

Sensitivity of Innovation Monitors to Uncertainty in Error Modeling

Birendra Kujur, Çağatay Tanıl, Samer Khanafseh, and Boris Pervan, Illinois Institute of Technology

BIOGRAPHIES

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 and navigation integrity monitoring.

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, was awarded by the 2017 Institute of Navigation (ION) Bradford W. Parkinson Award for excellence in global navigation satellite systems. With more than 13 years of guidance, navigation, and control experience, Dr. Tanıl fulfilled many research and development roles. From 2006 to 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). From 2016 to 2019, Dr. Tanıl worked at IIT as a Senior Research Associate, and at TruNav LLC as a research scientist, where he developed ARAIM-based satellite fault detection and exclusion algorithms, and autonomous car position integrity. Dr. Tanıl is currently a Navigation Research Scientist at Amazon Prime Air, working on drone navigation and safety.

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

The innovation sequence-based detector, which monitors time history of Kalman Filter (KF) innovations in a tightly coupled INS/GNSS integration, is a feasible anti-spoofing solution for navigation applications. The monitor with realistic error models has shown to achieve low missed detection rates for worst-case spoofing, even if the spoofer tracks the user position and smooths high-frequency tracking errors. The KF and monitor utilize error-models to account for the INS/GNSS system dynamics. However, the monitor performance suffers from modeling errors in

the INS and GNSS parameters as they deviate from the truth. This work first shows that the monitor is more sensitive to GNSS error model parameters compared to INS. We then quantified missed detection against conservatism and optimism in modeling systematic and random errors in code and carrier phase signals. The sensitivity analysis results in this paper are the foundation for eventual implementation and certification of the monitor.

I. INTRODUCTION

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

Augmenting data from auxiliary sensors such as Inertial Measurement Units (IMU), barometric altimeters, and independent radar sensors to discriminate spoofing has also been proposed [9], [10]. The first stochastic description and quantification of the performance of IMU-based GNSS spoofing monitor against worst-case faults was introduced by us [11]–[17]. We investigate anti-spoofing solutions utilizing IMUs since all modern vehicles are equipped with them, thereby not requiring any 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. An Inertial Navigation System (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.

One of the most effective anti-spoofing implementations is the Chi-squared innovation sequence-based detector which monitors time history of Kalman filter (KF) innovations in a tightly coupled INS/GNSS integration [17]. The KF innovation sequence monitor provides superior detection capability against slowly growing faults. In our prior work [17], [18] we evaluated the performance of the monitor against worst-case sequence of GNSS faults both analytically and experimentally. The worst-case fault here represents a spoofed GNSS signal profile that maximizes integrity risk, which in turn, is defined as the probability that undetected faults exceed a position alert limit. In the prior work we also showed that even if the spoofer is capable of tracking and estimating the user receiver position with sub-centimeter level of accuracy, the monitor detects the attack easily.

However, Chi-squared based monitors are known to be more sensitive to error modeling than solution separation-based monitors which directly checks the discrepancy in position domain. Uncertainty in error-models for a system can arise from either limited knowledge of user about the system or due to constantly changing parameters such as the multipath environment. Preliminary analysis from our prior work [18] indicated that the detection capability of innovation sequence monitor is sensitive to mismodeling carrier phase thermal noise and multipath. In this paper, we first identify the error model parameters that the monitor is most sensitive to. We simulate mismodeling for those parameters by using values different from the truth, in the KF models. Using these incorrect values for parameters, we analyze the robustness of the monitor under both spoof free and spoofing cases.

II. INNOVATION MONITOR

An Inertial Navigation System (INS) provides navigation solution as states of user position r_x, r_y, r_z , velocity v_x, v_y, v_z , and attitude ϕ, θ, ψ (Euler angles), using IMU measurements. An IMU consists of tri-axis accelerometer and gyroscope to provide measurements of acceleration and body angular rate. The acceleration measurements are integrated once to obtain velocity and then integrated again to get position, whereas attitude is obtained by integrating angular rate measurement. These measurements have errors (bias and noise), therefore position solution drifts over time. In a tightly coupled INS/GNSS architecture, Kalman filter (KF) uses raw code and carrier measurements to estimate and correct the error in the INS states to provide the integrated navigation solution.

