한국통신학회논문지(J-KICS) '13-11 Vol.38C No.11
http://dx.doi.org/10.7840/kics.2013.38C.11.1044

역 위상 코드를 이용한 기만신호 대응방법

김 태 희◆, 이 상 욱°, 김 재 훈*

The Anti-Spoofing Methods Using Code Antiphase of Spoofing Signal

Taehee Kim◆, Sanguk Lee°, Jaehoon Kim*

요 약

본 논문은 ETRI에서 개발한 GPS RF 신호생성기와 상용수신기인 U-Blox 수신기를 이용하여 기만신호의 공격을 완화하는 방법에 대하여 분석하였다. 기만신호는 대상 수신기의 코드 및 반송파 성분의 변이를 이용하여 대상 수신기가 비정상적인 위치를 생성하도록 하는 것이다. 우리는 이러한 기만신호 공격에 따른 수신기에서의 신호세기 및 항법해 영향을 분석하였다. 또한 기만신호를 제거하기 위하여 기만신호와 역위상 코드를 가지는 신호를 고려하였다. GPS RF 신호생성기를 이용하여 정상적인 GPS 신호, 기만신호, 기만신호와 역위상을 가지는 항기만신호를 생성하였고 기만신호와 항기만신호간의 코드 위상차이에 따른 기만신호 공격의 영향을 수신기를 통하여 확인하였다. 기만 신호의 코드 지연과 동일한 코드지연의 신호를 생성할 경우 기만신호가 상쇄되는 것을 확인하였다.

Key Words : Spoofing, Anti-Spoofing, GPS

ABSTRACT

This paper analyzes what is mitigated as spoofing attack using the U-Blox Receiver and GPS RF signal generator developed at ETRI. Generally the spoofing attack made the target receiver to be wrong navigation solution by providing false measurement of code and carrier. So we analyzed the impact of spoofing attack through the signal strength and navigation solution. In oder to test of effect of anti-spoofing signal, we consider the signal with antiphase code to spoofing signal and generated GPS normal signal and spoofing signal and anti-spoofing signal using GPS RF signal generator. This paper analyzed that the GPS receiver was responded to the spoofing attack according to code phase difference between spoofing and anti-spoofing signal. We confirmed that the spoofing signal was disappeared by anti-spoofing signal if code phase is an exact match.

Ⅰ. 서 론

최근 위성항법 시스템은 군사적 목적 이외에 사회 전 분야에서 활용하고 있다. 예를 들어 위성항법 시스템에서 제공하고 있는 시각 및 위치에 대한 정보를 이용한 시스템간의 시각동기, 개인 항법이 주를 이루며 더 나가 인명구조, 화제진화 등의 사회안전분야로 확대할 수 있다. 반면 이러한 위성항법시스템의 활용을 개인적 목적 또는 사회혼란을 야기할 목적으로 재밍 및 기만등과 같은 악의적 신호를 발생하는 사건들이

※ 본 연구는 방송통신위원회의 2012년도 방송통신 연구개발사업의 일환으로 수행하였음. [2012-S-301-01,다원화 항법주파수 감시 및 이용기술 개발]
◆ First Author : 한국전자통신연구원 위성항법연구실, thkim72@etri.re.kr, 정회원
° Corresponding Author : 한국전자통신연구원 위성항법연구실, slee@etri.re.kr, 정회원
* 한국전자통신연구원 위성항법연구실, jhkim@etri.re.kr, 정회원
논문번호 : KICS2013-08-375, 접수일자 : 2013년 8월 30일, 최종논문접수일자 : 2013년 10월 28일

