논문 20-45-03-20 The Journal of Korean Institute of Communications and Information Sciences '20-03 Vol.45 No.03
https://doi.org/10.7840/kics.2020.45.3.609

표적 탐지 정확도가 낮은 환경에서 무인기 기만을 위한 단일 및 다중 스푸핑 기술 분석

이 치 헌◆, 이 상 정°

Anlaysis of Single and Multiple Spoofing Techniques for GPS Receiver Deception in Low Target Detection Accuracy

Chi-Hun Lee◆, Sang Jeong Lee°

요 약

무인기 기술이 감시 또는 테러로 악용되었을 경우를 대비하여 이를 공격하기 위한 기술 연구가 활발히 진행 중이다. 자율 항법 시스템의 핵심기술로 저비용의 높은 항법 정확도를 갖는 위성항법 기술이 많이 사용된다. 본 논문은 위성항법을 이용하는 무인기를 표적으로 재밍 공격 시 탑재체의 수신기에서 나타나는 효과를 분석한다. 대상 무인기의 탐지 정확도가 낮은 환경 조건에서 여러 가지 시나리오의 다양한 기만 신호를 생성하여 주입할 경우 위성 신호와 기만 신호의 위치/속도 오차로 인한 항법 결과를 소프트웨어 수신기에서 살펴본다. 하나의 위성항법 기만 신호를 이용하여, 위치 오차가 있을 때 위치 정확도에 따라 기만 성능의 차이가 어떻게 달라지는지 실험한다. 이후 낮은 탐지 정확도를 극복하기 위한 몇 가지 형태의 다중 기만 기술을 적용하였을 경우 실험 결과와 한계점을 분석한다.

Key Words : GNSS, jamming, single spoofing, multi spoofing, synchronous spoofing

ABSTRACT

Considering that Unmanned Aerial Vehicle technology is used for as surveillance & terrorism, technical research to attack it is also in progress. Satellite navigation technology is used for common autonomous navigation due to its low cost and high accuracy. This paper analyzes the effect of navigation result during jamming attack to drone target using satellite navigation. It generates various spoofing signals in various scenarios under low detection accuracy environments. The navigation results due to the detection error are examined in the software defined receiver. We test whether the deception performance is different in the condition of one deception signal. We analyze the test results and limitations when applying a simple multi-spoofing technique to overcome the low detection accuracy.

Ⅰ. 서 론

위성항법 신호는 지상에 도달하는 전력세기가 약 -130 dBm/MHz 정도로 미약하여 고의적이거나, 비고의적인 간섭신호에 취약하다[1,2]. GPS L1 신호의 경우 1023개의 코드길이를 가지는 C/A 코드를 이용하

※ 본 연구는 국방과학연구소의 지원으로 수행되었습니다.
◆ First Author : Agency for Defense Development, cameleon10@naver.com, 정회원
° Corresponding Author : Chungnam National University, Department of Electronics Engineering, eesjl@cnu.ac.kr, 정회원
논문번호 : 201911-271-0-SE, Received September 28, 2019; Revised December 13, 2019; Accepted December 13, 2019

여 확산 변조된 신호로 송신하고, 지상에서는 잡음 신호 레벨 아래의 신호를 프로세싱 이득을 통해 복조하는 방식으로 신호를 수신한다. 이러한 신호 특성으로 인해 이론적으로 10 mW 정도의 낮은 전력의 재밍 신호를 이용하여 수 km 정도 이격된 수신기를 교란할 수 있다[3,4].

위성항법 기만 기술은 기만 표적(Spoofing target)이 되는 무인기에 탑재되어 있는 위성항법 수신기를 대상으로 실제 위성을 모사한 기만신호를 생성하여 수신기의 항법해를 교란시키는 것이다. 대상 수신기는 실제와 다른 허위 위치와 속도를 인식하도록 유도된다[5-7]. 이러한 기만 기술은 미코닝, 비동기 스푸핑, 동기 스푸핑 기술로 구분된다.

미코닝 기법은 재방송 기법이라고도 불리며, 기만 신호 발생 원점에서 위성 신호를 수신하여 단순하게 재방사하는 기법이다. 미코닝 기법의 기대효과는 재방사 신호를 수신하도록 하여 실제 위치/속도가 아닌 재방사 원점 위치로 오인시키는 것이다[8]. 미코닝 기법을 발생하는 장치는 기술적 난이도가 높지 않아 제작이 용이한 장점이 있다.

