Turkish Journal of Electrical Engineering and Computer Sciences

Volume 25 | Number 4 Article 60

1-1-2017

Optimal fusion of multiple GNSS signals against spoofing sources

SELÇUK ŞAHİN

ABEDALLATIF BABA

TOLGA SÖNMEZ

Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2017) 25: 3289 – 3299

doi:10.3906/elk-1604-123

Optimal fusion of multiple GNSS signals against spoofing sources

Selçuk ŞAHİN[1], **Abdellatif BABA**[2,*], **Tolga SÖNMEZ**[1]
[1]Department of Command, Control, and Combat Systems, HAVELSAN, Ankara, Turkey
[2]Department of Mechatronics Engineering, Turkish Aeronautical Association University, Ankara, Turkey

Received: 10.04.2016 • **Accepted/Published Online:** 30.12.2016 • **Final Version:** 30.07.2017

Abstract: Electronic attacks such as spoofing are becoming an increasing threat for satellite-based navigation receivers. The aim of this paper is to develop a preventive method against such electronic attacks. In our scheme, the localization system uses four different Global Navigation Satellite Systems (GNSSs): GPS, Galileo, GLONASS, and Compass. The signals received from these satellite systems will be fused inferentially and will be tracked according to a linear model. The linear model that we developed is solved with a Kalman filter and simulated under different scenarios. When a discrepancy is detected in the output of one of the GNSS receivers due to spoofing, it is excluded from the fusion.

Key words: Spoofing signals, asymmetric threat, jamming signal, navigation systems

1. Introduction

For many years, the function of Global Navigation Satellite Systems (GNSSs) has been considered trustworthy and continuously available. However, jamming and spoofing have recently become a concern for military systems. Jamming is the intentional interference targeting the unavailability of the system, and spoofing is transmitting a false position/time towards a target GNSS receiver [1]. Many studies have recently been conducted in this domain. In [2], the authors proposed a detection and protection scheme consisting of several statistical tests based on the computations of moving variances of Doppler offset and SNR estimates, together with a consistency test of the position, velocity, and time computation. They evaluated the performance of the proposed scheme through simulations and used a measurement setup consisting of a Spirent GSS8000 full constellation simulator whose output is combined with that from a rooftop GPS antenna before being fed to a receiver front-end.

In general, spoofers have a major limitation. They must have several correlated GNSS satellite signals in order to transmit and present a seemingly true navigation solution to the receiver. However, different GNSS satellite signals coming from a single transmitter essentially have the same spatial tag, which can be utilized to discriminate spoofing signals as in [3], where the authors used an antenna array to nullify the signals coming from a jammer or a spoofer source. This method requires a highly specialized antenna array and embedded processing. In [4], the authors focused on a robust and precise car navigation system, which can also be used in GNSS-denied or spoofed environments. The system is based and designed for so-called on-board units, which are already used for professional road toll and tracking applications. The system combines the GNSS and dead-reckoning trajectories based on odometry and inertial navigation. Using other sensors also helps to detect spoofing signal presence.

In this paper, four GNSSs are used to simulate these attacks. These systems are the American Global

*Correspondence: baba@thk.edu.tr

Positioning System (GPS), Galileo, the Russian Global Navigation Satellite System (GLONASS), and Compass. The signals processed by these systems will be modeled with a Kalman filter and will be simulated with the help of MATLAB. Finally, three different scenarios will be provided to prove the proficiency of our approach by showing that the spoofing attack signals will be determined and stopped by the system. All of the simulations and the fusion filter and spoofer detection methods developed in this paper are original work. Although there has been much research on antispoofing based on signal powers and multiple antennae, fault detection and isolation-type fusion filters are used here for the first time in GNSS antispoofing systems according to the authors' best knowledge.

2. Global Navigation Satellite Systems

GNSSs have become the base for any advanced autonomous navigational system in different domains (e.g., aviation, automotive, marine, space, agriculture, and military). GNSSs have generally been defined as time and position detection systems that include a set of satellites for triangulation. The most prevalent GNSS systems are GPS and GLONASS. The other infrequently used systems are the Chinese Compass and the European Galileo [5]

- GPS enables users to obtain information such as location, speed, and time at any place and time in all weather conditions by using 31 satellites moving around the earth at an altitude of about 20,000 km at a speed of 3.9 km/s. GPS satellites spin around the world two times per day. Each satellite transmits radio waves towards the earth to provide information on position and time. The frequency bands actively used by the GPS system are as follows: L1: 1575.42 MHz, L2: 1227.60 MHz, L3: 1381.05 MHz, L4 1379.913 MHz, L5: 1176.45 MHz.