발생하고 있다. GPS 신호에 대한 전파교란의 형태는 크게 GPS 신호가 사용하는 주파수 대역에서 GPS 수신 세기보다 높은 신호를 송출하는 형태인 재밍(Jamming)과 항법수신기로 하여금 잘못된 위치 및 시각정보를 산출토록 하는 기만(Spoofing)으로 나눌 수 있다.[1] 재밍신호는 위성항법 신호가 먼 거리의 위성으로부터 전송되는 신호세기(-163dBW)특성을 이용하여 훨씬 강한 신호를 톤, 협대역, 광대역 신호를 발생하여 위성항법 수신기를 무력화 하는 반면 기만신호는 위성항법 신호보다 3-5dB 높은 신호레벨로 신호의 코드지연 및 반송파 변이를 이용하거나 항법메시지 내의 궤도데이터 및 시각정보를 변경하여 수신기의 항법해를 혼란시키는 것이다. 기만신호의 다양한 피해사례로 미국의 경우 이라크 및 아프가니스탄 지역 등에서 진행한 군사작전 중에 유도무기 일부가 당초 목표로 했던 장소가 아닌 지역에 떨어져 민간인 피해가 발생한 적이 있다. 이와 같은 형태는 GPS 항법신호를 처리하는 수신기가 자신이 현재 전파교란을 당했는지를 감지하지 못하여 발생한 것으로 추후에도 항법수신기의 위치 및 시각정보를 그대로 믿고 군사작전을 감행할 경우, 상당한 피해가 발생할 가능성이 높다고 할 수 있다[1]. 따라서 이러한 악의적 의도로 전송하는 신호에 대한 대응이 필요하며 본 논문에서는 기만신호에 대한 대응 방법을 제시하고자 한다.

Ⅱ. 본 론

2.1. 기만신호특성

GPS 기만신호는 GPS 신호와 동일한 구조를 가지며, 기만공격 대상 수신기가 정확한 위치 및 시각을 구하지 못하도록 거짓된 위성 궤도정보 및 시각 오차정보를 변경하여 항법메시지에 포함하거나 잘못된 코드 및 반송파 변이를 인가한 신호를 갖는다. 즉 기만신호 생성기는 기만대상 수신기가 수신 가능하도록 GPS 위성신호와 동일한 코드, 주파수, 항법메시지, 신호세기 등을 기만대상 수신기의 위치를 고려하여 신호를 생성하여 방송해야 한다[2]. 기만신호 세기는 기만신호 생성기와 기만대상 수신기 간의 거리 및 주변 환경에 따라 변화가 심하고, 수신기에서는 수신된 신호 세기를 비교하여 기만신호임을 판단할 수 있으므로, 기만신호 생성기는 기만 범위를 정하여 기만신호 생성기와 기만대상 수신기 사이의 거리로부터 신호세기를 조정하여 생성한다[3]. 다음은 GPS L1 C/A 위성항법신호를 수식으로 나타낸 것이다.

$$S_{L1} = AC(t)D(t)\cos(w_{L1}(t)+\phi_0) \quad (1)$$

S_{L1}은 시간 t에서 정상적으로 입력되는 GPS 신호를 나타내며, 수식(1)에서 A는 GPS 신호의 전력, $C(t)$는 코드위치, $D(t)$는 데이터 비트, $\cos(w_{L1}(t)+\phi_0)$는 주파수 성분을 나타낸다. 주파수 성분 중 $w_{L1}(t)$은 L1 주파수의 반송파 주파수 성분이며 ϕ_0는 GPS신호의 초기 위상값이다 .
일반적으로 기만신호는 정상신호보다 신호세기가 크며 코드의 시간지연이 발생하며 도플러의 변이 값이 존재하게 된다. 따라서 기만신호의 특성은 수식 2와 같이 나타낼 수 있다[4].

$$S_{L1}' = A' C(t-\tau)D(t)\cos((w_{L1}+\triangle w)(t)+\phi_0) \quad (2)$$

S_{L1}'은 시간 t에서 입력되는 기만신호를 나타내며, S_{L1}'의 A'는 기만신호의 전력으로 A보다 3~5dB 큰 값을 갖는다. $C(t-\tau)$는 기만신호의 코드값으로 t에서 τ 만큼의 지연된 시점의 코드위치의 코드값을 생성한다. τ는 1칩보다 작은 시간을 가져야 한다. $\cos((w_{L1}+\triangle w)(t)+\phi_0)$는 기만신호의 주파수 성분으로 $\triangle w$ 만큼의 도플러 변이가 발생한다.
다음 그림 1은 위성에서 전송하는 정상적인 항법신호(S_{L1})와 기만기에서 전송하는 기만신호(S_{L1}')를 수신기에서 수신하는 것을 나타내고 있다.

