.

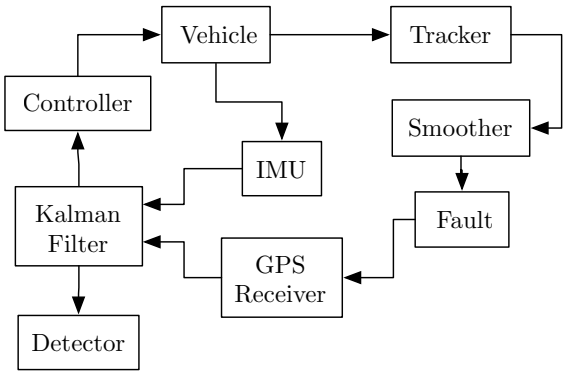

Fig. 1: Block diagram of a real-time closed-loop tracking and spoofing scenario targeting a moving vehicle with onboard INS/GNSS integrated navigation and guidance system.

The impact of the real-time position tracking and spoofing on the target guidance and navigation system is described in Fig. 1. The block diagram captures the closed-loop relation between the INS/GNSS estimator (observer) and the controller in presence of a GNSS spoofing attack with position tracking. The spoofers deliberate fault is optimally computed using the smooth track position and exact error models of estimator and detector implemented on target navigation system.

IV. Experimental Setup and Spoofing Scenario

To test the monitor performance under the closed-loop tracking and spoofing scenario, a static hardware test setup is built in Navigation Laboratory of Illinois Institute of Technology, using a GNSS simulator (Spectracom GSG 6) integrated with an external rubidium oscillator (Smart LPFRS-01/AV1), a multi-constellation dual frequency receiver (Septentrio AsteRx-m UAS receiver), and a low-end tactical grade inertial sensor (STIM300), shown in Fig. 2.

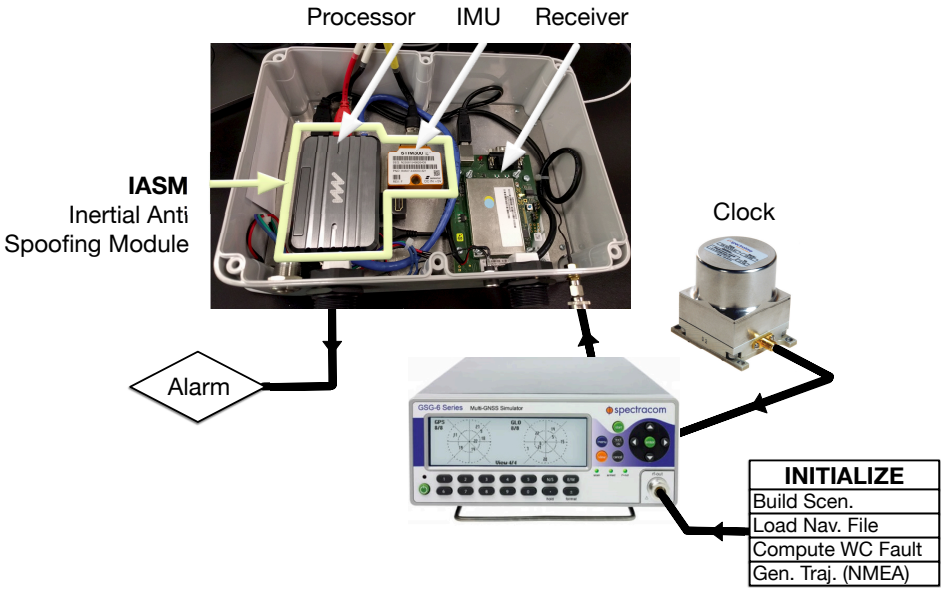

Fig. 2: Prototype of Inertial Anti Spoofing Monitor (IASM) and experimental realization of a spoofing attack using a static hardware setup.

A. GNSS Simulator

The worst-case GPS spoofed signals are generated through the simulator. For initialization of a spoofing attack, the time sequence of the worst-case position offset is first computed using replica statistical models of onboard estimator and detector, satellite navigation file, and authentic vehicle trajectory; then, fed into the simulator as an antenna trajectory in NMEA (National Marine Electronics Association) format. It should be noted that the fault generation method here is conservative because it assumes that the attacker has the full knowledge of not only the current but also the future trajectory of the target antenna. In each experiment, an horizontal alert limit of 10 m is used such that the position offset due to worst-case fault sequence reaches to 10 m in the east direction at the end of the pre-defined attack window. The spoofed signals for 8 channels are transmitted to the receiver through a hard cable. Ionospheric errors are deliberately turned off in the simulator setting because for the simplicity in the experiments we assumed an iono-free dual frequency implementation. The multipath setting is adjusted to suburban environment. To experimentally realize the spoofer's tracking and smoothing action, in some of the experiments we conservatively introduce an additional white and time correlated noise samples on the position offset without any time delays.

