Journal of KIIT. Vol. 16, No. 5, pp. 53-65, May 31, 2018. pISSN 1598-8619, eISSN 2093-7571 53
http://dx.doi.org/10.14801/jkiit.2018.16.5.53

상용 GPS 수신기와 항재밍 기능을 보유한 군용 EGI 수신기를 사용한 실시간 GPS 재밍 탐지 가능 연구

이영중*, 나성웅**

A Study on Real Time GPS Jamming Detection Possibility Using Commercial GPS Receiver and Military EGI Receiver with Anti-jamming Function

Young-Joong Lee*, Sung-Woong Ra**

요 약

GPS(Global Positioning System) 수신기는 오래전부터 상용과 군용 플랫폼 시스템에 기본적으로 적용되는 필수장치이다. 이러한 GPS 수신기를 무력화하기 위한 GPS 재밍 또한 오래전부터 매우 심각한 위협이었다. GPS 수신기를 장착하여 운용하는 시스템이 탑재된 플랫폼에서 독립적으로 GPS 재밍을 실시간으로 탐지하기란 매우 어렵다. GPS 수신기가 GPS 재밍에 취약한 이유는 GPS 수신기와 위성간 거리가 GPS 수신기와 재머간 거리보다 훨씬 멀기 때문이다. 이러한 거리차는 신호세기 측면에서 재머신호 세기가 GPS 위성신호세기보다 매우 크므로, GPS 수신기가 처리이득을 고려하더라도 재머에 취약할 수 있다. 본 논문은 GPS 위성과 재머 신호에 대한 GPS 수신기에서의 재밍신호 대 위성신호비(JSR)을 분석하였다. 이러한 분석을 통해 독립적인 플랫폼에서 GPS 재밍을 실시간으로 탐지하기 위하여, 상용 GPS 수신기와 군용 EGI(Embedded GPS&INS) 시스템으로 구성되는 새로운 방법을 제안한다.

Abstract

The GPS(Global Positioning System) receiver has long been a essential equipment for commercial and military platform systems. GPS jamming to disable these GPS receivers has also been a very serious threat for many years. It is very difficult for a system equipped with a GPS receiver to independently detect GPS jamming in real time. The GPS receiver is vulnerable to GPS jamming because the distance between the GPS receiver and the satellite is much longer than that the GPS receiver and jammer. Since the jammer signal power is much higher than the GPS satellite signal power in terms of signal power, the GPS receiver may be vulnerable to jammer even if the GPS processing gain is considered. This paper analyzes Jamming signal to satellite Signal Ratio(JSR) in GPS receiver for GPS satellite and jammer signal. In order to detect GPS jamming in real time on an independent platform through this analysis, we propose a new method consisting of commercial GPS receiver and military EGI(Embedded GPS&INS) system.

Keywords
GPS receiver, GPS jammer, GPS jamming detection, Multiple GPS receiver channel, SAASM, CRPA, EGI

* 국방과학연구소 선임연구원(교신저자)
- ORCID: https://orcid.org/0000-0003-3495-7014
** 충남대학교 전자전파정보통신공학과 교수
- ORCID: https://orcid.org/0000-0002-1708-3186

· Received: Mar. 13, 2018, Revised: Apr. 18, 2018, Accepted: Apr. 21, 2018
· Corresponding Author: Young-Joong Lee
Electronic Warfare PEO, Agency for Defense Development
YuSeong P.O. Box 35, DaeJeon, 34186, Korea,
Tel.: +82-42-821-2866, Email: youngcenter@add.re.kr

Ⅰ. 서 론

GPS(Global Positioning System) 수신기는 상용, 군용 전자시스템에서 필수적인 장치이다. GPS 신호는 대역확산되어 저피탐확률(LPI) 특성을 가지나, GPS 제원이 알려져 있고, GPS 위성과의 거리가 멀어 전파손실에 의해 GPS 재머에 취약할 수 있다. 군용 GPS 수신기는 재머에 내성을 갖기 위한 방법들을 적용하여 운용되나, GPS 재밍의 인가여부와 재밍종류를 판별하는 것은 매우 어렵다.

기존에는 GPS 재밍을 탐지하기 위하여 위성신호에 대한 상관도 측정 등을 통해 GPS 수신기 내부에서 탐지하거나, ELINT(Electronic Intelligence) 전자정보 수신기 시스템 등 GPS 수신기 외부에서 GPS 재밍 신호의 탐지 및 위치를 식별하는 방법 들이 사용되었다[1]-[6].

본 논문은 항공기, 함정 등 단일 플랫폼에 탑재된 GPS 수신기를 다중으로 구성하여 GPS 재밍 인가여부와 종류를 판별하는 방법에 대한 내용이다.

본 논문은 GPS 수신기와 GPS 재머에 대한 전파가시선 분석을 통한 실질적인 지상 환경에서의 J/S를 도출하였다. 일반적으로 군용 GPS 수신기는 항재밍 안테나(CRPA, Controlled Reception Pattern Antenna), 안테나 전자부(AE, Antenna Electronics, 이하 항재밍 안테나시스템), SAASM(Selective Availability Anti Spoofing Module) 칩이 적용된 EGI(Embedded GPS/INS)로 구성된다. 본 논문은 상용 GPS와 군용 GPS 수신기를 혼합한 다중 GPS 수신기 채널을 활용한 실시간 GPS 재밍 탐지방법에 대한 내용을 기술하였다. 이러한 방법을 통해 GPS 재밍에 신속히 대처할 수 있을 것으로 판단된다.

Ⅱ. 관련 연구

2.1 GPS 수신기 특징

GPS 위성군은 총 24개의 위성으로 구성되며 고도 20,200km의 원궤도를 돌고 있다. 각 위성은 수신기가 위성을 식별할 수 있도록 위성의 위치, 상태정보 및 지상 수신기 시간보정용 송신시간을 항법메시지 속에 포함시켜 전송한다.