The INS states are

$$X_{INS} = [r_x \ r_y \ r_z \ v_x \ v_y \ v_z \ \phi \ \theta \ \psi]^T \quad (1)$$

IMU measurement \tilde{u} has errors such as constant and time dependent bias, and noise. Therefore it is modeled as true measurement u^* , corrupted with a constant bias b_c , time dependent component of bias b , and additive White-Gaussian noise (WGN) η_u as represented in Equation 2. The constant bias is usually specified as bias repeatability and additive WGN η_u is commonly derived from specifications of velocity random walk (VRW) of accelerometer and angular random walk (ARW) of gyroscope.

$$\tilde{u} = u^* + b_c + b + \eta_u \quad (2)$$

The time dependent component of bias is modeled as a First order Gauss-Markov random process (GMRP) with time constant τ_b and driving WGN v_b . This driving WGN v_b for bias is derived from the specification of bias instability.

$$\dot{b} = -\frac{1}{\tau_b}b + v_b \quad (3)$$

The bias dynamics are included in the process model with augmentation of bias states \mathbf{X}_{bias} to the INS states. Thus, for three different IMU axes, the bias states for both acceleration and angular rate measurements are shown in Equation 4. Equations 1 and 4 show all the nominal states that are propagated to obtain the INS navigation solution.

$$X_{bias} = [b_{a_x} \ b_{a_y} \ b_{a_z} \ b_{\omega_x} \ b_{\omega_y} \ b_{\omega_z}]^T \quad (4)$$

Equation 5 shows the GNSS measurement equation. The code measurement ρ for each satellite is composed of true range p , satellite and receiver clock bias dt_{sv} and dt_{rc} , code ionospheric delay I_ρ , code tropospheric delay T_ρ , code multipath m_ρ , and receiver code thermal WGN $v_{th(\rho)}$. Similarly, the carrier phase measurement $\lambda\phi$ for each satellite is composed of true range p , satellite and receiver clock bias dt_{sv} and dt_{rc} , carrier ionospheric delay I_ϕ , carrier tropospheric delay T_ϕ , carrier phase multipath m_ϕ , carrier phase cycle integer ambiguity N_ϕ and receiver carrier thermal WGN $v_{th(\phi)}$.

$$\begin{bmatrix} \rho \\ \lambda\phi \end{bmatrix} = \begin{bmatrix} p \\ p \end{bmatrix} + \begin{bmatrix} c(dt_{rc} - dt_{sv}) \\ c(dt_{rc} - dt_{sv}) \end{bmatrix} + \begin{bmatrix} I_\rho \\ -I_\phi \end{bmatrix} + \begin{bmatrix} T_\rho \\ T_\phi \end{bmatrix} + \begin{bmatrix} m_\rho \\ m_\phi \end{bmatrix} + \begin{bmatrix} 0 \\ \lambda N_\phi \end{bmatrix} + \begin{bmatrix} v_{th(\rho)} \\ v_{th(\phi)} \end{bmatrix} \quad (5)$$

where, c is the speed of light in vacuum, and λ is the carrier wavelength.

Considering availability of dual frequency GNSS measurements, elimination of ionospheric delay can be achieved using ionospheric free measurements. Tropospheric delay is also assumed to be estimated using a tropospheric model or eliminated using a reference antenna measurements in a differential implementation. Thus, here we focus on errors such as clock bias, multipath and receiver thermal noise reducing the GNSS measurement equation as

$$\begin{bmatrix} \rho \\ \lambda\phi \end{bmatrix} = \begin{bmatrix} p \\ p \end{bmatrix} + \begin{bmatrix} c(dt_{rc} - dt_{sv}) \\ c(dt_{rc} - dt_{sv}) \end{bmatrix} + \begin{bmatrix} m_\rho \\ m_\phi \end{bmatrix} + \begin{bmatrix} 0 \\ \lambda N_\phi \end{bmatrix} + \begin{bmatrix} v_{th(\rho)} \\ v_{th(\phi)} \end{bmatrix} \quad (6)$$