B. GNSS Receiver

The L1 code and carrier phase measurements are utilized in the experiments. Using code minus carrier and carrier de-trending methods, the statistical properties of the generated GPS measurements obtained through the receiver are characterized in Appendix A. The approximate values for GPS code- and carrier-phase measurements used in the estimator, are presented in Table I.

TABLE I: Estimator GPS Settings

Parameter	Code	Carrier	units
Multipath time constant	5	20	s
1-σ multipath error	15	1.1	cm
1-σ receiver thermal noise	5.0	0.1	cm

C. Inertial Measurement Unit

Inertial measurements are obtained from the STIM300 mounted together with the receiver on a static platform. We selected a static platform to test the INS monitor performance for two reasons: 1) augmenting a controller and actuator to the setup would increase the hardware cost, and 2) the static testing is more conservative than testing the monitor on a moving platform because high-frequency motions induced by controller's response to spoofing faults which are instantaneously sensed the IMU but may not be reflected in the spoofed signals (due to limits in tracking capability in the hardware setup), would leverage the detection [15].

TABLE II: Estimator INS settings for STIM300

Parameter	Value	Units
Gyro bias stability	0.5	deg/hr
Accelerometer bias stability	0.05	mg
Angular random walk	0.15	deg/$\sqrt{\text{hr}}$
Velocity random walk	0.07	m/s/$\sqrt{\text{hr}}$
Bias time constants	10^4	s
Sampling frequency	125	Hz

The STIM300 manufacturer specifications are presented in Table II and directly used in the estimator. The bias stability and random walk parameters are verified with the values obtained from the characterization of IMU measurements in Appendix A.

D. Inertial Aided Anti Spoofing Monitor (IASM)

The IASM module is implemented on a processor that utilizes a nominal INS/GPS tightly coupled mechanization. The Kalman filter estimator is assumed to be at its steady-state condition prior to spoofing attack. To do that, we initialized the hardware setup using authentic GPS signals for 10 min at the beginning of each experiment. Once the spoofing attack starts, the monitor accumulates the norm of innovations and compares against a threshold as prescribed in (4). The threshold is computed using a false alarm probability of 10^{-2}. The monitor gives alarm if the accumulated norm of innovations exceeds the threshold. The controlled experiment for each spoofing scenario is repeated 20 times using independent INS and GPS measurements. Out of the 20 trials the number of alarms are recorded and used to compute the probability of missed detection in the performance evaluation section.

V. Performance Evaluation

A. Fault Free Performance

To test false alarm rate of the detector, the tightly-coupled INS/GPS system is first tested under fault-free conditions. The iono-free estimation performance of the lateral position, velocity, and attitude is shown in Fig. 3. The green highlighted curves represents the covariance bounds whereas different tones of the black points show the state estimation errors obtained from the controlled experiments. The estimator is conservatively used a floating estimation instead of integer fixing methods for the cycle ambiguity states. The floating integer cycle ambiguity estimates are shown in Fig. 4. In Fig. 3, it can be seen that 1-σ steady-state lateral position and velocity estimation errors are 1.5 cm and 0.0025 m/s, respectively. On the other hand, the yaw attitude estimation error grows unboundedly over time because it is unobservable in the static setup unless an aiding sensor like a magnetometer is used. Starting with a steady-state Kalman filter, the monitor has been run for 18 min time window with authentic GPS signals, and has given no alarm out of the 20 independent runs. Recalling that the detection threshold is computed using a false alarm rate of 1%, the fault-free performance of the monitor observed per number of the experiments is more conservative than that expected theoretically.

B. The Characteristic of Worst Case Fault

This section investigates the impact of the worst-case fault profile, derived in our prior work [18], on the cumulative innovation norms (test statistic) of a INS/GNSS tightly-coupled integration. Some of the common spoofing threat models in the literature are constant velocity, constant acceleration and constant jerk [19], [20], and [21]. The monitor