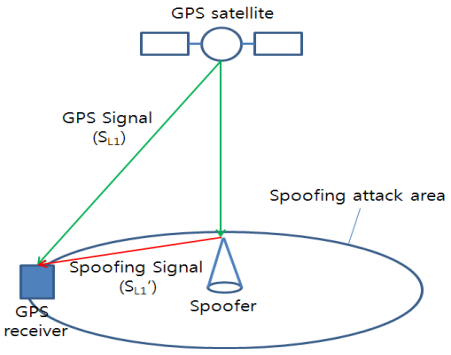


그림 1. 기만 공격 개념
Fig. 1. The Concept of Spoofing attack

기만신호를 생성하는 첫 번째 방법으로 GPS 시뮬레이터와 같이 GPS와 동기되지 않은 임의의 항법 신호를 생성하여 송출하는 방법이 있다. 이와 같은 기만신호 생성방법은 보다 간단한 구조로 기만신호를 생성

하며 공격 대상 수신기는 불특정 다수를 기만하는 방법이다. 두 번째 방법으로 현재 GPS 신호를 수신하여 GPS와 동기된 기만된 항법신호를 생성하는 방법이 있다. GPS수신기를 부착하여 기만신호를 생성하는 방법은 공격 대상수신기가 GPS와 동기된 기만신호, 즉 GPS 신호와 유사한 신호를 수신하기 때문에 기만신호 판단이 어려운 장점을 가지고 있다[5]. 이와 같은 공격은 이동통신 기지국, DGPS기준국과 같이 사용자의 위치가 고정된 환경에서 효과적으로 동작할 수 있다.

2.2. 기만신호 대응 방법

기만공격에 대한 대응 측면을 위성에서 대응과 수신기에서의 대응 두 가지로 나눠볼 수 있다.

2.2.1. 위성측면에서 기만대응 방법

위성측면에서 대응방법으로 미국에서 제시하고 있는 GPS 신호에 사용자 인증과 관련된 요소를 추가하여 신호를 송신하는 방법이다. 따라서 기만기는 해당 인증장비를 추가한 수신기는 기만공격을 할 수 없게 된다. 기만 신호 관련하여 일반적으로 GPS L1 C/A 코드에 대해 이루어진다. 이는 해당 코드에 인증 및 인코딩과 같은 기능이 포함되지 않아 해당 서비스를 제공 받는 사용자를 손쉽게 기만할 수 있기 때문이다. 따라서 새롭게 발사되는 GPS 위성에 해당 코드에 인증 및 인코딩 기능을 추가하여 사용자는 인증 및 인코딩 모듈을 추가하여 기만 신호의 영향을 제거하고자 한다. 이는 기만신호의 발생 원인을 제거함으로써 기만에 대처하는 방안이다. 그러나 이러한 방법은 수신기에서 해당 인증코드에 대한 처리를 수행하기 때문에 기존의 GPS 수신기의 수정 및 교체가 필요한 문제점을 가지고 있다.

2.2.2. 수신기측면에서 기만대응 방법

수신기 측면에서 대응방법은 수신기에서 기만신호에 대한 검출을 수행하고 대응하는 것이다. 기만공격이 발생하면 수신기는 기만공격을 다양한 방법으로 검출할 수 있어야 한다. 예를 들어 수신기에서 신호추적 동안 발생된 코드 및 도플러의 변화 정보를 저장하여 새로운 기만신호가 입력될 경우 기만신호를 인지할 수 있게 된다. 일반적으로 상용 수신기에서는 신호추적 결과를 생성되는 파라메터를 저장하지 않고 위치 산출 기능이 주가 되고 있다. 이러한 신호추적 결과를 저장할 경우 기만신호 발생 시 갑작스러운 신호추적 파라메터 변경이 발생한 경우 기만으로 손쉽게 판단할 수 있다. 또 다른 검출 방법으로 위성신호의 절대적 신호세기를 확인하고 신호 추적채널의 신호세기의 변화 감시, GPS L1, L2, L5 등의 서로 다른 주파수와의 상대적 신호세기 감시, 의사거리의 변화율 및 도플러 변화 감시 등이 있다[6,7].