Satellite clock offsets are available from the navigation message and receiver clock offset is eliminated using a single-difference measurements between two satellites. Multipath being time correlated, is modeled as a First order GMRP with auto-correlation time constant τ_m and driving WGN v_m .

$$\dot{m} = -\frac{1}{\tau_m}m + v_m \quad (7)$$

Constant carrier phase cycle integer ambiguity along with code and carrier phase multipath, is included in the modeled GNSS measurement states.

$$X_{GNSS} = [m_\rho^{1:n} \ m_\phi^{1:n} \ \lambda N_\phi^{1:n}]^T \quad (8)$$

where, n is the number of satellites.

The final state vector of the INS/GNSS system is

$$X = [X_{INS} \ X_{bias} \ X_{GNSS}]^T \quad (9)$$

This augmented system dynamics is perturbed to obtain the linear error-state $\delta\mathbf{x}$ process model, to be utilized in the KF. The error-state process model in discrete time can be represented as

$$\delta\mathbf{x}_{k+1} = \Phi_k \delta\mathbf{x}_k + \Gamma_{w_k} \mathbf{w}_k \quad (10)$$

where, Φ is the state transition matrix, Γ_w is the process noise model and \mathbf{w} is the additive noise with respective process noise covariance \mathbf{Q} .

The error-state measurement model in discrete time is represented with observation matrix \mathbf{H} and additive measurement noise \mathbf{v}_k with respective measurement noise covariance \mathbf{V} as

$$\delta\mathbf{z}_k = \mathbf{H}_k \delta\mathbf{x}_k + \mathbf{v}_k \quad (11)$$

where, $\delta\mathbf{z}$ is the error between GNSS measurement and predicted measurement obtained from prior knowledge. The KF error state estimates is used to correct the INS navigation solution to obtain the integrated navigation solution.

The innovation sequence-based monitor is a Chi-squared monitor which utilizes cumulative normalized innovations from a KF as the test statistic, and compares it against a threshold. The innovation vector γ at time epoch k is defined as

$$\gamma_k = \delta\mathbf{z}_k - \mathbf{H}_k \delta\bar{\mathbf{x}}_k \quad (12)$$

Where, $\delta\bar{\mathbf{x}}$ is the a priori error state vector. A cumulative test statistic q_k is defined as the sum of squares of the normalized innovation vectors over time as

$$q_k = \sum_{i=1}^k \gamma_i^T \mathbf{S}_i^{-1} \gamma_i \quad (13)$$

Where, \mathbf{S}_i is the 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

$$q_k \geq T_k^2 \quad (14)$$

For a given false alarm rate requirement under fault free scenario, the threshold T_k^2 is determined from the inverse Chi-square cumulative distribution function (CDF). The innovation monitor alarms for a fault if $q_k > T_k^2$.

Since error model parameters such as time constants and standard deviation of WGN that are utilized by the KF and monitor, any deviation in these parameters from the truth could degrade the monitor performance. Mismodeling in error models could result in false alarms in spoof free case and may impact missed detection probability under a spoofing fault scenario. Thus, sensitivity analysis of the monitor to error model parameters was done considering both spoof free and spoofing scenario. The details of the spoofing scenario utilized for this sensitivity analysis is described in the next section.

III. SPOOFING SCENARIO

The closed loop tracking and spoofing method described in our prior work [18] is used here as the spoofing scenario. In this method of spoofing, 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 code and carrier 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 [14,15]. The spoofers deliberate fault is optimally computed using the tracked position and exact error models of estimator and detector implemented on target navigation system.

