공학석사학위논문

A Detection and Localization Method Based on Multiple Base Stations for GNSS Spoofing Signal

다중 기준국 기반의 위성항법시스템 기만신호 검출 및 위치추정 기법

2015 년 2 월

서울대학교 대학원

기계항공공학부

김 선 영

A Detection and Localization Method Based on Multiple Base Stations for GNSS Spoofing Signal

다중 기준국 기반의 위성항법시스템 기만신호 검출 및 위치추정 기법

지도교수 박 찬 국

이 논문을 공학석사 학위논문으로 제출함

2014 년 12 월

서울대학교 대학원

기계항공공학부

김 선 영

김선영의 공학석사 학위논문을 인준함

2014 년 12 월

위 원 장 : 김 유 단

부위원장 : 박 찬 국

위　　원 : 기 창 돈

Abstract

A Detection and Localization Method Based on Multiple Base Stations for GNSS Spoofing Signal

KIM, SUN YOUNG
SCHOOL OF MECHNICAL AND
AEROSPACE ENGINEERING
COLLEGE OF ENGINEERING
SEOUL NATIONAL UNIVERSITY

The Global Navigation Satellite System (GNSS) is a radio navigation system using satellites and has been widely used by both military and civilian systems since it can provide an accurate position and timing information to users. However, the strength of the GNSS signal on the user’s receiver is weak since GNSS satellites are approximately 20,000 Km away and transmit several watts of signal power such that at the ground level. Therefore, GNSS signal is quite vulnerable to different types of interference.

Interference signals can be categorized as unintentional and intentional. Intentional interference, such as jamming, meaconing, and spoofing, are specifically designed with malicious intention to deny or mislead GNSS receivers, thus they are serious threat to GNSS applications. Among them, spoofing is much more dangerous since it is designed to mislead their target receiver that is not aware of the attack and this can lead to disastrous consequences in scores of applications. Therefore, in this thesis, a detection and localization method for GNSS spoofing signal based on multiple base stations has been researched for monitoring the quality of navigation solutions.

There are various spoofing detection methods according to detection parameters and spoofing scenarios. The related researches have been actively performed for recent years. In this thesis, GNSS spoofing detection method based on adaptive fading Kalman filter is proposed to detect spoofing signal and the fading factor of the filter is used as a detection parameter. In order to detect spoofing signal regardless of spoofing scenarios, the proposed method is based on multiple base stations whose locations are fixed and already known. The effect of the spoofing is modeled by the ramp type bias error of the pseudorange to emulate smart spoofer. In addition, the change of the fading factor according to ramp type bias error is quantitatively analyzed and the detection threshold is established to detect spoofing signal by analyzing the change of the error covariance. The proposed method also has an effect on spoofing mitigation by adjusting the Kalman gain of the filter.

If spoofing signal is detected by using the proposed method, spoofing localization method based on multiple base stations is performed to estimate spoofing location. There are various localization methods according to measurements. However, in this thesis, spoofing location is estimated by differential received signal strength (DRSS) method because of simplicity and efficiency. The carrier to noise ratio (C/No) measurement characterizes the received signal strength (RSS), therefore, the difference of the C/No between main station (MS) and each base station (BS) is used as measurement for DRSS method. In addition, the Cost231-Walfisch-Ikegami model is applied as path-loss model for calculating signal attenuation.

To verify the performance analysis of the proposed spoofing detection and localization method, simple simulations are implemented, respectively. This method can be applied for integrity monitoring algorithm in case of fixed user because it can detect abnormal pseudorange of each channel. In addition, this method is expected to be easily applied to practical system because they do not need to additional hardware and realization of complex algorithm.

Keywords: GNSS Spoofing, Spoofing Detection, Spoofing Localization, Multiple Base Stations

Student Number: 2013-20649

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation and Background

Recently, as quite a number of applications relying on GNSS in various fields are increasing, the quality of navigation solutions has been threatened by intentional interference signal. For that reason, the damage cases related intentional interference has been constantly reported.

Therefore, it is necessary to prepare countermeasures because it can cause the damage of human life in the worst case. There are various types of intentional interference signal and it can be typically classified as jamming, meaconing, and spoofing. Jamming signal has much stronger signal power than the received GNSS signal, so it makes receivers useless. Meaconing signal transmits recorded signal which is stored after receiving from GNSS satellites. Spoofing signal attempts to deceive a GNSS receiver by broadcasting a slightly more powerful signal than that received from the GNSS satellites, structured to resemble a set of normal GNSS signals. Spoofing signal is more threaten than other intentional interferences because it can result in large navigational solution errors by deceiving users. The countermeasures for jamming signal have been diversely studied for years and various anti-jamming related products are available commercially. However, the countermeasures for spoofing signal are insufficient because spoofer is difficult to design and there are various types of spoofing scenarios by attacker. It comes to be realized that the effects of spoofing signal are very severe and confirmed that the implementation of spoofer is possible through Todd Humphreys' research team who demonstrates first successful GPS spoofing of UAV. Therefore, the countermeasures for spoofing signal have been actively studied in universities, research institutes, and government agencies.

1.2 Objectives and Contributions

The main objectives of this thesis are proposing a detection and localization method for GNSS spoofing signal based on multiple base stations to monitor the quality of navigation solutions.

Various spoofing detection methods according to measurements have been researched to reduce the effects of spoofing signal. However, these methods have some limitations according to spoofing scenarios.

The proposed spoofing detection and localization method can detect and localize spoofing signal without limitation according to spoofing scenarios because this method is based on multiple base stations whose locations are fixed and already known. The proposed method can be applied for integrity monitoring algorithm in case of fixed user because it can detect abnormal pseudorange of each channel. In addition, this method is expected to be practical in operational view because they do not need to additional hardware and realization of complex algorithm.

1.3 Organization

This thesis is organized as follows: In chapter 2, GNSS intentional interference is introduced. In this chapter, various types of GNSS intentional interference signal are explained. In chapter 3, a spoofing detection method based on adaptive fading Kalman filter is proposed to detect spoofing signal and the fading factor of the filter is used as a detection parameter. In addition, the change of the fading factor according to ramp type bias error is quantitatively analyzed and the detection threshold is established to detect spoofing signal by analyzing the change of the error covariance. To verify the performance analysis of the proposed spoofing detection method, simple simulations are implemented. In chapter 4, a spoofing localization method based on multiple base stations is introduced. Spoofing location is estimated by differential received signal strength (DRSS) method. The performance of the proposed spoofing localization method is analyzed by simple simulations. Finally, chapter 5 concludes this thesis.

Chapter 2

GNSS Intentional Interference

2.1 Introduction

Radio frequency signals received from a global navigation satellite system (GNSS) are extremely weak and their signal power on the ground are about -160 dBW which is 20 dB below than noise level. For that reason, GNSS signals are quite vulnerable to different types of interference. Interference affects the GNSS receiver’s ability to acquire and track a sufficient number of satellites to provide a reliable navigation solution. There are many types of radio frequency (RF) interference, including tones, swept waveforms, pulse, narrowband noise, broadband noise and other multi-frequency and time-varying versions of most of the same methods [1]. Interference signal can be classified unintentional interference signal and intentional interference signal. Intentional interferences, such as jamming, meaconing, and spoofing, are specifically designed signals with malicious intention to deny or mislead GNSS receivers, thus they are serious threat to GNSS applications. Among them, meaconing and spoofing are structural types of interference that aim to deceive a receiver into tracking false signals while the receiver is not aware of the attack [2]. For that reason, this can lead to disastrous consequences in scores of applications [3]. In order to find countermeasures for intentional interference, it needs to be investigated about intentional interferences. Therefore, the characteristics, related damage events, and research trends of representative intentional interferences are described from next session.

2.2 Jamming

Jamming signal emits radio frequency energy with sufficient power to make a receiver not to acquire and track GNSS signal. In general, GNSS signal can be incapacitated when jammer to signal ratio (JSR) is higher than 25 dB. The previous work [4] has been studied the effect of interference on a receiver and the effective C/No is used as a parameter to evaluate the effect of it. Figure 2.1 shows effects of jamming signal according to JSR and the quality of GNSS signal is largely affected by interference when the power of interference signal is high [4].

Many damage events related to jamming signal are reported because jamming signal is more common and practical interference type than other intentional interferences. In recent years, South Korea also has experienced intentional GPS jamming several times.

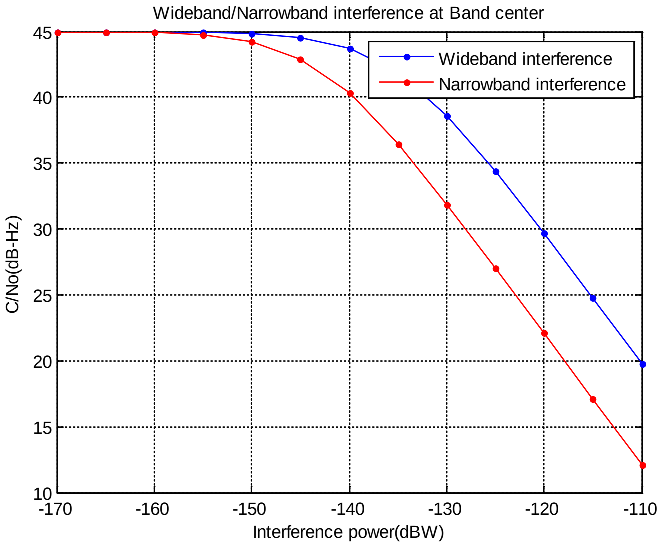

Figure 2.1 Effect of the power of interference signal

Influenced area was northwestern of metropolitan and specifics of those incidents are summarized in Table 2.1. Electronics and Telecommunications Research Institute (ETRI) analyzed saved GPS data during those periods and found out that single-tone continuous wave interference (CWI) influenced L1 frequency band and swept CWI disrupted L2 and L5 frequency bands by sweeping its frequency with 24 MHz bandwidth [5].

In order to cope with various jamming attacks, the analysis of jamming signal and the researches on different countermeasures for jamming attacks are needed to be performed.