고난이도 스푸핑 신호는 실제 위성신호와 스푸핑 신호를 같은 신호로 인식할 수 있도록 위성신호와의 동기가 필요하다[6]. 위성신호와의 동기는 메시지 동기, 코드지연 동기, 도플러 동기로 구분할 수 있다. 3가지 동기 중 하나라도 맞지 않으면 비동기 스푸핑 기술이다[9]. 비동기 스푸핑 기법은 미코닝 기법과 달리 표적 수신기의 항법해를 교란시켜 위치와 속도 정보 조작이 가능하다. 수신기에 입력되는 비동기 스푸핑 신호는 큰 잡음 신호처럼 보인다. 잡음 신호로 인해 위성신호를 tracking 하지 못하고, 항법을 하지 못하는 상태에서 수신기는 비동기 스푸핑 신호를 획득(acquistion) 후 추적(tracking)하는 순서로 기만된다.

동기 스푸핑 기법은 비동기 스푸핑 기술과 비교하여 복잡한 하드웨어 구조와 소프트웨어 신호 처리 기술이 요구된다. 동기된 스푸핑 신호를 만들기 위해서는 대상 표적 무인기의 위치와 속도 정보가 필요하다. 위치와 속도 정보는 레이더와 같은 탐지 측정 장비를 통하여 얻어진다. 동기 스푸핑은 비동기 스푸핑과 달리 항법 불능상태 이후 다시 항법을 하는게 아니라, 위성 채널별로 correlation peak를 실제 위성신호와 동일하도록 정렬함으로써, 표적 수신기의 항법 결과를 자연스럽게 기만시킬 수 있다.

레이더 장비에는 추적 오차가 있고, 레이더와 기만 장비 간 연동을 하게 되면 이에 따른 지연오차도 추가된다. 여기에 발생장치에서 만들어진 기만신호가 공간을 통해 전파하게 되면 전파 지연으로 인한 오차 및 신호 발생장치 내부 오차도 더해진다. 이런 오차가 있는 기만 신호들이 수신기에 입력되었을 경우 오차 정도에 따른 항법 결과 영향성을 분석할 필요가 있다.

본 논문에서는 위성항법 기만신호를 시뮬레이션을 통해 생성하여 소프트웨어 수신기에서 위성항법 기만 신호에 의해 어떠한 변화가 있는지 검토한다. 하나의 위치와 속도를 만들어 내는 기만 신호를 단일 기만 신호라 하고, 2개 이상의 위치와 속도를 만드는 신호를 다중 기만 신호라 한다. 우선 단일 기만 신호의 발생 위치 오차에 따른 분석한다. 이후 다중 기만 신호를 동시에 발생하였을 경우 결과가 어떻게 달라지는지를 시뮬레이션을 통해 분석하였다.

Ⅱ. 본 론

2.1 단일 기만신호 고정 이격 기만 결과

시뮬레이션은 오스트리아 Teleorbit 社의 GSDR^{2}X 소프트웨어 수신기와 GIPSIE GNSS 시뮬레이터를 이용하여 수행되었다. 실제 위성 신호는 아래와 같은 수식 (1)로 모델링하였다.

$$S(t)=\sum Ai(t)Ci(t)Di(t)\sin(2\pi fit+\phi i) + w(t) \quad (1)$$

여기서, i는 PRN(Psuedo Random Number) 번호, t는 항법위성의 시각, A는 신호세기, C는 C/A PRN 코드, D는 항법데이터, f는 L1 반송파 주파수, ϕ는 반송파 초기위상, w는 잡음이다. 그림 1은 시뮬레이션 환경을 보여준다. 시뮬레이터는 표적 무인기에서 입력받는 위성신호를 모의하고, 스푸퍼는 위성항법 기만신호를 발생한다. 수신기는 시뮬레이터의 신호와 스푸퍼 신호가 합하여 입력된다. 수신기 내부의 신호를 추적하여 항법 결과를 도출하는 추적루프 변수는 표 1과 같다. 시뮬레이터 및 스푸퍼 설정 값과 SDR 수신기에

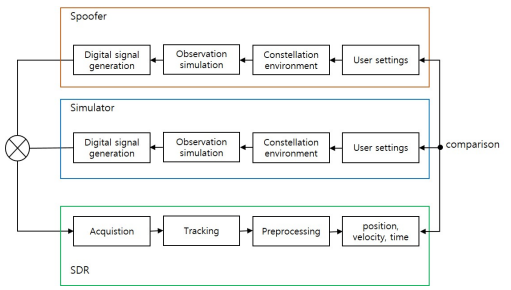

그림 1. 시뮬레이션 환경
Fig. 1. Simulation environments

표 1. SDR 수신기 추적루프 설정 변수
Table 1. SDR receiver tracking loop parameters

Tracking parameters	Values
Correlation spacing	0.25 chip
E-L Spacing	0.5 chip
FLL order	2
FLL bandwidth	20 Hz
PLL order	3
PLL bandwidth	18 Hz
DLL order	3
DLL bandwidth	10 Hz

서 항법결과를 비교 분석하였다.