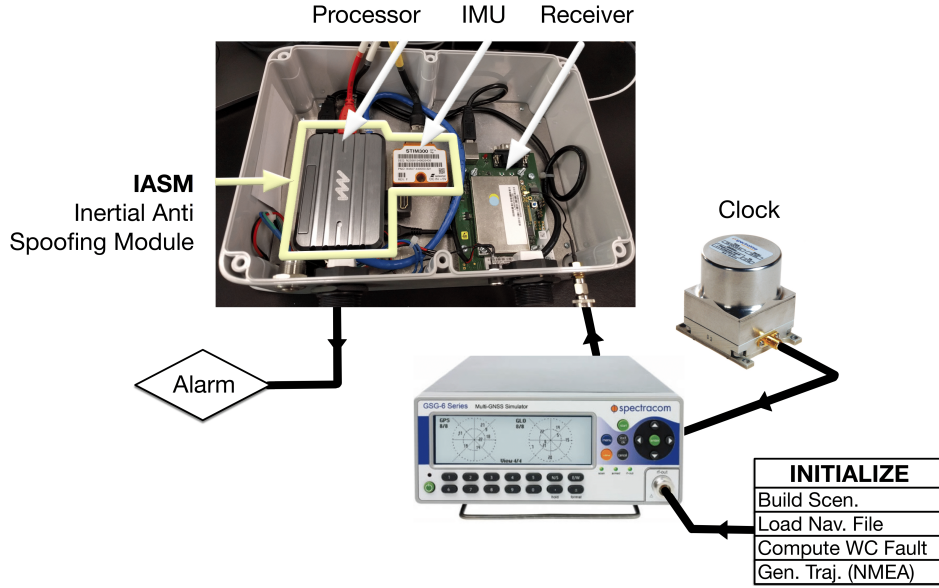


Fig. 1: Setup for realization of spoofing attack.

We used the static setup described in our prior work [18], where 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) as shown in Fig. 1, comprised the spoofing attack setup. To simulate the closed loop tracking and spoofing method, based on static user position, time sequence of the worst-case position offset is first computed using replica statistical models of user 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. An alert limit of 10 meters is used such that the position offset due to worst-case fault sequence reaches to 10 meters at the end of the pre-defined attack window of 120 seconds. Ionospheric delays are deliberately turned off in the simulator setting because we assumed an iono-free dual frequency implementation. A multipath error equivalent of being in a suburban environment [19] is generated using first order GMRP model. This multipath error is then added to the code and carrier phase measurements obtained from the GNSS simulator. Additional WGN is added to the measurements to obtain specific standard deviation values of receiver thermal noise.

IV. ERROR MODEL PARAMETERS

Section II, introduced all the error-models used in the KF estimator and innovation monitor. Table I shows the different error-model parameters in the KF. The WGN of the error models are represented as normally distributed zero mean noise with certain standard deviation σ . The state transition matrix includes time constants of error models. The process noise covariance matrix contains standard deviation of driving WGN for first order GMRP error models, time constants of first order GMRP error models, and standard deviation of WGN of IMU measurements. The measurement noise covariance consists of standard deviation of receiver code and carrier phase thermal WGN.

TABLE I: System error-model parameters

	Parameters			
	Accelerometer	Gyroscope	Multipath	Thermal Noise
Φ - State Transition Matrix	τ_{b_a}	τ_{b_ω}	$\tau_{m_\rho}, \tau_{m_\phi}$	
\mathbf{Q} - Process Noise Covariance	$\eta_a, \sigma_{b_a}, \tau_{b_a}$	$\sigma_\omega, \sigma_{b_\omega}, \tau_{b_\omega}$	$\sigma_{m_\rho}, \sigma_{m_\phi}, \tau_{m_\rho}, \tau_{m_\phi}$	
\mathbf{V} - Measurement Noise Covariance				$\sigma_{rh(\rho)}, \sigma_{rh(\phi)}$