Table 2.1 GNSS jamming events in Korea

	1st event (23 ~ 26 Aug, 2010)	2nd event (4 ~ 14 Mar, 2011)	3rd event (28 April ~ 13 May, 2012)
Jammer Location	Gaeseong	Gaeseong, Haeju	Gaeseong
Signal Strength	-70 dBm ~ -60 dBm	-60 dBm	-80 dBm ~ -60 dBm
2G/Wibro station	181 sites	145 sites	64 sites
Air Plane	15 civil airliner	106 civil airliner	21 civil airliner
Ship	1 military vessel	3 military vessel, 7 civil vessel	2 civil vessel

The previous work [1] surveyed the signal properties of commercial GPS jammers purchased online. The GPS jammers examined in [1] are grouped into three categories based on power source and antenna type. Table 1 shows sweep behavior of the GPS jammers and Table 2 shows mean jammer power for different bandwidths about L1 and L2, and indicators of power at other frequencies [1]. The test of jammers provided information about the characteristics of current civil GPS jammer signals. The majority of the jammers used chirp type signals, all jammed L1 band, only six jammed L2 band and none jammed L5 band. The sweep rate of jammers is on average about $1 \sim 2\times10^{12}$ Hz/sec [1].

In order to deal with the threat, detecting and characterizing interference, and giving timely alert, are important for safe GPS operation in all countries, as well as in South Korea. The researches to reduce damage from jamming attacks have been constantly studied for many years and there are various methods to detect and mitigate jamming signal. They are mainly classified as pre-correlation detection and post-correlation detection method depending on where the algorithms are applied [6].

In the previous works, the GNSS interference simulator using MATLAB SIMULINK is designed to evaluate interference effect assessment [7] and the effect of interference and the performance of various detection parameters are analyzed by using this simulator [8]. In addition, various types of interference signals are detected and identified by using AGC and adaptive IIR notch filter [6] and detection method using adaptive notch filter is also applied to multiple ground stations [9]. The [10-12] papers have focused on detecting the existence of continuous wave interference (CWI) using an adaptive notch filter. This approach has a limitation on detection and mitigation of chirp type interference, because its sweep rate degrades the signal tracking performance of the adaptive notch filter. Therefore, it is necessary to classify the chirp type interference according to sweep rate by using different detection and tracking algorithm. In order to reduce the frequency estimation error, adaptive fading Kalman filter is applied to the proposed algorithm in [13-16]. Furthermore, the low pass differentiator (LPD) and the pattern enhancement algorithm are used to estimate the sweep period of chirp type interference, which is used to improve the performance of the frequency tracking.

2.3 Meaconing

Meaconing, known as a repeat-back spoofer [17], refers to the reception, delay and rebroadcast of GPS signals to disturb a target receiver [2]. Meaconing transmits the received GPS signals at its location with stronger power in order that the target receiver locks on meaconing signal instead of the authentic signal. Since the meaconing signal arrived at the target receiver is naturally delayed according to the distance between the meaconing transmitter and the receiver, the receiver provides wrong navigation solutions by tracking the meaconing signals. On the other hand, spoofing is very complicated attack that generates artificial GPS signals to make the receiver to capture the spoofing signal. Because meaconing is easier to implement and more realistic threat than spoofing and can affect both civilian and military receivers, it is needed to investigate the effects of meaconing and its mitigation methods. The effect of the receiver by the meaconing attack may differ according to a relative delay between the meaconing signal and the authentic signal at the input of the receiver. If the relative delay is within the correlator spacing of the receiver, correlation outputs are distorted like multipath. Whereas, if the relative delay is longer than the correlator spacing, the receiver acquires delayed meaconing signal beacuse the amplitude of the meaconing signal is normally stronger than the authentic signal. Unless the meaconing transmitter is located near the target, a long delay meaconing seems to be the most likely meaconing scenario beacuse the meaconing transmitter first acquires GPS signal and rebroadcasts it without any signal modification except the delay and amplitude of the signal [2].

The effects of meaconing are more menacing than jamming. It can mislead the receiver to track wrong signal with less power than jamming. Meaconing is easy to implement and can interfere both C/A and P(Y) code. Thus, it is needed to analyze the effects of meaconing on GPS receivers and perform meaconing simulation using commercial software based GPS signal simulator and GPS SDR. In addition, the meaconing effects are analyzed according to the time delay of meaconing signal.

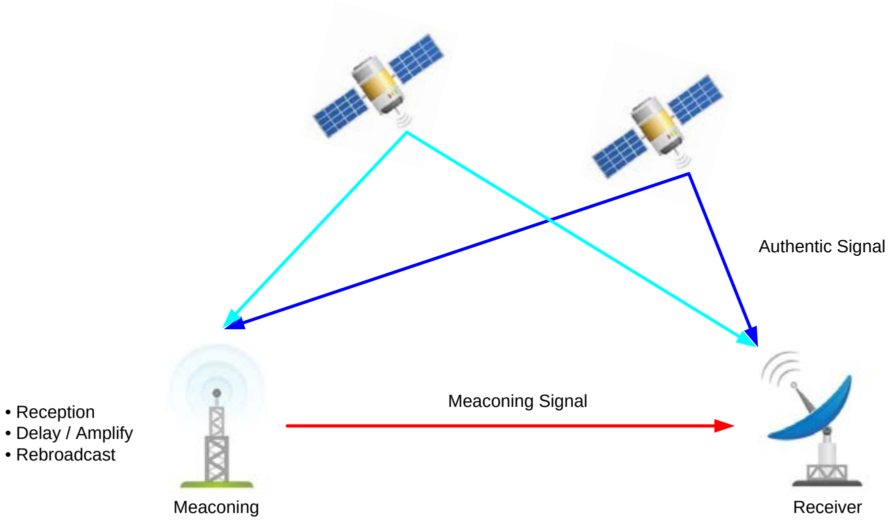

Figure 2.2 Meaconing signal

The received signal with meaconing attack for the GPS C/A code can be modeled as follows [2]:

$$\begin{aligned} S_{IF}(t) &= \sum_{i=1}^{K} \sqrt{P_i^a} C_i^a (t-\tau_i^a) D_i^a (t-\tau_i^a) \cos\left(\left(\omega_{IF}+\omega_{d_i}^a\right)(t-\tau_i^a)+\phi_i^a\right) \\ &+ \sum_{j=1}^{L} \sqrt{P_j^m} C_j^m (t-\tau_j^m) D_j^m (t-\tau_j^m) \cos\left(\left(\omega_{IF}+\omega_{d_j}^m\right)(t-\tau_j^m)+\phi_j^m\right)+v(t) \end{aligned} \quad (2.1)$$

where P is the signal power, C is the C/A code, D is the navigation data bit, ω_{IF} is the intermediate frequency (IF), τ is the cod delay, ω_d is the doppler frequency, and ϕ is the carrier phase. The superscripts a and m correspond to the authentic and meaconing signals, respectively. The subscripts i and j refer to i-th authentic signal and j-th meaconing signal, respectively and $v(t)$ is the additive white Gaussian noise [2].

Some events by meaconing signal have been recently reported. There is interference by a GPS repeater operated in a hangar in Hannover Airport, Germany. In addition, meaconing signal resulted in an alert of Enhanced Ground Proximity Warning System during taxing and departure.

In order to detect and mitigate meaconing signal, various researches related to meaconing have been performed in the previous works. In [18], the meaconing effects on GPS receiver is analyzed. Long delay meaconing mitigation method based on subspace projection has been studied in [2]. In general, the subspace projection method is used to reduce the effects of multipath. However, multipath detection and mitigation methods also can be used as meaconing countermeasures because meaconing signal is the delayed signal form of the authentic signal and its effects are similar to multipath.

In addition, the meaconing detection and localization method using C/No monitoring is proposed in [19] and [20], respectively. These approaches could be possible to implement because the proposed methods are based on multiple base stations whose locations are already known and fixed.

2.4 Spoofing

A GPS spoofing attempts to deceive a GPS receiver by broadcasting a slightly more powerful signal than that received from the GPS satellites, structured to resemble a set of normal GPS signals. These spoofed signals, however, are modified in such a way as to cause the receiver to determine its position to be somewhere other than where it actually is, specifically somewhere determined by the attacker. Therefore, such spoofing signals can result in large navigational solution errors that are passed onto the unsuspecting user with potentially dire consequences. However, there are practical limitations to generate spoofing signal because spoofer has to know exact position and velocity of target to deceive target user.

The representative damage incidents related to spoofing attack are as follows: It has been suggested that the capture of a Lockheed RQ-170 drone aircraft in northeastern Iran in December, 2011, was the result of such an attack. This event makes threat of spoofing attack to recognize even though an exact cause of this accident is not yet founded. In addition, Dr. Humphreys' research team implemented a portable civilian GPS spoofer [21, 22] and successfully demonstrated hijacking of civilian UAV and yacht using the civil GPS spoofer in 2012 and 2013, respectively. Through these demonstrations, the possibility of spoofer implementation and spoofing attack is confirmed.

A spoofer can be classified with different types of spoofing scenarios according to dynamics and tracking performance. Thus, the spoofing countermeasures have been diversely studied based on various spoofing scenarios [23, 24] and the range of the researches can be extended based on dynamic user or static base station. In addition, spoofing detection and mitigation methods have been researched according to detection parameters, such as the characteristics of the antenna, received power strength, and the receiver measurements, etc. The works related to antenna have been still researched until a recent date and the previous works proposed the spoofing detection algorithm using a GPS tracking antenna [25, 26]. The spoofing detection methods using the change of C/No which presents the strength of the received signal power have been studied [27, 28].

The researches on spoofing countermeasures have been actively studied up to recently and related contents are additionally explained on the next chapter.

Chapter 3

Spoofing Detection Method

3.1 Introduction

A spoofer which is a device to deceive GNSS signal can be identified according to spoofer tracking and its movement. Accordingly, characteristics and effects by spoofer are appeared differently [24]. Therefore, spoofing detection methods can be also diversely classified according to detection parameter and spoofing scenario. In addition, spoofing detection methods have been studied on the static and dynamic situation of spoofing scenario. In recent years, spoofing detection methods using array antenna studied actively and these methods are simple and general method which is based on distinguishing characteristics of signal transmission and reception using antenna. Thus, spoofing detection method using receiving antenna motion [29] has been studied and this method can determine the existence of the spoofing signal by using difference of carrier phase get from receiving antenna motion. The spoofing detection method using the received signal strength is representative among spoofing methods using measurements of receiver. Spoofing signal can be detected by monitoring the change of the received signal strength by checking the received signal strength while vehicle is moving [30]. Table 3.1 shows various types of spoofing detection methods based on the previous works. Each method has difference of performance and limited conditions by spoofing environment and spoofing scenario [31]. There are various test statistics of spoofing detection for stand-alone GPS receivers. These parameters can be used by measurements of multiple base stations. In this thesis, a spoofing detection method using an adaptive fading Kalman filer is explained.