표적 무인기의 위치를 레이더와 같은 탐지장치에서 입력받았을 경우 기본적으로 탐지장치의 측정 정확도에 의한 오차가 있고, 탐지장치와 기만송신장치간의 정보교환 시간지연에 따른 오차 등이 발생할 수 있다. 기만신호와 표적 무인기 간의 위치오차를 C/A 코드 chip을 기준으로 그림 2와 같이 이격거리 1/2 chip(150 m), 1 chip(300 m), 3 chip 이상(1,000 m)으로 달리하여 실제 위성과 동기된 기만신호를 60초 후에 인가하였을 때 기만 효과를 분석하였다.

그림 3은 1/2 chip 이격 위치에 동기화 기만 신호를 인가하였을 시 수신기에서 나타난 항법 위치 결과를 시간 순서에 따라 보여준다. Time < 60 sec 조건은 항법 신호가 인가되기 전 단계로 기준위치 (0, 0)에서 항법을 하고 있다. Time ≥ 60 시점에 서 기만신호가 인가되었을 때 (150, 0) 위치에 가깝게 위치 이동을 한 항법 결과를 나타내었다. 항법 수신기 내부의 위성 PRN 별로 tracking correlator에서의 변화를 확인할 수 있다. 일반적인 수신기의 tracking correlator의 간

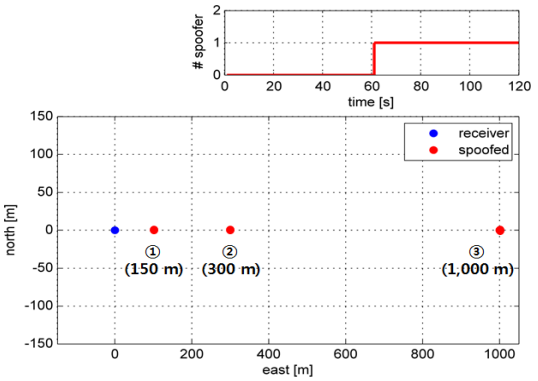

그림 2. 고정위치 단일 기만 시뮬레이션 조건
Fig. 2. Simulation condition of static single spoofing

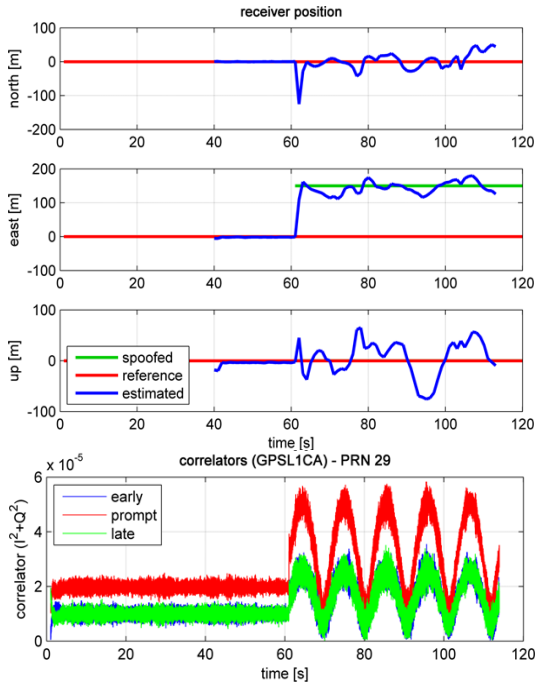

그림 3. 수신기 내부 기만효과(이격거리 : 150 m)
Fig. 3. Receiver navigation result (spacing : 150 m)

격이 1/2 chip 이므로, 스푸핑 신호가 correlator window 내부에 있어 효과적인 기만 효과를 나타내는 것으로 판단할 수 있다.

