Pages: 17-24 / Vol.18 / Issue 2 / Summer- Fall 2025

Journal of Aerospace Science and Technology

Journal Homepage: https://jast.ias.ir

Original Research Article

Spoofing Attack Detection in Integrated GNSS/INS Navigation System Using Self-tuning Kalman Filter

Mohsen Shadmehri[1] and Reza Mahboobi Esfanjani[2]*

Department of Electrical and Computer Engineering, Sahand University of Technology, Tabriz, Iran

ARTICLE INFO

Received: 14 July 2024
Revised: 15 June 2025
Accepted: 29 June 2025
Available online: 07 July 2025

KEYWORDS:

Spoofing attack

Integrated navigation

Kalman Filter

Detection latency

ABSTRACT

Spoofers may attack Global Navigation Satellite System (GNSS) data, resulting in positioning errors in navigation. The features of the prediction of the Kalman filter are utilized to detect spoofing attacks in most of the existing attack monitors. However, the basic assumption in the conventional Kalman filter is that the noise characteristics in the system model are known in advance, which is often violated in real-world navigation systems. So, a novel spoofing attack monitor for a loosely coupled integrated GNSS/INS system is developed here utilizing the self-tuning Kalman filter concept in which the covariance matrices of the dynamic and measurement noises are adapted online, during the operation of the system. The proposed attack detector is designed based on the covariance matching idea in the adaptive Kalman filter, wherein the covariance matrices of the noise models are adapted based on the residual and innovation sequences within a moving sampling window. Comparative simulations demonstrate that the suggested method significantly outperforms the one based on the conventional Kalman filter.

DOI:
https://doi.org/10.22034/jast.2025.467877.1199

1 INTRODUCTION

In the integrated GNSS/INS navigation systems, the complementary properties of the satellite and inertial navigation systems are merged to obtain a more accurate navigation solution. The most implemented integration scheme for vehicle navigation is called loosely coupled, in which the GNSS data are used to construct a complementary measurements vector for the Kalman filter, which estimates the errors of the INS that are then subtracted from the INS measurements [1].

The GNSS data accuracy is subject to malicious cyber-attacks, including spoofing. In GNSS spoofing, an external agent provides false information in the output of the GNSS receiver by intentionally broadcasting a fake signal. So, the positioning result calculated by the GNSS/INS navigation system deviates from the real value [2].

The fake signal imitates the primary GNSS signal with higher power and then may go undetected through measurement monitoring methods employed

* Corresponding Author's Email: mahboobi@sut.ac.ir

Print ISSN:1735-2134 Online ISSN: 2345-3648

in the receiver. Therefore, the motion of the victim can be controlled by the invader. Recently, beyond signal-based methods, control-theoretic approaches have been developed at the navigation solution level to detect spoofing attacks using observers, especially the Kalman filter [3]. In this framework, the detector monitors inconsistencies between the GNSS spoofed data and the INS measurements, utilizing the statistical features of the innovation signal of the Kalman filter. The innovation sequence of the Kalman filter is used to create test statistics for attack detection in two directions. In the snapshot scheme, the innovation of the current time is employed; while in the sequential method, innovations inside a sliding window are averaged to identify slow attacks.

In [4], the Receiver Autonomous Integrity Monitoring (RAIM) concept was extended to spoofing detection by incorporating the statistical distribution of the system state derived from the extended Kalman filter. In [5], an innovation-based spoofing detector was proposed and integrated into the Kalman filter of a tightly coupled GNSS/INS system. In [6], a monitor was developed to detect GNSS spoofing attacks in a tightly coupled INS/GNSS navigation system using a Kalman filter. Moreover, by theoretically analyzing the worst-case spoofing profile, the performance of the innovation-based spoofing detector was evaluated in the presence of spoofers capable of tracking aircraft position. In [7], the spoofing impacts were analyzed on the Kalman filter of the integrated navigation system. It was revealed that the statistical properties of innovations are changed under a spoofing attack, which leads to potential statistical tests for spoofing detection. In [8], a Kalman filter estimates the error compensations of the inertial sensors, and an attack is declared whenever abrupt changes arise in the values of the filter variables.

In [9] and [10], in the RAIM framework, redundant satellite data were used to detect GNSS integrity, based on the parity space method as in fault detection and isolation (FDI) strategies. In [11], two strategies were employed to detect slow attacks. One way was based on averaging the innovations; the other was averaging the observations within the entire time window. Moreover, these averaging strategies were merged as the autonomous integrity-monitored extrapolation (AIME) approach.

