

고출력 GPS 재방송 교란을 위한 무선 교란 장치

Wireless Meaconing Jammer for High-Power GPS Meaconing

이병현¹ · 이정란² · 김정한³ · 박성균⁴

Byung-Hyun Lee¹ · Jung-Ran Lee² · Jeong-Han Kim³ · Sung-Kyun Park⁴

요약

본 논문에서는 고출력 GPS 재방송 교란을 수행하기 위한 무선 재방송 교란 장치를 제안했다. GPS 재방송 교란은 위성 신호를 수신하여 재방송함으로써 표적의 GPS 수신기가 잘못된 위치를 계산하도록 하는 데에 목적이 있다. 이때 수신하는 GPS 신호와 송신하는 교란 신호의 주파수가 동일한 주파수이기 때문에 유효방사출력이 1 Watt(30 dBm)인 경우, -160 dB의 안테나 후엽감쇄 성능이 필요하다. 따라서 송수신부가 근접 또는 하나의 장치에 위치한 경우, 안테나의 후엽감쇄만으로는 재방송 교란이 불가능하다. 이러한 송수신 간섭을 제거하기 위해 시분할 방식, 또는 전이중 통신방식을 적용하지만 그 성능에는 제한이 있다. 따라서 원거리 이격을 통해 송수신 간섭 영향을 제거하기 위해 무선 재방송 교란 장치를 설계했다.

Abstract

In this study, we propose a wireless meaconing jamming system for use in high-power GPS meaconing. The purpose of GPS meaconing is to ensure that the target GPS receiver calculates the intended jammer position by repeating the jammer-received GPS signal. In this case, because the received and transmitted signals have the same frequency, the front-back Ratio(FBR) of the antenna should be -160 dB when the effective radiated power(ERP) is 1 W(30 dBm). Thus, the meaconing jammer can malfunction by reducing the back-lobe level of the antenna when the receiver and transmitter are located in a jammer device. In general, the receiver and transmitter are isolated by the time-division or duplex-communication method in order to eliminate reception/transmission interference; however, this performance is still limited. Thus, we designed a wireless meaconing jammer to eliminate reception/transmission interference by long-distance separations.

Key words: Meaconing, GPS, Jamming, High Power Jamming, Repeat Jamming

I. 서론

무인시스템을 구성하는데 기본적으로 사용되는 것이 미국의 GPS와 같은 위성항법시스템이다. 일반적인 GPS 교란은 크게 잡음 교란(noise jamming), 기만 교란

(spoofing), 그리고 재방송 교란(meaconing)이 있다. 잡음교란은 잡음 신호를 GPS 수신신호보다 강하게 송출하여 GPS 신호를 수신하지 못하게 방해하는 것을 말한다^[1]. 기만교란은 의도하는 모의 GPS 신호를 생성하여 표적 수신기가 교란장치가 의도한 위치로 잘못 인

한화시스템 전자전연구센터(EW R&D Center, Hanwha Systems)

1: 전문연구원(<https://orcid.org/0000-0003-2985-0861>), 2: 수석연구원(<https://orcid.org/0000-0003-4944-6364>,

3: 수석연구원(<https://orcid.org/0000-0002-2492-0579>), 4: 수석연구원(<https://orcid.org/0000-0002-2133-5876>)

· Manuscript received May 30, 2019 ; Revised July 18, 2019 ; Accepted August 27, 2019. (ID No. 20190530-003S)

· Corresponding Author: Byung-Hyun Lee (e-mail: byunghyun.lee@hanwha.com)

식하도록 교란하는 방법으로, 모의 GPS 신호를 생성하기 위해 공개된 민간신호만 교란이 가능하다^[2]. 재방송 교란은 기만 교란과 달리 수신된 신호를 재방송하는 구조이기 때문에 신호의 구조에 대한 정보가 필요 없다. 따라서 군용신호와 같이 암호화 된 신호까지 교란이 가능하다. 각 교란 기법을 통해 생성된 교란 신호는 고출력 앰프(high power amplifier)와 안테나를 이용하여 고출력으로 송출된다. 그러나 재방송 교란은 실 위성신호를 수신하여 재방송하는 구조이기 때문에 교란 장치에 신호 수신부와 송신부가 동시에 존재하게 된다. 이러한 구조에 의해 고출력으로 교란 신호를 송출할 때 송출 신호가 교란 장치의 수신부로 인가되어 교란 장치가 망가지게 된다. 따라서 재방송 교란을 위해서는 수신부와 송신부를 전파적으로 격리해야만 한다^[3].

II. 일반적인 재방송 교란 장치

재방송 교란장치의 구조는 그림 1과 같다.