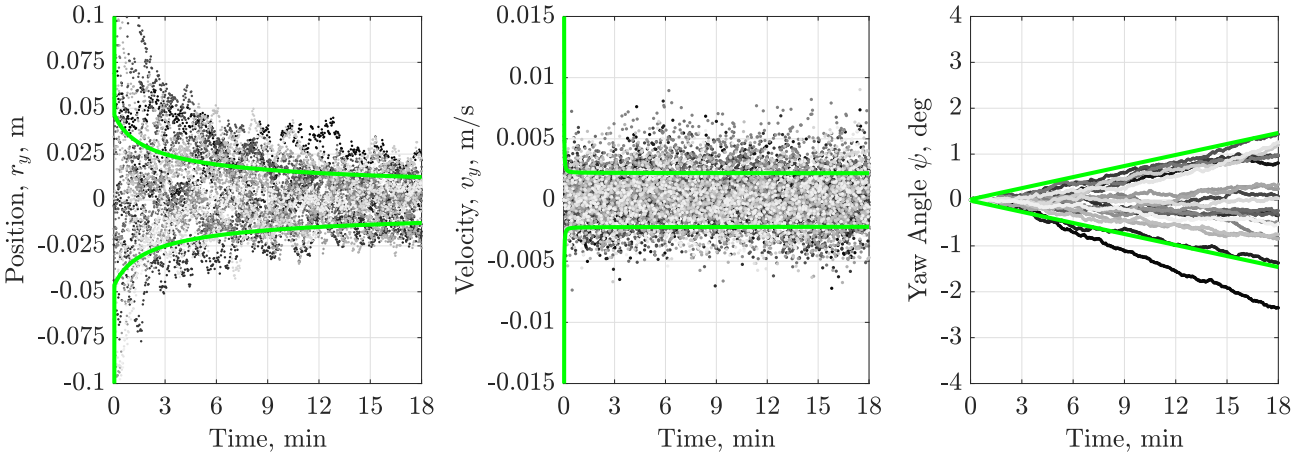

Fig. 3: Estimates of lateral position, velocity, and attitude errors in tightly-coupled INS/GPS configuration with authentic signals from 8 satellites.

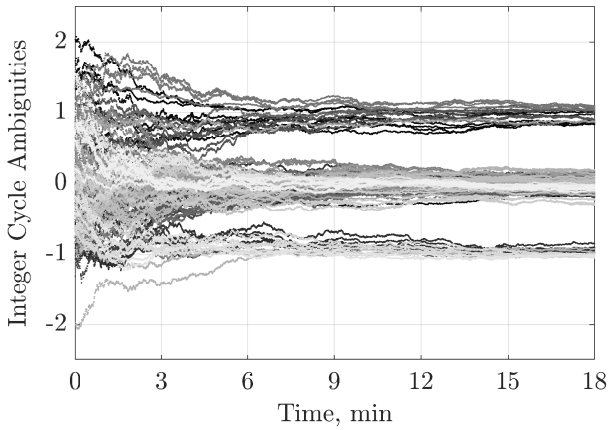

Fig. 4: Integer cycle ambiguity (floating) estimates in tightly-coupled INS/GPS configuration with authentic signals collected from 8 satellites.

has been tested for a 30 s attack window with these conventional threat models as well as the worst-case fault model, of which results are shown in Fig. 5. In the figure, the effect of fault on the position estimate is presented on the left plot whereas its effect on test statistic is given on the right plot. Each transparent region in the left plot represents the bound of test statistic for each fault type observed through the experimental trials.

As seen in the figure, compared to the fault-free test statistic (light brown), the constant velocity fault (black) impacts the test statistic slope the most, causing an immediate jump at the beginning. This is expected because it injects a step velocity to the system without initially introducing accelerations, which reflects as an abrupt inconsistency between INS and GNSS measurements in the monitor. Within the 30 s attack window, the constant jerk fault (light gray) results in an exponentially increasing growth in the test statistic, whereas the constant acceleration (dark gray) fault causes a near-linear growth in the test statistic.

Even though the effect of the worst-case fault (purple) on the estimation error looks similar to that of the constant acceleration fault, its impact on the test statistic is clearly different from that of the constant acceleration. The reason is that as seen in the plot, the worst-case fault profile injects slightly larger acceleration initially; however, once the estimator is drifted to the minimum velocity that will result in a required position error (e.g. 8 m for this experiment) at the end of attack period, it stops injecting acceleration and preserves a constant velocity fault profile throughout the rest of the attack. This unique characteristic of the worst-case fault causes a decay in the slope of test statistic,

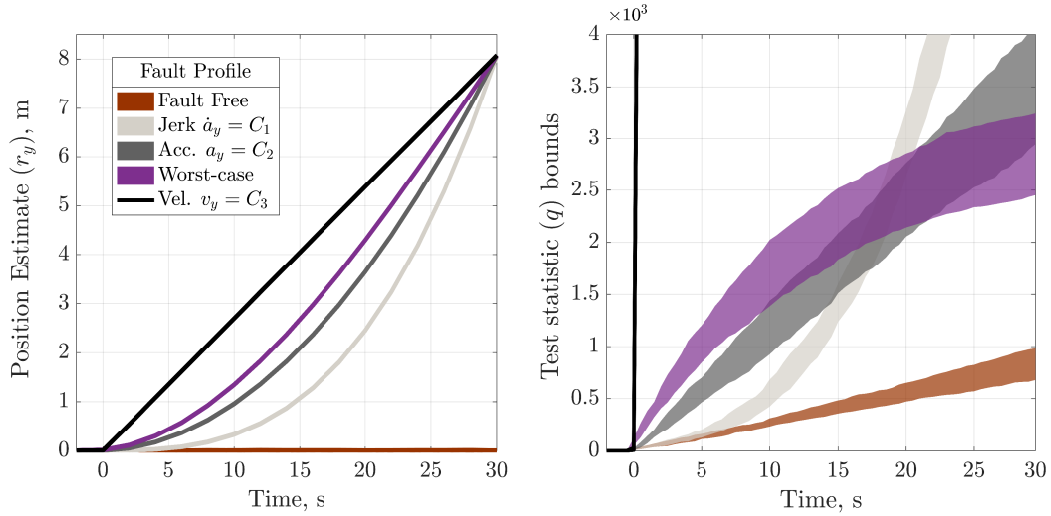

Fig. 5: Impact of different fault profiles on detection test statistic for a 30 s spoofing attack.