그림 4는 1 chip(300 m) 이격 시 기만 결과이다. 기만 인가 전(t < 60 sec)에는 기준 위치에서 항법을 하고 있으나, 기만신호 인가 후(t ≥ 60 sec)에는 기만 위치 (300, 0) 부근으로 항법 결과가 이동하였다. 다만 1/2 chip 조건 대비 up-down 방향 및 north-south 방향의 의도하지 않은 위치 변화가 다소 크게 발생하였다. 이는 수신 tracking window의 edge 근처에서 기만신호를 발생시킴으로 기존 항법 신호와 기만신호의 결합으로 pseudo-range가 변경되어 항법결과에 오차가 발생된 것으로 판단된다.

그림 5는 1,000 m 정도로 크게 이격 시켰을 때의 기만 효과를 나타낸다. 1/2 chip, 1 chip 이하의 결과와 다르게 기만 위치 (1,000, 0) 부근으로 항법 결과가 이동하지 않았고, north 방향과, up 방향으로 위치 오차가 발생하는 효과가 나타났다. 이는 tracking window와 이격이 큰 기만 신호는 의도한 기만 위치로 기만 효과를 발생하기 어렵다는 결과를 나타낸다[10].

실험 결과 1 chip 보다 많이 이격된 스푸핑 신호로는 의도된 위치로 기만을 하기는 어려웠고, 효과적인

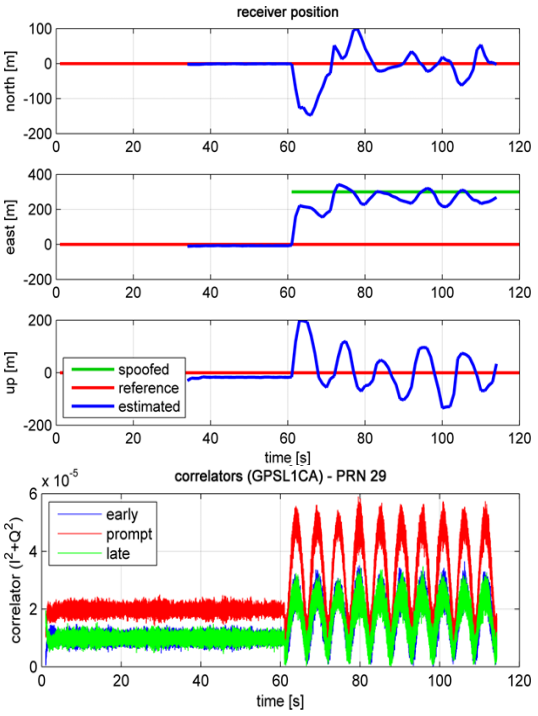

그림 4. 수신기 내부 기만효과(이격거리 : 300 m)
Fig. 4. Receiver navigation result (spacing : 300 m)

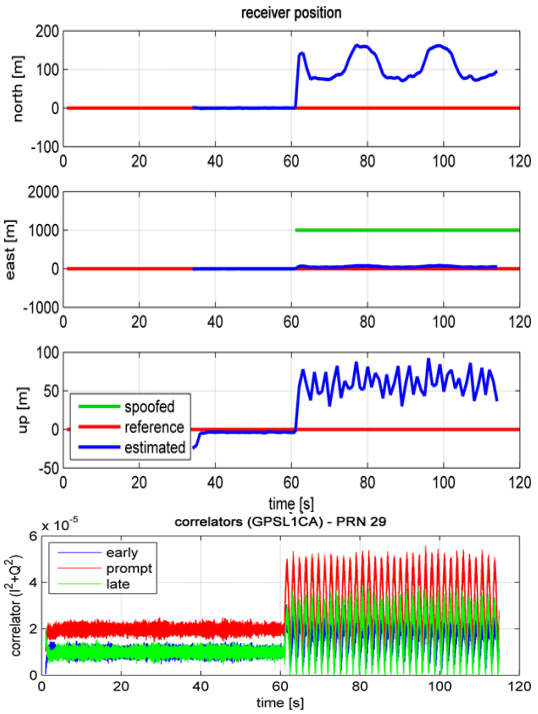

그림 5. 수신기 내부 기만효과(이격거리 : 1,000 m)
Fig. 5. Receiver navigation result (spacing : 1,000 m)

기만을 위해서는 1 chip 이내의 정확도로 기만신호를 생성하여야 함을 알 수 있었다.