Table 3.1 Summary of spoofing detection techniques

Anti-Spoofing method	Spoofing feature	Complexity	Effectiveness	Receiver required capability	Spoofing scenario generality
C/No monitoring	Higher C/No	Low	Medium	C/No monitoring	Medium
Absolute power monitoring	Higher amplitude	Low	Medium	Absolute power monitoring	High
Power variation versus receiver movement	Higher power variations due to proximity	Low	Low	Antenna movement/C/No monitoring	Low
L1/L2 power comparison	No L2 signal for spoofer	Medium	Low	L2 reception capability	Low
Direction of arrival comparison	Spoofing signals coming from the same direction	High	High	Multiple receiver antennas	High
Pairwise correlation in synthetic array	Spoofing signals coming from the same direction	Low	High	Measuring correlation coefficient	High
TOA discrimination	Inevitable delay of spoofing signal	Medium	Medium	TOA analysis	Low
Signal quality monitoring	Deviated shape of authentic correlation peak	Medium	Medium	Multiple correlators	Low
Distribution analysis of the correlator output	Perturbed amplitude distribution due to spoofing-authentic interaction	Low	Medium	Distribution analysis of correlator outputs	Medium

Consistency check with other solutions	Inconsistency of spoofing solution	High	High	Different navigation sensors	High
Cryptographic authentication	Not authenticated	High	High	Authentication	High
Code and phase rate consistency check	Mismatch between artificial code and phase rate	Low	Low	-	Low
GPS clock consistency check	Spoofing/authentic clock inconsistency	Low	Medium	-	Medium

3.2 Adaptive Fading Kalman Filter

3.2.1 Background

An adaptive fading Kalman filter [32] is implemented by using fading factor of the Kalman filter to robust disturbance. The fading factor is called a memory factor and defined as comparison between residual of calculated covariance using past measurements and residual of estimated covariance at the present. By comparing a threshold which is set the reference value with fading factor, it is determined whether trust past measurement or present estimation. As a result, by adjusting Kalman gain, it is possible to estimate by using model to robust disturbance. This structure is used to improve estimation performance of filter in case of unexpected disturbance environment. The basic system and measurement model equations of an adaptive fading Kalman filter are as follows:

$$\begin{aligned}
x_k &= F_{k-1}x_{k-1} + G_{k-1}u_{k-1} + w_{k-1} \\
z_k &= H_k x_k + v_k \\
E\left(w_k w_j^T\right) &= Q_k \delta_{k-j} \\
E\left(v_k v_j^T\right) &= R_k \delta_{k-j} \\
E\left(w_k v_j^T\right) &= 0
\end{aligned} \tag{3.1}$$

The Kalman filter is initialized as follows:

$$\begin{aligned}
\hat{x}_0^+ &= E\left(x_0\right) \\
\tilde{P}_0^+ &= E\left[\left(x_0 - \hat{x}_0^+\right)\left(x_0 - \hat{x}_0^+\right)^T\right]
\end{aligned} \tag{3.2}$$

Based on how much user wants the filter to forget past measurements, memory factor (or fading factor), α is set larger than 1. If α is equal to 1, the fading Kalman filter is equivalent to the standard Kalman filter. In most applications, α is set only slightly greater than 1 (for example, $\alpha \approx 1.01$) [32].

Using Eq. (3.1) and through time update and measurement update for each time step, k, estimation results are given as follows:

$$\begin{aligned}
\tilde{P}_k^- &= \alpha^2 F_{k-1}\tilde{P}_{k-1}^+ F_{k-1}^T + Q_{k-1} \\
K_k &= \tilde{P}_k^- H_k^T \left(H_k \tilde{P}_k^- H_k^T + R_k\right)^{-1} \\
\hat{x}_k^- &= F_{k-1}\hat{x}_{k-1}^+ + G_{k-1}u_{k-1} \\
\hat{x}_k^+ &= \hat{x}_k^- + K_k\left(z_k - H_k \hat{x}_k^-\right) \\
\tilde{P}_k^+ &= \left(1 - K_k H_k\right)\tilde{P}_k^-
\end{aligned} \tag{3.3}$$

where $\tilde{P}$ is not equal to the covariance of the estimation error. However, fading Kalman filer is more robust to modeling errors than the standard Kalman filter. Generally, an adaptive fading Kalman filer is designed to trust model than measurement in case of detection fault and estimates by adjusting fading factor.

Therefore, in this thesis, the adaptive fading Kalman filter is used to detect and mitigate spoofing signal. The filter model which is applied to spoofing detection method is explained in detail on the next session.

3.2.2 Adaptive Fading Factor

Using the most similar signal with GNSS signal to deceive system based on GNSS signal maximizes the effect by spoofing signal. The pseudorange and Doppler of specific time and area are determined by the characteristics of GNSS signal and movement of spoofing object. Therefore, the change of the pseudorange each channel is increased when spoofing signal is received and affected. For that reason, the change of the pseudorange is used as important parameter to detect spoofing signal.

The state variables of the filter are position and velocity of user. The measurement model is used the equation of the linearized pseudorange. The pseudorange equation of one channel is expressed by

$$\rho_N = \sqrt{\left(x_u - x_N\right)^2 + \left(y_u - y_N\right)^2 + \left(z_u - z_N\right)^2} + c\Delta t \tag{3.4}$$

where ρ_N is the pseudorange of the N-th channel, $\left[x_u \quad y_u \quad z_u\right]^T$ is the user position, $\left[x_N \quad y_N \quad z_N\right]^T$ is the satellite position of the N-th channel, c is the velocity of the light, and Δt is the clock error of the receiver. The pseudorange of Eq. (3.4) is linearized at the nominal point, $\mathbf{x} = \left[\hat{x}_u \quad \hat{y}_u \quad \hat{z}_u\right]^T$ and can be expressed by

$$\rho_N = \rho_{\mathbf{X}} + h_{x,N} x_u + h_{y,N} y_u + h_{z,N} z_u + c\Delta t \tag{3.5}$$

where $\mathbf{x}$ is the position of the estimated user, $\rho_{\mathbf{x}}$ is the estimated pseudorange at the nominal point, $h_{x,N} = \partial\rho_N / \partial x_u$, $h_{y,N} = \partial\rho_N / \partial y_u$, and $h_{z,N} = \partial\rho_N / \partial z_u$. The linearized pseudorange can be expansively expressed as follows [33]:

$$\begin{bmatrix} \rho_1 \\ \rho_2 \\ \vdots \\ \rho_N \end{bmatrix}_k - \begin{bmatrix} \hat{\rho}_1 \\ \hat{\rho}_2 \\ \vdots \\ \hat{\rho}_N \end{bmatrix}_k = H_k \begin{bmatrix} x \\ y \\ z \\ v_x \\ v_y \\ v_z \\ b \\ \dot{b} \end{bmatrix}_k + \begin{bmatrix} n_{\rho 1} \\ n_{\rho 2} \\ \vdots \\ n_{\rho N} \end{bmatrix}_k$$
$$H_k = \begin{bmatrix} h_{x,1} & h_{y,1} & h_{z,1} & 0 & 0 & 0 & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_{x,N} & h_{y,N} & h_{z,N} & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{3.6}$$

where $\begin{bmatrix} \rho_1 & \rho_2 & \cdots & \rho_N \end{bmatrix}_k^T$ is the pseudorange of the N-th channel satellite, $\begin{bmatrix} \hat{\rho}_1 & \hat{\rho}_2 & \cdots & \hat{\rho}_N \end{bmatrix}_k^T$ is the pseudorange at the estimated user position, and $\begin{bmatrix} n_{\rho 1} & n_{\rho 2} & \cdots & n_{\rho N} \end{bmatrix}_k^T$ is the measurement noise. $\begin{bmatrix} h_{x,N} & h_{y,N} & h_{z,N} \end{bmatrix}$ is the line-of-sight vector between each satellite and base station and can be expressed as bellows [34]:

$$\begin{aligned} h_{x,N} &= \frac{\hat{x}_u - x_N}{\sqrt{(\hat{x}_u - x_N)^2 + (\hat{y}_u - y_N)^2 + (\hat{z}_u - z_N)^2}}, \\ h_{y,N} &= \frac{\hat{y}_u - y_N}{\sqrt{(\hat{x}_u - x_N)^2 + (\hat{y}_u - y_N)^2 + (\hat{z}_u - z_N)^2}}, \\ h_{z,N} &= \frac{\hat{z}_u - z_N}{\sqrt{(\hat{x}_u - x_N)^2 + (\hat{y}_u - y_N)^2 + (\hat{z}_u - z_N)^2}} \end{aligned} \tag{3.7}$$

where $\begin{bmatrix} \hat{x}_u & \hat{y}_u & \hat{z}_u \end{bmatrix}^T$ is the estimated position of user and the position error is expressed in ECEF coordinate. An adaptive fading Kalman filter is used to monitor the change of the pseudorange each channel can reduce the measurement error effect on estimation by adjusting Kalman gain. In general, the fading factor is calculated by the relation between the calculated innovation covariance and the estimated innovation covariance. The calculated innovation covariance is from the Kalman filter [35].

$$C_k = E\left[\left(z_k - \hat{z}_k^-\right)\left(z_k - \hat{z}_k^-\right)^T\right] = H_k P_k^- H_k^T + R_k \tag{3.8}$$

where C_k is the covariance of filter, z_k is the measurement, $\hat{z}_k^-$ is the estimated measurement of the filter, H_k is the measurement matrix, P_k^- is the prior predicted error covariance using system model, R_k is the measurement noise covariance of the filter. The estimated innovation covariance using measurement can be expressed by [35]

$$\hat{C}_k = \frac{1}{M-1}\sum_{i=k-M+1}^{k}\left(z_i - \hat{z}_i^-\right)\left(z_i - \hat{z}_i^-\right)^T \tag{3.9}$$

where $\hat{C}_k$ is the estimated innovation covariance using measurement, M is the window size which means sample number of measurement. The fading factor by using upper two equations is defined as bellows [35]:

$$\alpha_k = \begin{bmatrix} \alpha_k(1) \\ \alpha_k(2) \\ \vdots \\ \alpha_k(N) \end{bmatrix} = \max\left(\mathbf{T}, \frac{diag\left(\hat{C}_k\right)}{diag\left(C_k\right)} \right) \tag{3.10}$$

where $\max(\ )$ is the function which returns the largest elements and $diag(\ )$ is the function presenting diagonal elements of matrix. $\mathbf{T}$ is the matrix with $1 \times N$ dimension. In this thesis, fading factor is used to monitor pseudorange change of each channel because pseudorange is used as measurement and the calculated principle of fading factor is as follows. The estimated covariance by measurement is larger than the calculated covariance by system model when pseudorange error is occurred. Therefore, the fading factors of the channels affected by spoofing are larger than $\mathbf{T}$ and those of the rest channels become $\mathbf{T}$. By using this feature, it is possible to detect spoofing signal and got satellite channel affected by spoofing signal. After finding satellite channels affected by spoofing signal, Kalman gain is adjusted by fading factor as bellows using the features of the filter to prevent spoofing signal from affecting on whole system.