수백 Watt 이상의 유효방사출력을 견디기 위해 혼안테나를 송신안테나로 설계할 수 있다. 그림 1에서처럼 송신부와 수신부가 하나의 장치에 있는 경우, 안테나의 후엽 신호와 주변 환경에 의한 반사신호가 수신안테나로 인가되어 시스템이 망가지게 된다. 후엽감쇄를 위해 설계된 안테나의 경우 47 dB의 FBR 특성을 보인다^[4]. 유효출력이 1 W(30 dBm), 재방송 송수신 안테나 이격거리가 10 m일 때 자유공간 신호손실모델에 의해 신호감쇄는 약 57 dB이고, 47 dB의 FBR 특성을 갖는 송신안테나를 적용하면 수신안테나에 인가되는 후엽신호의 세기는 -74 dBm이다. 일반적인 GPS 수신신호인 -130 dBm^{[5],[6]}보다 약 56 dB 이상 강한 신호가 인가된다. 이는 곧 재방송 교란장치가 정상동작하지 않음을 의미한다.

따라서 전파적 분리를 위해서 송수신 안테나를 물리적으로 원거리 이격하고, 특수 장치 및 지형지물 등을 이용하여 송출 교란신호가 수신안테나에 도달하지 않도록 해야 한다. 실제로 재방송 교란 장치를 전개함에 있어 원거리 이격된 송수신부를 유선으로 연결하는데에는 한계가 있다. 따라서 본 논문에서는 무선으로 재방송 교란 장치의 송수신부를 연결하는 구조를 제안했다.

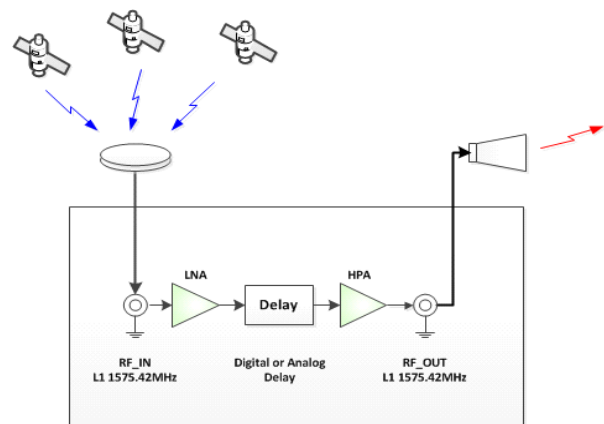


그림 1. 일반적인 재방송 교란 장치의 구조
Fig. 1. Structure of conventional meaconing jammer.

III. 무선 재방송 교란 장치

재방송 교란이 성공적으로 수행되기 위해서는 송수신 신호의 분리가 필요하다. 일반적인 재방송 교란에 대한 연구는 재방송 신호 생성과 지연시간 등 특성을 분석하는 내용이 주로 이루어졌고^[7], 고출력 송신 시 수신부에 영향을 제거하는 방법에 대해서는 시분할 방식을 적용한 연구가 있다^[3]. 본 논문에서는 송수신 안테나를 물리적으로 이격시켜 수신안테나에 인가되는 송신 교란신호의 영향을 제거하는 재방송 교란 장치의 구조를 제안했다. 그림 2는 제안한 무선 재방송 교란 장치의 구조를 나타낸다.

GPS 신호는 L대역 신호이기 때문에 송수신부에서 간섭제거 및 신호전송 시 신호 손실을 최소화하기 위해 저대역 주파수로 변환하여 무선으로 전송한다. 본 논문에서는 무선 송수신부의 신호감쇄 및 안테나 크기를 고려하여 160.42 MHz로 주파수 변환기를 설계했다. 이때 송수신부의 국부발진기는 동일한 주파수를 적용해야 실제 수신한 GPS 신호와 동일한 신호로 상향변환이 가능하다.