In [12], based on estimating the spoofing profile by the innovation and the propagation process of the Kalman filter, a spoofing identification method was introduced for a tightly coupled INS/GNSS integrated system. In [13], a spoofing detection technique was suggested utilizing a generalized likelihood ratio test (GLRT), which is implemented by a matrix multiplication approach. Computational complexity compared to innovation-based approaches is considerable. In [14], GNSS spoofing in the integrated navigation is detected employing the positioning solution of the INS and the predicted position in the Kalman filter; then, the observation update process is executed when the GNSS position data passes the attack detection criterion. A secondary INS was used in [15], whose data is corrected by the Extended Kalman filter. The spoofed a priori estimate in the filter is replaced using this additional INS data to create an improved innovation. In [16], an INS-based steady-state spoofing detector was developed by evaluating the relation between the output of the INS and the Doppler frequency from the navigation signal. The detection method uses raw observations from the two sensors and prior information about the position [17-18].

Most of the innovation-based detection schemes are based on the conventional Kalman filter, wherein the fundamental assumption is that the noises are white, and their stochastic characteristics are exactly known a priori, which is violated in many practical applications such as navigation systems. Namely, the performance of the Kalman filter and consequently the related detection method depends on the accuracy of prior assumptions about the covariance matrices of the measurement and the process noises. Inexact modelling of the covariance matrices of the noises can even lead to estimation error divergence. In the adaptive filtering framework, various approaches have been developed to adjust online the measurement and process noise covariance matrices to cope with the uncertainties in the navigation sensors [11, 12].

To the best of the authors' knowledge, only Kalman filters with known constant covariance matrices are used in the existing innovation-based GNSS spoofing monitors. Different from the literature [3]-[16], in this paper, a self-tuning Kalman filter is employed in the spoofing detector, in which the covariance matrices of the noises in the system model are adapted online. The key idea is to utilize the covariance matching notion in the adaptive Kalman filter in the spoofing monitor, which is developed for a loosely coupled integrated GNSS/INS navigation system. The covariance matrices of the noise models are adjusted based on the residual and innovation sequences in a moving window. The comparative simulation results demonstrate the improvements of the proposed

detector in different scenarios over the methods based on the conventional Kalman filter. The efficiency of the proposed detection technique is evaluated in a challenging attack, where the spoofing trajectory *slowly* diverges from the true one, which is hard to detect compared to simple *jump* attacks.

The rest of the paper is arranged as follows. Section 2 describes the GNSS/INS dynamical model in the state space. Section 3 presents the novel spoofing detection scheme based on a self-tuning Kalman filter. Section 4 analyses the simulation results in the presence of ramp-type spoofing profiles; finally, Section 5 concludes the paper.

2 SYSTEM DESCRIPTION

Consider a navigation system including a GNSS receiver and an INS, equipped with an accelerometer and a gyroscope in a loosely-coupled configuration that aims at estimating the position. Using the error state of the navigation, the system's dynamics is described as follows [1], [7]:

$$\dot{x}(t) = F(t)\,x(t) + w(t) \tag{1}$$

where the state vector is defined as $x(t) = [\,\phi^T\ (\delta v^n)^T\ (\delta p)^T\ (\varepsilon^b)^T\ (\nabla^b)^T\,]^T$ in which, $\phi = [\phi_E\,, \phi_N\,, \phi_U]^T$ is the misalignment angle, $\delta v^n = [\delta v_E^n\,, \delta v_N^n\,, \delta v_U^n]^T$ is the velocity error, $\delta p = [\delta L\,, \delta\lambda\,, \delta H\,]^T$ is the position error, $\varepsilon^b = [\varepsilon_R^b\,,\ \varepsilon_F^b\ \,, \varepsilon_U^b\,]^T$ and $\nabla^b = [\nabla_R^b\,,\ \nabla_F^b\ \,, \nabla_U^b\,]^T$ are the bias vectors of gyro and accelerometer, respectively. The superscripts n and b represent navigation and body frames, respectively; the subscripts *N*, *E*, and *U* symbolize the north, east, and up in the navigation coordinate. The subscripts, *F*, *R*, and *U* denote the forward, right, and up in the body coordinate. $w(t)$ is the process noise, which is a zero-mean Gaussian vector with covariance matrix $Q(t)$. The system matrix, $F(t)$ is as follows

