AI-based Algorithm for GNSS Spoofing Detection

Jae Hwan Bong
Department of Human Intelligence
Robot Engineering
Sangmyung University
Cheonan, South Korea
drbong@smu.ac.kr

Doyoung Kim
Department of Human Intelligence
Robot Engineering
Sangmyung University
Cheonan, South Korea
202121395@sangmyung.kr

Seongkyun Jeong
Department of Human Intelligence
Robot Engineering
Sangmyung University
Cheonan, South Korea
skjeong@smu.ac.kr

***Abstract*— GNSS is extensively employed for applications requiring high reliability. However, GNSS inherently encompasses varying error factors and is susceptible to malicious attacks such as spoofing. To ensure stable GNSS utilization, it is imperative to incorporate GNSS spoofing signal detection mechanisms into GNSS signal processing. In this paper, artificial intelligence (AI) to detect the spoofing in GNSS signal is proposed. The developed AI model effectively detects the spoofing within GNSS signals while the satellite navigation solutions changing over time. The AI was trained using simulated GNSS data, confirming the feasibility of employing AI techniques for GNSS signal processing.**

Keywords—Anomaly Detection, GNSS, Artificial Intelligence

I. Introduction

Global Navigation Satellite Systems (GNSS) have emerged as a cornerstone of modern society. GNSS such as GPS, GLONASS, Galileo, and BeiDou is crucial for a wide range of applications that depend on accurate positioning, navigation, and timing information. GNSS affects our daily lives in various aspects enabling efficient transportation and precision agriculture, enhancing response against natural and man-made disasters, and promoting scientific research.

The aviation industry heavily relies on GNSS for precise navigation, approach, and landing procedures. GNSS aids in reducing pilot workload and enhancing safety during flight operations [1, 2]. In agriculture, GNSS is used for precision planting, spraying, and harvesting. Accurate positioning allows farmers to optimize resource usage, increase yields, and reduce environmental impact [3]. GNSS aids in real-time vehicle tracking, route optimization, and fleet management. It enhances efficiency, reduces fuel consumption, and improves customer service [4]. GNSS enables rapid and accurate location determination during emergencies, facilitating timely response and rescue operations [5]. GNSS synchronization is vital for the reliable functioning of telecommunication networks, ensuring accurate timing for cellular networks, broadband, and satellite communication systems [6]. GNSS plays a role in space science and exploration, including satellite missions and spacecraft navigation. Precise positioning is essential for space-based observations and data collection [7]. GNSS synchronization is crucial for maintaining stability and synchronization in power distribution grids, ensuring accurate power flow measurements, and facilitating grid management [8].

GNSS is very convenient for obtaining the positioning, navigation, and timing information, but the signal strength is weak and is easily affected by nearby interference signals, which is likely to cause large errors and malfunctions. GNSS fault has a serious negative impact on various applications. GNSS fault yields erroneous positioning data to aircraft navigation systems, which can lead to catastrophic consequences during critical approach and landing phases. Disaster response teams can be directed to the wrong locations, slowing down rescue operations in the midst of crises. Robots for precision agriculture can be controlled inaccurately, resulting in uneven crop distribution and wastage of resources.

There are two types of GNSS error sources: systematic errors and random errors. The systematic errors are also called deterministic errors. The systematic errors exhibit consistent patterns which can be modeled and corrected. The systematic errors include clock errors, ephemeris errors, ionospheric delay, tropospheric delay, multipath effects. Although the atomic clocks on GNSS satellites are very accurate, small discrepancies occur between the satellite clocks and the receiver's clocks, resulting in clock errors. Ephemeris errors are come from inaccurate prediction of orbital positions and velocities of the satellites. The GNSS signals are delayed while passing through the ionosphere and the troposphere, which produces the ionospheric delay and the tropospheric delay. GNSS signals can reflect off surfaces such as buildings or the ground before reaching the receiver, producing additional signal paths and errors.

The random errors, also known as stochastic errors, are typically not consistent and can vary unpredictably over time and space. The random errors result from receiver noise, signal interference, and environmental variations. The inherent noise in the electronics of GNSS receiver introduces fluctuations in the received signal, lowering accuracy. External signals like radiofrequency interference disrupt GNSS signals. Rapidly changing of atmospheric conditions causing unpredictable errors.