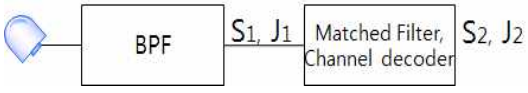


그림 1. GPS 수신기 개략 모델
Fig. 1. GPS receiver simple model

수신기는 수신 신호들의 전파시간차를 측정하여 수신기의 위치를 계산한다. GPS는 L1 반송파인 1575.42MHz와 L2 반송파인 1227.60MHz 주파수를 사용한다. 또한 주파수 대역이 각각 1.023MHz와 10.23MHz인 C/A 코드와 P(Y) 코드를 제공한다. P(Y) 코드와 C/A 코드는 L1 반송파에 실려 송신되며, L2 반송파에는 P 코드만 실려 송신된다. C/A 코드는 민간용으로 개방되어 사용되며 P 코드는 군용으로 사용되고 있다[1]-[3].

지상 수신기에 도착하는 GPS 위성 신호의 세기가 매우 작기 때문에 지상의 GPS 수신기는 지상 재머에 취약하며, 이를 이용한 GPS 재머들이 개발되고 있다[4]-[6].

GPS 수신기의 간소화된 구조는 그림 1과 같이 안테나, 대역통과필터(BPF), 정합필터(Matched Filter), 채널 디코더 등으로 구성된다. 대역통과필터를 통과한 GPS 위성신호(S1)와 재머신호(J1)는 정합필터와 채널 디코더를 거치며 S2, J2로 변경된다. GPS 위성에서는 50Hz 대역의 항법 메시지를 1.023MHz의 C/A 코드와 10.23MHz의 P(Y) 코드로 대역 확산(Spread Spectrum)하여 송신하며, 상용 GPS 수신기에서는 동일한 C/A 코드로, 군용 GPS 수신기에서는 동일한 P(Y) 코드로 정합필터링되어 식 (1), (2)와 같은 처리 이득(Processing Gain)을 얻는다.

또한 채널 디코더를 거치며 코딩 이득(Coding Gain)을 얻는다. GPS 수신기의 대역통과필터 후단의 이론적인 감도(Sensitivity)는 대역통과필터의 밴드폭(Bandwidth)에 의한 열잡음(Thermal Noise)인 -114dBm(상용GPS), -104dBm(군용GPS) 보다 처리이득(상용 43dB, 군용 53dB) 만큼 낮은 -157dBm이다[8]-[10].

$$G_{p(\text{상용})} = 10Log\left(\frac{1.023MHz}{50Hz}\right) = 43.12\ [dB] \qquad (1)$$

$$G_{p\,(\text{군용})} = 10Log\left(\frac{10.23MHz}{50Hz}\right) = 53.12\ [dB] \qquad (2)$$

GPS 신호의 C/A 코드를 이용하는 기만 재밍의 경우 정합필터에서 GPS 위성 신호와 동일한 G_p 수준 또는 시간 동기 오류 등에 의한 G_p 이하의 처리 이득을 얻을 수 있으나, 잡음과 같은 비동기 재밍의 경우 정합필터에서 $\sqrt{G_p}$ 의 처리 이득을 얻을 수 있다[11].

2.2 GPS 재밍에 대한 기존 탐지 방법

기존의 GPS 재밍 탐지 방법은 크게 GPS 수신기 내부와 GPS 수신기가 아닌 다른 장치를 이용한 방법으로 나눌 수 있다. GPS 수신기 내부에서의 재밍 탐지는 지상(항공기 고도 포함)에서 수신할 수 있는 GPS 위성신호의 세기가 매우 작은 범위이므로 이 신호세기 이상의 큰 신호를 재밍으로 판단하는 방법이다. 이는 다시 절대적인 신호세기가 수신 예측 신호세기 보다 매우 큰 경우와 급격한 신호세기의 변화의 경우로 나누어 탐지할 수 있다. 또한 수신 코드와 반송파의 변화율을 비교, 도플러 변화량 검사, L1-L2 측정치 비교, 위성 궤도력 검사, 점프 검출 등의 방법이 있다[1]-[6].

GPS 수신기 외부에서의 탐지 방법은 DGPS (Differential GPS), TDOA(Time Difference Of Arrival) 수신기, ELINT 수신기 등을 이용한 방법 등이 있다. DGPS 방법은 기존의 정밀한 측정위치에 설치한 GPS 수신기에서 출력되는 좌표와 기 정밀 측정 좌표와의 차이에 의해 재밍을 탐지하는 방법이다. TDOA 수신기는 고감도 고정밀의 2개 이상의 수신 안테나를 이용하는 전자전(Electronic Warfare) 수신기를 이용하여 안테나에 도착하는 GPS L1, L2 주파수에서 스프레드 스펙트럼(Spread Spectrum) 성을 갖는 재밍 신호의 시간차로부터 재밍 신호원의 위치를 표정한다. ELINT 수신기를 이용한 방법은 광대역 고감도 전자전 수신기를 이용하여 GPS L1, L2 주파수에서 스프레드 스펙트럼 특성을 갖는 재밍 신호의 방향을 탐지하고 누적 방향으로부터 위치를 표정하는 방법이다[5][12][13].

III. GPS 재밍 탐지를 위해 제안한 상용 GPS 수신기와 항재밍 기능을 보유한 군용 EGI 수신기를 동시에 사용한 실시간 GPS 재밍 탐지 방법

기존의 GPS 수신기 내부와 외부에서의 재밍 탐지 방법은 단편적으로 GPS 재밍에 대해 식별할 수는 있으나, 공통적으로 재밍의 출력과 재밍 종류를 판별하는데 제한적이다. 본 논문에서 제시한 GPS 재밍 탐지 방법은 기존의 방법과 혼용하여 사용할 경우 오탐지 없이 보다 정확한 GPS 재밍의 탐지가 가능하다.

3.1 상용 및 군용 GPS 수신기 구성

상용 및 군용 GPS 수신기의 구성은 그림 2와 같다. 상용 GPS는 안테나, GPS 수신기, 시현장치로 구성되며, 군용 GPS는 항재밍 안테나, 항재밍 안테나시스템, EGI, 시현장치로 구성된다. 상용 GPS는 GPS 재밍에 대한 내성특성과 GPS 재밍 신호에 대한 탐지능력을 보유하고 있지 않다. 군용 GPS에서 항재밍 안테나와 항재밍 안테나시스템은 일반적으로 잡음재밍에 대한 항재밍 능력을 보유하고 있다. SAASM 칩이 내장된 EGI는 기만재밍에 대한 항기만 능력을 보유하고 있다. 이러한 항재밍 안테나, 항재밍 안테나시스템, EGI의 조합이 일반적인 군용 GPS로서, GPS 재밍에 대응하기 위한 수단으로 활용되고 있으나, GPS 재밍에 대한 내성특성은 보유할 수 있지만 정확한 GPS 잡음재밍과 기만재밍을 구분하여 탐지할 수는 없었다[14]-[21].