2.2 다중 기만신호 고정 이격 기만 결과

단일 스푸핑 신호를 이용하여 효과적으로 수신기를 기만하기 위해서는 기만신호가 표적 무인기의 위치 오차 및 신호 발생오차 전파지연 오차 등 모든 오차를 포함하여 1 chip 이내로 수신기 단에서 입력 되어야한다. 현실적인 구현 가능성을 고려 시 1 chip 이내로 기만 신호를 만드는 것은 어렵다. 이러한 어려움을 극복하기 위해 여러 위치를 동시에 만들어내는 다중 스푸핑 신호를 고려하였다. 다시 말해 하나의 스푸핑 신호가 아닌 여러 개의 스푸핑 신호가 동시에 있을 경우 효과가 어떻게 달라지는지 시뮬레이션 하였다.

그림 6은 다중 기만 신호의 발생 조건을 도식적으로 표현하였다. 표적 수신기는 원점에서부터 북쪽 방

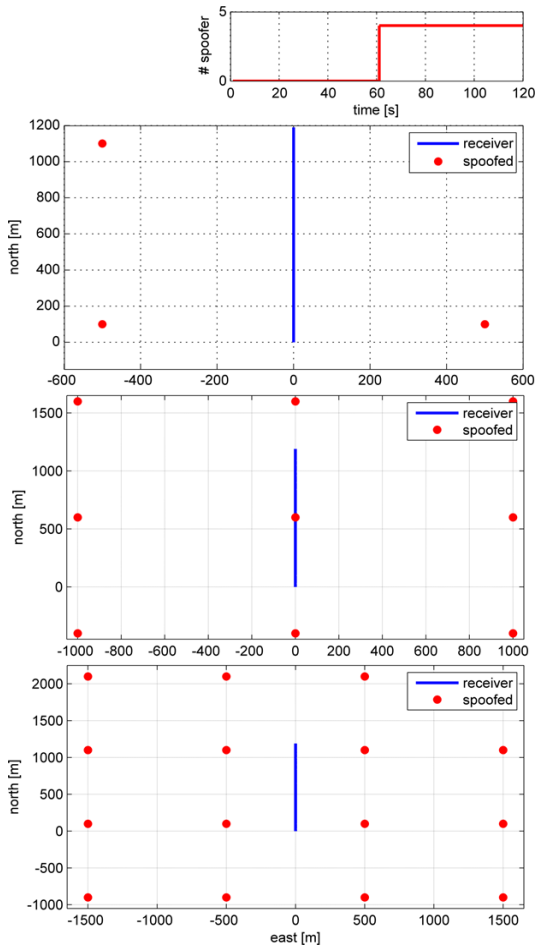

그림 6. 고정위치 다중 기만 시뮬레이션 조건
Fig. 6. Simulation condition of static multiple spoofing

향으로 시속 80km/h 속도로 움직이는 탑재체로 가정하였다. 고정 위치를 모의하는 스푸핑 신호는 표적 수신기의 이동 중심에서 1km 이격 간격으로 배치하였다. 다중 스푸핑 개수를 4개, 9개, 16개로 늘려나가며 실험하였다.

다중 신호를 수신기 이동 경로에 여러 개를 만듦으로써 기대한 기만 효과는 수신기가 경로를 따라 항법을 하던 중 기만 신호가 인가되면 여러 개의 고정 기만 신호 중에 가장 가까운 기만 위치로 기만 되어지는 것이었다. 그림 7은 4개, 9개, 16개로 다중기만 신호를 생성하였을 때의 결과이다. 공통적인 결과는 60초 이후 기만 신호를 인가하더라도 수신기의 위치가 고정되는 것이 아니라, 북쪽으로 오차를 가지고 이동하는 항법 결과를 보인 것이다.

다중 기만 개수에 따라서 원래의 이동 경로에 비해 오차가 커지는 결과를 나타내지만, 수신기가 항법을 하면서 이동한다는 결과는 동일하였다. 이는 수신기가 본래의 위성신호를 이용하여 항법을 지속적으로 하였음을 의미한다. 그림 7의 마지막 그림은 16개의 다중 신호가 입력되었을 때 신호 대 잡음 결과이다. 다중 기만 신호는 각 채널 별로 잡음으로 작용하여 C/No 값이 낮아지는 결과를 가져왔다[11].

다중 기만 신호의 서로 다른 위치의 신호들은 위성 신호의 time domain에서의 code delay된 여러 신호의 조합과 같다. 수신기 입력에서는 같은 위성의 신호가 시간 차이를 두고 입력되는 것과 같은 효과가 있다.

$$y(t)= \sum A_n x(t-t_n)\times e^{2\pi jtfn} \quad (2)$$

$$Y(f)=X(f) \cdot (e^{-\pi j(n-1)\tau f}) \cdot \sin(\pi N\tau f)/\sin(\pi\tau f) \quad (3)$$

이것은 spectral effects로, 시간 축에서의 신호가 주파수 축에서 신호로 표현하면 식 (2)와 식 (3)과 같다. 식 (3)은 식 (2)의 푸리에 변환 식으로 신호 개수가 증가함에 따라 spectral deforming 되어 다중 기만은 잡음 신호와 같은 효과로 작용하는 결과를 가져온다는 것을 의미한다.