To determine the impact of these parameters on the performance of innovation monitor, one-factor-at-a-time method is utilized. For the IMU error models, the true (nominal) values of time constants and standard deviation of WGN is obtained from manufacturer specifications. For the GNSS error models, true value of multipath parameters are known since the error was generated using a first order GMRP. Receiver thermal noise standard deviation values are also known. Thus, the true value of these parameters is known and each parameter is varied individually in KF error models from those nominal values to represent the uncertainty in those parameters. As these parameters are changed from their nominal values the impact on the test statistic q_k is observed. Fig. 2 shows an example of performance degradation of the monitor when a parameter was changed from its nominal value. This spoofing scenario in Fig. 2 shows an attack window of 120 seconds during which the spoofer tries to divert the user position. During this attack window, spoofing is detected when the test statistic exceeds the threshold at any time epoch of the 120 second interval. In this figure the test statistic normalized by the threshold exceeding value of 1 shows spoofing detection. In this particular scenario, when correct error model is used, spoofing was detected as shown by the normalized test statistic exceeding the normalized threshold of one. On the other hand, when an incorrect model is used for the same scenario the test statistic never exceeded the threshold and the monitor is unable to detect spoofing resulting in missed detection.

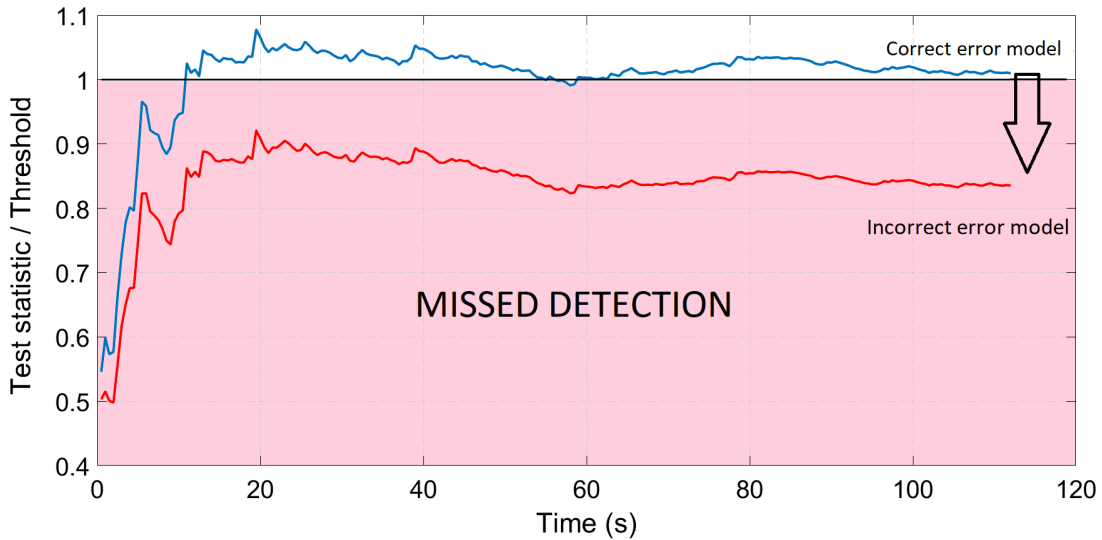


Fig. 2: Illustration of innovation monitor performance degradation when an incorrect error model is used.

The incorrect error models can arise from parameters either being overestimated or underestimated from the true value. This overestimation or underestimation is the uncertainty of the parameters. Thus, for this sensitivity analysis, the parameters were changed one at a time to both an underestimated or overestimated value in the KF error model. The magnitude of uncertainty introduced in these parameters is based on some general assumptions. In case of time constants of IMU biases, it is safe to assume that multiple data samples can be collected and a good approximation can be made as compared to time constants of multipath model where the environment is constantly changing. In our prior work [19], we showed that even for a specific environment such as urban canyon or open sky, the multipath error correlation time and the bounding CDF standard deviation varies. In the simulations, the uncertainty in time constants of IMU biases, WGN power spectral density (PSD) of IMU biases and IMU measurements, and standard deviation of multipath and receiver thermal noise is taken to be half and twice the nominal values. The uncertainty in time constant of multipath on the other hand is taken to be a tenth and ten times the nominal values. These are example uncertainty bounds considered for this sensitivity analysis.