which ultimately levels off the test statistic and results in a lowest probability of detection. In the right plot, it can be observed that its test statistic distribution at the end of the attack period is lower than those due to the constant acceleration and other fault profiles. The experiments in the following sections are conducted using the worst-case fault profile for varying attack windows and an alert limit of 10 m.

C. The Effect of Tracking Noise

The performance evaluation approach with the worst-case fault assumes that the spoofer is able to estimate the current receiver antenna position and project it over the attack period perfectly. In a more realistic scenario, the errors in tracking and estimating the target antenna position introduced by the attacker must be accounted for. The prior work in [18] showed that due to the cumulative nature of the proposed innovation sequence monitor even millimeter-level tracking errors (in position domain) have a considerable influence on the detection test statistic.

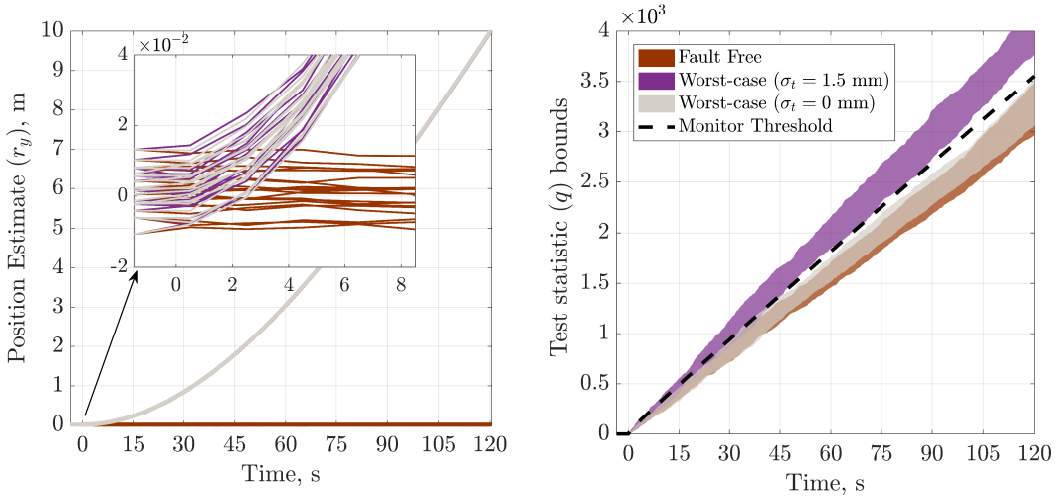

Fig. 6: Controlled experiments with hardware setup. The effect of 2-min worst-case spoofing attack on position estimates and detection detection test statistics with various tracking errors.

This makes the monitor remarkably sensitive to the spoofing attacks, which was previously shown in the covariance analysis for a B747 approach equipped with navigation-grade inertial sensors [14].

To experimentally show the effect of high-frequency components of tracking errors, we add a small zero-mean white noise on the exact antenna trajectory, and quantify the sensitivity of the monitor to these tracking errors by computing the missed detection rates for experiments with a 2 min attack window. Fig. 6 shows the resulting estimation error and test statistic distributions for different scenarios with 1) no-fault (light brown), 2) a worst-case fault and perfect tracking (light gray), and 3) a worst-case fault and 1.5 mm 1-σ white tracking noise (purple). As shown in the left hand side of the figure, compared to the fault-free case the worst-case fault with zero tracking error introduces a big error to the position estimate, reaching to 10 m at the end of attack, while having a test statistic that is pretty close to the fault-free one. As a result, a high probability of missed detection (95%) is recorded, which illustrates and validates how powerful a spoofer can be on such a scenario with perfect tracking. However, once even a small tracking noise ($\sigma_t = 1.5$ mm) is introduced, even though its effect on the position error is negligible, it causes a tremendous growth in test statistic that ultimately exceeds the threshold within the attack window. All of the spoofing attempts with this scenario are easily detected (i.e., zero probability of missed detection).

D. Experimental Validation of Covariance Results

For more comprehensive experimental validation of theoretical integrity risk results, using the error models in Table II and Table I, we first performed a covariance analysis and obtained integrity risk values for a tightly-coupled STIM300 and GPS navigation system in Fig. 7, which captures the effect of the attack period ($1 \leq t_s \leq 8$ min) and the tracking errors ($0 \leq \sigma_t \leq 2$ mm). The integrity risk results here are very promising because such millimeter level tracking accuracy is unrealistically high using any combination of existing high-grade position tracking systems (e.g., laser, radar, vision) [26].