- In the GLONASS GNSS, there are 24 usable satellites. These satellites use a frequency division multiple access (FDMA) working system.

- The usage of the GPS and GLONASS systems for military purposes influenced the European Union to set up a new navigation system. The Galileo system was started to serve civilian usage in European Union countries under the leadership of Germany, with the contributions of France, the United Kingdom, and Italy. This system, planned as 24 satellites in service and 6 active spares, totaling 30 satellites, will be fully operational by the end of 2019. The working principle of the Galileo system is similar to the GPS system, but the signal frequency is different.

- The Beidou-2 GNSS system, which is called Compass, is going to be an operational GNSS system consisting of 35 satellites by 2020. The Compass system uses code division multiple access (CDMA) working principles like GPS and Galileo.

GPS, Galileo, and Compass work with CDMA, but GLONASS works with FDMA.

CDMA is a transmission technology that uses the spread-spectrum technique. It forms distinct channels by giving a different code to each different satellite. While FDMA has 15 channels between 1602.5625 MHz and 1615.5 MHz, each one is conveyed at a different frequency. All satellites share the same satellite frequency band simultaneously but each one transmits at a single frequency channel in an instant.

3. Multi-GNSS

A multi-GNSS receiver is able to calculate position, velocity, and time by receiving satellite signals broadcasted from multiple navigation satellite systems. CDMA is used today for digital communication in GPS receivers. However, interoperability and compatibility have been important issues for the design of Galileo and Compass and the regeneration of the GLONASS system. If interoperable and compatible signals can be synergistically used in navigation systems, it would be beneficial to use this additional information. Consequently, we conduct this study to illustrate the benefits of such a multi-GNSS receiver in an interference environment. We will concentrate on civil signals in our study. GPS is beginning to introduce three new civil signals, namely L1C, L2C, and L5. The Galileo signals on E1, E6, and E5 will also be open signals. Compass will have only two open signals, which are similar to the Galileo system. Similarly, GLONASS also introduces two new CDMA signals on L1 and L5. We will create some scenarios and simulate and compare the results of analyses for multi-GNSS receivers [6,7].

3.1. Modeling multi-GNSS with a Kalman filter

In our study, four GNSS systems were used, but we can generalize the framework to include more than four GNSS systems. As we have already explained, our aim is to filter out the signals of deception and interference from outside to guarantee the normal operation of position detection. Therefore, as illustrated in Figure 1, we will obtain a filtered output signal while the four GNSS channels are feeding the model.

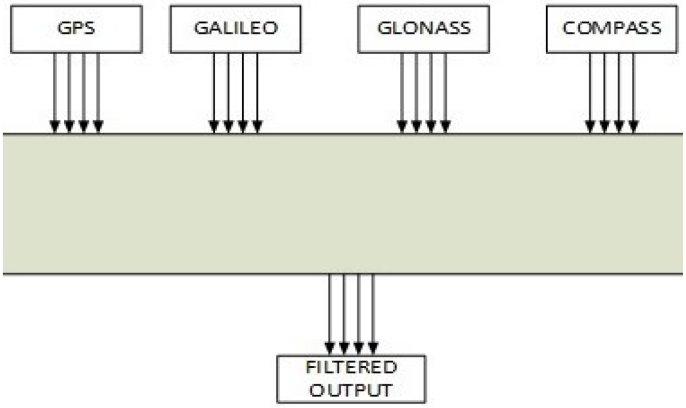

Figure 1. The fusion of multi-GNSS receivers with a Kalman filter.

However, the created system is linear, and the value of the output depends on each given input. A Kalman filter is a good tool for sensor fusion, where we can blend and compare measurements coming from different types of sensors. A Kalman filter is optimal for such linear systems [8,9]. In general, at each separate receiver, nonlinear filters work to form the position solution, but we are treating them as separate sources of measurement. In general, this would not be a problem because these filters, positioned at the receivers, are very robust [5]. The performance of our filter depends on interference from other sources and measurement errors in the model.

In the created model, two types of noise must be considered. These are Q (process noise) and R (measurement noise).