$$F(t) = \begin{bmatrix} F_{11} & F_{12} & F_{13} & -C_b^n & 0_3 \\ F_{21} & F_{22} & F_{23} & 0_3 & C_b^n \\ 0_3 & F_{32} & F_{33} & 0_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & 0_3 & 0_3 \\ 0_3 & 0_3 & 0_3 & 0_3 & 0_3 \end{bmatrix} \tag{2}$$

where in, 0_3 is a 3×3 zero matrix, C_b^n represents the matrix of body frame to navigation frame rotation; F_{ij} s are 3×3 matrices given in the Appendix. The observation, which is the difference between the INS and GNSS position values, is represented by p_{INS} and p_{GNSS}, is modeled as follows:

$$z(t) = p_{INS} - p_{GNSS} = H\,x(t) + v(t) \tag{3}$$

wherein, $v(t)$ represents the GNSS position noise, which is a zero-mean Gaussian vector with covariance matrix $R(t)$, and $H = [\,0_3\ 0_3\ I_3\ 0_3\ 0_3\,]$ is the observation matrix defined, in which I_3 denotes the 3-by-3 identity matrix. It is assumed that the process noise, $w(t)$, and the measurement noise, $v(t)$ are not correlated. An attacker sends a spoofing signal to the GNSS receiver to produce a false position. The spoofing value, α is considered in the measurement model as $p_{GNSS} + \alpha$.

It is worth noting that the variations applied by a typical spoofing attack do not significantly influence the calculation of the state matrix F. For example, if a 5 km error is induced in each of the position components, the maximum variation of each entry of F is about 2%.

The problem of interest is to develop a monitoring technique to detect the spoofing attack at the GNSS, as soon as possible, by employing the innovations of the Kalman filter, despite uncertainties in the noises' parameters *Q* and *R*.

3 KALMAN FILTER-BASED SPOOFING DETECTOR

Generally, change detection algorithms are composed of two successive stages: First, the generation of artificial measurements as sufficient statistics; Second, decision-making based on these signals to announce a detection alarm. The main criterion in these monitors is the delay for detection, which reflects the ability of the detector to set an alarm as soon as a change occurs. In what follows, a novel detector that utilizes the innovation vector of a self-tuning Kalman filter, together with a chi-square test, is developed to reduce the detection delay compared to the conventional Kalman filter, which is commonly used in literature.

1-3 Conventional Kalman Filter

By discretizing (1) and (3), the system equations that are used by the Kalman filter algorithm are obtained as follows:

$$\begin{aligned} x_k &= \Phi_k\,x_{k-1} + w_{k-1} \\ z_k &= H\,x_k + v_k \end{aligned} \tag{4}$$

The Kalman filter involves time update (prediction) and measurement update (estimation) as follows [13]

Time update (prediction):

$$\hat{x}_{k|k-1} = \Phi_k\,\hat{x}_{k-1} \tag{5}$$

$$P_{k|k-1} = \Phi_{k-1}\, P_{k-1}\, \Phi_{k-1}^{T} + Q$$

Measurement update (estimation):

$$\begin{aligned} K_k &= P_{k|k-1}\, H_k^T (H P_{k|k-1} H^T + R)^{-1} \\ \hat{x}_k &= \hat{x}_{k|k-1} + K_k (z_k - H \quad \hat{x}_{k|k-1}) \\ P_k &= (I - K_k\, H \quad)\, P_{k|k-1} \end{aligned} \tag{6}$$

where " ^ " is the symbol for the estimated state; P is the error covariance matrix of the estimation; and K is the filter gain. The innovation of the Kalman filter at time k is as follows:

$$\gamma_k = z_k - H\, \hat{x}_{k|k-1} \tag{7}$$

whose statistical distribution is normal with zero mean. The innovation sequence, which is the difference between the observation, z_k received by the filter, and its predicted value is employed to construct test statistics for the detection process.

2-3 Self-tuning Kalman Filter

The accuracy of prior assumptions about the covariance matrices of the process and measurement noises, Q and R are important factors that determine the performance of the Kalman filter. In the innovation-based adaptive estimation techniques, the mentioned statistics of the noise signals are adjusted during filtering, because the innovation sequence is white when these parameters are correct. In the employed self-tuning Kalman filter, the stochastic parameters of the noises are estimated online by the covariance matching approach, which makes the elements of the obtained covariance matrices consistent with their theoretical values.