It should be noted that the principal reason that the integrity risk plummets when the tracking error standard deviation increases is the high frequency content of the tracking error. Such significant high-frequency variations with a millimeter level amplitudes in the carrier phase of the spoofed GNSS signals would look suspicious to the monitor implemented on a tightly-coupled INS/GNSS system. This statement is valid as long as the multipath error changes slowly and the clock driving the GNSS receiver has a millimeter level accuracy. For example, in aircraft operations, the multipath time constant is usually long (e.g., 100 s) and the carrier phase thermal noise has a standard deviation of a couple of millimeters, therefore the likelihood of the high-frequency tracking errors

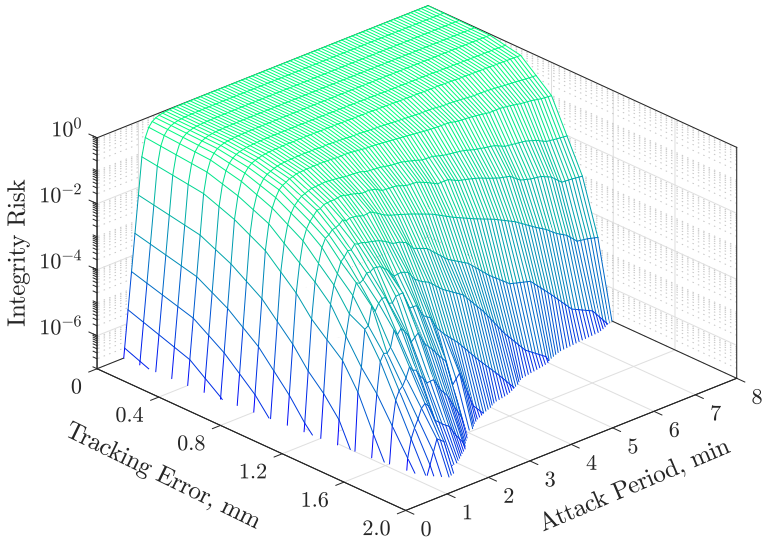

Fig. 7: The analytical covariance analysis results for STIM300 showing the impact of attack period and white tracking errors in the spoofed signal. The integrity risk surface obtained with worst-case fault sequence using a false alarm probability of 10^{-2}.

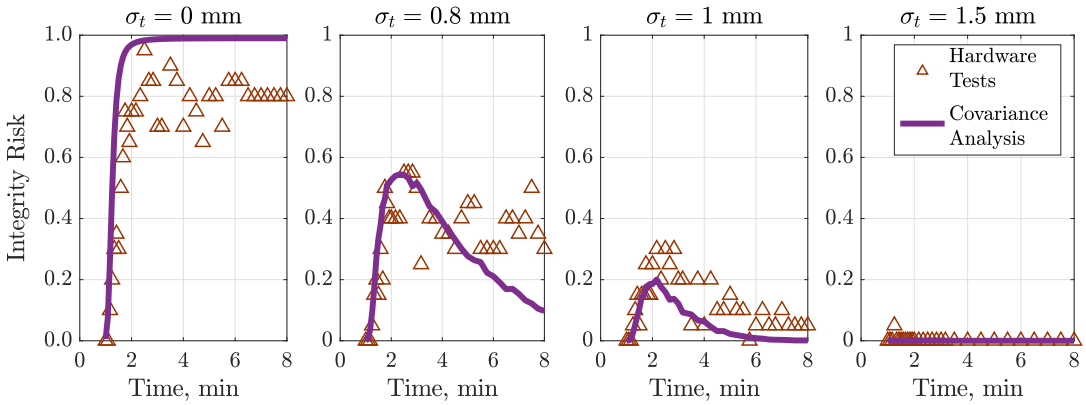

Fig. 8: Experimental miss-detection rates vs analytical integrity risks with worst-case fault sequence over various attack periods and tracking errors.

on the carrier signal to be shadowed by the multipath error or the thermal noise is too small. As a result, the proposed monitor is expected to have a high detection performance. It should also be noted that the detection leverage due to tracking errors will be attenuated as the coupling between IMU and GNSS receiver gets looser (e.g., loosely-coupled integration scheme), or there will be no leverage when when using other snapshot- or solution separation-based monitors (e.g. uncoupled integration) [16].

For experimental validation of the analytical integrity results, we selected 4 different tracking error values ($\sigma_t = 0$, 0.8, 1.0, and 1.5 mm) on the y axis of the surface plot, and computed the experimental missed detection rates out of 20 independent attempts. Fig. 8 shows that when $\sigma_t = 0$, the covariance analysis results are slightly more conservative than the experimental results whereas when $\sigma_t \geq 0$, the covariance results becomes slightly optimistic especially for attack periods longer than 4 min. The experimental missed detection rates sometimes exceed the analytical integrity risks mainly because the number of experiments required to converge a correct probability increases as the standard deviation of the tracking noise gets larger. In the experiments, due to the time constraints we used a fixed number of independent trials (e.g., 20). Regardless, these results are promising and show that the experiments roughly match the covariance analysis result, which validates our previous work, where we showed that the monitor is effective in detecting spoofing attacks with very low integrity risks, as long as the spoofer has tracking errors more than millimeter level.