First, the classical equations used in Kalman filtering should be noted:

$$X_{k=}AX_{k-1} + BU_K + W_{k-1}, \tag{1}$$

$$Z_k = HX_k + V_k, \tag{2}$$

$$P_k^- = AP_{k-1}A^T + Q, \tag{3}$$

$$K_k = P_k^- H^T (HP_k^- H^T + R)^{-1}, \tag{4}$$

$$\hat{X}_k = \hat{X}_k^- + K_k(Z_k - H\hat{X}_k^-), \tag{5}$$

$$P_k = (I - K_k H)P_k^-, \tag{6}$$

where X_k is an $[n \times 1]$ state vector, Z_k is an $[i \times 1]$ measurement vector, U_K is an $[r \times 1]$ deterministic input vector, A is an $[n \times r]$ time-varying input coupling matrix, H is a $[t \times n]$ time-varying measurement sensitivity matrix, B is an $[i \times r]$ time-varying output coupling matrix, W_k is an $[r \times 1]$ zero-mean uncorrelated "plant noise" process, V_k is an $[i \times 1]$ zero-mean uncorrelated "measurement noise" process, P_k is a covariance matrix, K_k is the Kalman gain, R is measurement noise covariance, Q is process noise covariance, $\hat{X}_k$ is the estimate state vector, and I is the identity matrix.

As we do not have any control signal U_K, we have accepted this value as zero.

To create the measurement matrix H, the relation between the real positions, bias values of the satellite, and measurement errors are required. The generally needed structure to create matrix H is shown in Eq. (7):

$$\begin{bmatrix} x_{GNSS} \\ y_{GNSS} \\ z_{GNSS} \\ t_{GNSS} \end{bmatrix} = \begin{bmatrix} x + x_{BiasGNSS} \\ y + y_{BiasGNSS} \\ z + z_{BiasGNSS} \\ t + t_{BiasGNSS} \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix}. \tag{7}$$

Accordingly, the created model is explained below [8–10].

x, y, z, and t are the real position and time values of the GNSS receiver. However, $x_{BiasGNSS}$, $y_{BiasGNSS}$, $z_{BiasGNSS}$, and $t_{BiasGNSS}$ are the bias-type errors specific to the respective constellation, which are composed of the position and time differences. When satellites send their own position-related information, deviation in the signal speed, even in a very small amount, occurs due to atmospheric conditions and relative movement of the earth and satellites. Each transmitted signal will then have some small differences. In this case, it will be required to calculate the accuracy of the signal by considering these errors. v_1, v_2, v_3, and v_4 are the measurement noise variables [9,10].

The measurement matrix H is considered in our model as a matrix of size 4×20. The matrix considered for each GNSS is shown in the Table.

In our model, the state transition matrix is defined as an identity matrix of size 20×20 because the system has low dynamics. Finally, it is required to define the state vector X_k, formed as a 20×1 vector. It is illustrated as:

$$X_k = [x\ y\ z\ t\ x_1\ y_1\ z_1\ t_1\ x_2\ y_2\ z_2\ t_2\ x_3\ y_3\ z_3\ t_3\ x_4\ y_4\ z_4\ t_4]^T, \tag{8}$$

where:

$$[x_1\ y_1\ z_1\ t_1] = [x_{BiasGPS}\ y_{BiasGPS}\ z_{BiasGPS}\ t_{BiasGPS}],$$

$$[x_2\ y_2\ z_2\ t_2] = [x_{BiasGLONASS}\ y_{BiasGLONASS}\ z_{BiasGLONASS}\ t_{BiasGLONASS}]$$

Table. The measurement matrix: one matrix for each GNSS.

$H_{GPS}=$	$\begin{pmatrix} 1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \end{pmatrix}$
$H_{GLONASS}=$	$\begin{pmatrix} 1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \end{pmatrix}$
$H_{GALİLEO}=$	$\begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \end{pmatrix}$
$H_{COMPASS}=$	$\begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \end{pmatrix}$

$$[x_3\ y_3\ z_3\ t_3] = [x_{BiasGALILEO}\, y_{BiasGALILEO}\, z_{BiasGALILEO}\, t_{BiasGALILEO}]$$

$$[x_4\ y_4\ z_4\ t_4] = [x_{BiasCOMPASS}\, y_{BiasCOMPASS}\, z_{BiasCOMPASS}\, t_{BiasGOMPASS}].$$

The position values of the receiver (x,y,z) are supposed to be constant in this model. The position output of each GNSS system has some deviations from the true position due to inaccuracies in each satellite system. These deviations are defined as bias values. All the required inputs for the model are given in the Table. Finally, we assume that noise variances of the initial state estimates are small at the beginning of our scenario.

The designed Kalman filter has the capability to track the uncertainty levels of each state variable and their dependency on each other. Using these uncertainty levels and the measurements, it will be possible to detect abnormalities such as spoofing signals.