기만신호에 대한 검출이 이루어지면 기만신호의 대응을 위하여 기만된 채널의 위성 PRN을 항법해를 산출하는데 이용하지 않는 방법이 있다. 이러한 대응 방법은 간단하면서도 효율적인 방법이다. 그러나 현재 상용으로 사용하고 있는 수신기에서는 이러한 기능이 포함되지 않아 새로운 펌웨어 수정이 요구된다. 또 다른 대응방법으로 RF 입력단에서 수신되는 기만신호를 제거하는 방법이 있다. 기만신호는 정상신호의 코드 및 반송파 성분의 변이를 가하므로 이러한 기만신호를 역위상을 갖는 코드 및 반송파를 발생하여 이를 제거하는 방법이다. 해당 방법은 기존 수신기의 수정이 필요 없으며 RF 입력단에 추가 장비를 부착하여 기만을 대응할 수 있는 장점이 있다.
다음 수식은 기만신호를 제거하기 위하여 역위상 코드가 반영된 신호를 나타낸 것이다.

$$S_{L1}'' = A' C'(t-\tau) D(t) \cos((w_{L1} + \triangle w)(t) + \phi_0) \quad (3)$$

수식 (2)에서 기만신호(S_{L1}')와 동일한 신호세기와 주파수를 A'와 $\cos((w_{L1} + \triangle w)(t) + \phi_0)$같이 일치한 후 기만신호($S_{L1}'$)의 $t-\tau$ 시점에서의 코드값인 $C(t-\tau)$에 역인 코드값인 $C'(t-\tau)$을 반영하여 신호를 생하여 기만신호와 결합하여 기만신호를 제거한다. 본 논문에서는 기만신호의 코드 지연값인 τ을 찾기 위하여 일정한 시간간격으로 이동하여 기만신호가 제거되는 시점을 확인하였다.

Ⅲ. 실 험

3.1. 실험 환경

본 논문에서는 역위상 코드성분을 가지는 신호를 발생하여 기만신호와 결합하여 기만신호를 제거하는 방법을 모의실험을 통하여 확인하였다. 다음 그림은 모의실험을 위한 환경으로 본 과제에서 개발한 RF 신호생성 보드에서 정상신호와 기만신호를 생성하여 상용수신기인 U-Blox 수신기에 인가하여 결과를 확인하였다.

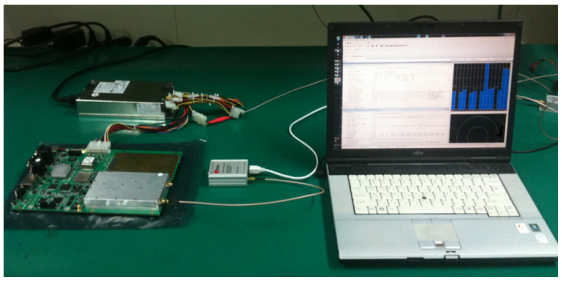


그림 2. 실험 환경
Fig. 2. Test Environment

3.2. 기만신호 영향 시험

기만신호 영향 시험을 위한 파라메터는 표 1에 정의하였다.