Table II shows the nominal values of the time constants with the lower and upper values used in KF error models. Table III shows the nominal values of WGN PSD and standard deviation with the lower and upper values. For each

of the parameters shown in Table II and III, the parameters are changed individually to both lower and upper bound values in the KF error models.

TABLE II: Utilized time constants of the parameters in the error-model

	Parameters			
	τ_{b_a}	τ_{b_ω}	τ_{m_ρ}	τ_{m_ϕ}
Nominal values	1 hr	1 hr	20 s	20 s
Lower uncertainty bound	0.5 hr	0.5 hr	2 s	2 s
Upper uncertainty bound	2 hr	2 hr	200 s	200 s

TABLE III: Utilized PSD and standard deviations in the error model

	Parameters							
	η_a	η_ω	v_{b_a}	v_{b_ω}	v_{m_ρ}	v_{m_ϕ}	$v_{th(\rho)}$	$v_{th(\phi)}$
Nominal values	0.0048 m/s^2	$3.5 \times 10^{-4} \text{ rad/s}$	$1.2 \times 10^{-5} \text{ m}\sqrt{\text{s}}/\text{s}^2$	$5.7 \times 10^{-8} \text{ rad}/\sqrt{\text{s}}$	0.5 m	1 cm	20 cm	2 mm
Lower bound	0.0024 m/s^2	$1.8 \times 10^{-4} \text{ rad/s}$	$0.6 \times 10^{-5} \text{ m}\sqrt{\text{s}}/\text{s}^2$	$2.9 \times 10^{-8} \text{ rad}/\sqrt{\text{s}}$	0.25 m	0.5 cm	10 cm	1 mm
Upper bound	0.0096 m/s^2	$7 \times 10^{-4} \text{ rad/s}$	$2.4 \times 10^{-5} \text{ m}\sqrt{\text{s}}/\text{s}^2$	$11.4 \times 10^{-8} \text{ rad}/\sqrt{\text{s}}$	1 m	2 cm	40 cm	4 mm

V. RESULTS

In spoof free and spoofing case, when each of the error model parameters were tuned within bounds shown in Table II and III, the test statistic increased or decreased in magnitude relative to when nominal or true values were used. This relative change of test statistic on whether an incorrect value of error model parameter was used resulted in false alarm for spoof free and missed detection of spoofing case. Fig. 3 and Fig. 4 show relative change in test statistic for spoof free and spoofing case, respectively.