3.2. Simulation of our model using MATLAB

To analyze the efficiency of our algorithm, we have developed a simulation model. In this simulation model, we are able to create spoofing signals and true signals under different scenarios. As an imaginary spoofing signal, we have selected GPS. We have to note that any other GNSS could also be selected. According to this scheme, three different responses have been analyzed with three different scenarios in MATLAB, and then the outputs were evaluated. These three responses are:

- Normal condition
- Glitch without reject condition
- Glitch and reject condition

As expressed previously, the aim of this study is to show that our system has electronic protection against spoofing signals. To evaluate our approach, in this simulation we are trying to affect the system by deceiving the values of position and time. The actual case here is to disturb the position time accuracy to prevent the

normal operation of the positioning system. To deceive the system, the value of the glitch as a spoofing tool was randomly selected to be 300 m. It should be noted that any other significantly large value could also be selected. Four aspects of the filter were then analyzed in each scenario. These are:

- Measurement values of the GNSS
- All GNSS bias estimation errors
- Covariance matrix
- Error values according to the real x, y, z, and t (time) position of the receiver

3.2.1. The working strategy of the scenarios

- A dynamic model is developed and initialized for the fusion of multi-GNSS systems. Kalman filter equations are initialized.
- Position and time measurements from multi-GNSS receivers are collected.
- The state estimation due to measurement is calculated. If there is too much discrepancy between the a priori and the a posteriori estimation value with respect to its covariance, the measurement is rejected.
- Accepted measurements are used to update state estimates according to Kalman filter equations and covariance matrix.

3.2.1.1. Scenario 1 (normal condition)

In this case, we suppose all measurements from GNSS receivers are compatible with each other as in a normal operation without any attack or deception. The measurement state values of the GNSS are shown in Figure 2. We can observe four measurements of the system and they are constant, describing nearly the same information and working without any signal interference or deception. At this point, the system shows all the measurements from receivers without filtering or rejection by our Kalman filter. If the measurement values are in normal condition, all GNSS bias estimate error values are also normal. The errors of the x bias position of the GNSS are shown in Figure 3. In this case, although the errors of the GNSS are high due to uncertainty at the first occurrence time, the error rate decreases with time and converges toward values around zero.

Without any spoofing attack on the system, the range of error measurements is in accordance with the covariance matrix, and the filter appears to regulate the system's errors. Therefore, according to the analysis in Figure 4, the Kalman filter algorithm has been successfully executed as a prediction method. The covariance matrix, which is used to verify the errors of GNSS bias prediction, is shown in Figure 4. This matrix shows the amount of error in the state estimations according to the received measurements. As can be seen, the error covariance curves are bounded and convergent.

The errors of the filter output in terms of the x, y, and z positions and t (time) are shown in Figure 5 for normal condition. The range of x, y, and z receiver position error is between –0.4 m and 0.4 m, and this is an acceptable range. The time error is very small (this is because the receiver is considered as moving slowly). Therefore, the time error, as illustrated in Figure 5, follows a value close to zero in the range of 20 ns.

To calculate this, we use the following equation:

$$t^{'} = t_{SatellitClock} - t_{ReceiverClock}, \tag{9}$$

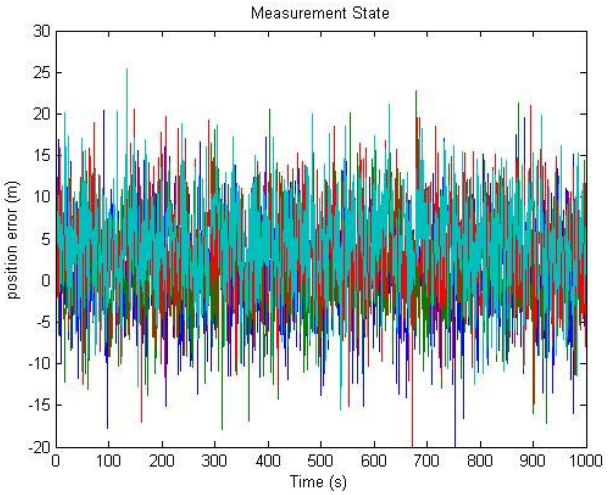

Figure 2. GNSS measurement state.