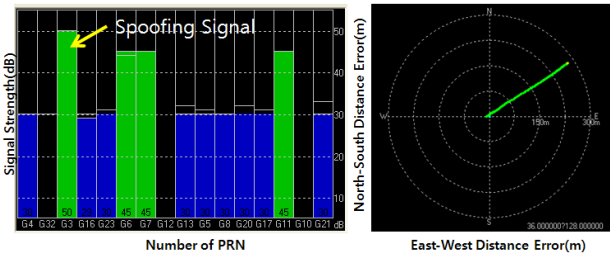
표 1. 기만신호 영향 시험을 위한 파라메터
Table 1. The parameter of spoofing

Parameter	Value
# of Channel	5
PRN of Normal Signal	3,6,7,11
PRN of Spoofing Signal	3
Code Delay of Spoofing	1chip
Receiver Position	Latitude : 36.000000 Longitude : 128.000000

그림 3은 기만신호를 생성하여 U-Blox수신기에 신호를 인가하였을 경우 수신기에서 신호세기와 항법해를 나타낸 것이다. 신호세기의 경우 3번 위성의 신호세기가 나머지 3개 위성의 신호세기보다 약 5 dB 높게 측정되고 있는 것을 확인할 수 있다. 이는 수신기가 정상신호세기보다 5 dB 높은 기만신호를 처리하고 있는 것을 보여주는 것이다. 또한 항법해 영향을 보면 정상신호만을 수신할 경우 수신기 좌표지점인 위도 36도, 경도 128도를 나타내나 기만신호가 인가된 후에 항법해가 북동방향으로 이동하는 것을 확인할 수 있다. 이는 기만된 신호를 수신기가 처리함으로써 기만된 의사거리를 측정하기 때문에 기만된 항법해가 생성된 것이다.

3.3. 기만신호 대응 시험

기만신호 대응 시험을 위한 파라메터는 표 2에 정의하였다.



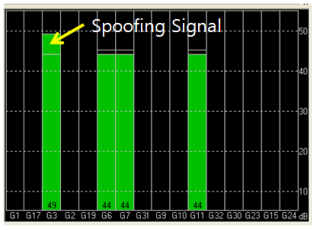
(a) Signal Strength (b) Navigation Solution

그림 3. 기만신호에 따른 신호세기 및 항법해 영향
Fig. 3. Signal strength and Navigation Solution according to Spoofing Sginal

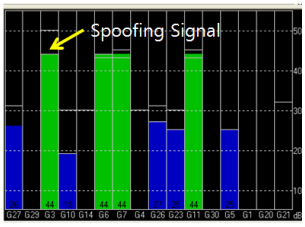
표 2. 기만신호 대응 시험을 위한 파라메터
Table 2. The parameter of Anti-spoofing

Parameter	Value
# of Channel	6
PRN of Normal Signal	3,6,7,11
PRN of Spoofing Signal	3
Generation time of Spoofing	100 sec
Generation time of Anti-Spoofing	150 sec
Code Phase difference between Spoofing and Anti-Spoofing	500nsec, 200nsec, 0nsec

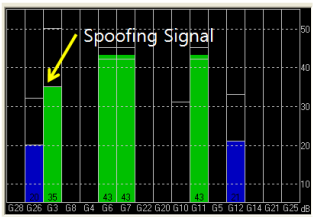
그림 4는 기만신호 대응 실험을 위하여 RF 신호생성기에서 정상신호와 기만신호를 발생한 경우 U-Blox 수신기에서 측정한 신호세기를 나타낸 것이다. 그림4의 (a)에서 보면 기만된 PRN 3번 위성의 신호세기가 다른 PRN 6,7,11위성보다 높게 측정되는 것을 확인할 수 있다. 그림 4의 (b)는 기만신호 대응을 위하여 역위상 코드를 기만신호와 500 nsec 차이를 가지면 신호를 생성했을 때 신호세기를 측정한 결과이며 (c)는 200 nsec 차이가 있을 때 신호세기를 측정한 것이다. 그림에서 보면 역위상 코드와 기만신호의 코드 간의 시각차이가 줄어들수록 신호세기가 감소되는 것을 확인할 수 있었다. 그림 4의 (d)에서 역위상 코드를 가지는 기만신호 대응 신호와 기만신호가 정확히 동기가 맞을 경우 완전히 기만신호가 제거되어 PRN 3의 신호세기가 잡음레벨로 측정되는 것을 확인할 수 있었다. 이는 기만신호의 코드와 반대 정보를 갖는 기만신호를 정확히 일치시킴으로써 기만신호를 완전히 제거할 수 있는 것을 검증한 것이다.