2.3 다중 기만신호 동적 이격 기만 결과

움직이는 무인기를 표적으로 여러개의 기만신호를 생성하는 것은 의도한 기만 효과와 다르게 신호대 잡음비를 낮추는 정도의 효과(spectral effects)로 작용하여 항법 오차 범위를 증가시키는 결과를 가져옴을 앞서 확인하였다. 만일 움직이는 무인기가 아닌 고정된 표적에 동적 스푸핑 신호를 여러개 인가하였을 경우

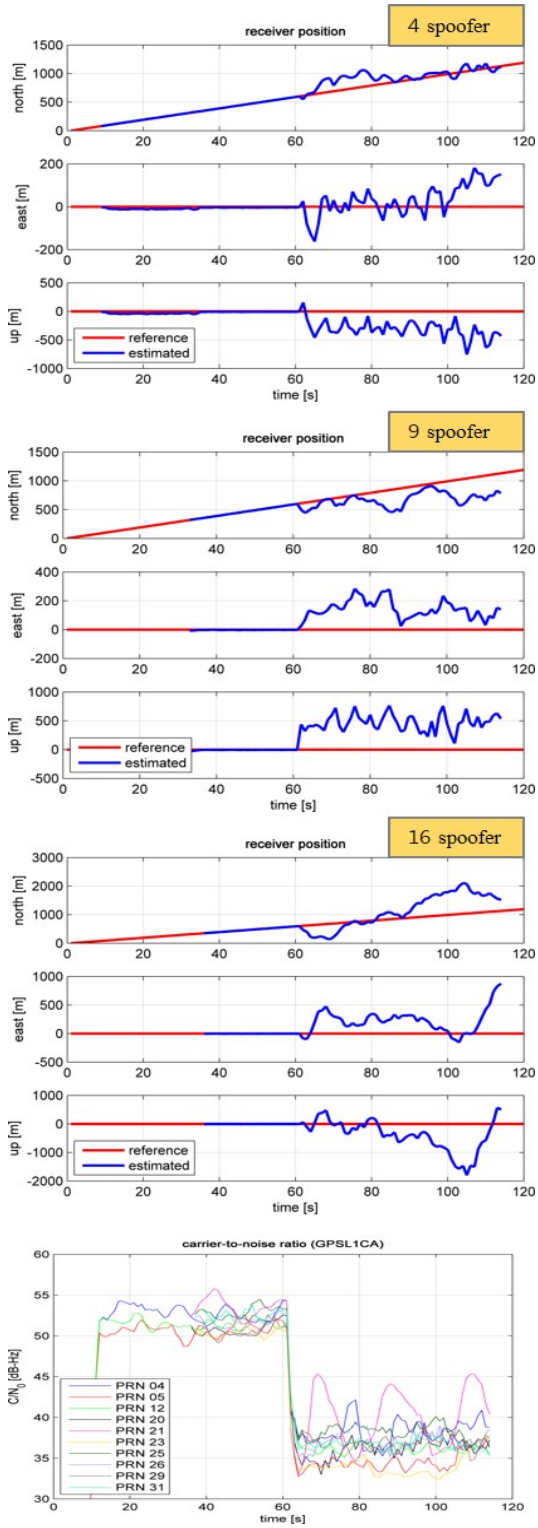

그림 7. 수신기 내부 기만 효과(다중 정적 기만신호)
Fig. 7. Receiver navigation result (4, 9, 16 multiple static spoofing)

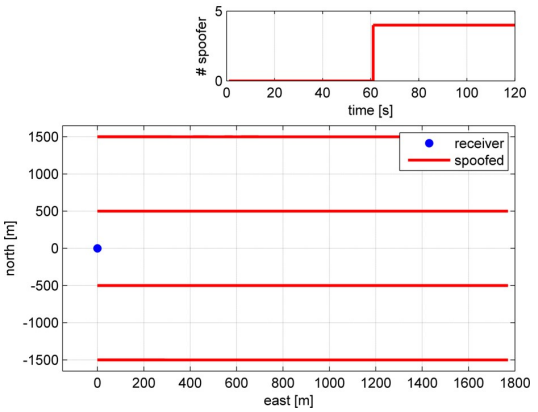

그림 8. 동적 다중 기만 시뮬레이션 조건
Fig. 8. Simulation condition of dynamic multiple spoofing

에 결과가 어떻게 되는지 추가로 확인하였다.