$$\bar{K}_k = \begin{bmatrix} \frac{1}{\alpha_k(1)}K_{11} & \frac{1}{\alpha_k(2)}K_{12} & \cdots & \frac{1}{\alpha_k(N)}K_{1N} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{1}{\alpha_k(1)}K_{81} & \frac{1}{\alpha_k(2)}K_{82} & \cdots & \frac{1}{\alpha_k(N)}K_{8N} \end{bmatrix} \tag{3.11}$$

where $\bar{K}_k$ is the adjusted Kalman gain with dimension of $8 \times N$ by fading factor and $1/\alpha_k(N)$ means inverse of fading factor of each channel. K_{ij} is Kalman gain before adjusting and is the updated by using below equation in Kalman filter.

$$K_k = P_k^- H_k^T \left[H_k P_k^- H_k^T + R_k \right]^{-1} \tag{3.12}$$

where K_k is the Kalman gain matrix with dimension of $8 \times N$ and is composed of the value of K_{ij}. The fading factor which is a detection parameter, α_k and setting of threshold, $\mathbf{T}$ are explained in detail on the next session.

3.2.3 Parameter Analysis

One state of one channel is only considered to analyze quantitatively the effect of spoofing signal on fading factor and Kalman gain. In addition, it is assumed that the ramp type bias error is added on the k-th step and it is shown as Figure 3.1.

The estimation result can be expressed as bellows using the ramp type bias error and measurement input on the k-th step [36].

$$\begin{aligned} \hat{x}_k^+ &= \hat{x}_k^- + K_k \left(\overline{z}_k - H_k \hat{x}_k^- \right) \\ &= \hat{x}_k^- + K_k \left(z_k + b_k - H_k \hat{x}_k^- \right) \end{aligned} \tag{3.13}$$

where $\overline{z}_k$ means the measurement with bias error and b_k presents ramp type bias error. To analyze the estimation performance of the filter, error components can be expressed by using the residual as follows:

$$\overline{e}_k = \left(z_k - H_k \hat{x}_k^- \right) + b_k = e_k + b_k \tag{3.14}$$

where $\overline{e}_k$ is the error components including the bias error, e_k is the error components without the bias error. As shown upper equations, the effects on it appear in the error components on the k-th step because ramp type bias, b_k is added on the k-th step. The window size set three to get estimated error covariance and the error on the k-1 and k-2 step expressed respectively as follows:

$$\begin{aligned} \overline{e}_{k-1} &= e_{k-1} \\ \overline{e}_{k-2} &= e_{k-2} \end{aligned} \tag{3.15}$$

From above equation, it does not effect on the previous interval bias error because bias error exists after k-th step. The estimated error covariance is obtained by using error in the three intervals and can be expressed as follows:

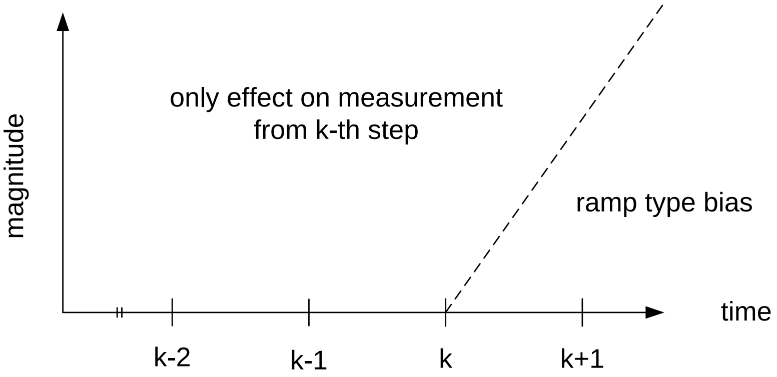

Figure 3.1 The input of the ramp type bias on the k-th step

$$\begin{aligned} \overline{C}_k &= \frac{1}{2}\sum_{i=k-2}^{k}\overline{e}_i^2 = \frac{1}{2}\left((e_k+b_k)^2+e_{k-1}^2+e_{k-2}^2\right) \\ &= \frac{1}{2}\left(e_k^2+e_{k-1}^2+e_{k-2}^2\right)+e_k b_k+\frac{1}{2}b_k^2 \\ &= \hat{C}_k+e_k b_k+\frac{1}{2}b_k^2 \end{aligned} \tag{3.16}$$

Regardless of bias error, the calculated error covariance can be equal as bellows:

$$C_k = H_k P_k^- H_k^T + R_k \tag{3.17}$$

The fading factor, $\bar{\alpha}_k$ is defined as the proportion of the estimated error covariance obtained Eq. (3.16) to the calculated error covariance when bias error is added and can be expressed by

$$\begin{aligned}\bar{\alpha}_k &= \frac{\bar{C}_k}{C_k} = \frac{\hat{C}_k}{C_k} + \frac{e_k b_k + \frac{1}{2} b_k^2}{C_k} \\ &= \alpha_k + \frac{e_k b_k + \frac{1}{2} b_k^2}{C_k}\end{aligned} \tag{3.18}$$

where $\beta_k = \left(e_k b_k + \frac{1}{2} b_k^2 \right) \Big/ C_k$ is defined and fading factor can be expressed as bellows and this value is larger than 1.

$$\bar{\alpha}_k = \alpha_k + \beta_k > 1 \tag{3.19}$$

From above equation, the fading factor is effected on β_k of the ramp type bias error. Here, the fading factor without bias error, α_k can be expressed by the proportion of the estimated error covariance, $\hat{C}_k$ to the calculated error covariance, C_k, that is, $\hat{C}_k / C_k$. In general, the fading factor α_k is always smaller than one because $\hat{C}_k$ is smaller than C_k since the measurement does not include error components affected by bias. This can be expressed as follows:

$$\begin{aligned} &\min\{\alpha_k\} < \alpha_k < \max\{\alpha_k\} \\ &\min\{\alpha_k\} \geq 0,\ \max\{\alpha_k\} \leq 1 \end{aligned} \tag{3.20}$$

However, the range of the fading factor $\bar{\alpha}_k$ is changed by β_k when bias error components is added to measurements.

$$\begin{aligned} &\min\{\alpha_k\} + \beta_k < \alpha_k + \beta_k < \max\{\alpha_k\} + \beta_k \\ &\bar{\alpha}_k = \alpha_k + \beta_k > \min\{\alpha_k\} + \beta_k > 1 \end{aligned} \tag{3.21}$$

The detectable condition of bias magnitude can be finally founded by rearranging upper equation.

$$\begin{aligned} &\beta_k = \frac{e_k b_k + \frac{1}{2} b_k^2}{C_k} > 1 - \min\{\alpha_k\} \\ &b_k^2 + 2e_k b_k - 2C_k + 2C_k \min\{\alpha_k\} > 0 \\ &b_k > -e_k + \sqrt{{e_k}^2 + 2C_k - 2C_k \min\{\alpha_k\}} \\ &(\because e_k > 0,\ b_k > 0,\ C_k > 0) \end{aligned} \tag{3.22}$$

The Eq. (3.19) is established when the bias condition is satisfied with upper equation. If e_k (about 1 m on the base station) and C_k are decided, the bias, b_k, which is greater than those values, can be detected.

The fading factor is multiplied Kalman gain by the form of a reciprocal number and this can be expressed as follows:

$$\bar{K}_k = \frac{1}{\bar{\alpha}_k} K_k = \frac{1}{\alpha_k + \beta_k} K_k \tag{3.23}$$

By using above equation, the difference between the Kalman gain without bias error, K_k and the Kalman gain with ramp type bias error, $\bar{K}_k$ is expressed as follows:

$$\begin{aligned} K_k - \bar{K}_k &= K_k - \frac{1}{\bar{\alpha}_k} K_k = K_k - \frac{1}{\alpha_k + \beta_k} K_k \\ &= \left(1 - \frac{1}{\alpha_k + \beta_k}\right) K_k = \left(\frac{\alpha_k + \beta_k - 1}{\alpha_k + \beta_k}\right) K_k \end{aligned} \tag{3.24}$$

As known above result, the Kalman gain with bias error is smaller than that of without bias error case. From this result, the estimation performance against the disturbance can be possible because the estimated value is more reliable the model than the measurement.

While the fading factor without bias does not exceed $\mathbf{T}$, the fading factor with bias is greater than 1 by β_k. Therefore, the detection is easy if the threshold, $\mathbf{T}$ for detection sets one. The related simulation results are presented on the next session.

3.3 Simulation

The proposed detection method can be applied for the base station or static user. The effect of spoofing signal is modeled by the ramp type bias error of the pseudorange in order to emulate smart spoofer.

In this thesis, the proposed method is distinguished from the previous methods [31] by detecting based on multiple base stations whose positions are already known and fixed. This method is designed for detecting comprehensively various spoofing scenarios and is verified by three simulations. The conditions of simulations are as follows: first, the spoofing effect is modeled by ramp type bias of pseudorange and secondly, only four satellites which are need at least for position estimation are considered. When DOP is calculated with these four satellites, PDOP is average of 6.4506 and GDOP is average of 8.1499. The change of the fading factor is presented by monitoring the change of pseudorange on each channel. It is assumed that spoofing signal is affected on the only one channel due to confirm the effect of the bias. Thus, spoofing signal is applied to only one channel as ramp type bias. The thermal noise is only considered when measurement is generated and pseudorange measurement noise of filter model sets about 5.5 m of standard deviation. In all simulations, spoofing signal is added as ramp type bias with the slope of 10 m/s on pseudorange of channel 2. In addition, total simulation time sets 1800 sec and spoofing signal is added after 500 sec.

First simulation is performed to analyze the effects of ramp type bias error on the fading factor which is used as the detection parameter. Figure 3.2 shows the change of the fading factor on channel 2 when ramp type bias is added on channel 2. Figure 3.3 shows the expansion of the Figure 3.2 to recognize well the change of the fading factor and the threshold. It is confirmed that the fading factor is greater than threshold due to bias error.