Inspired by [11], in this approach, the matrix R is updated as:

$$R_k = C_v + H\, P_k H^T \tag{8}$$

where, C_v is calculated by averaging within a moving window of size w as follows:

$$C_v = \frac{1}{w} \sum_{i=0}^{w-1} v_{k-i}\; {v_{k-i}}^T \tag{9}$$

in which, v_k denotes the residual sequence that is the difference between the real observation, z_k received by the filter and its estimated value, computed as follows:

$$v_k = z_k - H\, \hat{x}_k \tag{10}$$

It is worth noting that the estimation obtained for R in (8) based on the residual sequence is guaranteed to be positive definite.

For the known R_k and $P_{k|k-1}$, matrix Q is scaled based on the ratio between the predicted and the estimated innovation covariance as follows:

$$Q_k = Q_{k-1}\sqrt{\alpha} \tag{11}$$

with,

$$\alpha = \frac{trace\{C_\gamma - R_k\}}{trace\left\{ H P_{k/k-1} H^T \right\}} \tag{12}$$

in which,

$$C_\gamma = \frac{1}{w} \sum_{i=0}^{w-1} \gamma_{k-i}\; {\gamma_{k-i}}^T \tag{13}$$

with γ_k defined in (7). The noise parameters R and Q in the Kalman filter relations (5) and (6) are replaced by R_k and Q_k in (8) and (11).

3-3 Chi-squared Test

Based on the statistical characteristics of the innovation, the test statistic is defined as the following:

$$\begin{aligned} q_k &= \frac{1}{N} \sum_{i=k-N-1}^{k} {\gamma_i}^T\, S_i^{-1}\; \gamma_i \\ S_i &= H P_{i|i-1} H^T + R_i \end{aligned} \tag{14}$$

which follows a chi-squared distribution with $3(N+1)$ degrees of freedom (DOF); note that 3 is the dimension of the observation vector. The spoofing is detected by a hypothesis test whose significance threshold, T_d is computed using the inverse chi-squared cumulative distribution function [6]:

$$\begin{aligned} T_d = F^{-1}[(1 - P_{PM}) \mid 3] \\ = \{\, x : F(\, x \mid 3\,) \\ = 1 - P_{PM}\, \} \end{aligned} \tag{15}$$

where PM is the required false alarm rate; and

$$F(x \mid m) = \int_0^x \frac{t^{(m-2)/2}\, e^{-t/2}}{2^{m/2}\, \Gamma(m/2)}\, dt \tag{16}$$

in which, Γ is the gamma function. If the test statistic, q_k is greater than the threshold, T_d an attack alarm is announced; otherwise, the system is in a normal situation.

Remark: The inverse innovation covariance matrix, S_i as the normalization factor in (14) plays an essential role in attack detection. In the adaptive Kalman filter, small values of S_i and its dynamic adjustment enables the detection of even relatively small spoofing. In contrast, the standard Kalman filter, being rigid with fixed noise assumptions, exhibits larger innovation magnitudes, yet the corresponding monitor responds more slowly because of large values of S_i, often delaying the identification of the attack.

4 COMPARATIVE SIMULATION

The detection performance of the introduced scheme is verified by comparing it to the detector that uses a conventional Kalman filter [19]. First, the simulation scenario is described; then, the efficiency of the suggested algorithm is discussed in terms of the time to detection criterion.

1-4 Trajectory and Measurement

The trajectories are generated based on the public database of an aircraft flight. The records contain geodetic latitude, longitude, and altitude together with velocities and accelerations with a 160 Hz sampling frequency for INS and 10 Hz for GNSS. Measurement data from INS and GNSS sensors are obtained from the mentioned trajectories, employing the models of the navigation toolbox of Matlab®. The total time of the simulation is 30 seconds, and in the interval of 20 to 25 seconds, a slowly growing spoofing attack is applied. Namely, the spoofed trajectory first coincides with the true one and then diverges gradually at time 20 up to 25 seconds.

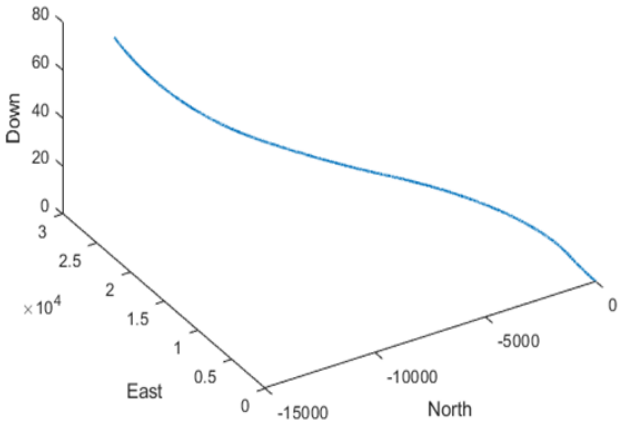

Fig. 1. Flight trajectory in East-North-Down frame.