IV. 실험 결과

제안한 무선 재방송 교란 장치에 대한 검증을 위해서 송수신부와 수신부를 약 40 m 이격시켜 위치한 후 160.42

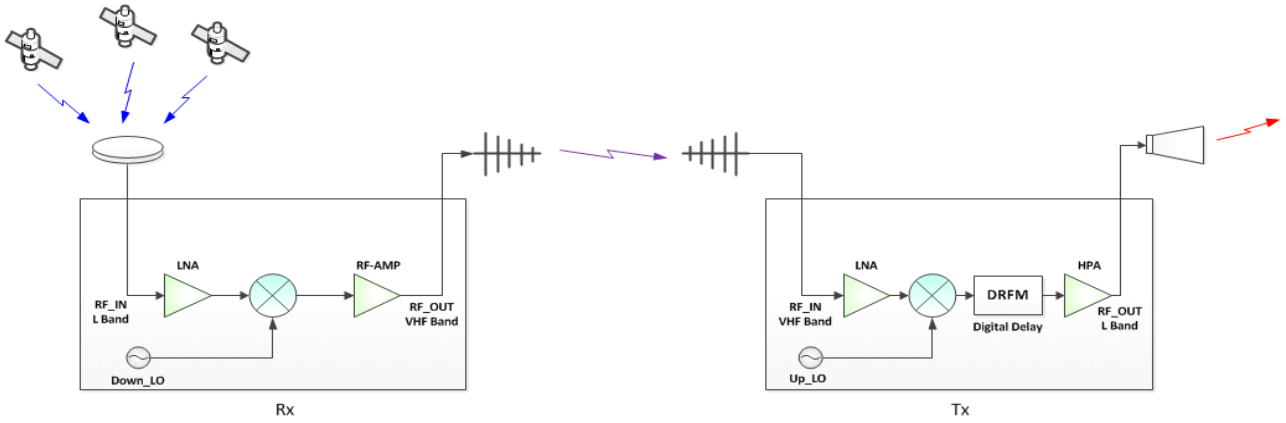


그림 2. 제안한 구조의 무선 재방송 교란 장치의 구조
Fig. 2. Structure of proposed wireless meaconing jammer.

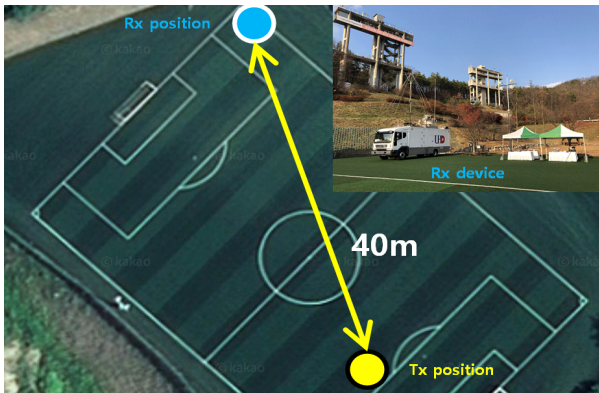


그림 3. 야외 실험 구성
Fig. 3. Outdoor test configuration.

MHz로 하향변환된 신호는 무선으로 신호를 송수신하고, 실제 GPS 교란을 수행할 수 없기 때문에 GPS L1 대역 신호는 재방송 교란장치 송신부에서 주입시험으로 대체했다.

야외에서 그림 3과 같이 장치를 위치하고 실험을 수행했다. 수신부에서는 실제 GPS 신호를 수신하고, 약 40미터 이격 지점에서 송신부를 위치한 후, 상용 GPS 수신기(U-blox AEK-M8N)를 사용하여 성능을 검증했다. 성능을 검증하기 위해 수신부의 안테나에 상용 GPS 수신기를 연결하고, 그 결과를 비교했다.

실험 결과, 제안한 무선 교란 장치의 송신부에서 송출하는 신호와 수신부에서 수신한 신호가 동일한 측위

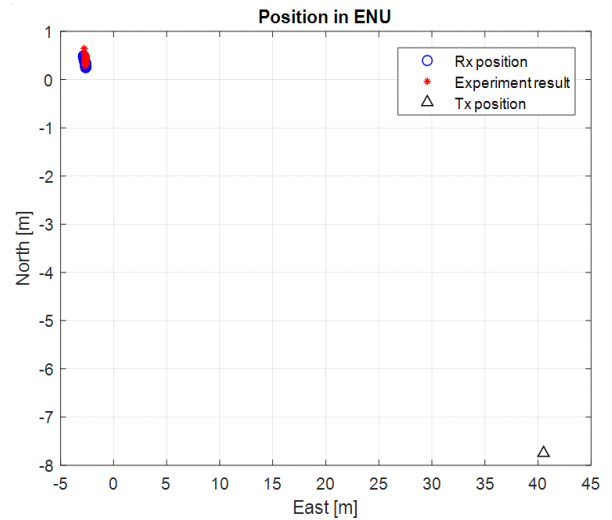


그림 4. 측위 결과(o: 수신부 위치, *: 실험 결과, △: 송신부 실제 위치)
Fig. 4. Result(o: Rx position, *: result, △: Tx position).