E. The Effect of Track Smoothing

Spoofer's tracking data (for example obtained from radar or lidar) will not typically have a smooth appearance since the data contain significant high frequency noise. The previous section focused on quantifying leveraging effect of this high-frequency noise component in spoofing detection. On the other hand, the smoothing filters are intended to mitigate high-frequency noise in the tracking data. An optimum choice of smooth bandwidth can be selected such that it does not significantly changes the low-frequency signal component representing the payload motion along the trajectory. That is, the spoofer is limited by the bandwidth of the vehicle, it can not go beyond that otherwise it may smooth the vehicle motion as well. Regardless, the smoothing filters systematically distort the nominal trajectory causing offsets that may be larger than the rms noise levels in the smoothed data [25].

This section describes the experimental analysis of this systematic error component in smoothed tracking data. To capture the effect of filtering, we conduct a parametric analysis for different driving noises and bandwidths ranging from large transport aircraft (B747) to small unmanned aerial vehicles (e.g., drones). Note that the methodology in our prior work [18], also summarized in Sect. II-A, provides an analytical upper bound to integrity risk only if the tracking errors are zero (perfect tracking) or non-zero but uncorrelated over time (white noise). Therefore, in this section we present only the experimental missed detection rates in the existence of the colored tracking noise. Independent samples of the colored noise are generated using a first order Gauss Markov process and fed into the GNSS simulator before generating the GPS signals.

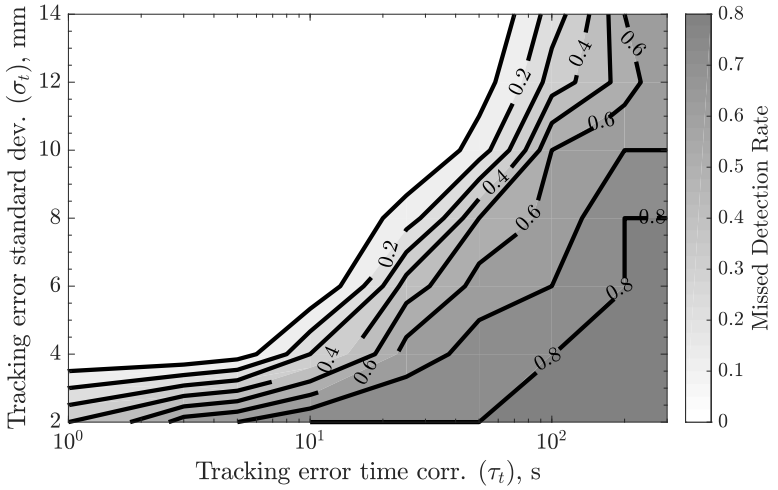

Fig. 9: The effect of track smoothing in detection performance. Spoofer's tracking errors are modeled as first order Gauss-Markov process with varying correlation time constant and standard deviation over 5 min attack window.

The missed detection rates are shown with the contour plot in Fig. 9 for varying standard deviations ($2 \leq \sigma_t \leq 14$ mm) and correlation time constants ($1 \leq \tau_t \leq 300$ s). There, to avoid trivial detections due to initial jumps we conservatively assume that the initial tracking error is zero. As seen in the figure, in order to achieve a spoofing attack to a small drone ($\tau \approx 1$ s) with a 10% or more chance of being not detected, the spoofer needs to have a maximum rms tracking error of 3.5 mm whereas it is slightly larger, 5 mm, for a B747 ($\tau \approx 8$ s for short-period mode). Once again, these rms tracking errors are unrealistically small compared to the available remote tracking technology [26], therefore the analysis results show that realistically, even with the track smoothing the monitor will be able to detect spoofing attacks with low missed detection probability. It should also be noted that the longer time constant region (far right of the plot) represents the effect of additional offsets in the track data that are near-constant, or slowly varying, for example uncertainties in lever-arm distance (between IMU and antenna), laser reflection point location, or target antenna phase center variation. It can be seen from the figure that these errors are additional means of detection as long as they are in centimeter level.