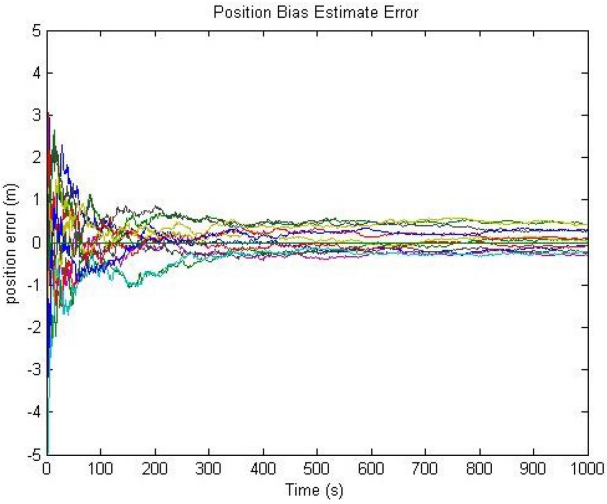

Figure 3. All GNSS bias estimate errors.

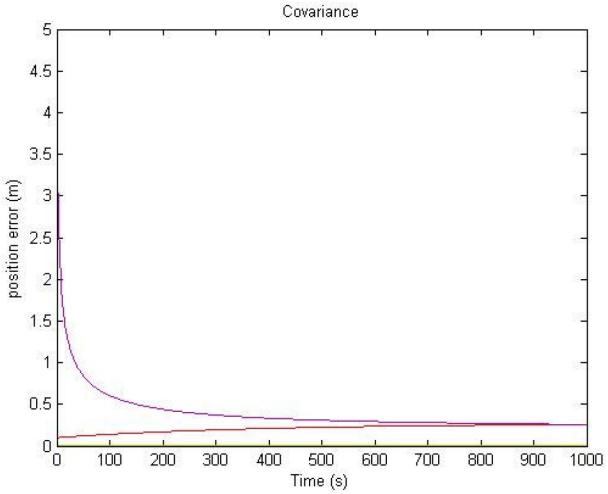

Figure 4. Covariance matrix (covariance values for the 20 variables in the state vector). All GNSS bias estimate errors are depicted with purple lines while the receiver estimate error is represented by a red line.

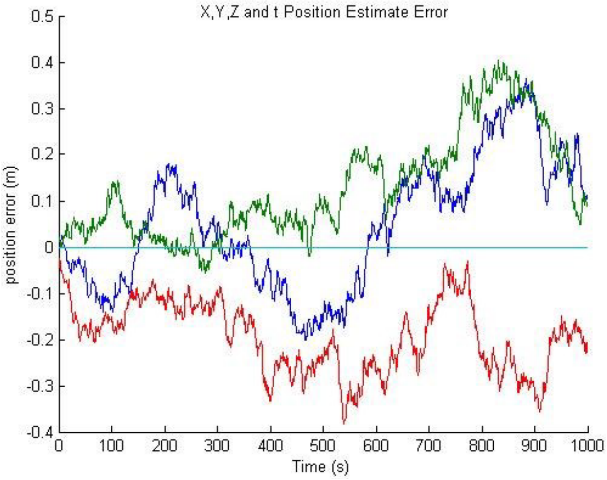

Figure 5. Receiver estimate errors on x (blue), y (red), z (green), and time (cyan) curves, respectively.

where $t^{'}$ is the time error, $t_{SatellitClock}$ is the time of the satellite atomic clock, and $t_{ReceiverClock}$ is the time of the receiver clock.

3.2.1.2. Scenario 2 (glitch and without reject condition)

The purpose of this scenario is to spoof the GPS by sending a deception signal to the system. However, we can suppose that the system does not check the consistency of separate fusion filter inputs and directly uses all of the measurements it is fed. As shown in Figure 6, the system creates incorrect measurements; it is shown as an x-axis position error on the receiver. In this case, while the other GNSS output measurements stay the same, the distorted GPS signal has a deviation of 300 m. These measurements are the actual outputs of several GNSS receivers, so no correction is done at this stage. At the beginning of the illustrated curve in Figure 7, the GNSS bias estimation error remains zero for a while before applying the error to the GPS signal. It then

increases to 300 m according to the spoofing signal. The fusion filter produces a slow response to the spoofing signal and slowly increases the GPS x coordinate bias to 300 m because the uncertainty about the x-axis bias was 10 m in the beginning. When the covariance matrix is examined in Figure 8, it can be seen that the perceived covariance matrix in this situation is normal since it does not depend on data but only the model. As the spoofing signal is not compatible with the dynamic model, system errors and the covariance matrix are dissimilar. As no measurement is rejected, we see the effect of spoofing in the estimation errors in Figure 9 (the graph of x, y, and z and t receiver estimate error). As can be seen, the 300-m deviation in the GPS x-coordinate also affects the filter x-position state. Although it is not as high as in the spoofer signal, it still degrades the performance of the fusion filter. The lessened effect of the spoofer is due to the compensation of the x-coordinate with the help of the other GNSS constellations.