GNSS signal cause a malfunction even by a deliberate and malicious attack such as jamming and spoofing. The jamming focuses on disrupting or overpowering the authentic GNSS signals. The jamming interferes with the reception of GNSS signals through the intentional transmission of radiofrequency signals. Unlike the jamming, the goal of the spoofing attack is to trick GNSS receivers into calculating incorrect position, velocity, and timing information. The spoofing uses fake signals to deceive GNSS receivers. The fake signals are counterfeit GNSS signals that mimic the signals transmitted by actual satellites. The fake signals are carefully designed to appear stronger or more authentic than the actual satellite signals, causing the receiver to believe it is at a different location or time than it actually is.

Both the spoofing and the jamming attacks highlights the vulnerabilities of GNSS signal anomaly and failure. In the event of anomaly and failure, detection and correction methods are required to provide integrity and reliability of GNSS signal and protect applications of GNSS.

979-8-3503-1327-7/23/$31.00 ©2023 IEEE

In this paper, deep neural network-based algorithm for detecting anomaly and failure of GNSS signal is presented. Developed deep neural network predicts GNSS measurements based on the past information. Difference between the prediction of the deep neural network and the measurement of the receiver is calculated. Anomaly and failure of GNSS signal are detected from the difference. The proposed algorithm verified the detection performance through simulation.

II. METHODS

A. Algorithm Overview

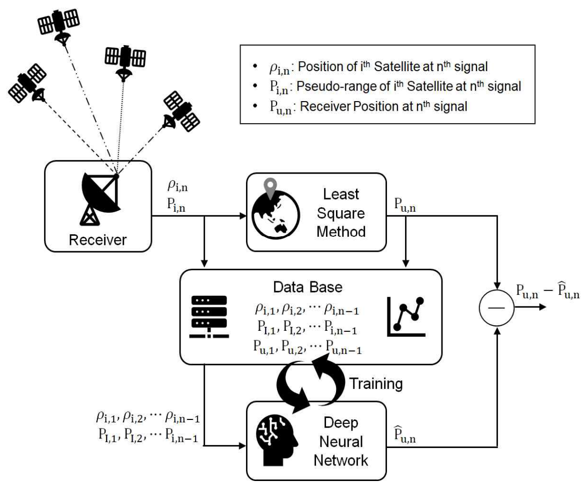
Receiver for GNSS captures satellites signals and measures the pseudo-range between the receiver and the satellites. Using the satellite positions broadcast from the satellites and the pseudo-range, the satellite navigation solution which includes location and time of the receiver is calculated via least square method.

The measured pseudo-range, however, is not the exact distance between the satellite and the receiver due to the systematic errors and the random errors. The satellite position broadcast from the satellite also includes an error component. Therefore, the satellite navigation solution inherently have errors.

The satellite navigation solution is calculated for every captured satellite signals. Because the relative position between the receiver and the satellite changes with time, and the number and types of visible satellite are varied with time. Model parameters for the satellite navigation solution are calculated by the least square method. The model parameters change every time while the number and types of visible satellite are changing, but if the visible satellites are constant and the abnormal situation does not occur, the model parameters do not change significantly.

On the other hand, if there are the GNSS spoofing signal, not only does the value of measurements change, but it also changes the relationship between the measurements, resulting the wrong satellite navigation solution.

Developed algorithm described in Fig. 1 detects the GNSS spoofing signal. The algorithm was designed to capture the relationship changes between the measurements when the GNSS spoofing signal was occurred. As described earlier, it is difficult to capture the relationship between the measurements because the model parameters for the satellite navigation solution are changed every time depending on the satellite position. In order to tackle these problem, deep neural network techniques were applied to the algorithm to capture the relationship between the measurements.



$\rho_{i,n}$: Position of ith Satellite at nth signal
$P_{i,n}$: Pseudo-range of ith Satellite at nth signal
$P_{u,n}$: Receiver Position at nth signal
Receiver
$\rho_{i,n}$
$P_{i,n}$
Least Square Method
$P_{u,n}$
Data Base
$\rho_{i,1}, \rho_{i,2}, \cdots \rho_{i,n-1}$
$P_{I,1}, P_{I,2}, \cdots P_{i,n-1}$
$P_{u,1}, P_{u,2}, \cdots P_{u,n-1}$
Training
$\rho_{i,1}, \rho_{i,2}, \cdots \rho_{i,n-1}$
$P_{I,1}, P_{I,2}, \cdots P_{i,n-1}$
Deep Neural Network
$\widehat{P}_{u,n}$
$P_{u,n} - \widehat{P}_{u,n}$

Fig. 1. Diagram of GNSS spoofing signal detection algorithm

The detection algorithm uses both least square method and deep neural network to get the satellite navigation solution. The leas square method calculates the satellite navigation solution from the current satellite signal. Whereas, the deep neural network predicts the satellite navigation solution from the past satellite signal. the GNSS spoofing signal can be detected via difference between the results from the least square method and the deep neural network.