항재밍 안테나와 항재밍 안테나시스템은 함께 연동하여 안테나 빔 스티어링-널링 등에 의한 이득을 얻을 수 있으며, 85dB 이내의 항잡음재밍 능력을 보유한다. 대표적인 장비는 EDO사의 항재밍 안테나(7소자), Rockwell Collins사의 DIGAR(Digital Integrated GPS Anti-jam Receiver) 등이 있다. SAASM 칩이 적용된 EGI 등은 P(Y) 코드 처리 이득 등에 의해 53dB 수준의 항잡음 및 항기만 재밍 능력을 보유한다. 대표적인 장비는 Rockwell Collins 사의 ASR(Airborne SAASM Receiver) 등이 있다 [22]-[25].

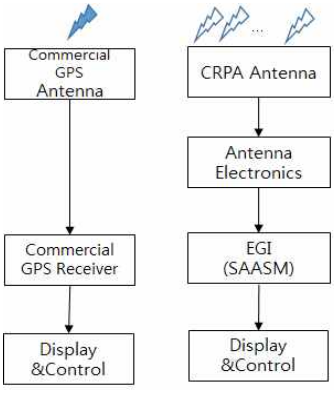


그림 2. 상용 GPS와 군용 EGI 수신기
Fig. 2. Commercial GPS and military EGI receiver

군용 GPS 시스템의 경우 항재밍 안테나-항재밍 안테나시스템-EGI(SAASM) 조합한 구성으로 주로 사용하여 항재밍 능력을 극대화한다.

3.2 GPS 재밍 탐지를 위한 다중 GPS수신기 채널 구성

상용 GPS 수신기는 대역확산되어, LPI 특성을 가지나, 제원이 노출되어 있고 GPS 위성과 수신기간 거리가 멀기 때문에 GPS 재밍에 취약하고, 군용 GPS 수신기는 구성품별로 항잡음 내성과 항기만 내성을 보유한다. 따라서 이러한 수신기의 특성을 조합하여 GPS 재밍 인가여부와 재밍종류를 판단할 수 있다. 그림 3과 같이 다중 채널로 구성함으로써, GPS 잡음재밍과 기만재밍을 탐지할 수 있으며, 상용 GPS 안테나 1대, 상용 GPS 수신기 2대, 항재밍 안테나 1대, 항재밍 안테나시스템 1대, EGI (SAASM 보유) 1대, 탐지장치 1대, 시현 및 음성경보 장치 1대로 구성된다.

상용 및 군용 GPS수신기로 구성된 다중 GPS수신기의 GPS 수신 채널은 그림 3과 같이 3가지 경로로 구성된다.

1번 채널은 상용 GPS1 안테나와 수신기로 구성된 경로로서 GPS1 수신기에서 출력되는 좌표를 A라 하자. 이 채널은 GPS 잡음재밍에는 상용 GPS 처리이득과 관련된 항잡음 능력이 있으나, 코히렌트(Coherent) 기만재밍의 경우 GPS 위성신호와 동일한 처리이득을 가지므로 항기만 능력을 보유하지 못한다.

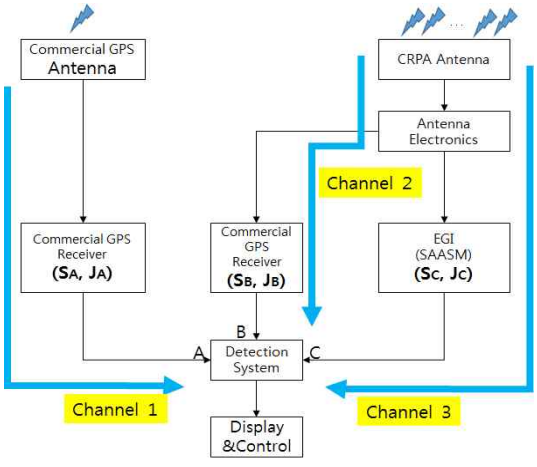


그림 3. 제안된 GPS/EGI 채널 모델
Fig. 3. Proposed GPS/EGI channel model

2번 채널은 항잡음 재밍 능력을 보유한 항재밍 안테나-항재밍 안테나시스템과 상용 GPS2 수신기로 구성된 경로로서 GPS2 수신기에서 출력되는 좌표를 B라 하자. 이 채널은 GPS 잡음재밍에는 상용 GPS 처리이득 및 항재밍 안테나-항재밍 안테나시스템에 의한 항잡음 이득과 관련된 항잡음재밍 능력을 보유하지만, 코히렌트 기만재밍의 경우 GPS 위성신호와 동일한 처리이득을 가지므로 항기만 능력을 보유하지 못한다.

3번 채널은 항잡음재밍 능력을 보유한 항재밍 안테나-항재밍 안테나시스템과 SAASM이 적용된 EGI 수신기로 구성된 경로로서 EGI 수신기에서 출력되는 좌표를 C라 하자. 3번 채널의 경우, GPS 잡음재밍은 항재밍 안테나-항재밍 안테나시스템에 의한 항잡음 이득과 군용 GPS 처리이득과 관련된 항잡음재밍 능력을 보유하며, 코히렌트 기만재밍의 경우 SAASM칩에 의한 처리이득과 관련된 항기만 능력을 갖는다.

3.3 채널별 이득 모델링

3.3.1 GPS 위성신호 수신 세기

GPS 위성은 고궤도 상공에서 운용되므로 지상 GPS 수신기까지 도달하는 GPS 위성신호는 자유공간에서의 전파 방정식을 적용할 수 있다.