F. Discussion on Robustness of the Monitor

The robustness of the residual-based detectors was discussed in [24]. To investigate the robustness of the proposed innovations-based monitor to the error models used in the estimator and detector, we performed preliminary analyses, results of which will be presented in details in a future work. This section briefly summarizes the initial findings and discussion on the robustness of the monitor. The monitor's performance in this paper is validated for slow multipath environments, such as suburban ground or aviation navigation applications; however, it should be noted that the detection performance may be degraded in high-multipath environments such as urban-canyon navigation, where the multipath time constant is short therefore it is likely to shadow the leveraging effect of the high frequency tracking errors in detection. Furthermore, recall that in Sect. V-D we explain that variation of the carrier phase receiver thermal noise plays an important role in detecting spoofing attacks with tracking errors even in millimeter-levels. Therefore, the monitor is obviously sensitive to how accurate the carrier phase thermal noise is modeled in the estimator. The detection performance may also be degraded if the error model associated with the carrier phase thermal noise is too conservative.

VI. Conclusion

In this paper, we experimentally verified the feasibility of the Inertial Aided Anti-Spoofing Monitor (IASM) on a tightly-coupled INS/GNSS navigation system. For low- to high-bandwidth dynamic vehicles (from small drones to transport aircraft), the experiments demonstrated low missed detection rates resulting from worst-case spoofings of

all available receiver channels, even if the spoofer tracks the position of the antenna and smooth the high-frequency tracking errors. Some of the future work includes analyzing the robustness of the monitor and field testing against live spoofing signals.

APPENDIX A
HARDWARE CHARACTERIZATION

This section present data characterization of the raw IMU and GPS signals used in the experiments. Fig. 10 shows the lateral position, velocity, and yaw angle estimates obtained from INS-only propagation of 20 independent sets of inertial data. The 1-σ covariance bounds are computed using the manufacturer's stability and random walk parameters, presented in Table II, and highlighted with green in the figure.

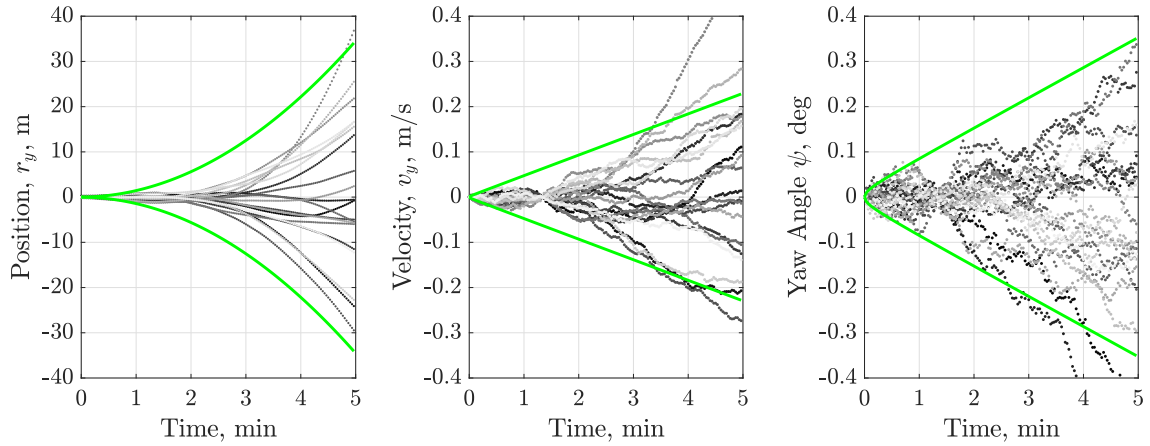

Fig. 10: Error propagations of position, velocity, and attitude errors in INS-only configuration. The curves are obtained for individual runs of STIM300 at rest. The highlighted regions are 1-σ covariance bounds.