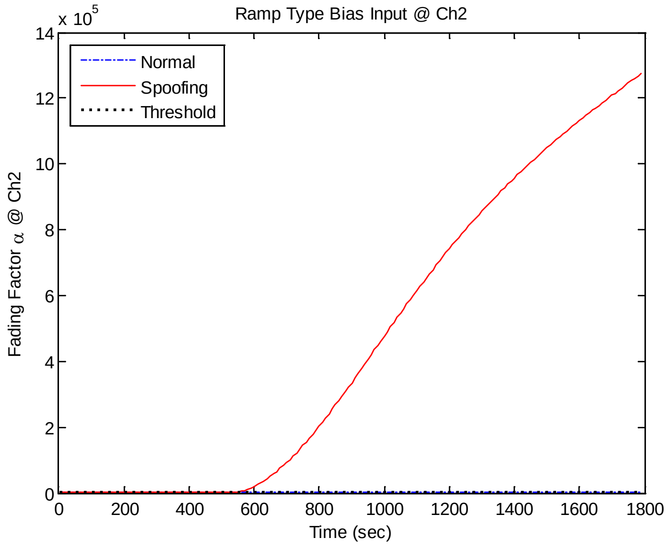

Figure 3.2 Fading factor of ch2

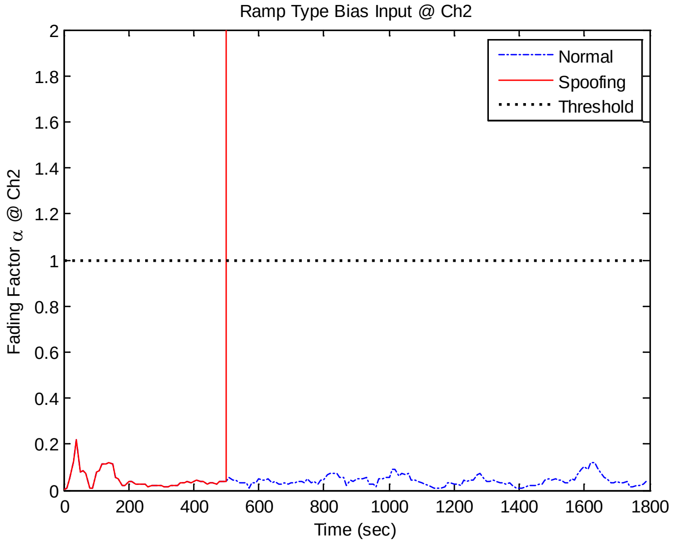

Figure 3.3 Fading factor of ch2 (expansion)

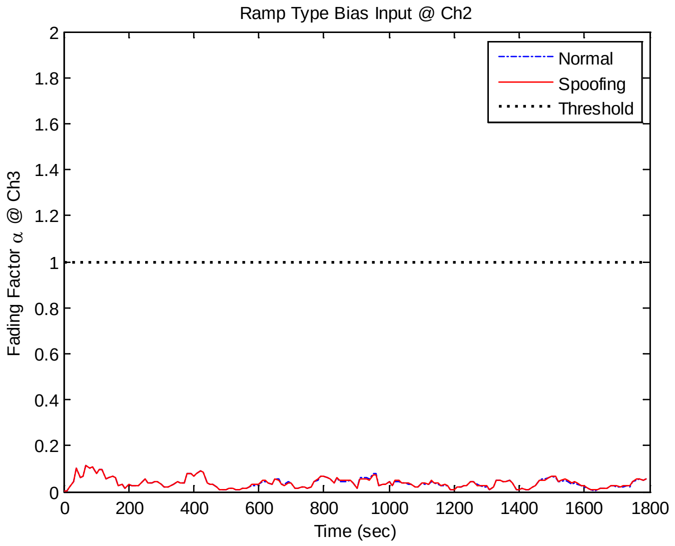

Figure 3.4 Fading factor of ch3

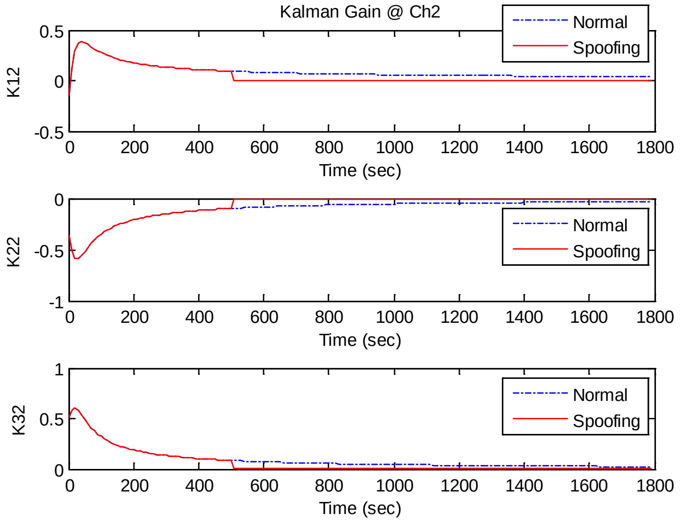

Figure 3.5 Kalman gain of ch2

Figure 3.4 shows the change of the fading factor on channel 3 when ramp type bias is added on channel 2. The fading factor does not change largely and is smaller than one because bias is not added on channel 3.

Second simulation is performed to analyze effects of fading factor on Kalman gain. Figure 3.5 shows the change of the Kalman gain on channel 2 when ramp type bias is added on channel 2. The Kalman gain related filter states are presented in order. As shown Figure 3.5, the Kalman gain is reduced by bias. It is reason that Kalman gain is adjusted by fading factor when bias is added. It has an effect on spoofing mitigation by reducing estimated error of bias inputs.

Third simulation is performed to analyze the detection performance of the proposed detection method. The position of the user is estimated by using pseudoranges of four channels. By using spoofing detection based on the adaptive fading Kalman filter, the spoofing detection results show Figure 3.4 through 3.10. Figure 3.6 shows the position error of static user when channel 2 is affected by spoofing signal. If the adaptive fading filter is not used, the estimated position error changes largely by ramp type bias error. However, if the adaptive filter is used, the estimated position error does not change. Table 3.2 shows the position result of proposed method by using adaptive fading Kalman filter. Figure 3.7 shows the change of the fading factor according to the pseudornage change of the GNSS signal. As shown in this figure, the fading factor of channel 2 increases when the bias exits. Figure 3.8 shows the difference between true and estimated pseudorange on each channel. From this figure, the ramp type bias error is generated by bias input comes from simulation scenario.