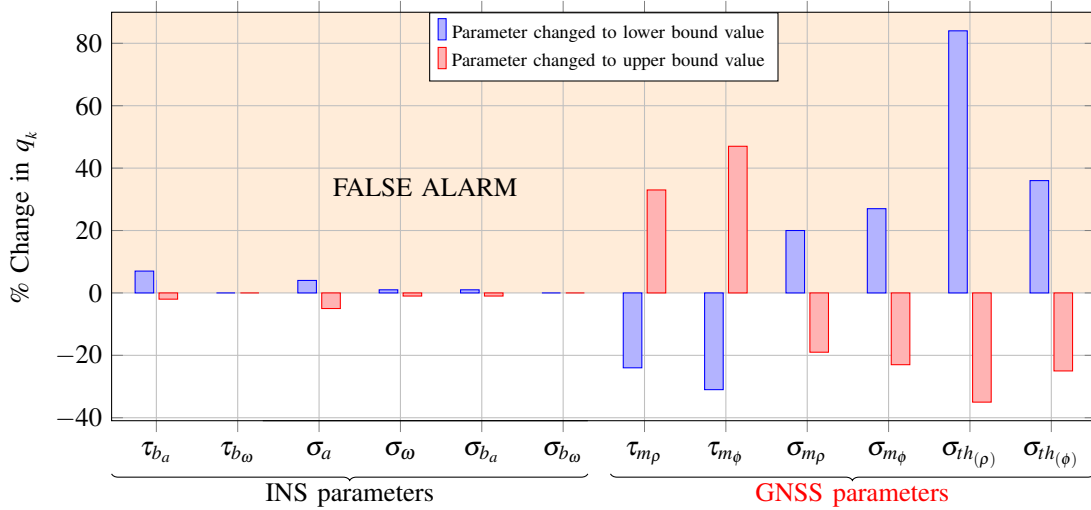


Fig. 3: Spoof free case results

For both spoof free and spoofing case scenarios, the innovation monitor is not as sensitive to mismodeling in INS error models as compared to GNSS error models. In Fig. 3 any positive change in test statistic increases the chance for false alarm whereas in Fig. 4 any negative change in test statistic causes missed detection. Since, for spoof free and spoofing case relative change in test statistic has opposite effects of false alarm and missed detection, there is a trade off between continuity and integrity. For example if time constant of multipath is overestimated it might not cause missed detection in spoofing case as shown in Fig. 4, but as seen in Fig. 3 increases the chance of false alarm

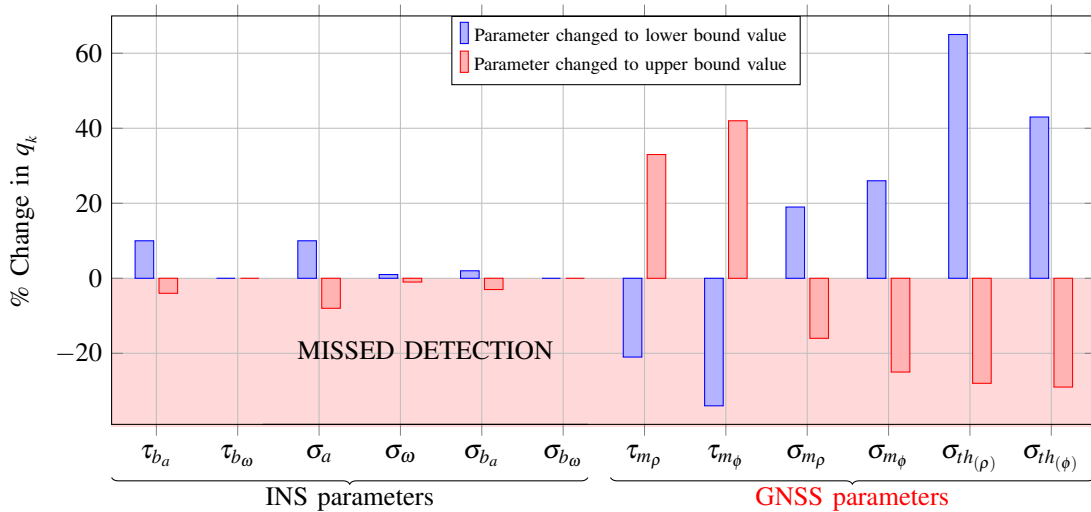


Fig. 4: Spoofing case results

for spoof free case. Therefore, from an integrity standpoint the time constant of multipath first order GMRP model must not be underestimated. Also, the standard deviation of code and carrier phase thermal noise and multipath noise must not be overestimated. This result poses an interesting conundrum when evaluating fault free protection level given required integrity risk.

Fault free protection level is computed for given integrity risk requirements and position estimate error standard deviation. To ensure correct protection level calculation the standard deviation values in the error models must always be greater than or equal to the true standard deviation to conservatively bound the true protection level. This is opposite to what was shown in the previous result where the standard deviation must not be overestimated to ensure that spoofing is detected. We will investigate approaches to use two different values of standard deviation such that the fault free protection level is valid, while preserving the missed detection probability under spoofing scenarios.

In designing the innovation monitor, the above results serve as a guideline to determine which parameters need more attention. The results show the uncertainty bounding one should have for these parameters to ensure continuity and integrity of the system. Also, it is clear that there exists a trade-off between spoofing detection and fault free protection level computation. Detailed analytical analysis of how error model parameters influence test statistic is still under investigation.