L1, L2 주파수를 대상으로 기본적인 전파 방정식에 송수신 케이블 손실, 대기 손실을 고려한 GPS 수신기에서의 GPS 위성신호 수신 세기는 식 (3)과 같다[10].

$$S = \frac{P_{tt} G_{tt} G_{tr} \lambda^2}{(4\pi R_{tr})^2 L_{tt} L_{ta} L_{tr}} G_p \, G_c \; [dBm]. \tag{3}$$
$$= \frac{P_{tt} G_{tt} G_{tr} \lambda^2}{(4\pi R_{tr})^2 L_{tt} L_{ta} L_{tr}} \frac{G_p \, G_c}{B_{tt}} \; [dBm/Hz].$$

여기서 P_{tt}는 GPS 위성 출력, G_{tt}는 GPS 위성 안테나 이득, G_{tr}은 GPS 수신기 안테나 이득, λ는 파장, R_{tr}은 GPS 위성과 수신기간 거리, L_{tt}는 송신 케이블 손실, L_{tr}은 수신 케이블 손실, L_{ta}는 대기 손실 포함 안테나 패턴 손실, G_p는 처리 이득, G_c는 코딩 이득, B_{tt}는 C/A코드 또는 P(Y)코드 대역폭이다.

3.3.2 GPS 재머신호 수신 세기

3.3.2.1 GPS 재머

GPS 재밍이 가능한 가장 큰 이유는 거리차에 따른 신호세기 측면에서 GPS 재머가 매우 유리하기 때문이다. 링크 버짓을 분석하면, 이러한 GPS 위성과 GPS 수신기간 거리상 전파손실이 매우 크므로 GPS 수신기의 처리이득이 있더라도 GPS 수신기는 잡음과 기만 재밍 모두에 취약할 수 있다[10][26]-[30].

GPS 재밍의 종류는 크게 잡음재밍(일반적으로 비동기 재밍)과 기만재밍(일반적으로 동기 재밍)으로 구분된다. 잡음재밍은 GPS 신호세기보다 큰 잡음신호를 GPS 신호대역(GPS 신호대역 일부 또는 전체) 또는 인접대역에 송출하여 항법서비스를 불가능하게 만드는 것이다. 기만재밍은 기만(Spoofing)과 항로혼란(Meaconing)이 대표적이며, 기만은 GPS 신호 구조를 모방하여 GPS 신호와 동일하게 모사 항법신호를 생성하여 실제 GPS 신호보다 높은 신호세기로 전송하여 위치정보 오차를 유발하는 것이다. 항로혼란은 GPS 신호를 수신하여 저장한 후 일정 시간 후에 재출력하여 항로를 교란시키는 것이다.

이러한 GPS 재밍에 대응하기 위해, 항재밍 안테나, 항재밍 안테나시스템 및 SAASM 칩이 적용된 EGI(Embedded GPS and INS)를 사용하고 있으나, 이들 장비들은 자체 플랫폼에 탑재한 EGI의 GPS 수신기에 대한 항재밍 및 항기만 능력을 보유하고 있지만 GPS 잡음재밍과 기만재밍을 구분하여 탐지하는 기능은 보유하지 못하였다[10][31]-[34].

GPS 수신기를 탑재한 이동 플랫폼의 경우 실시간으로 잡음, 기만, 동시 잡음/기만 GPS 재밍을 구분하여 인지하고 탐지하는 장치가 없다. 그래서 GPS 좌표 정보가 간헐적 또는 완전히 소실되거나, 완전히 허위 좌표로 유도될 때, 운용자가 단순히 육안으로 상황을 인지하고 상황을 추정할 뿐 정확한 GPS 잡음재밍, 기만재밍, 잡음과 기만의 동시재밍인가 여부 및 GPS 재밍 종류를 판단할 수 없다. 이러한 GPS 재밍으로 인해 이동 플랫폼은 정확한 현재 좌표를 얻을 수 없어, 사고 등의 위험성에 노출되어 있는 상황이다.

3.3.2.2 GPS 수신기에서의 재머신호 수신 세기

자유공간에서의 재머신호의 GPS 수신기에 수신되는 신호의 세기는 식 (4)와 같다.

$$J = \frac{P_{jj} G_{jj} G_{jr} \lambda^2}{(4\pi R_{jr})^2 L_{jj} L_{ja} L_{jr} M} G_p{}' \; [dBm]. \tag{4}$$
$$= \frac{P_{jj} G_{jj} G_{jr} \lambda^2}{(4\pi R_{jr})^2 L_{jj} L_{ja} L_{jr} M} \frac{G_p{}'}{B_{jj}} \; [dBm/Hz].$$

여기서 P_{jj}는 재머 출력, G_{jj}는 재머 안테나 이득, G_{jr}은 재머 신호의 입사각에 따른 GPS 수신기 안테나 이득, R_{jr}은 재머와 수신기간 거리, L_{jj}는 송신 케이블 손실, L_{ja}는 대기 손실 포함 안테나 패턴 손실, L_{jr}는 수신 케이블 손실, 대기 손실, M은 재밍을 위한 마진, $G_p{}'$는 재머 신호의 처리이득, B_{jj}는 재머 신호의 대역폭이다.

지상 재머와 지상 GPS 수신기는 지구의 지리적인 영향을 받으므로 자유공간에서의 전파 전파 방정식에 추가적인 요소를 고려해야 한다.

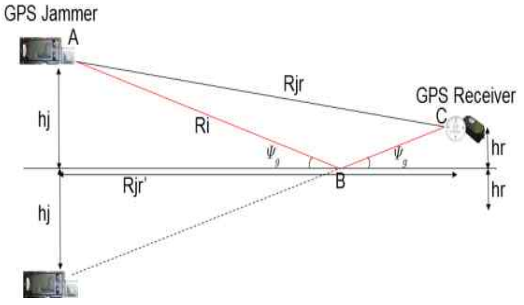


그림 4. 평면 지구 반사 모델
Fig. 4. Reflection model of flat earth

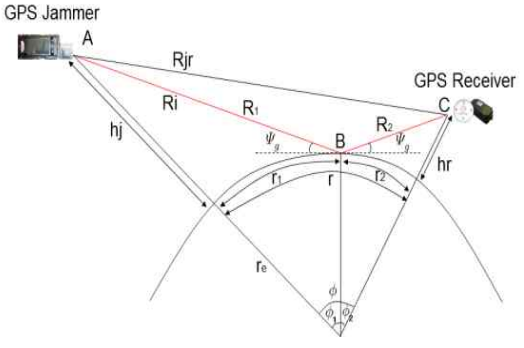


그림 5. 곡률 지구 반사 모델
Fig. 5. Reflection model of curved earth

굴절과 반사의 전파요소가 고려된 그림 4의 평면 지구 모델과 그림 5의 곡률 지구 모델에서의 GPS 수신기에서의 재밍신호의 수신 세기 J', J"은 각각 식 (5), (6)과 같이 표현된다.