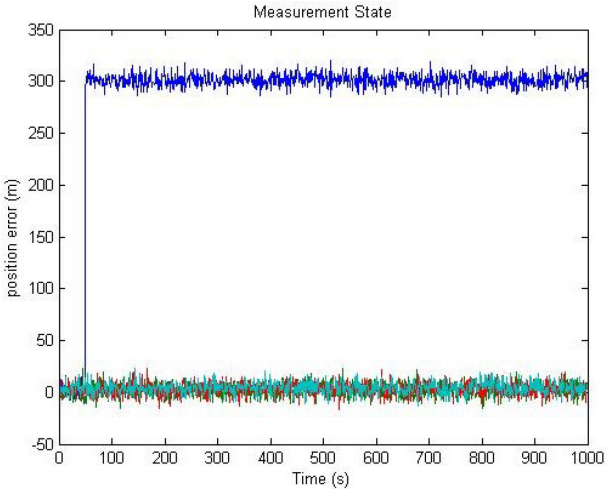

Figure 6. GNSS measurement state.

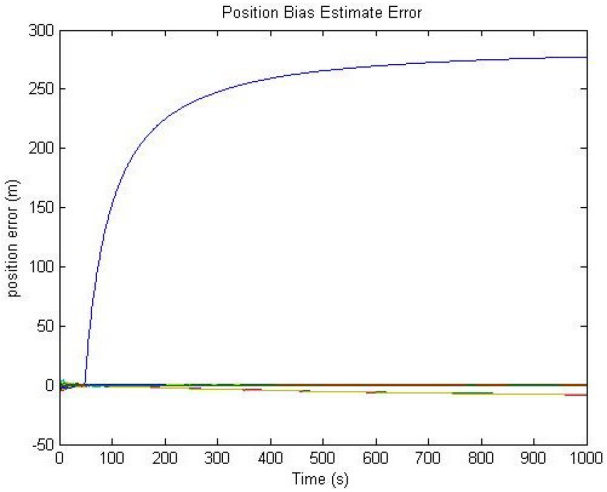

Figure 7. All GNSS bias estimate errors.

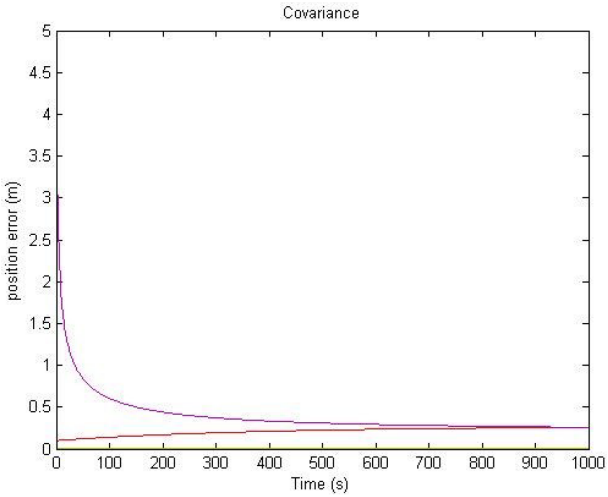

Figure 8. Covariance matrix (covariance values for the 20 variables in the state vector).

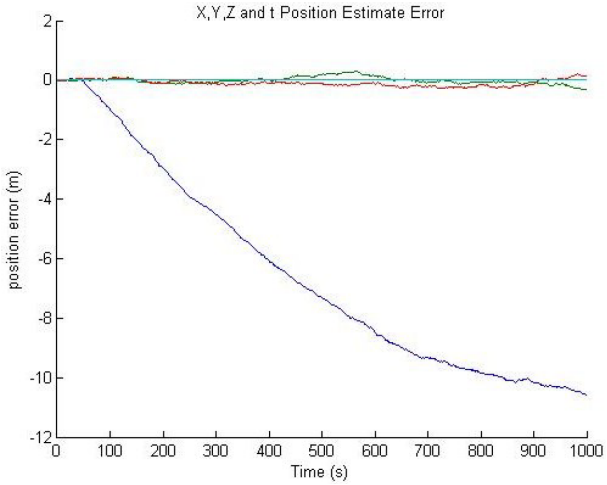

Figure 9. Fusion-filter estimation errors on x (blue), y (red), z (green), and time (cyan) curves, respectively.