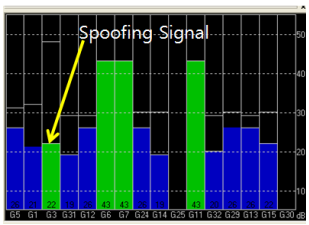
(a) No Anti-Spoofing



(b) Anti-Spoofing (500 nsec)



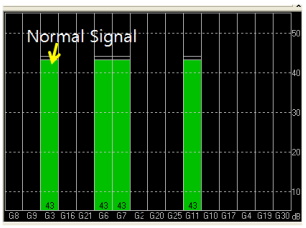
(c) Anti-Spoofing (200 nsec)



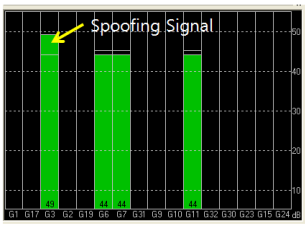
(d) Anti-Spoofing (0 nsec)

그림 4. 항기만신호의 위상에 따른 신호세기
Fig. 4. Signal strength of PRN according to code phase of anti-spoofing

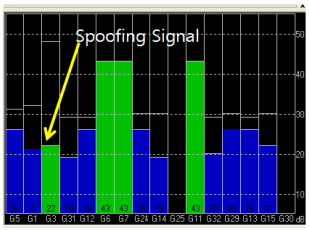
그림 5 와 6은 U-Blox 수신기에서 기만신호 및 기만신호와 코드위상이 정확히 동기된 항기만신호를 인가할 경우 신호세기 및 항법해 영향을 나타낸 것이다. 그림 5 와 6의 (a)는 신호생성 후 기만신호가 입력되지 않은 시점에서의 신호세기 및 항법해를 나타낸다. 신호세기는 다른 채널과 동일하게 측정되며 항법해 또한 수신기 좌표인 위도 36도 경도 128도인 위치에서 측정되는 것을 확인하였다. 그림 5 와 6의 (b)에서는 처음 신호생성 시점에서 100초 후 기만신호가 인가 될 경우 신호세기와 항법해를 나타낸 것이다. 기만신호가 인가된 시점에서 신호세기가 5 dB 높게 측정되며 항법해가 북동방향으로 이동하는 것으로 측정된다. 이는 기만신호의 영향으로 항법해가 비정상적으로 측정되는 것을 의미한다. 그림 5 와 6의 (c)는 기만신호 입력 후 50초 후 항기만신호가 인가된 시점에서의 신호세기 및 항법해를 나타낸 것이며 그림 5 와 6의 (d)에서 항기만신호에 의해 기만신호가 완전히 제거되고 정상신호만을 처리한 신호세기와 항법해를 나타내고 있다. 항기만신호가 인가되자 현재 처리하고 있는 기만신호의 세기가 급격이 줄어들고 기만신호 채널이 완전히 사라진 후 정상신호채널을 처리하므로 신호세기가 정상신호의 신호세기를 나타내고 항법해 또한 북동쪽으로 이동되는 항법해가 다시 원래의 수신기 좌표인 위도 36도 경도 128도인 위치로 이동하는 것을 확인하였다.



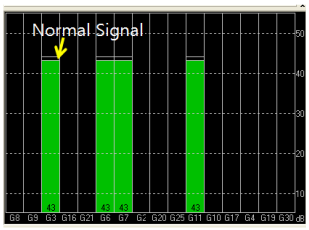
(a) Normal Signal Only



(b) Spoofing Generation



(c) Anti-Spoofing (0 nsec)



(d) Spoofing Elimination

그림 5. 기만신호 및 항기만신호(코드위상차 0nsec) 입력에 따른 신호세기
Fig. 5. Signal strength of PRN according to spoofing and anti-spoofing(code phase 0nsec) signal