$$J' = J \times 4\left(\sin\frac{2\pi h_j h_r}{\lambda R_{jr'}}\right)^2 \tag{5}$$
$$= \frac{P_{jj}G_{jj}G_{jr}\lambda^2}{(4\pi R_{jr})^2 L_{jj}L_{ja}L_{jr}M}\frac{G_p{}'}{B_{jj}}4\left(\sin\frac{2\pi h_j h_r}{\lambda R_{jr'}}\right)^2$$
$$[dBm/Hz].$$

$$J'' = J \times 4\left(\sin\left(\frac{\pi}{\lambda}\frac{4R_1R_2(\sin\Psi_g)^2}{R_1+R_2+R_{jr}}\right)\right)^2 \quad (6) \tag{6}$$
$$= \frac{P_{jj}G_{jj}G_{jr}\lambda^2}{(4\pi R_{jr})^2 L_{jj}L_{ja}L_{jr}M}\frac{G_p{}'}{B_{jj}} \times$$
$$4\left(\sin\left(\frac{\pi}{\lambda}\frac{4R_1R_2(\sin\Psi_g)^2}{R_1+R_2+R_{jr}}\right)\right)^2 [dBm/Hz]$$

그림 2, 3에서 재머의 고도가 h_j, GPS 수신기의 고도가 h_r이고 입사각이 Ψ_g이고, 재머의 송신 에너지는 직접경로 R_{jr}(A-C)와 간접경로 R_i(A-B-C)에 의해 GPS 수신기 안테나에 전달된다. R_1, R_2는 재머와 수신기의 반사점까지의 거리이다. r_e는 전파 굴절에 의해 확장된 지구반지름을 의미한다[10]. 평면 지구 모델은 재머와 GPS 수신기의 고도가 낮아 거리가 가까운 경우에 효과적이나 고도가 증가하여 거리가 멀어질 경우는 오차가 증가하게 된다. 곡률 지구를 고려할 때 전자파는 대기 굴절로 굽은 경로를 진행한다.

식 (3)~(6)의 변수를 표 1, 2와 같이 임의 데이터를 적용하면, 그림 3의 1, 2, 3번 채널에서의 안테나 단부터의 채널 별 내부 이득은 그림 6, 표 3과 같이 모델링될 수 있다. 또한 표 1, 2에서 사용한 유효방사출력(ERP), 송신케이블 손실, 거리에 따른 공간손실, 대기손실 등과 표 3의 내부 이득 데이터를 통해, 수신기 채널별 내부에서의 GPS 위성신호, 재밍신호의 세기 및 JSR은 표 4, 5와 같다. 이들 표에서 사용한 데이타들은 임의로 선정한 시험용 값으로서 채널을 구성하는 제품 및 방법에 따라 상이할 수 있다.

표 1. GPS 위성-수신기에 사용된 시뮬레이션 재원
Table 1. Simulation variables of GPS satellite-receiver

	Data	
P_{tt}	Arbitrary Ommission	
G_{tt}	Arbitrary Ommission	
G_{tr}	-1dBi	L1 band
	0dBi	L2 band
f	L1 frequency	L1
	L2 frequency	L2
R_{tr}	20,200km	
L_{tt}	Arbitrary Ommission	
L_{tr}	-1dB	
L_{ta}	Arbitrary Ommission	
G_p	43.12dB	L1
	53.12dB	L2
G_c	Arbitrary Ommission	
B_{tt}	1.026MHz	L1
	10.26MHz	L2

표 2. GPS 재머-수신기에 사용된 시뮬레이션 재원
Table 2. Simulation variables of GPS jammer-receiver

	Data	
P_{jj}	Arbitrary Ommission	
G_{jj}	Arbitrary Ommission	
G_{jr}	-7.5dBi	L1
	-45dBi	L2
R_{jr}	Arbitrary Ommission	
L_{jj}	Arbitrary Ommission	
L_{ja}	Arbitrary Ommission	
L_{jr}	-1dB	
M	7dB	
G_p'	Arbitrary Ommission	Noise Jamming(L1)
	Arbitrary Ommission	Noise Jamming(L2)
	Arbitrary Ommission	Deception Jamming(L1)
	Arbitrary Ommission	Deception Jamming(L2)
B_{jj}	2.052MHz	Noise Jamming(L1)
	20.52MHz	Noise Jamming(L2)
	1.026MHz	Deception Jamming(L1)
	10.26MHz	Deception Jamming(L2)

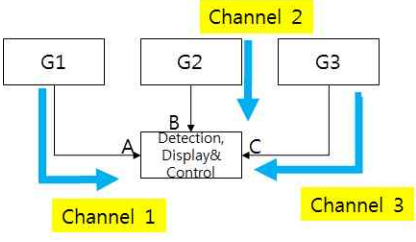


그림 6. 채널 이득 모델
Fig. 6. Channel gain model

표 3. 채널 이득 [dB]
Table 3. Channel gain [dB]

		Channel 1	Channel 2	Channel 3
GPS		44.12	45.12	55.12
Jammer	Noise	6.06	-31.44	-26.44
	Deception	24.62	-12.88	-4.88

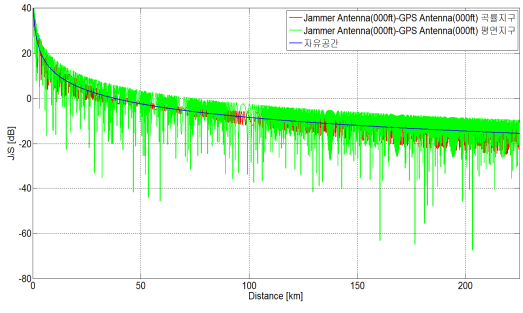
표 4. 각 채널의 수신신호 세기 [dBm]
Table 4. Received power of each channel [dBm]

		Channel 1	Channel 2	Channel 3
GPS		-84.86	-83.86	-71.69
Jammer	Noise	-91.33	-128.83	-121.66
	Deception	-72.77	-110.27	-100.10