3.2.1.3. Scenario 3 (glitch and reject condition)

In this section, in accordance with the created scenario, we illustrate how to detect the spoofing signal with the system and how to keep it out in the fusion process. It can be examined in Figure 10 that measurements remain the same compared to the last scenario where the GPS receiver output has the same 300-m deviation in the x-coordinate. As shown in Figure 11, the faulty data, which have been injected into the system, are noticed by the system and prevented. As a result, GPS position data, which were given as an intentional error, are hindered and rejected by the system. According to the same figure, the received GPS signal was accurate in the first stage when there was no spoofing. It could be also noted that the system has kept its accuracy during the spoofing stage, and the spoofing signal was rejected according to the criterion given in [10]. This criterion basically compares the value of innovation and innovation covariance. If it is larger than 3 σ, it means that this measurement is abnormal with a probability of 99.7% for a normal distribution. In other words, this measurement is most probably coming from a spoofing signal and should be rejected.

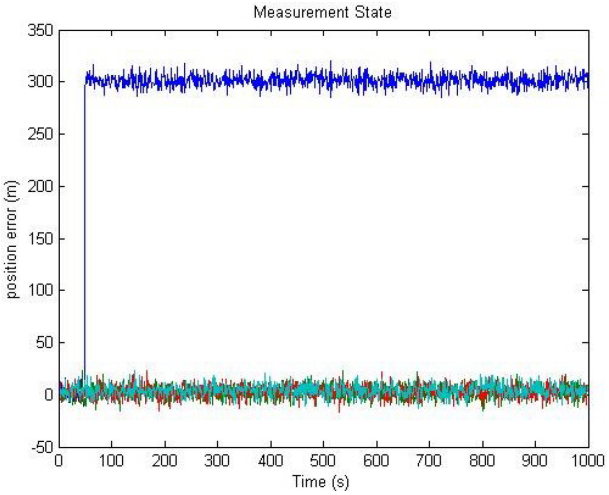

Figure 10. GNSS measurement state: the blue track is the x-position from the spoofed GPS signal; the other position measurements are approximately the same.

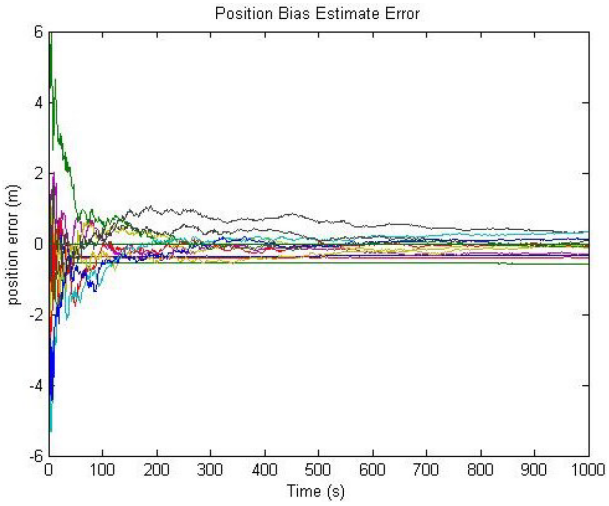

Figure 11. All GNSS bias estimate errors (estimation errors of the last 16 variables in the state vector).

$$\gamma := (Z_k - H_{gps}\hat{X}_k^-)/sqrt(H_{gps}P_k^- H_{gps}^T + R) > 3 \tag{10}$$

When we examine Figure 8, we may mention that the covariance matrix remains the same as the spoofing signal was not detected. However, in this case, the spoofing has been detected and the GPS signal is rejected; therefore, the other GNSS covariance values stay the same as illustrated in Figure 12 with the purple line. According to Figure 12, after rejecting the error signal, the covariance value for the GPS bias states does not decrease, and we do not use any GPS information during the spoofing. In Figure 13, after recognizing the spoofing signal, the changes of GPS receiver inputs are filtered by the system, and they are not included in the calculation of the receiver position. This shows that our system is working correctly by continuously filtering the spoofer.

4. Conclusion

GNSSs were explained in the first part of this paper. The working principle of these systems was also briefly explained. The required analyses and the overall maps of the systems were illustrated. Four GNSSs were

handled. A Kalman filter was used as a statistical estimation algorithm for the developed model. The model built was simulated by using MATLAB, in which three different scenarios were prepared to clarify the aim of this study and to prove the efficiency of our approach. However, as it is illegal to broadcast spoofing signals, we modeled these signals in this study, and we simulated the performance of the filter. We would like to later conduct these tests with GNSS simulators and RF signals in a realistic environment. The high dynamics of the platform on which the receiver is placed could also degrade the effects of the performance of our filter. In the future, we would like to try more complex test scenarios using real RF signals and high dynamic platforms.