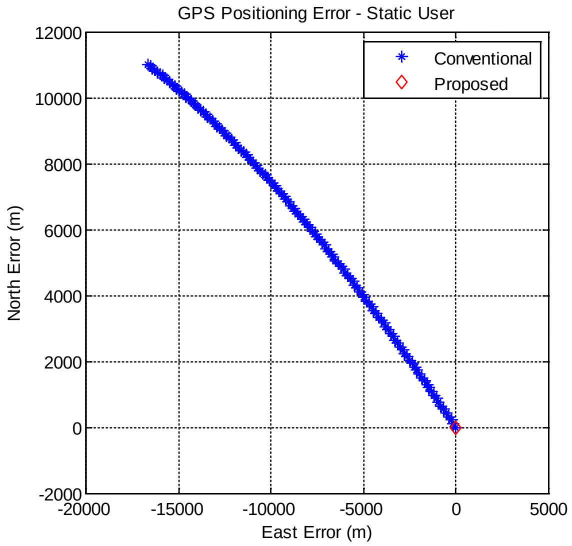

Figure 3.6 GPS position error of static user

Table 3.2 GPS position error of static user

	Conventional	Proposed
RMSE (m)	7424.2	1.4282

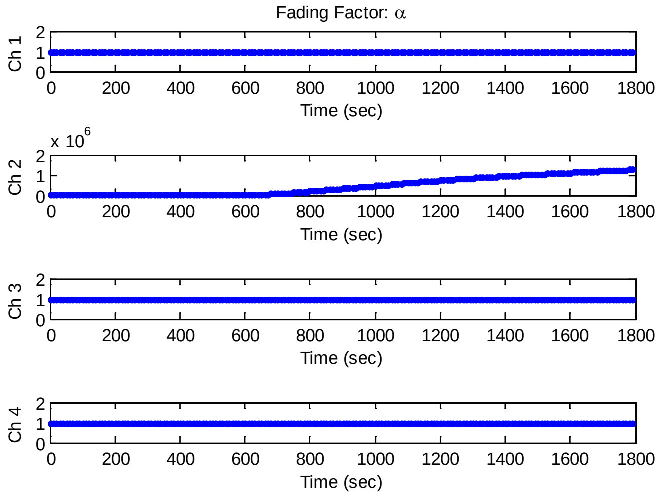

Figure 3.7 Fading factor as detection parameter

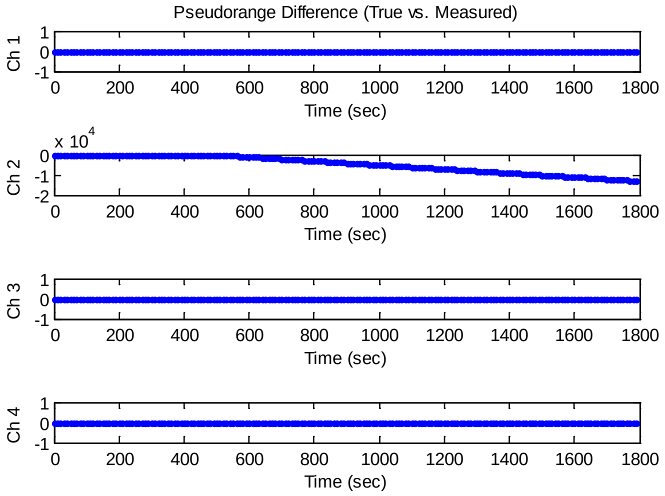

Figure 3.8 Pseudorange difference between true and measured

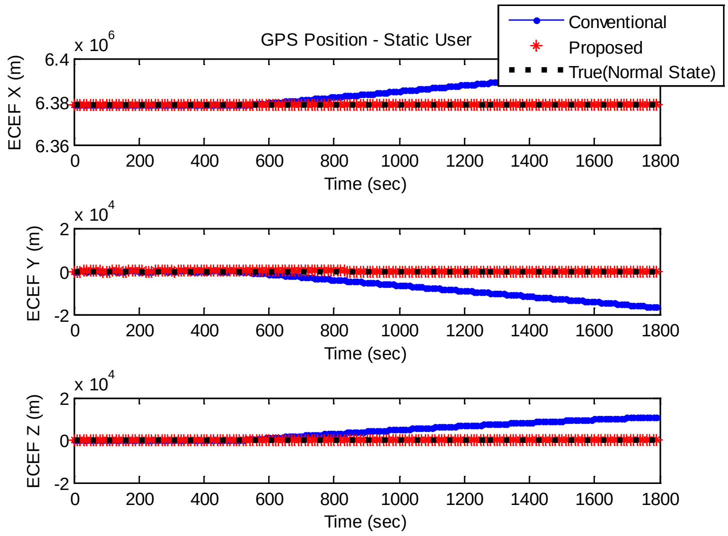

Figure 3.9 GPS position of static user

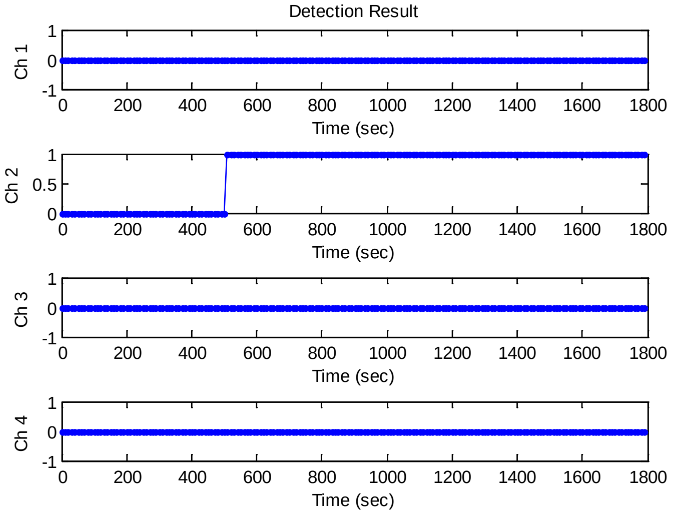

Figure 3.10 Detection Result

Figure 3.9 shows the estimated position of user by each method when spoofing signal affects. From the second simulation result, the effect of spoofing signal is minimized by multiplying fading factor gain to Kalman gain. Lastly, Figure 3.10 shows detection result. By setting detection threshold, it is considered spoofing signal does not exist and detection result can be expressed as 1 when fading factor is smaller than 1. If fading factor is greater than 1, it is considered spoofing signal exists and detection result can be expressed as 0. As shown this figure, spoofing signal is detected on channel 2 after 500 sec because spoofing signal is added on channel 2.

Chapter 4

Spoofing Localization Method

4.1 Introduction

If spoofing signal is detected by using the proposed spoofing detection method as mentioned in the previous chapter, spoofing localization method based on multiple base stations is performed to estimate spoofing location. To estimate the location of the signal source, localization method usually requires two or more base stations (BSs) [37]. In localization techniques, the estimation methods used for source localization are typically based on received signal strength (RSS), time of arrival (TOA) [38], time difference of arrival (TDOA) [39, 40], angle of arrival (AOA) [41], or their combinations [42, 43]. Despite of lower location accuracy with a small number of nodes in general, differential received signal strength (DRSS)-based localization is a cost-effective solution with low-complexity. Specifically, it is attractive because DRSS is readily available in most types of wireless systems, and does not require accurate knowledge of transmitter such as the transmitted power [44].

For that reason, in this thesis, spoofing location is estimated by using DRSS method [45]. The C/No measurement characterizes the RSS [46], therefore, the difference of the C/No between MS and each BS is used as measurement for DRSS method. In addition, the Cost231-Walfisch-Ikegami model is applied as path-loss model for calculating signal attenuation. The performance of the proposed method is evaluated by simple simulations.

4.2 DRSS Method

In a normal RSS localization system using the log normal fading path-loss model, the RSS can be expressed by

$$RSS_i = P_0 - 10n\log_{10}\left(\frac{d_i}{d_0}\right) + \sigma_i \tag{4.1}$$

where P_0 is the transmission power measured at a distance.

The difference of fading path-loss model eliminates the transmit power variable and it can be represented as follows:

$$DRSS_{i-j} = RSS_i - RSS_j = 10n\log_{10}\left(\frac{d_j}{d_i}\right) + \sigma_i - \sigma_j \tag{4.2}$$

where RSS_i is the signal strength of the source measured at base station i . d_i is the distance between the sensor and the spoofing source. n is the path-loss exponent of the propagation environment and its value is changed according to radio environment. σ_i is shadowing noise of radio propagation [44].

With the distance ratio between base stations, d_j / d_i , Eq. (4.2) can be rearranged as follows:

$$r_{ij} = {}^{d_j}\!/\!_{d_i} = 10^{\left(DRSS_{i-j}/10n\right)-(\sigma_i-\sigma_j)/10n} \tag{4.3}$$

The trajectory of Eq. (4.3) is shown in Figure 4.1. The distance ratio, $d_j / d_i = r_{ij}$, defines a circle trajectory [47]. It is shown that the estimated location of spoofing signal can be calculated by three DRSS circles at least. In other words, four base stations are needed for spoofing location by using DRSS method.

$$\left(x-x_{ij}\right)^2+\left(y-y_{ij}\right)^2=R_{ij}^2 \qquad (4.4)$$

where $x_{ij}=\dfrac{r_{ij}^2 x_j - x_i}{r_{ij}^2-1}$, $y_{ij}=\dfrac{r_{ij}^2 x_j - y_i}{r_{ij}^2-1}$, $R^2=x^2+y^2$,

$$R_{ij}^2=\left[\left(\frac{1}{r_{ij}^2-1}\right)^2+\frac{1}{r_{ij}^2-1}\right]\left[\left(x_i-x_j\right)^2+\left(y_i-y_j\right)^2\right]$$

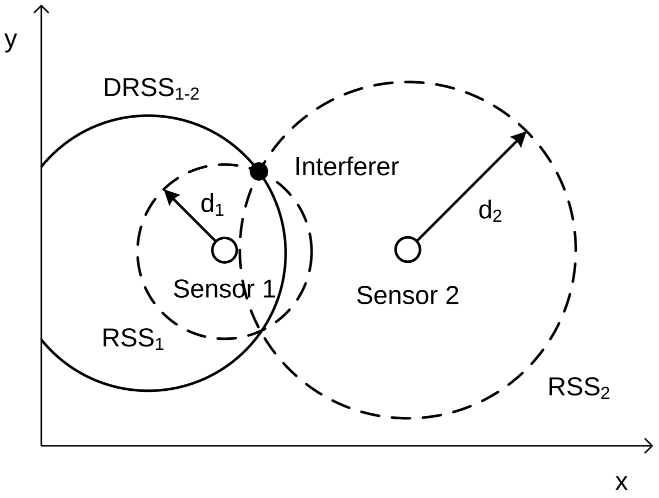

Figure 4.1 A DRSS equation by using the difference of RSS equations

In order to obtain an intersection point of DRSS circles, Eq. (4.5) can be expressed in matrix form. The equation for position estimation when four base stations are arranged can be expressed as bellows [37].

$$\mathbf{A}x_i=b \qquad (4.5)$$

where $\mathbf{A}=\begin{bmatrix} x_{12} & y_{12} & -0.5 \\ x_{13} & y_{13} & -0.5 \\ x_{14} & y_{14} & -0.5 \end{bmatrix}$, $b=\frac{1}{2}\begin{bmatrix} x_{12}^2+y_{12}^2-R_{12}^2 \\ x_{13}^2+y_{13}^2-R_{13}^2 \\ x_{14}^2+y_{14}^2-R_{14}^2 \end{bmatrix}$, $x_i=\begin{bmatrix} x \\ y \\ R^2 \end{bmatrix}$

The localization method using signal strength should need the path loss model. In order to estimate position by using RSS, the transmitted signal strength should be known. However, the transmitted signal strength of spoofing signal could not know because spoofing signal is intentional interference. Therefore, the difference of the received signal strength is used as a measurement for localization method. The strength of spoofing signal is weak than other intentional interferences because the power of spoofing signal is received alike signal power of GNSS signal in order to deceive GNSS signal. In addition, it is assumed that spoofing signal is located close to spoofing target. For that reasons, the path loss model which is applied to the propagation environment for short distance is used to estimate spoofing signal.

Therefore, the Cost231-Walfisch-Ikegami model and a Gaussian random variable are applied for the path loss and shadowing simulations, respectively. This model has some constraints as follows: frequency is between 800 MHz and 2,000 MHz, spoofer height is between 4 and 50 m, base station height is between 1 and 3 m, and the distance between spoofer and base station is between 0.02 and 5 Km. These values are calculated by using below equation when line of sight is valid.

$$L_{LOS}\ [dB]=42.6+26\log_{10} d\ [km]+20\log_{10} f\ [MHz] \tag{4.6}$$

where d is the distance between the sensor and the spoofing source, and f is the frequency of spoofing signal.

4.3 Simulation

The proposed spoofing localization method is applied to multiple base stations system. In order to arrange of multiple base stations, it is supposed that the signal power of spoofing signal sets -160 dBw (-130 dBm) and spoofing signal affects within a circle with radius of 300 m.

Figure 4.2 shows the arrangement of multiple base stations and the range of spoofing effect. Multiple base stations for spoofing localization consists of seven base stations. Six base stations (ID : 1 ~ 6) with a hexagon form are located around the main station (ID : M). The distance between each base station sets 300 m which is considered sufficiently including the range for spoofing signal detection. Table 4.1 shows the location of each base station.