When the received satellite signal has the spoofing, the currently received signal has the distorted measurements. The distorted measurements abnormally change the relationship between measurements, resulting the wrong satellite navigation solution via least square method.

Deep neural network in the algorithm was trained to capture the current receiver position from the past dataset of satellite position and pseudo-range. Though the current satellite signal has the spoofing, the deep neural network uses the past satellite signal to predict the satellite navigation solution. Since the prediction of deep neural network is not affected by the distorted measurements, the prediction is close to the correct satellite navigation solution.

When comparing the satellite navigation solution calculated by the last square method with the satellite navigation solution predicted by the deep neural network, a small difference means that there is no spoofing in the GNSS signal, and a large difference means that there exist spoofing in the GNSS signal.

B. Satellite Navigation Solution

The measurements and the position of the receiver have relationship in equation (1), where ρ_i is the pseudo-range of the i-th satellite, (x_i, y_i, z_i) is the position of the i-th satellite, (x_u, y_u, z_u) is the position of the receiver, b_u is the clock bias of the receiver, and e_i is the pseudo-range error of the i-th satellite.

$$\rho_i = \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} + b_u + e_i \qquad (1)$$

Equation (1) can be linearized as equation (2) at local minima. Substituting equation (1) to equation (2) excluding error term, equation (3) is obtained.

$$\delta\rho_i = \frac{(x_i - x_u)\delta x_u + (y_i - y_u)\delta x_u + (z_i - z_u)\delta x_u}{\sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2}} + \delta b_u \qquad (2)$$

$$\delta\rho_i = \frac{(x_i - x_u)\delta x_u + (y_i - y_u)\delta x_u + (z_i - z_u)\delta x_u}{\rho_i - b_u} + \delta b_u \qquad (3)$$

Equation (4) is obtained by applying equation (3) to all the measured pseudo-range of the visible satellite. In equation (4), the number of the visible satellite is denoted by n and matrix $\boldsymbol{A} \in \mathbb{R}^{n\times4}$ is calculated by using equation (5). The position of the receiver is calculated as in equation (7) by organizing equation (6).

The satellite navigation solution is calculated as in equation (7) by randomly setting the initial position and applying equation (6) with the measurements.

$$\begin{bmatrix}\delta\rho_1\\ \delta\rho_2\\ \delta\rho_3\\ \delta\rho_4\\ \vdots\\ \delta\rho_n\end{bmatrix} = \boldsymbol{AU} = \begin{bmatrix}a_{11} & a_{12} & a_{13} & 1\\ a_{21} & a_{22} & a_{23} & 1\\ a_{31} & a_{32} & a_{33} & 1\\ a_{41} & a_{42} & a_{43} & 1\\ \vdots & \vdots & \vdots & \vdots\\ a_{n1} & a_{n2} & a_{n3} & 1\end{bmatrix}\begin{bmatrix}\delta x_u\\ \delta y_u\\ \delta z_u\\ \delta b_u\end{bmatrix} \tag{4}$$

$$a_{i1} = \frac{x_i - x_u}{\rho_i - b_u},\ a_{i2} = \frac{y_i - y_u}{\rho_i - b_u},\ a_{i3} = \frac{z_i - z_u}{\rho_i - b_u} \tag{5}$$

$$\begin{bmatrix}\delta x_u\\ \delta y_u\\ \delta z_u\\ \delta b_u\end{bmatrix} = [\boldsymbol{A}^T\boldsymbol{A}]^{-1}\boldsymbol{A}^T\begin{bmatrix}\delta\rho_1\\ \delta\rho_2\\ \delta\rho_3\\ \delta\rho_4\\ \vdots\\ \delta\rho_n\end{bmatrix} \tag{6}$$

$$X_L = \begin{bmatrix}x_u\\ y_u\\ z_u\\ b_u\end{bmatrix} \tag{7}$$

C. Deep Neural Network

Transformer is a deep neural network model developed by Google researcher [9]. The Transformer uses the encoder-decoder structure but is implemented by only attention mechanism. The Transformer demonstrated superior performance over the recurrent neural network(RNN) in sequence data processing, even though the transformer uses the encoder-decoder structure without using RNN.