2-4 Time to Detection

To compare the efficiency of the techniques, we use the "time to first detection" (detection latency) criterion when an attack starts. Regarding sensors' specifications, the initial values of filter parameters are chosen as follows:

$$R = diag([3.7\ m, 3.7\ m, 6\ m])^2$$

$$Q = diag([0.005\ {}^{\circ}/\sqrt{h}, 0.005\ {}^{\circ}/\sqrt{h}, 0.005\ {}^{\circ}/\sqrt{h},$$
$$20\ \mu g/\sqrt{Hz}, 20\ \mu g/\sqrt{Hz}, 20\ \mu g/\sqrt{Hz},$$
$$1\ m/\sqrt{h}, 1\ m/\sqrt{h}, 1\ m/\sqrt{h},$$
$$0, 0, 0, 0, 0, 0])^2 \times (1/160)$$

$$P_{-1} = diag([20^{\circ}, 20^{\circ}, 180^{\circ}, 0.1\ m/s, 0.1\ m/s, 0.1\ m/s,$$
$$3.7\ m, 3.7\ m, 6\ m, 0.01\ {}^{\circ}/h, 0.01\ {}^{\circ}/h, 0.01\ {}^{\circ}/h,$$
$$100\ \mu g, 100\ \mu g, 100\ \mu g] \times 3)^2$$

In the first scenario, the attacker applies a small ramp spoofing profile between 20 and 25 seconds, which leads to a 2 m/s deviation in east and north directions. Note that the flier velocity in the east is 200 m/s and in the north is 50 m/s. Figs. 2 and 3 depict the measurement vectors (position errors) and their estimations versus time. In Fig. 2, the performance of the standard Kalman filter is comparatively limited. The filter's response to the attack is significantly poor. Its fixed noise parameters cause a lag in updating state estimates when the measurements deviate due to the injected attack. In Fig. 3, the adaptive Kalman filter demonstrates more accurate state estimation.

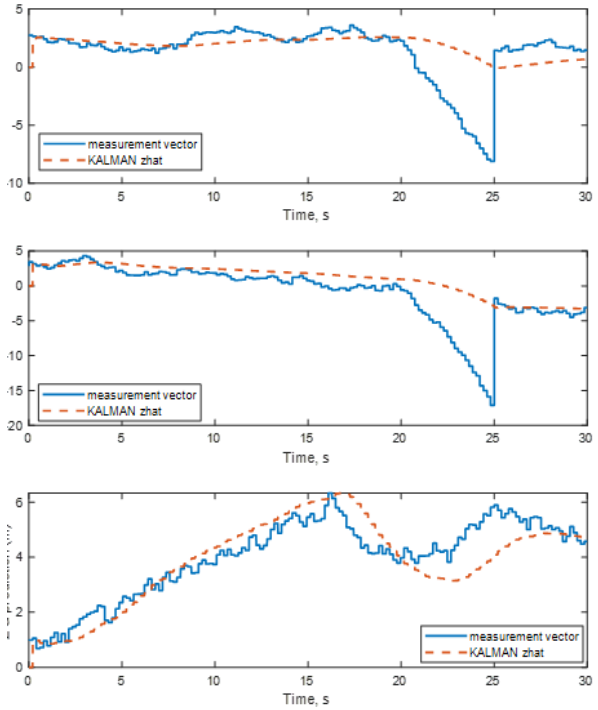

Fig. 2. Position errors and their estimations by the common Kalman filter (meters).

The detection threshold is set to 25.9 such that the false alarm probability, $P_{PM} = 10^{-5}$ is satisfied with DOF=3; then, the value of the time to first detection is computed. The test statistics of the developed and rival methods are shown in Figs. 4 and 5. The red lines represent the detection threshold. Since the innovation of the self-tuning Kalman filter and its corresponding error covariance matrix is more sensitive to measurement changes, the value of q_k is affected faster and further compared to the standard Kalman filter, as shown in Figs. 4 and 5. So, regarding our criteria for evaluation of detector performance, i.e., detection latency, the proposed method is more efficient compared to the one that uses a standard Kalman filter with constant noise parameters.