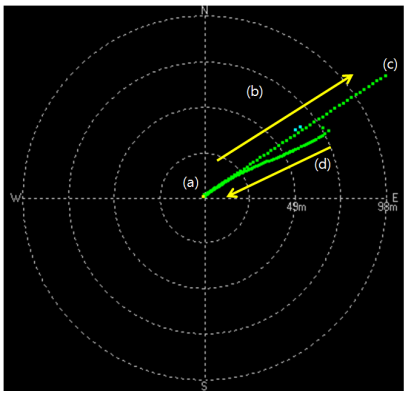
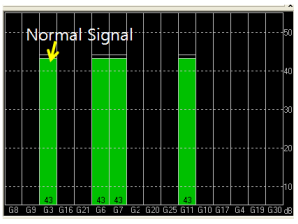
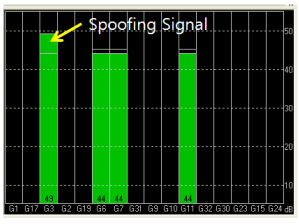


그림 6. 기만신호 및 항기만신호(코드위상차 0nsec) 입력에 따른 항법해
Fig. 6 Navigation Solution according to spoofing and anti-spoofing(code phase 0nsec) signal

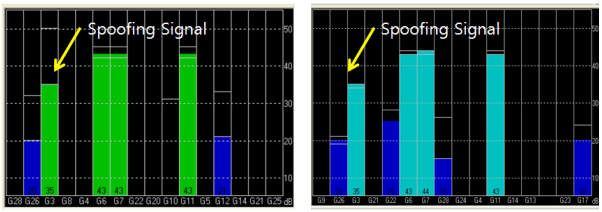
그림 7 과 8은 U-Blox 수신기에서 기만신호 및 기만신호와 코드위상이 200 nsec 차이가 있는 항기만신호를 인가할 경우 신호세기 및 항법해 영향을 나타낸 것이다.



(a) Normal Signal Only



(b) Spoofing Generation



(c) Anti-Spoofing (200 nsec)　(d) Spoofing Remains

그림 7. 기만신호 및 항기만신호(코드위상차 200nsec) 입력에 따른 신호세기
Fig. 7. Signal strength of PRN according to spoofing and anti-spoofing(code phase 200nsec) signal

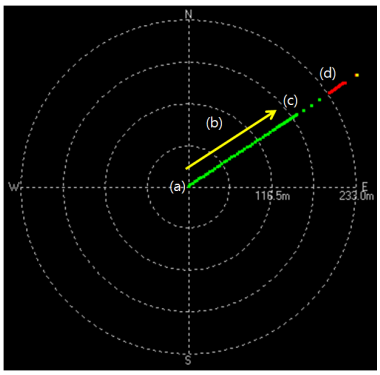


그림 8. 기만신호 및 항기만신호(코드위상차 200nsec) 입력에 따른 항법해
Fig. 8 Navigation Solution according to spoofing and anti-spoofing(code phase 2000nsec) signal

그림 7과 8의 (a)와 (b)의 상황은 그림 5와 6의 (a) (b) 상황과 동일하게 신호세기 및 항법해 결과가 측정되었다. 그림 7과 8의 (c)에서는 항기만신호를 200 nsec 이동하여 생성할 경우 기만된 PRN 3의 신호세기 영향 및 항법해 영향을 나타낸 것이다. 신호세기는 기만된 신호세기보다 작아지는 것을 확인할 수 있으며 항법해 또한 기만된 신호를 이용하여 항법해가 생성되는 것을 확인할 수 있다. 마지막으로 그림 7과 8의 (d)에서 보면 200 nsec 이동된 항기만신호를 입력한 일정 시간 후에 항법해 생성이 중단되는 것을 확인하였다. 그러나 소프트웨어 수신기를 이용하여 신호처리를 수행한 결과 항법해가 기만된 위치에서 연속적으로 생성되나 U-Blox 수신기에서는 항법해 생성이 중단되는 상황이 발생한 것이다.

Ⅳ. 결 론

본 논문은 기만신호 대응 모듈 및 상용수신기인 U-Blox 수신기를 이용하여 기만신호 발생시 수신기의 신호세기 및 항법해 영향을 분석한 후 기만신호를 제거하기 위해 역위상 코드를 가지는 항기만신호를 생성할 경우 수신기의 항법해 영향을 분석하였다.