A small-sized transformer was used to detect the GNSS spoofing signal. Major hyperparameters of the transformer were set as followings. The size of the input and output in the encoder and decoder was set to be 256. The number of encoder-decoder layer was set to be 4, where a encoder-decoder layer is composed by one encoder and one decoder. The number of heads to be used in parallel in multi-head attention mechanism was set to be 4. Feed-forward neural network in the encoder used two 1D convolution layers.

During the training process of the transformer, the optimizer, the learning rate, and the loss function were set to be Adam, 0.0001, mean squared error, respectively. Sequential data for training were generated from the normal satellite signal by setting the time step to 7. Sequential data for test were generated from the normal satellite signal and the spoofing signal by using the same time step as training data.

III. Results

One of ten training data was used as validation data. The loss values during the training process for the training data and the validation data are described in Fig. 2. Using the 11-th generation intel i5-11320H CPU, 294 sequential data were used for training, requiring 40ms per epoch for training. Since the loss value converged at about 175 epochs, the total training time of about seven seconds was required.

IV. CONCLUSIONS

GNSS inherently contains variable error factors in the measurements and is vulnerable to the jamming and the spoofing attacks due to low signal strength. GNSS is widely used for the applications need high reliability. Detection of the GNSS spoofing signal is mandatory to use GNSS stably and response to the malicious attack.

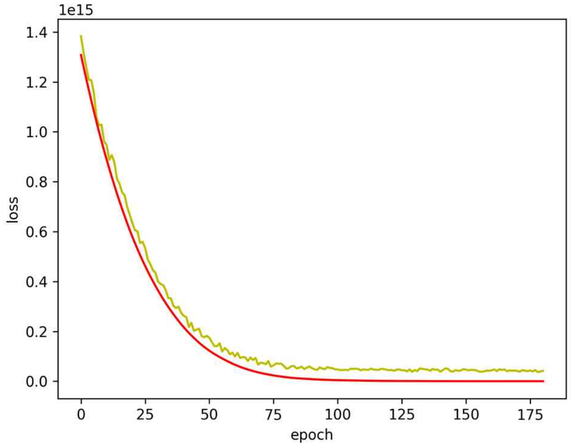


Fig. 2. Loss values for training and validation data

In this paper, authors suggest deep neural network based algorithm to detect the GNSS spoofing signal. The satellite navigation solution using GNSS signal changes according to the environmental reason and the relative position between the satellites and the receiver. The developed algorithm captures the satellite navigation solution changing over time and is capable of the GNSS spoofing signal detection.

The convergence of loss values shows that the deep neural network can learn from simulated GNSS data. The proposed algorithm captures the characteristics of sequence data based on the deep neural network, enabling continuous detection of the GNSS spoofing signal.

The proposed algorithm is expect to play an important role in securing the reliability of GNSS and contributes to expanding the field of GNSS application. The feasibility of GNSS signal processing using a deep neural network was confirmed.

References

[1] E. D. Kaplan and C. J. Hegarty, Understanding GPS: Principles and Applications, 2nd ed., Artech House, 2006, pp. 635-661.

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

[3] S. Gao, "Development of GNSS-based precision agriculture technology for site-specific nutrient management," PhD Thesis, Kansas State University, 2016.

[4] D. Tarchi, "Reliable and secure GNSS-based solutions for autonomous vehicle navigation," PhD Thesis, University of Pisa, 2018.

[5] A. Hossain, "GNSS and IoT-based emergency response system for disaster management," PhD Thesis, University of Trento, 2019.

[6] D. Brevnov, "High-precision GNSS-based time and frequency synchronization for telecommunication networks," PhD Thesis, Lomonosov Moscow State University, 2015.

[7] D. R. Seepersad, "Characterization of GNSS signal fluctuations in the ionosphere for space weather applications," PhD Thesis, University of Calgary, 2014.

[8] O. Sundström, "GPS/GNSS-based time transfer for power system applications," PhD Thesis, Uppsala University, 2014.

[9] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is All you Need," Adv. Neural Inf. Process. Syst., 30, 2017.