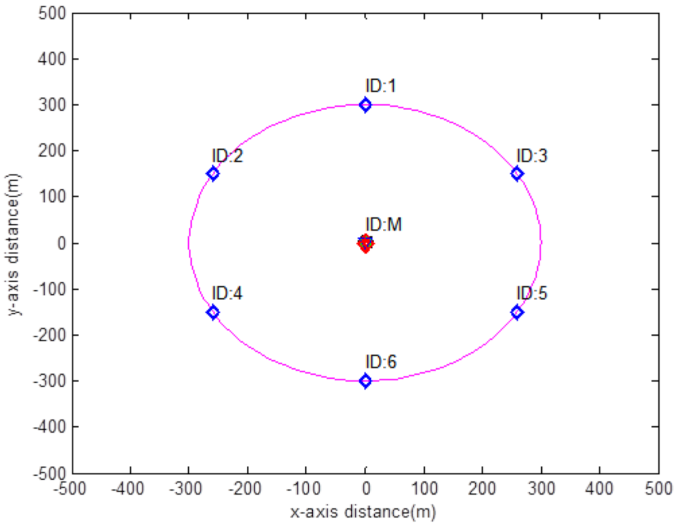

Figure 4.2 The arrangement of multiple base stations

Table 4.1 Locations of base stations

Station number	Location (m)
Base station 1	(0, 300)
Base station 2	(-260, 150)
Base station 3	(260, 150)
Base station 4	(-260, -150)
Base station 5	(260, -150)
Base station 6	(0, -300)

The basic unit cell of base stations is composed of seven base stations and it is extended around by the same way. This arrangement is effective to improve energy efficiency by using circle-based scheme. This method is used to wireless sensor network and it is one of the sleep scheduling method. The concept of this method as follows: seven base stations are operated for estimating the position of spoofer by activating sub base stations when spoofing signal is detected, while the main base station of basic unit cell is only operated when it is normal state.

Computer simulations have been conducted to evaluate the performance of the proposed DRSS-based location method. Two scenarios are used to verify the performance of the proposed method. For simulations, it is assumed that spoofing signals are located on different position within the range for spoofing detection.

The first scenario is supposed that the location of spoofing signal is at (0,200). The second scenario is supposed that spoofing signal is located on (100,150). The estimation results are shown as Figure 4.3 and 4.4, respectively. The range affected by spoofing signal is presented as magenta solid line. The base stations which detect spoofing signal are presented as red diamond and the base stations which is failed to detect spoofing signal are presented as blue diamond. In addition, the estimated position is shown as black circle. The DRSS circles are shown as cyan dotted line. In order to verify the performance of the proposed method, the scenario is performed by Monte-Carlo simulations on the basis of 100 iterations. The result of localization for each scenarios shows in Table 4.2.

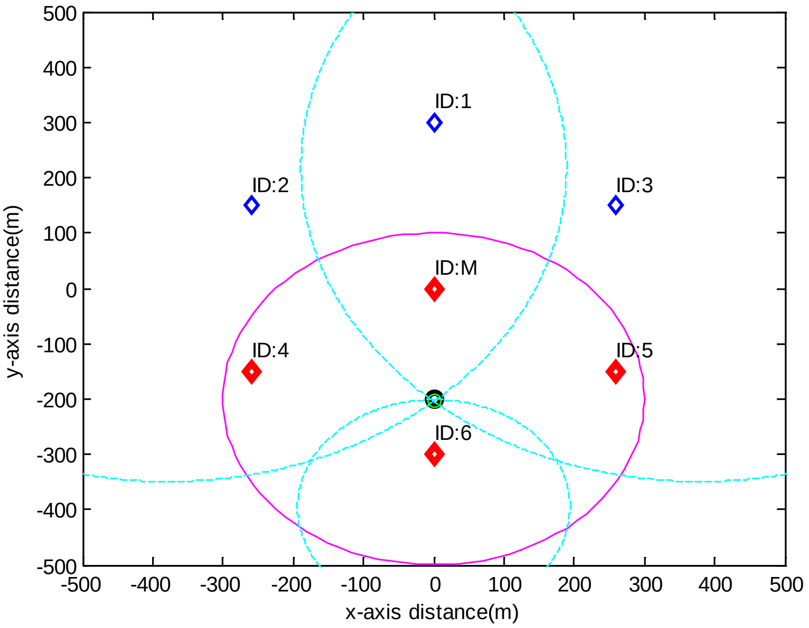

Figure 4.3 Result of localization in the first scenario

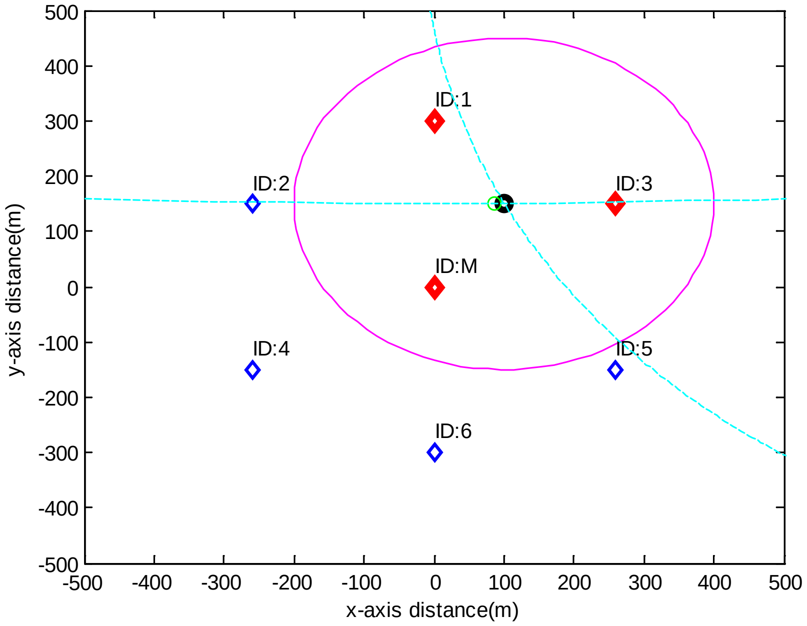

Figure 4.4 Result of localization in the second scenario

Table 4.2 RMSE of localization

	Scenario 1	Scenario 2
RMSE (m)	3.4290	13.3975

The localization of spoofing signal using DRSS method is verified its performance by simulations. The proposed method based on multiple ground stations can find the localization of spoofing signal efficiently on bad condition. The estimation error of spoofing localization is relatively small, but the performance depends on arrangement of multiple ground stations.

The performance of the proposed method is analyzed by simulations and a circle-based scheme is applied for effective operation of multiple base stations in real situation. By analyzing simulations, the proposed arrangement and operation of multiple base stations improves the estimation performance. The estimated position error is affected according to spoofing position and arrangement between base stations. However, even if the number of active base stations is changed, the estimated position error converged to a few meters when spoofing signal is located within designated hexagon form.

Chapter 5

Conclusions

In this thesis, the vulnerability of GNSS and various types of unintentional interference signal are introduced. Among others, this research is focused on spoofing signal which is the most threaten.

In order to detect and mitigate spoofing signal, a spoofing detection method based on adaptive fading Kalman filter is proposed. The fading factor of the filter is used as a detection parameter. For simulations and quantitatively analysis of the filter parameter, the effect of the spoofing is modeled by the ramp type bias error of the pseudorange to emulate a smart spoofer. In order to verify the performance analysis of the proposed spoofing detection, simple simulations are implemented. If the bias error exists, the fading factor is greater than the detection threshold by increasing the fading factor. Therefore, spoofing signal can be detected by monitoring the change of the fading factor. In addition, it is confirmed that the spoofing detection method works well through simulations when multi-channel error exist.

If spoofing signal is detected, a spoofing localization method is applied to remove spoofing signal source. To estimate the location of spoofing signal, the spoofing localization method based on multiple base stations is proposed and spoofing location is estimated by differential received signal strength (DRSS) method. The performance of the proposed method is analyzed by simulations and a circle-based scheme is applied for effective operation of multiple base stations in real situation. By analyzing simulations, the proposed arrangement and operation of multiple base stations improves the estimation performance. The estimated position error is affected according to spoofing position and arrangement between base stations. However, even if the number of active base stations is changed, the estimated position error converged to a few meters when spoofing signal is located within designated hexagon form.

In this thesis, the proposed spoofing detection and localization method can be applied for integrity monitoring algorithm in case of fixed user because it can detect abnormal pseudorange of each channel. In addition, this method is expected to be easily applied to practical system because they do not need to additional hardware and realization of complex algorithm.

Bibliography

[1] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, and B. W. O’hanlon, J. A. Bhatti, and T. E. Humphreys, “Signal Characteristics of Civil GPS Jammers,” *ION GNSS 2011*, 2011, pp. 1907-1919.

[2] Y. B. Park, C. G. Park, K. H. Lee, and M. J Yu, "Assessment of Long Delay Meaconing Mitigation Based on Subspace Projection During Signal Acquistion," *ENC-GNSS 2014*, 2014.

[3] Ali Jafarnia Jahromi, “GNSS Signal Authenticity Verification in the Presence of Structural Interference,” *UCGE Reports*, 2013.

[4] S. Y. Kim, C. H. Kang, J. H. Yang, and C. G. Park, "Performance Analysis of Interference on the Software GPS Receiver," *GNSS Workshop 2011(in Korean)*, 2011.

[5] I. W. Joo, C. S. Sin, J. H. Kim, and J. H. Lee, “Technical Trends of Monitoring GPS Jamming,” *Electronics and Telecommunications Trends*, Vol. 26, 2011, pp. 115-122.

[6] J. H. Yang, C. H. Kang, S. Y. Kim, and C. G. Park, "Intentional GNSS Interference Detection and Characterization Algorithm using AGC and Adaptive IIR Notch Filter," *IJASS 2012*, 2012.

[7] J. H. Yang, C. H. Kang, S. Y. Kim, and C. G. Park, "Design of GNSS Interference Simulator using MATLAB SIMULINK," *KGS 2012(in Korean)*, 2012.

[8] S. Y. Kim, C. H. Kang, J. H. Yang, and C. G. Park, "Performance Analysis of GNSS Interference Detection Parameters," *KGS 2012(in Korean)*, 2012.

[9] S. Y. Kim, C. H. Kang, J. H. Yang, C. G. Park, J. M. Joo, and M. B. Heo, "A GNSS

Interference Detection Method Based on Multiple Ground Stations," *Journal of the Korean GNSS Society*, Vol. 1, No. 1, 2012, pp. 15-21.

[10] S. Y. Kim, C. H. Kang, J. H. Yang, C. G. Park, M. B. Heo, and M. J. Yu, "GNSS Interference Detection using Adaptive notch filter," *KSAS Spring Conference 2012(in Korean)*, 2012.

[11] C. H. Kang, S. Y. Kim, J. H. Yang, and C. G. Park, “Detection and Characterization Algorithm of Swept Continuous Wave Interference for Safe GBAS Operation,” *ION GNSS 2012*, 2012.

[12] C. H. Kang, S. Y. Kim, J. H. Yang, and C. G. Park, “Adaptive Cascading IIR Notch Filter for GNSS Interference Detection,” *IGNSS 2012*, 2012.