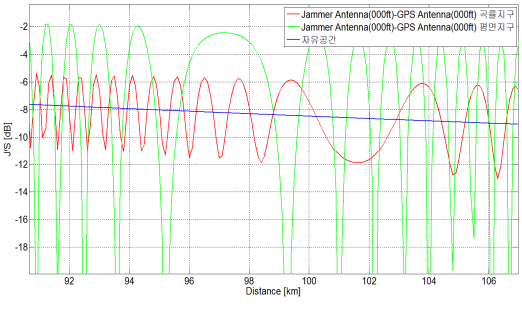
표 5. 각 채널의 JSR [dB]
Table 5. JSR of each channel [dB]

	Channel 1	Channel 2	Channel 3
Noise	-6.47	-44.97	-49.97
Deception	12.09	-26.41	-28.41

GPS 재밍 신호는 자유공간이 아닌 지구의 지리적 영향을 받으므로, 표 4, 5에서 기술된 재밍신호의 세기는 식 (5), (6)의 전파요소 성분이 고려되어야 한다. GPS 수신기의 고도 h_r, GPS 재머의 고도 h_j를 임의 설정하여 1,2,3번 채널에 대해 잡음재밍과 기만재밍이 인가된 JSR과 100km 근처에서 확대한 JSR은 그림 7~12와 같다. 각 그림에서는 자유공간, 평면지구, 곡률지구에서의 전파요소에 의해 거리에 따른 이득과 손실이 변경되는 페이딩(fading)이 발생한다. 이러한 페이딩은 정확한 예측이 어려우나, 실제 지구와 가장 유수한 곡률지구 모델의 경우 JSR의 변동 범위가 4~6dB 수준으로 이 수치는 표 5에 각 채널에 이득 또는 손실로서 공통적으로 적용된다.

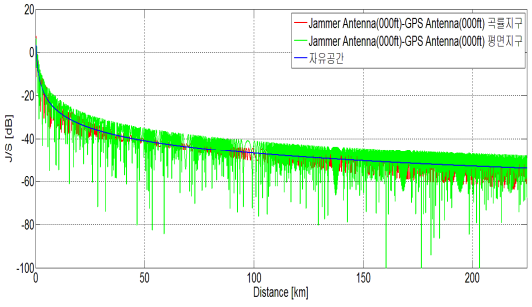


(a) Wide range

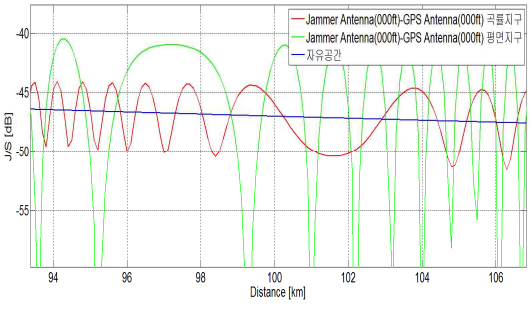


(b) Concerned narrow range

그림 7. 지리적 효과에 의한 JSR(채널 1, 잡음재밍)
Fig. 7. JSR on geographic effect(channel 1, noise jamming)



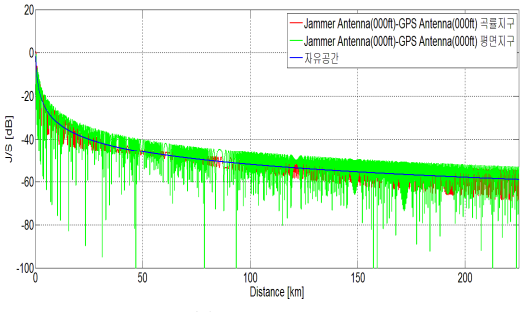
(a) Wide range



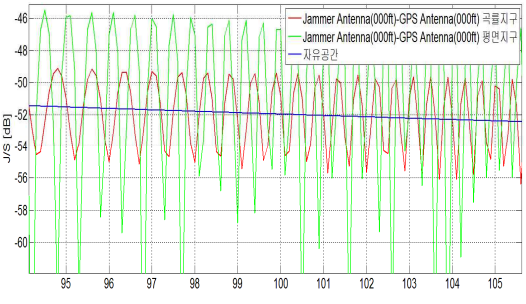
(b) Concerned narrow range

그림 8. 지리적 효과에 의한 JSR(채널 2, 잡음재밍)

Fig. 8. JSR on geographic effect(channel 2, noise jamming)



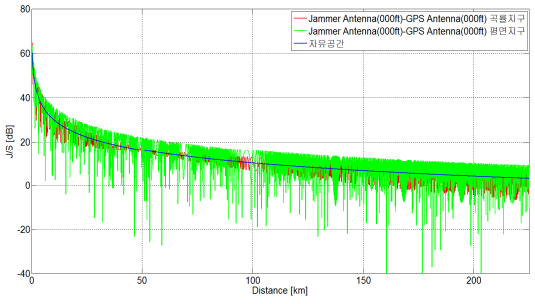
(a) Wide range



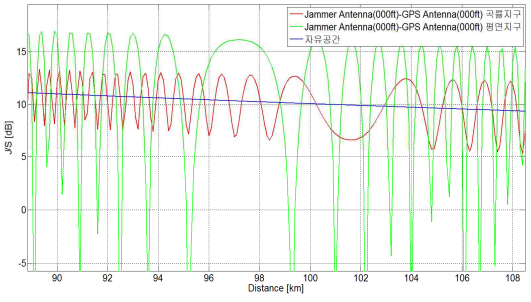
(b) Concerned narrow range

그림 9. 지리적 효과에 의한 JSR(채널 3, 잡음재밍)

Fig. 9. JSR on geographic effect(channel 3, noise jamming)