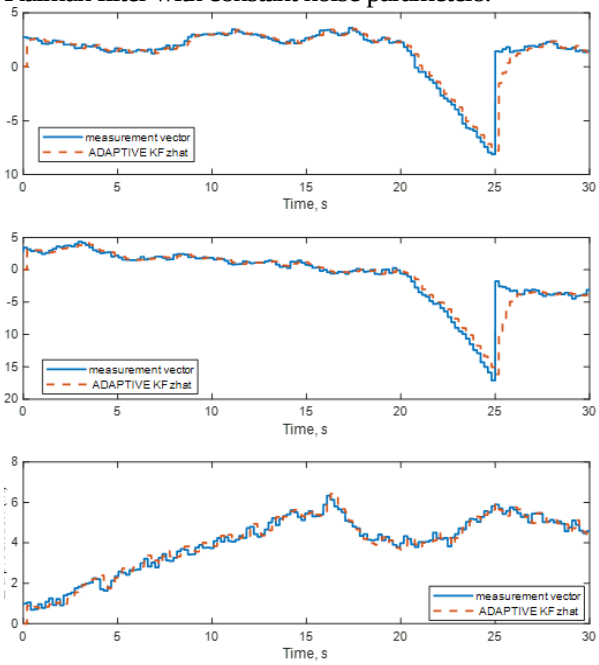

Fig. 3. Position errors and their estimations by the adaptive Kalman filter (meters).

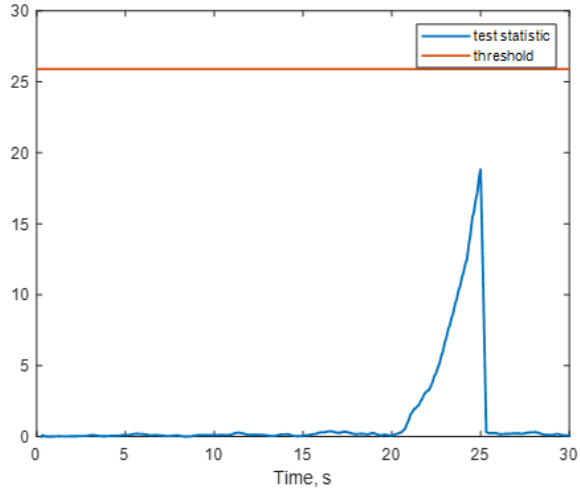

Fig. 4. Test statistics arising from the common Kalman filter and the threshold

Overall, the results demonstrate that while both filters are capable of estimating system states under nominal conditions, the adaptive filter outperforms the standard one in scenarios involving malicious changes. Note that although γ_i is small in Fig. 3, but S_i is proportionally reduced as well, and the resulting ratio becomes large and leads to detection. In other words, the absolute magnitude of innovation is not a sufficient condition for detection; rather, its ratio to the error covariance is the determining factor.

Although the innovation signal in the standard Kalman filter often exhibits a larger magnitude in response to an attack, anomaly detection tends to occur later compared to the adaptive Kalman filter. This counterintuitive behavior is primarily due to the role of the innovation covariance matrix in statistical decision metrics, defined in (14). As a result, in the case of small deviations in innovation, small values of covariance (uncertainty) can lead to significantly larger q_k when the filter adapts to changes, it enables earlier and more reliable detection of an attack.

Table 1 reports the comparison results of the proposed detection scheme with the common Kalman filter in terms of detection latency for different attack scenarios. As seen, for small spoofing values, the rival method cannot recognize the attack, while the proposed method with a self-tuning filter detects the attack. Moreover, in detectable attacks by both methods, the detection latency is considerably lower with the proposed scheme.

Table 1. Time to detect different attack intensities

Ramp Amplitude (m/s)	2	3	5
Attack duration (s)	5		
Common Filter	-	3.41	1.91
Self-tuning Filter	0.35	0.22	0.11

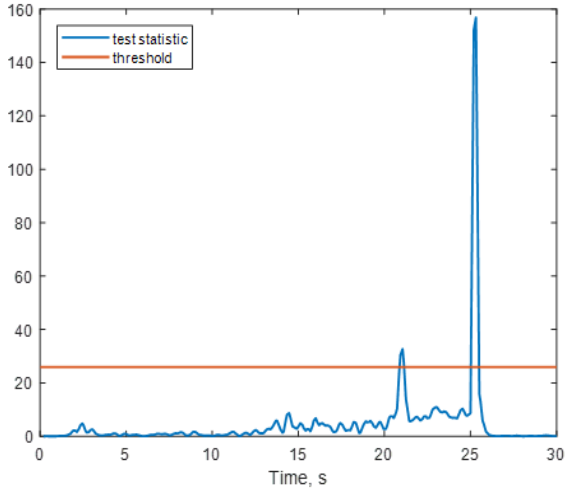

Fig. 5. Test statistics arising from the self-tuning Kalman filter and the threshold