VI. CONCLUSION

In this paper, we analyzed the sensitivity of innovation monitor under spoof free and spoofing cases on a tightly-coupled INS/GNSS navigation system. The monitor is most sensitive to GNSS error model of multipath and receiver thermal noise. It was shown from an integrity standpoint that the standard deviation of code and carrier phase receiver thermal noise and multipath must not be overestimated. The multipath time constant on the other hand must not be underestimated to reduce chances of missed detection. In conclusion, uncertainty of these parameters need to be both lower and upper bounded when designing an innovation monitor in order to ensure continuity and integrity requirements.

REFERENCES

- [1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, and B. W. O'Hanlon, "Assessing the spoofing threat: development of a portable GPS civilian spoofer," in Proc. IEEE/ION PLANS, Savannah, GA, 2008, pp. 2314–2325.
- [2] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "A proposed navigation message authentication implementation for civil GPS anti-spoofing," in Proc. IEEE/ION PLANS, Portland, OR, 2011, pp. 2314–2325.

- [3] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *Navigation*, vol. 59, no. 4, pp. 281–290, Winter. 2012.
- [4] J. Nielsen, A. Broumandan, and G. Lachapelle, "Spoofing detection and mitigation with a moving handheld receiver," *GPS World*, vol. 21, no. 9, pp. 27–33, Sep. 2010.
- [5] M. Meurer, A. Konovaltsev, M. Cuntz, and C. 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.
- [6] S. Moshavi, "Multi-user detection for DS-CDMA communications," *IEEE Communications Magazine*, vol. 34, no. 10, pp. 124–135, Oct. 1996.
- [7] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in *Proc. ION GNSS+*, Nashville, TN, 2013, pp. 2949–2991.
- [8] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables," *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, pp. 181–191, Jul. 2012.
- [9] P. F. Swaszek, R. J. Hartnett, and K. C. Seals, "GNSS spoof detection using independent range information," in *Proc. ION ITM*, Monterey, CA, 2016, pp. 739–747.
- [10] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.
- [11] S. Khanafseh, et. al., "GPS Spoofing Detection Using RAIM with INS Coupling," in *Proc. ION PLANS Conference*, Monterey, CA, 2014.
- [12] C. Tanil, S. Khanafseh, and B. Pervan, "Impact of Wind Gust on Detectability of GPS Spoofing Attack Using RAIM with INS Coupling," in *Proc. IEEE/ION PNT Conference*, Honolulu, HI, 2015, pp. 1232–1239.
- [13] C. Tanil, S. Khanafseh, and B. Pervan, "GNSS spoofing attack detection using aircraft autopilot response to deceptive trajectory," in *Proc. ION GNSS+*, Tampa, FL, 2015, pp. 3345–3357.
- [14] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "Kalman filter-based Innovation monitor to detect GNSS spoofers capable of tracking aircraft position," in *Proc. IEEE/ION PLANS*, Savannah, GA, 2016, pp. 1027–1034.
- [15] C. Tanil, S. Khanafseh, and B. Pervan, "An Innovation monitor against GNSS Spoofing Attacks during GBAS and SBAS- assisted Aircraft Landing Approaches," in *Proc. ION GNSS+*, Portland, OR, 2016.
- [16] C. Tanil, S. Khanafseh, and B. Pervan, "Detecting Global Navigation Satellite System spoofing using inertial sensing of aircraft disturbance," *Journal of Guidance, Control, and Dynamics*, vol. 40, no. 8, pp. 2006–2016, 2017.
- [17] C. Tanil, S. Khanafseh, M. Joerger, B. Pervan, "An Innovation monitor to Detect GNSS Spoofers Capable of Tracking Aircraft Position," *IEEE Transactions on Aerospace and Electronics*, vol. 54, no. 1, pp. 131–143, Feb 2018.
- [18] C. Tanil, P. M. Jimenez, M. Raveloharison, B. Kujur, S. Khanafseh, and B. Pervan, "Experimental Validation of Innovation monitor against GNSS Spoofing," in *Proc. ION GNSS+*, Miami, FL, 2018.
- [19] S. Khanafseh, et. al., "GNSS Multipath Error Modeling for Automotive Applications," in *Proc. ION GNSS+*, Miami, FL, 2018.