모의실험을 통하여 기만신호가 발생할 경우 수신기에서 정상 위성 PRN의 신호세기가 5dB정도 커지면서 항법해가 비정상적으로 생성되는 것을 확인하였다. 이는 수신기에서 정상신호보다 센 기만신호를 추적하고 측정값을 생성함으로써 항법해오차가 커지게 된다. 기만신호 제거를 위한 항기만신호 실험을 수행한 결과 기만신호와 정확하게 역위상 코드를 가지는 항기만신호에 기만신호가 완전히 제거되고 정상신호만 남아 수신기가 정상적으로 항법해를 생성하는 것을 확인하였다. 그러나 만약 항기만신호가 기만신호와의 코드위상을 정확히 일치하지 못할 경우(200 nsec, 500 nsec) 여전히 기만신호가 수신기에서 처리되며 항법해 또한 비정상적으로 생성되는 것을 확인하였다. 이는 기만신호에 대한 대응을 위한 방법으로 기만 대응신호를 생성하기 위해서는 반송파의 위상 및 코드위상이 정확히 일치해야하며 코드위상이 일치된 경우 역위상 코드 정보를 이용하여 대응신호를 생성할 경우 기만신호가 완전히 사라지는 것을 확인하였다.

References

[1] S. K. Jeong, T. H. Kim, C. S. Sin, and S. U. Lee, “Technical trends of smart jamming for GPS signal,” *Electron. Telecommun. Trends (ET Trends)*, vol. 27, no. 6, pp. 75-82, Dec. 2012.

[2] M. Nicola, L. Musumeci, M. Pini, M. Fantino, and P. Mulassano, “Design of a GNSS spoofing device based on a GPS/Galileo software receiver for the development of robust countermeasures,” in *Proc. European Navigation Conf. Global Navigation Satellite Syst. (ENC GNSS 2010)*, Braunschweig, Germany, Oct. 2010.

[3] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, “An in-line anti-spoofing device for legacy civil GPS receivers,” in *Proc. Inst. Navigation Nat. Tech. Meeting (ION NTM 2010)*, pp. 868-882, San Diego, U.S.A., Jan. 2010.

[4] S. Lim, M. Y. Shin, and S. L. Cho, “Design of

software-based GPS spoofing signal generator," in *Proc. Inform. Control Symp. (ICS'08)*, pp. 63-64, Apr. 2008.

[5] 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," in *Proc. Inst. Navigation Global Navigation Satellite Syst. (ION GNSS)*, pp. 2314-2325, Savanna, U.S.A., Sep. 2008.

[6] S. L. Cho, M. Y. Shin, and S. J. Lee, "Performance comparison of anti-spoofing methods using pseudorange measurements," *J. Korea Inst. Military Sci. Tech. (KIMST)*, vol. 13, no. 5, pp. 793-800, Dec. 2010.

[7] E. L. Key, "Techniques to counter GPS spoofing," *Internal memorandum*, MITRE Corporation, Feb. 1995.

김 태 희 (Taehee Kim)

1999년 2월 전북대학교 컴퓨터공학과 학사졸업

2001년 2월 전북대학교 컴퓨터공학과 석사졸업

2001년1월~현재 한국전자통신연구원 선임연구원

<관심분야> 위성항법, 통신프로토콜, 소프트웨어 기반 실시간 위성항법 수신기 및 신호생성기

이 상 욱 (Sanguk Lee)

1991년 2월 연세대학교 천문학과 석사졸업

1994년 2월 University of Auburn 항공우주공학과 박사졸업

1993년1월~현재 한국전자통신신연구원 책임연구원

<관심분야> 위성시스템. 위성항법, 탐색구조

김 재 훈 (Jaehoon Kim)

2001년 2월 충북대학교 컴퓨터공학 박사졸업

1983년1월~현재 한국전자 통신연구원 책임연구원

1992년~1994년 KOREASAT 프로젝트 개발

<관심분야> 위성시스템. 위성항법, 탐색구조