[13] C. H. Kang, J. M. Joo, M. J. Yu, and C. G. Park, “Tracking Algorithm of Chirp Type GNSS Interference in a GNSS Receiver,” *KIMST Annual Conference 2013(in Korean)*, 2013.

[14] C. H. Kang, S. Y. Kim, and C. G. Park, “A Novel Detection and Tracking Algorithm of Chirp Type Civilian GNSS Interference,” *ION GNSS 2013*, 2013.

[15] C. H. Kang, S. Y. Kim, and C. G. Park, “A GNSS interference identification using an adaptive cascading IIR notch filter,” *GPS Solutions*, Vol. 18, No. 4, 2014, pp. 605-613.

[16] C. H. Kang, S. Y. Kim, and C. G. Park, “A GNSS Interference Identification and Tracking based on Adaptive Fading Kalman Filter,” *IFAC 2014*, 2014.

[17] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications*, Artech House, Norwood, MA, 2006.

[18] Y. B. Park, C. H. Kang, and C. G. Park, "Analysis of GPS Meaconing Effects on

GPS Receiver," *KGS 2013(in Korean)*, 2013.

[19] S. Y. Kim, C. H. Kang, C. G. Park, M. B. Heo, and M. J. Yu, "A Detection Method of GNSS Meaconing Signal using C/No," *KSAS Spring Conference 2014(in Korean)*, 2014.

[20] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS Signal Spoofing," *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation*, Long Beach, CA, 2005.

[21] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," *ION GNSS 2008*, 2008.

[22] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer," *ION 2009 International Technical Meeting*, 2009.

[23] S. H. Im and G. I. Jee, "The Effects of Spoofing on GNSS Receiver and Anti-spoofing methods," *Journal of Institute of Control, Robotics, and Systems*, Vol. 18, No. 4, 2012*(in Korean)*, pp. 34-45.

[24] S. H. Im, J. H. Im, G. I. Jee, and M. B. Heo, "An Analysis of Spoofing Effects on a GNSS Receiver Using Real-Time GNSS Spoofing Simulator," *Journal of Institute of Control, Robotics and Systems(in Korean)*, Vol. 19, No. 2, 2013, pp. 113-118.

[25] C. H. Kang, S. Y. Kim, C. G. Park, M. B. Heo, and M. J. Yu, "GPS Spoofing Detection Algorithm using a GPS Tracking Antenna," *The 4th Surveillance, Reconnaissance, and Intelligence Conference(in Korean)*, 2014.

[26] C. H. Kang, S. Y. Kim, C. G. Park, J. M. Joo, and M. B. Heo, "GPS Spoofing Detection Using GPS Antenna-Movement Effects," *ISGNSS 2014*, 2014, pp. 896-901.

[27] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS Spoofer countermeasure effectiveness based on signal strength, noise power, and C/No measurements,” *International Journal of Satellite Communications and Networking*, Vol. 30, 2012, pp.181-191.

[28] J. Nielsen, V. Dehghanian, and G. Lachapelle, “Effectiveness of GNSS Spoofing Countermeasure Based on Receiver CNR Measurements,” *International Journal of Navigation and Observation*, Vol. 2012, 2012.

[29] M. L. Psiaki, S. P. Powell, and B. W. O’Hanlon, “GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data,” *ION GNSS 2013*, 2013.

[30] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS Spoofing Detection Based on Signal Power Measurements: Statistical Analysis," *International Journal of Navigation and Observation*, Volume 2012, 2012.

[31] A. J. Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques,” *International Journal of Navigation and Observation*, Vol. 2012, 2012.

[32] D. Simon, *Optimal State Estimation*, John Wiley & Sons, Inc., USA, 2006.

[33] R. G. Brown and P. Y. C. Hwang, Introduction to random signals and applied Kalman filtering, 3rd Ed., John Wiley & Sons, Inc., USA, 1997.

[34] C. H. Kang, S. Y. Kim, C. G. Park, J. M. Joo, and M. B. Heo, “Design of the Vector-tracking Loop Based on an Adaptive Fading Kalman Filter,” *ENC 2014*,

2014.

[35] K. H. Kim, J. G. Lee, and C. G. Park, “Adaptive Two-Stage Extended Kalman Filter for a Fault-Tolerant INS-GPS Loosely Coupled System,” IEEE Transactions on Aerospace and Electronic Systems, Vol. 45, No. 1, January 2009, pp. 125-137.

[36] M. J. Yu, “INS/GPS Integration System using Adaptive Filter for Estimating Measurement Noise Variance,” *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 48, No. 2, pp. April 2012, 1786-1792.

[37] K. W. Cheung, H. C. So, W. K. Ma, and Y. T. Chan, “Least Squares Algorithms for Time-of-Arrival-Based Mobile Location,” *IEEE Transactions on Signal Processing*, Vol. 52, No. 4, 2004. pp. 1121-1128.

[38] A. Panwar, A. Kumar, and Sh. A. Kumar, “Least Square Algorithms for Time of Arrival Based Mobile Source Localization and Time Synchronization in Wireless Sensor Networks,” *International Conference on Computer Communication and Networks CSI-COMNET-2011*, 2011, pp. 81-84.

[39] Y. Weng, W. Xiao, and L. Xie, “Total Least Squares Method for Robust Source Localization in Sensor Networks Using TDOA Measurements,” *International Journal of Distributed Sensor Networks*, Vol. 2011, 2011.

[40] J. I. Kim, “A Mitigation of Non-Line-of-Sight by TDOA Error Modeling in Wireless Communication Networks,” Master’s Thesis, Seoul National University, 2007.

[41] A. G. Dempster, “Dilution of precision in angle-of-arrival positioning systems,” *Electronics Letters*, Vol. 42, No. 5, 2006.

[42] R. T. Juang, D. B. Lin, and H. P. Lin, “Hybrid SADOA/TDOA mobile positioning

for cellular networks," *IET Communications*, Vol. 1, No. 22, 2007, pp. 282-287.

[43] E. Kim and K. Kim, "Distance Estimation With Weighted Least Squares for Mobile Beacon-Based Localization in Wireless Sensor Networks," *IEEE Signal Processing Letters*, Vol. 17, No. 6, 2010, pp. 559-562.

[44] C. H. Kang, S. Y. Kim, J. H. Yang, C. G. Park, "Study on Interference Localization using DRSS/AOA Integrated Method," *KGS 2012(in Korean)*, 2012.

[45] S. Y. Kim, C. H. Kang, and C. G. Park, "A Spoofing Localization using DRSS based on Multiple Ground Stations," *KSAS Spring Conference 2013(in Korean)*, 2013.

[46] J. B.-Y. Tsui, *Fundamentals of Global Positioning System Receivers A Software Approach*, John Wiley & Sons, Inc, Hoboken, New Jersey, 2005.

[47] R. T. Juang, D. B. Lin, and H. P. Lin, "Hybrid SADOA/TDOA Location Estimation Scheme for Wireless Communication Systems," *VTC 2006*, 2006, pp. 1053-1057.

국문초록

위성항법시스템은 인공위성을 이용하는 전파항법시스템으로 사용자의 위치 및 시각을 정밀하게 측정할 수 있어 국방뿐 아니라 다양한 민수분야에서 광범위하게 활용되고 있다. 그러나 약 2만킬로미터 상공으로부터 수신기에 도달하는 위성항법신호의 세기는 잡음 레벨 이하이므로 전파교란신호에 취약하다는 단점이 있다.

전파교란신호는 크게 자연적인 전파교란신호와 인위적인 전파교란신호로 구분할 수 있는데, 그 중에서 인위적인 전파교란신호는 특정 목적에 의해서 시스템에 악영향을 주므로 이에 대응하는 연구가 필요하다. 인위적인 전파교란신호는 재밍, 미코닝, 기만신호로 나눌 수 있고 이중에서 기만신호는 실제 위성항법신호를 그대로 모사하여 수신기를 기만시킨 후에 잘못된 항법해를 유발시키기 때문에 심각한 결과를 초래할 수 있다. 따라서 본 논문에서는 기만신호에 대한 대응기법으로 다중 기준국 기반에서 항법해 품질을 감시하기 위해 기만신호를 검출하고 위치를 추정하는 방법에 대한 연구를 진행하였다.

기만신호를 검출하는 방법은 검출 파라미터 및 기만 시나리오에 따라 다양한 방법들이 있으며 최근 몇 년 동안 연구가 활발히 진행되고 있다. 본 논문에서는 다양한 기만 시나리오를 포괄적으로 검출하기 위한 방법으로 이미 알고 있는 고정된 위치의 기준국 기반에서 적응 페이딩 칼만 필터의 페이딩 팩터를 검출 파라미터로 사용한 검출방법에 대해서 소개하였다. 이때 기만신호는 스마트 기만 시나리오를 모사하여 그 영향을 램프 바이어스 형태의 의사거리 오차로 모델링 하였다. 또한 이에 따른 페이딩

팩터 변화값을 정량적으로 분석하였고 분석결과를 바탕으로 기만신호 검출을 위한 임계치를 설정하였다. 이 방법은 최종적으로 페이딩 팩터로 칼만 게인을 조절함으로써 기만신호의 영향을 완화시키는 효과도 나타났다.

앞에서 설명한 기만신호 검출 방법을 이용하여 기만신호가 있다고 판단하면 다중 기준국에서의 측정치를 통해 기만신호원의 위치를 추정하게 된다. 전파간섭원의 위치를 추정하는 방법은 사용하는 측정치에 따라 다양하게 분류되는데 본 논문에서는 주기준국을 기준으로 하여 각 기준국에서 수신된 신호세기차이를 이용하여 위치를 추정하였으며, 이때 신호세기 측정치로 C/No를 사용하였고 시뮬레이션을 위해 전파손실모델은 COST231-Walfisch-Ikegami 모델을 사용하여 신호감쇄를 계산하였다.

본 논문에서 제안한 검출 및 위치추정 기법은 각각 간단한 시뮬레이션을 통해 성능을 분석하였다. 이러한 방법은 채널별 의사거리 이상을 검출할 수 있으므로 사용자의 위치가 고정된 경우 무결성 감시 알고리즘으로 사용이 가능할 것으로 기대된다. 또한 추가적인 하드웨어나 복잡한 알고리즘 구현이 필요하지 않아 실용적인 측면에서 유용할 것으로 기대된다.

주요어: GNSS 기만신호, 기만신호 검출, 기만신호 위치추정, 다중 기준국

이 름: 김 선 영

학 번: 2013-20649