시뮬레이션 조건은 그림 8과 같다. 원점에서 고정 위치로 항법을 하는 표적을 동쪽 방향으로 이동하는 기만 신호 4개를 동시에 생성하였다. 각 신호는 1 km 간격으로 이격하여 움직이는 형태로 생성하였다. 이러한 다중 기만 인가 조건의 경우 4개의 기만 신호 중 가장 가까운 신호 중 하나의 경로를 쫓아서 이동할 것으로 예상하였다.

그림 9의 시뮬레이션 결과를 보면, 고정 위치에 있던 수신기가 기만 신호가 인가된 후 동쪽 방향으로 이동하는 것으로 나타났다. 스푸핑 신호 인가 시점인 60 sec ≤ Time ≤ 80초 사이에서는 약 20초 기간에는 동쪽 방향으로 움직인 결과가 아닌 북쪽 방향으로 움직이는 결과를 보였지만, Time ≥ 80 sec 이후에는 동쪽 방향으로 시간차를 두고 이동하였다. 결과적으로 4개의 신호 중 하나를 따라 정확히 항법을 하지는 않았지만, 다중 스푸핑을 통해 의도하지 않은 임의의 경로로 이동하는 결과를 보였다. 그림 9의 Time ≥ 60 이후 Doppler 값이 변화되는 것을 확인할 때, 위치 이동과 동시에 속도 변화유도도 가능하다는 결과를 확인할 수 있다.

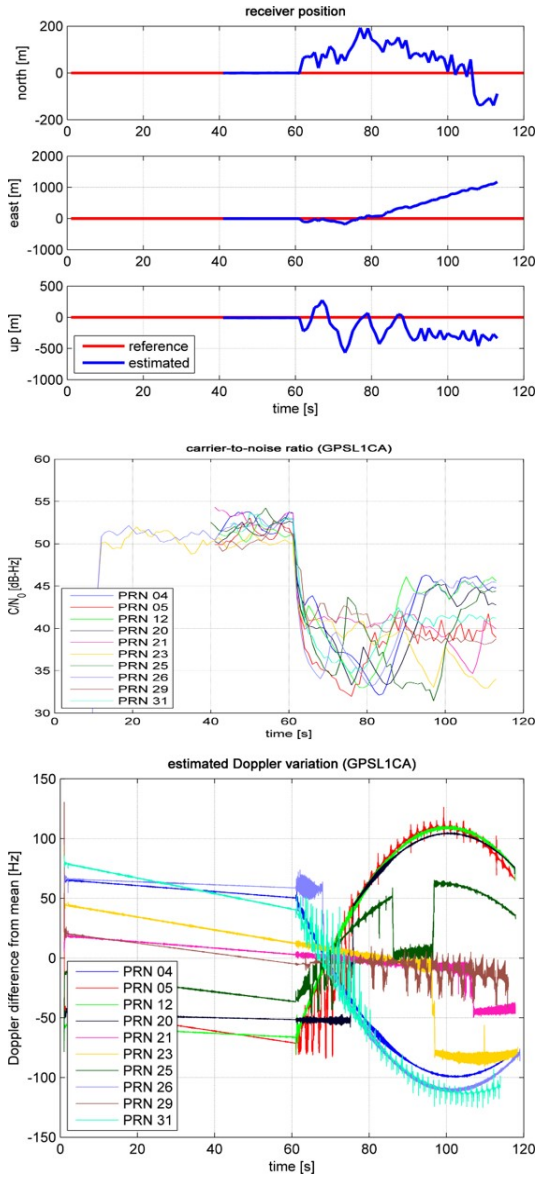

그림 9. 수신기 내부 기만 효과(다중 동적 기만신호)
Fig. 9. Receiver navigation result (multiple dynamic spoofing)

Ⅲ. 결 론

본 논문은 위성항법 신호를 생성하여 다양한 조건으로 기만 신호를 인가하였을 때 표적 수신기에서 나타나는 결과를 분석하였다.

고정위치의 목표물을 대상으로 표적 정보의 오차가 있을 때를 가정하여 이격 거리를 다르게 하면서 스푸핑 신호를 생성하여 인가하였다. 실험 결과는 1 chip 보다 많이 이격된 스푸핑 신호로는 의도된 위치로 기만하기 어렵다는 것이고, 효과적으로 의도한 위치로 기만하기 위해서는 1 chip 이내의 표적 위치로 기만신호를 생성할 수 있어야 한다는 것이다.