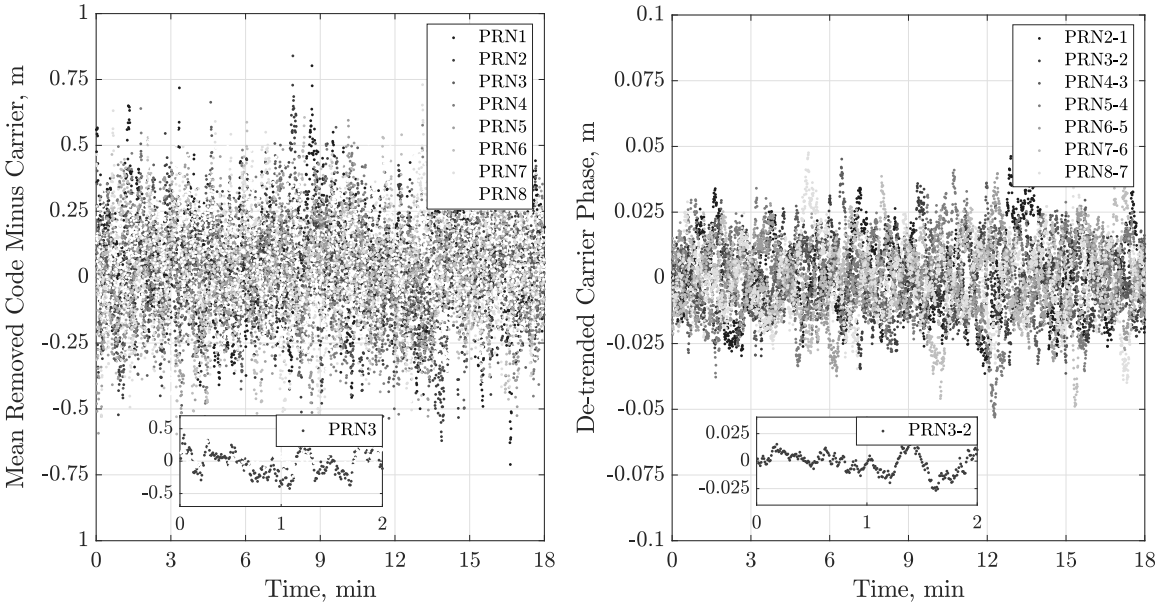

Fig. 11: GNSS signal characterization. Multipath and receiver thermal noise for code (left) and carrier (right) phase measurements obtained from GNSS Simulator through 8 GPS channels

The left plot of Fig. 11 shows the characterization results of GPS code measurement, the distribution is obtained from 20 independent experiments by differencing the code and carrier measurements after removing its integer mean (due to cycle ambiguities). From the plot, the 1-σ code thermal noise and multipath error is observed approximately as 20 cm with a correlation time constant of 5 s. For carrier phase measurement characterization, we used a carrier de-trending method that fits an orthogonal 5^{th}-order polynomial to the carrier measurements. The residual after the polynomial fit is approximated as the 1-σ carrier thermal noise and multipath error. The results are shown on the left plot of Fig. 11. The average value of 1-σ errors and the correlation time constants are obtained as 1.2 cm and 20 s, respectively. These values are used in the GPS estimator settings, presented in Table I.

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] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[3] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation, Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2016.

[4] D. M. Akos, "Whos afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *Navigation*, vol. 59, no. 4, pp. 281–290, Winter. 2012.

[5] 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.

[6] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "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.

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] Joerger, M., et. al., "RAIM Detector and Estimator Design to Minimize the Integrity Risk," in *Proc. ION GNSS Conference*, Nashville, TN, 2012.

[13] S. Khanafseh, N. Roshan, S. Langel, F-C. Chan, M. Joerger, and B. Pervan, "GNSS spoofing detection using RAIM with INS coupling," in *Proc. IEEE/ION PLANS*, Monterey, CA, 2014, pp. 1232–1239.

[14] C. Tanil,, "Detecting GNSS Spoofing Attacks Using INS Coupling," in *Ph.D. Dissertation, Department of Mechanical and Aerospace Engineering, Illinois Institute of Technology*, Chicago, IL, 2016,

[15] 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.

[16] C. Tanil, S. Khanafseh, and B. Pervan, "An INS Monitor against GNSS Spoofing Attacks during GBAS and SBAS- assisted Aircraft Landing Approaches," in *Proc. ION GNSS+*, Portland, OR, 2016.

[17] 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.

[18] C. Tanil, S. Khanafseh, M. Joerger, B. Pervan, "An INS 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.

[19] Manickam, S. , and O'Keefe, K., "Using Tactical and MEMS Grade INS to Protect Against GNSS Spoofing in Automotive Applications," in *Proc. ION GNSS+*, Portland, OR, 2016.

[20] Curran, J. T. , and Broumandan, A., "On the use of Low-Cost IMUs for GNSS Spoofing Detection in Vehicular Applications," in *Proc. International Technical Symposium on Navigation and Timing (ITSNT)*, Toulouse, France, 2017.

[21] Lo, Sherman, Chen, Yu Hsuan, Reid, Tyler, Perkins, Adrien, Walter, Todd, and Enge, Per, "The Benefit of Low Cost Accelerometers for GNSS Anti-Spoofing," in *Proc. the Institute of Navigation (ION) Positioning, Navigation and Timing Conference*, Honolulu, Hawaii, 2017.

[22] Lo, Sherman, Chen, Yu Hsuan, Reid, Tyler, Perkins, Adrien, Walter, Todd, and Enge, Per, "Consumer Mass Market Accelerometers for GNSS Anti-Spoofing," 2017.

[23] D.H Titterton, J.L. Weston, *Strapdown Inertial Navigation Technology*, 3rd ed. USA: AIAA, 2004.

[24] J. Rife, "Overbounding False-Alarm Probability for a Chi-Square Monitor with Natural Biases," *Navigation, Journal of the Institute of Navigation*, vol. 63, no. 4, pp. 455–467, 2016.

[25] J. V. White, "Radar Data Smoothing Filter Study," *NASA Technical Report, Patent Number: NASA-CR-168347*, 1984.

[26] Fernandez-Diaz, Juan Carlos and Carter, William E. and Glennie, Craig and Shrestha, Ramesh L. and Pan, Zhigang and Ekhtari, Nima and Singhania, Abhinav and Hauser, Darren and Sartori, Michael, *Remote Sensing*, vol. 8, no. 11, 2016.