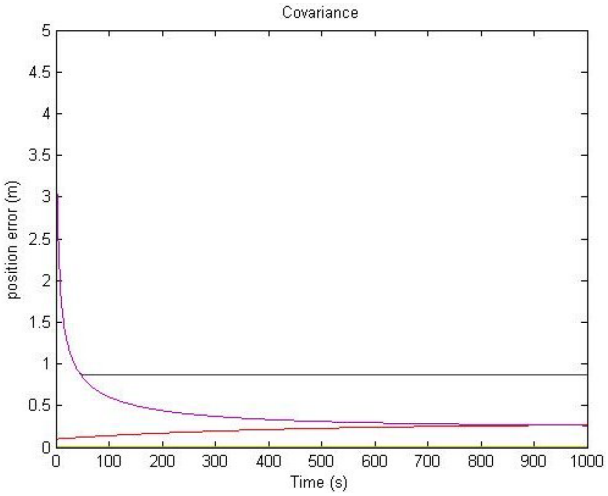

Figure 12. Covariance matrix (covariance values for the 20 variables of the state vector).

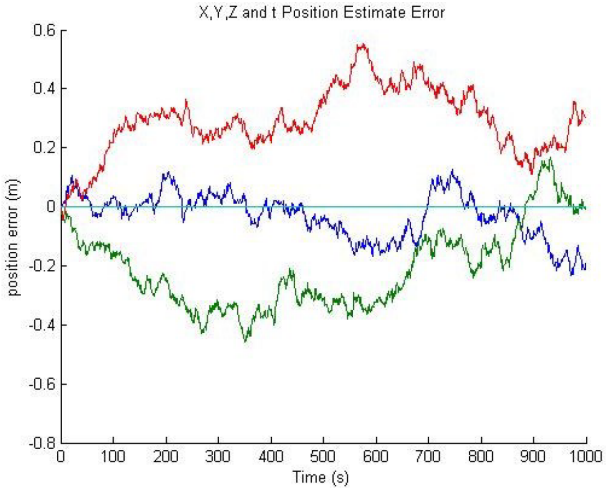

Figure 13. Receiver estimate errors on x (blue), y (red), z (green), and time (cyan) curves, respectively.

Acknowledgment

We would like to thank HAVELSAN for the valuable support during this study.

References

[1] Rügamer A, Kowalewski D. Jamming and spoofing of GNSS signals - an underestimated risk?! In: German Microwave Conference; 16–18 March 2015; Nuremberg, Germany. Pp. 38-39.

[2] Jovanovic A, Botteron C, Fariné PA. Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers. In: Position, Location and Navigation Symposium; 5–8 May 2014; Monterey, CA, USA. New York, NY, USA: IEEE. pp. 1258-1271.

[3] Broumandan A, Jafarnia-Jahromi A, Dehgahanian V, Nielsen J, Lachapelle G. GNSS spoofing detection in handheld receivers based on signal spatial correlation. In: Position, Location and Navigation Symposium; 23–26 April 2012; Myrtle Beach, SC, USA. New York, NY, USA: IEEE. pp. 479-487.

[4] Franzoni G, Marradi L, Scaciga L, Crosta P, Rovelli D, Fantinato S, Pessina I, Ramaioli P, Iacone P, Libertone M. Multi-constellation, multi-frequency, multi-signal reference station receiver for GPS/Galileo/Giove. In: 6th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing; 5–7 December 2012; Noordwijk, the Netherlands. New York, NY, USA: IEEE. pp. 1-8.

[5] Kaplan ED, Hegarty CJ. Understanding GPS: Principles, and Applications. 2nd ed. Norwood, MA, USA: Artech House, 2006.

[6] Engel U. Benefits of a Multi-GNSS Receiver in an Interference Environment. Wachtberg, Germany: Fraunhofer Institute for Communication, 2006.

[7] Schonemann E, Becker M, Springer T. A new approach for GNSS analysis in a multi-GNSS and multi-signal environment. Journal of Geodetic Science 2011; 3: 204.

[8] Çayıroğlu İ. Kalman Filtresi ve Programlama. Fen ve Teknoloji Bilgi Paylaşımı 2012; 1: 1-6 (in Turkish).

[9] Maybeck PS, Cox IJ, Wilfong GT. The Kalman filter: an introduction to concepts. In: Cox IJ, Wilfong GT, editors. Autonomous Robot Vehicles. New York, NY, USA: Springer-Verlag, 1990. pp. 194-204.

[10] Kleeman L. Understanding and Applying Kalman Filtering. Clayton, Australia: Department of Electrical and Computer Systems Engineering, Monash University, 1995.