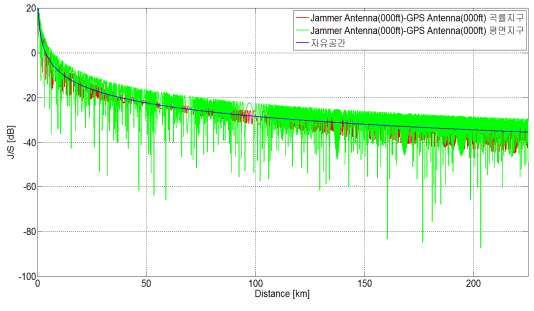
(a) Wide range



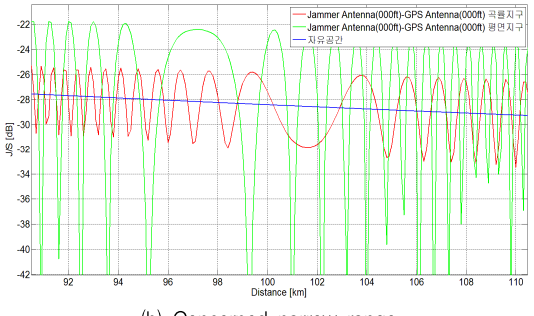
(b) Concerned narrow range

그림 10. 지리적 효과에 의한 JSR(채널 1, 기만재밍)

Fig. 10. JSR on geographic effect(channel 1, deception jamming)



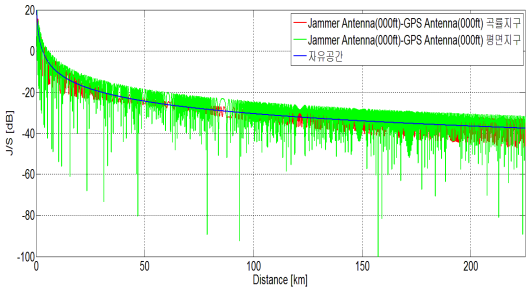
(a) Wide range



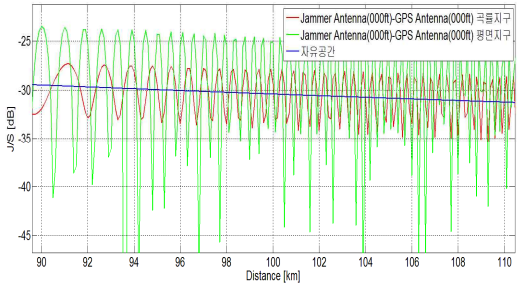
(b) Concerned narrow range

그림 11. 지리적 효과에 의한 JSR(채널 2, 기만재밍)

Fig. 11. JSR on geographic effect(channel 2, deception jamming)



(a) Wide range



(b) Concerned narrow range

그림 12. 지리적 효과에 의한 JSR(채널 3, 기만재밍)
Fig. 12. JSR on geographic effect(channel 3, deception jamming)

재밍이 없는 경우는 그림 13(a)와 같은 분포를 보일 것으로 예상된다.

잡음재밍은 비동기 재밍이라고도 하며 시간적으로나 GPS 위성신호의 주파수 등 신호특성과 무관하여 상관도가 작은 잡음을 사용하는 재밍이다.

기만재밍은 GPS 위성신호의 복사본을 이용하여 시간적으로도 동기를 맞추는 재밍으로서 GPS 위성신호와 상관도가 매우 높다.

잡음재밍과 기만재밍은 서로 상관도가 작다. 따라서, 잡음재밍과 기만재밍은 임의 데이터를 사용하여 작성된 표 5의 JSR의 동적범위 내에서 정의되는 저출력과 고출력의 재밍 신호의 세기에 따라 1, 2, 3번 채널에 서로 독립적으로 작용할 것이다.

잡음재밍의 경우, 저출력 잡음재밍의 경우, (b)와 같이 잡음에 취약한 1번 채널의 A좌표부터 소실될 것이다. 고출력 잡음재밍의 경우, (c)와 같이 A, B좌표가 소실될 것이다.

기만재밍의 경우, 저출력 기만재밍의 경우, (d)와 같이 가장 취약한 1번 채널의 좌표인 A가 기만되어 재밍이 유도하는 시나리오대로 이탈할 것이다. 고출력의 기만재밍인 경우, (e)와 같이 1번과 2번 채널의 좌표인 A, B가 이탈할 것이다.

상용 GPS 수신기의 2차원 위치 정확도가 100m(99%)이고, 군용 EGI 수신기 정확도가 16.8m(99%)로서 그림 14(a)와 같다[3][24].

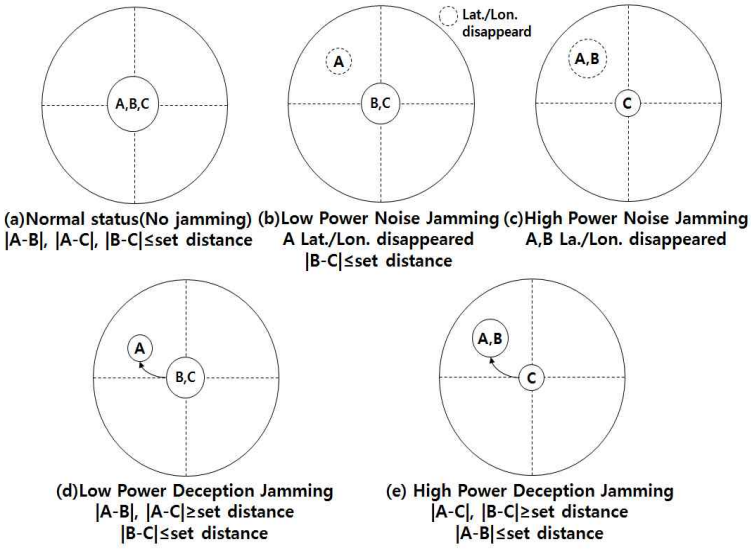


그림. 13. 재밍 종류에 의한 각 채널의 좌표 분포
Fig. 13. Position distribution of each channel by jamming kind

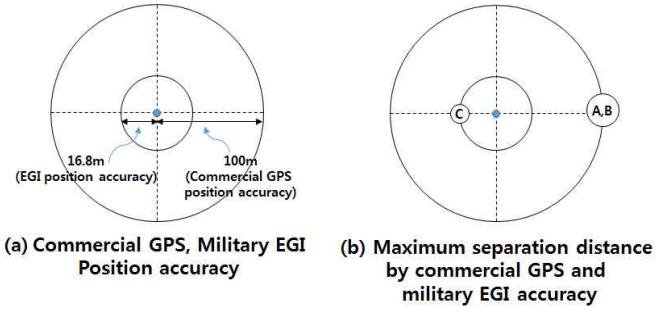


그림. 14. 상용 GPS, 군용 EGI 수신기의 위치 정확도
Fig. 14. Position accuracy of commercial GPS, military EGI receiver