현실적으로 정확한 표적 정보를 얻기 힘들기 때문에 움직이는 수신기를 대상으로 수신기의 이동 경로에서 고정 위치의 다중 기만 신호를 여러 조건으로 발생하여 실험하였다. 위치 및 속도 정보가 정확하지 않은 가정에서 여러 개의 기만 신호로 생성하면 여러 기

만신호 중 하나로 기만이 될 수 있을 것으로 기대하였다. 하지만 결과적으로 표적은 고정 위치의 다중 기만 신호로 기만 되지 않았고, 무인기의 이동 시 항법 오차를 발생시키는 잡음 재밍 수준 정도의 효과를 나타냈다.

이후 정확한 위치를 알지 못하는 고정된 표적을 대상으로 경로 이동을 하는 다중 기만 신호를 이용하여 표적의 위치와 속도를 변화시킬 수 있을 것인가를 실험하였다. 정확히 의도한 위치와 속도는 아니더라도 어느 정도의 오차를 가지고 이동시키는 것이 가능하다는 결론을 얻었다.

본 논문에서의 결과를 바탕으로 위성항법을 이용하는 무인기에 기만 신호가 인가하였을 때 기만신호의 정확도에 따라 기만 효과가 어떻게 달라질 수 있는지 예측할 수 있다. 향후 위치와 속도를 모르는 조건 하에서 의도한 위치와 속도로 정확히 기만을 할 수 있는 방법에 대한 추가적인 연구가 필요하다.

References

[1] E. D. Keplan, *Understanding GPS Principles and Applications*, 2nd Ed., Artech House, 2005.

[2] J. Carroll, "*Vulnerability assessment of the transportation infrastructure relying on the global positioning systems*," John A. Volpe National Transportation Systems Center Report for U.S. Department of Transportation, 2001.

[3] F. Dovis, *GNSS Interference Threats and Countermeasures*, Artech House, 2015.

[4] C. H. Lee, S. H. Choi, C. T. Choi, and U. S. Jeong, "The analysis of effectiveness for the noise jamming signal on the GPS receiver," in *Proc. KGS Conf.*, p. 84, 2013.

[5] T. E. Humphreys and F. Dovis., *GNSS Interference Threats and Countermeasures*, Artech House, 2015.

[6] 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.

[7] T. E. Humphreys, J. A. Bhatti, and B. M. Ledvina, "The GPS assimilator: A method for upgrading existing GPS user equipment to improve accuracy," *ION GNSS*, 2010.

[8] C. H. Lee, S. H. Choi, C. T. Choi, and W. H. Shin, "The effect analysis for the partial meaconing signal on the GPS receiver," in *Proc KGS Conf.*, pp. 76-79, 2016.

[9] C. H. Lee and S. J. Lee, "Influence analysis of satellite unsynchronized spoofing," in *Proc. KGS Conf.*, pp. 602-605, 2017.

[10] C. H. Lee, S. H. Choi, S. K. Kim, W. S. Choi, and L. K. Chang "Influence analysis of spreading modulated GNSS synchronous spoofing," in *Proc. KICS Conf.*, pp. 597-598, 2018.

[11] J. W. Betz, "Effect of partial-band interference on receiver estimation of C/No," in *Proc. The Inst. Navig. National Technical Meeting*, pp. 817-828, 2001.

이 치 헌 (Chi-Hun Lee)

2003년 2월 : 경북대학교 전자공학과 졸업
2005년 2월 : 한국과학기술원 전자공학과 석사
2017년 3월~현재 : 충남대학교 전자공학과 박사과정(현재)

2005년~2011년 : LG전자 선임연구원
2011년~현재 : 국방과학연구소 선임연구원
<관심분야> 3G/4G 이동통신, 전자전, 위성항법
[ORCID:0000-0002-3014-5118]

이 상 정 (Sang Jeong Lee)

1979년 2월 : 서울대학교 전자공학과 졸업
1981년 2월 : 서울대학교 전자공학과 석사
1987년 2월 : 서울대학교 전자공학과 박사

1994년~2002년 : (사)GNSS 기술협의회 회장
2010년~2018년 : 국방위성항법특화연구센터 센터장
1988년~현재 : 충남대학교 전자공학과 교수
<관심분야> Robust Control, GNSS
[ORCID:0000-0002-9400-5157]