결과를 나타내는 것을 확인했다(그림 4). 즉, 송신부에 연결한 상용 GPS 수신기가 계산한 위치는 실제 송신부의 위치가 아닌 이격된 재방송 교란 장치의 수신부 위치로 나타났다. 이는 곧 GPS 신호를 주파수 하향변환하여 무선으로 송신부에 전달하는 구조가 정상 동작하는 것을 의미한다. 즉, 제안한 무선 재방송 교란 장치를 통해 표적 수신기의 위치를 잘못된 곳으로 인식하게 할 수 있음을 실험을 통해 검증했다.

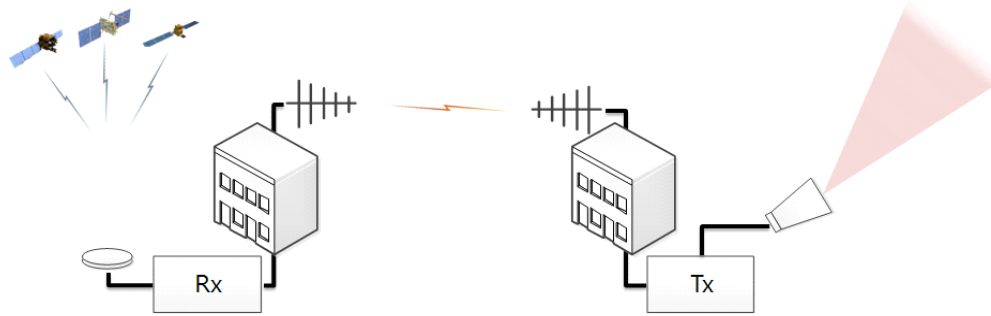


그림 5. 무선 재방송 교란 장치의 전개 예시
Fig. 5. Deployment example of wireless meaconing jammer.

V. 결 론

재방송 교란을 성공적으로 수행하기 위해서는 재방송 송신부에서 송출하는 신호가 수신부에 영향을 주지 않아야 한다. 본 논문에서는 재방송 교란 장치의 송수신부를 격리하기 위해 물리적 격리 방식을 사용했다. 수신부와 송신부를 원거리 이격하고, 지형지물을 통해 송신부의 후엽 신호를 차폐하면서 전개할 때 용이성을 확보하기 위해 무선으로 송수신부를 연결할 수 있는 시스템을 제안했다. 그림 5는 제안한 무선 재방송 교란 장치의 전개 예시를 표현한 그림이다. 제안한 시스템의 장점은 첫 번째로 고풍력 교란신호 송신 시 수신부에 영향을 주지 않는다는 점이고, 두 번째로는 저대역으로 하향변환하여 무선 통신하기 때문에 원거리 이격 시에 신호 손실이 적다는 점이다. 또한, 재방송 교란의 장점인 군용 GPS 수신기까지 위치 교란이 가능하다는 것을 포함하고 있다. 재방송 교란의 단점은 교란 장치의 위치가 표적 수신기에 노출이 된다는 점이다. 그러나 제안한 시스템은 송수신부가 분리되어 있기 때문에 원격지에 있는 수신부의 위치가 노출되어 송신부인 교란 장치는 보호될 수 있다.

References

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr., 2008, "Assessing the spoofing threat: Development of a portable GPS civilian

spoofers," in *Proceedings of the ION 21st International Technical Meeting of the Satellite Division of The Institute of Navigation*, Savannah, GA, Sep. 2008, pp. 2314-2325.

- [2] S. H. Seo, B. H. Lee, S. H. Im, and G. I. Jee, "Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal," *Journal of Positioning, Navigation, and Timing*, vol. 4, no. 2, pp. 57-65, 2015.
- [3] B. H. Lee, I. G. Oh, and S. I. Kim, "Design and analysis of switching timing for high power GPS meaconing jammer," *Journal of Positioning, Navigation, and Timing*, vol. 7, no. 4, pp. 227-233, Dec. 2018.
- [4] J. Y. Shin, H. S. Shim, B. H. Lee, J. R. Lee, and J. M. Woo, "Front-to-back ratio improvement of a high-power horn antenna," *The Journal of Korean Institute of Electromagnetic Engineering and Science*, vol. 29, no. 5, pp. 389-392, May 2018.
- [5] B. W. Parkinson, J. J. Spilker Jr., *Global Positioning System: Theory and Applications*, 1st ed. Washington, DC, American Institute of Aeronautics and Astronautics, 1996.
- [6] E. D. Kaplan, C. J. Hegarty, *Understanding GPS: Principles and Applications*, 2nd ed. Boston, MA, Artech House, 2006.
- [7] T. Kim, C. Sin, "Analysis of the GPS meaconing signal generator for the live GPS L1 signal," *Journal of Satellite, Information and Communications*, vol. 11, no. 4, pp. 15-20, Dec. 2016.