CONCLUSION

A novel spoofing detection technique has been introduced based on a self-tuning Kalman filter. The improvement of this approach comes from the online adaptation of the noise stochastic models that are used in the estimation algorithm. The comparative simulation results showed that the proposed detector is an efficient tool for detecting spoofing attacks with higher accuracy and less detection latency than the existing rival one. Considering more details about the uncertainties in the dynamical model of the navigation system, which is employed by the filtering procedure, defines future research lines.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

REFERENCES

[1] P. D. Groves, *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*, 2nd ed., Artech House, Boston, USA, 2013.

[2] M. L. Psiaki, T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol.104, 2016, pp. 1258–1270, https://doi.org/10.1109/JPROC.2016.2526658.

[3] Z. Wu, Y. Zhang, Y. Yang, C. Liang, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," *IEEE Access*, vol. 8, issu 6, 2020, 165444–165496, https://doi.org/10.1109/ACCESS.2020.3022294.

[4] S. Khanafseh, N. Roshan, S. Langel, F. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," *Proc. IEEE/ION Position, Location Navigation Symp*., Monterey, CA, USA, May 2014, https://doi.org/10.1109/PLANS.2014.6851498.

[5] C. Tanil, S. Khanafseh, M. Joerger, B. Pervan, "Kalman Filter-based INS monitor to detect GNSS spoofers capable of tracking aircraft position," *Proc. IEEE/ION Position, Location, Navigation Symp*., Savannah, Georgia, USA, April 2016, https://doi.org 10.1109/PLANS.2016.7479805.

[6] C. Tanil, S. Khanafseh, M. Joerger, B. Pervan, "An INS monitor to detect GNSS spoofers capable of tracking vehicle position," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54 Issu 1, 2018, pp. 131–143, https://doi,org/ 10.1109/TAES.2017.2739924.

[7] Y. Liu, S. Li, Q. Fu, Z. Liu, "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system," *Sensors*, vol. 18, no. 5, 2018, pp. 131-143, https://doi.org/10.3390/s18051433.

[8] R. Xu, M. Ding, Y. Qi, S. Yue, J. Liu, "Performance analysis of GNSS/INS loosely coupled integration systems under spoofing attacks," *Sensors*, vol. 18, no. 12, 2018, Art. no. 4108, https://doi.org/10.3390/s18124108.

[9] E. Bang, C. Milner, C. Macabiau, P. Estival, "Preliminary integrity assessment for GPS/GLONASS RAIM with multiple faults," *IEEE/ION Position, Location, Navigation Symp*., Monterey, California, USA, April 2018, https://doi.org/10.1109/PLANS.2018.8373398.

[10] M.R. Manesh, J. Kenney, W.C. Hu, V.K. Devabhaktuni, N. Kaabouch, "Detection of GPS spoofing attacks on unmanned aerial systems," *16th IEEE Annu. Consum. Commun. Netw.*, Las Vegas, NV, USA, January 2019, https://doi.org/10.1109/CCNC.2019.8651804.

[11] Y. Liu, S. Li, Q. Fu, Z. Liu, Q. Zhou, "Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system," IEEE Sensors J., vol. 19, no, 13, 2019, pp. 5167-5178, https://doi.org/10.1109/JSEN.2019.2902178.

[12] W. Yimin, L. Hong, and L. Mingquan, "Spoofing profile estimation-based GNSS spoofing identification method for tightly coupled MEMS INS/GNSS integrated navigation system," *IET Radar, Sonar Navigation*, vol. 14, no. 2, 2020, pp. 216–225, https://doi.org/10.1049/iet-rsn.2019.0264.

[13] M. Ceccato, F. Formaggio, N. Laurenti, and S. Tomasin, "Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU," *IEEE Transactions on Information Forensics and Security*, vol. 16, 2021, pp. 3496- 3509, https://doi.org/10.1109/TIFS.2021.3083414.

[14] W. Liang, K. Li, Q. Li, "Anti-spoofing Kalman filter for GPS/rotational INS integration," *Measurement*, vol. 193 Art. no. 110962, 2022, https://doi.org/10.1016/j.measurement.2022.110962.

[15] L. Zhang, H. Zhao, C. Sun, L. Bai, W. Feng, "Enhanced GNSS spoofing detector via multiple-epoch inertial navigation sensor prediction in a tightly-coupled system," *IEEE Sensors J.*, vol. 22, no. 9, 2022, pp. 8633–8647, https://doi.org/10.1109/JSEN.2022.3156112.

[16] Y. Wei, H. Li, M. Lu, "A steady-state spoofing detection and exclusion method based on raw IMU measurement," *IEEE Sensors J.*, vol. 22, no. 4, 2022, 3529–3539, https://doi.org/10.1109/JSEN.2022.3143150.

[17] W. Ding, J. Wang, and C. Rizos, "Improving adaptive Kalman estimation in GPS/INS integration," *The J. of Navigation*, vol. 60, no. 3, 2007, pp. 517-529, https://doi.org/10.1017/S0373463307004316.

[18] A. Almagbile, J. Wang, W. Ding, "Evaluating the performances of adaptive Kalman filter methods in GPS/INS integration," J. *of Global Positioning Sys.* vol. 9, no. 1, 2010, 33-40, https://doi.org/10.5081/jgps.9.1.33.

[19] M.S. Grewal, A.P. Andrews, *Kalman filtering: Theory and Practice with MATLAB*, 4th ed., John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2015.

APPENDIX

The entries of matrix F in (2) are as follows:

$$F_{11} = (-(w_{ie}^n + w_{en}^n) \times)$$

$$F_{12} = \begin{bmatrix} 0 & -1/R_{Mh} & 0 \\ 1/R_{Nh} & 0 & 0 \\ \tan L / R_{Nh} & 0 & 0 \end{bmatrix}$$

$$F_{13} = \begin{bmatrix} 0 & 0 & v_N^n / {R_{Mh}}^2 \\ -w_{ie} \sin L & 0 & -v_N^n / {R_{Nh}}^2 \\ w_{ie} \cos L + v_E^n \, sec^2 L / R_{Nh} & 0 & -v_E^n \tan L / {R_{Nh}}^2 \end{bmatrix}$$

$$F_{21} = ((C_b^n f^b) \times)$$

$$F_{22} = (v^n \times) F_{12} - \left((2w_{ie}^n + w_{en}^n) \times\right)$$

$$F_{23} = (v^n \times)$$

$$\begin{bmatrix} 0 & 0 & v_N^n / {R_{Mh}}^2 \\ -2w_{ie} \sin L & 0 & -v_E^n / {R_{Nh}}^2 \\ 2w_{ie} \cos L + v_E^n \, sec^2 L / R_{Nh} & 0 & -v_E^n \tan L / {R_{Nh}}^2 \end{bmatrix}$$

$$F_{32} = \begin{bmatrix} 0 & 1/R_{Mh} & 0 \\ \sec L / R_{Nh} & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$F_{33} = (v^n \times)$$

$$\begin{bmatrix} 0 & 0 & -v_N^n / {R_{Mh}}^2 \\ v_E^n \sec L \tan L / R_{Nh} & 0 & -v_E^n \sec L / {R_{Nh}}^2 \\ 0 & 0 & 0 \end{bmatrix}$$

where $(vec) \times$ stands for the skew-symmetric matrix of the vector vec. R_{Nh} and R_{Mh} denote the transverse and meridian radii of the curvature plus the height. L is the latitude. $v^n = [v_E^n, v_N^n, v_U^n]^T$ represents the velocity vector in the navigation coordinate. $f^b = [f_R^b \; f_F^b \; f_U^b]^T$ denotes the vector of the specific force in the body coordinate. w_{ie} is the constant Earth rotation rate. $w_{ie}^n = [0 \; w_{ie} \cos L \; w_{ie} \sin L]^T$ is the vector of the Earth's rotation, fixed in the local navigation coordinate. $w_{en}^n = [-v_N^n / R_{Mh} \; v_E^n / R_{Nh} \; v_E^n \tan L / R_{Nh}]^T$ is the rotation of the navigation coordinate regarding the earth-fixed and -centered coordinate represented in the local navigation coordinate.

HOW TO CITE THIS ATRICLE

M. Shadmehri and R. Mahboobi Esfanjani, "Spoofing Attack Detection in Integrated GNSS/INS Navigation System Using Self-tuning Kalman Filter," *Journal of Aerospace Science and Technology*, Vol. 18, Issue 2, 2025, pp. 17-24.

DOI: https://doi.org/10.22034/jast.2025.467877.1199

URL: https://jast.ias.ir/article_224357.html