표 6. 각 채널 위치 분포에 의한 재밍 종류 추정
Table 6. Estimation of jamming kind by each channel position distribution

Lat/Lon Distribution / Jamming	A Dis-appeared	B Dis-appeared	C Dis-appeared	|A-B|≥ set Distance	|A-C|≥ set Distance	|B-C|≥ set Distance
No Jam.						
Low Power Deception				√	√	
High Power Deception					√	√
Low Power Noise	√					
High Power Noise	√	√				

난수를 반복적으로 발생하여 통계치를 계산하는 몬테카를로(Monte-Carlo) 방식 대신 위치 정확도에 따라 그림 14(b)와 같이 위치가 분포된다고 가정을 단순화할 때, 상용 GPS 수신기와 군용 EGI 수신기의 위치 정확도에 따른 거리 오차는 116.8m가 되며, 이 값을 설정값으로 선정할 수 있다. 만약 각 채널별 좌표 위치간 설정값을 116.8m 보다 큰 값으로 선택하면 False Alarm율을 줄일 수 있다.

이러한 재밍신호 및 신호세기에 따라, 1,2,3번 채널 좌표인 A,B,C간 분포를 종합해 보면 표 6과 같다.

GPS 위성신호 모의기중 대표적인 장치가 SPIRENT사 제품이며 이러한 장비 등을 통해 기만재밍을 모의하였으며, 잡음재밍은 신호발생기 등을 통해 잡음을 모의하였다. 그림 3의 3개 채널로 구성된 장치의 시험 개념도는 그림 15와 같다.

그림 16(a)는 재밍이 없는 환경에서의 재밍탐지 장치 화면이다. (b)는 잡음 재밍 환경에서의 재밍탐지 장치 화면이다. (c)는 기만 재밍 환경에서의 재밍탐지 장치 화면이다. 이러한 시험결과들의 탐지장치 화면을 종합하면, 표 6에 기술된 A,B,C 좌표의 소실 여부와 |A-B|, |B-C|, |C-A|가 거리오차를 벗어나는지 여부에 따라 인가된 재밍의 신호세기 및 종류를 탐지할 수 있음을 확인하였다.

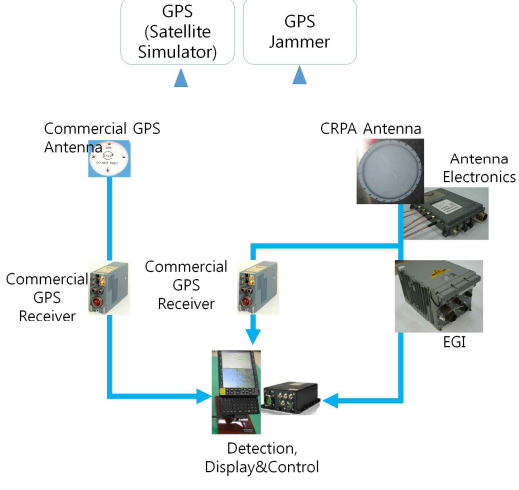
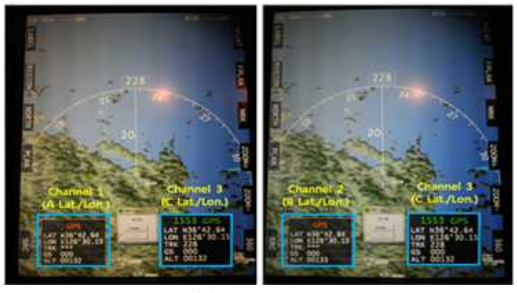
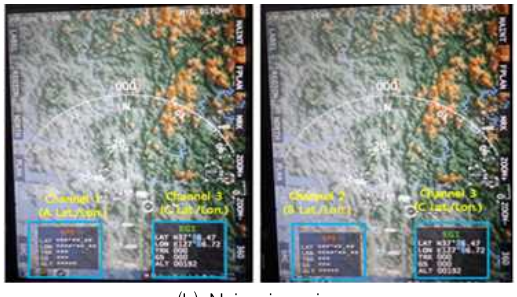


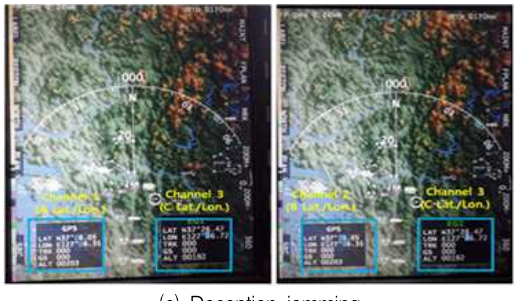
그림. 15. 재밍신호 탐지장치 시험 개념도
Fig. 15. Test configuration of jamming detection system



(a) No jamming



(b) Noise jamming



(c) Deception jamming

그림. 16. 재밍탐지 장치 화면 예

Fig. 16. Jamming detection equipment display example

IV. 결론 및 향후 과제

GPS 위성-수신기간 거리가 GPS 재머-수신기간 거리보다 매우 커서, 신호 세기 측면에서 GPS 수신기는 GPS 재밍에 매우 취약하다. GPS 신호가 대역 확산되어 저피탐확률 특징을 가지고 있어 GPS 위성신호를 탐지하기 쉽지 않다. 이에 GPS 재머들은 기존의 단순한 잡음재밍을 인가하는 방식에서 벗어나, 탐지하여 저장 또는 모의 생성된 GPS 위성신호를 정확한 시간동기를 맞추어 GPS 수신기에 방사하는 기만재밍 신호들이 주로 사용된다. 이에 군용 GPS 수신기는 잡음과 기만재밍에 대한 내성을 보유한 장치들을 구성하여 사용한다. 하지만 이러한 장치들은 재밍에 대한 내성은 일부 보유하나 GPS 재밍의 종류를 판단할 수는 없었다.

본 논문에서는 상용 GPS 수신기와 군용 GPS 수신기를 이용하여 GPS 재밍에 대한 내성 특성이 각기 다른 3개의 채널을 구성함으로써 GPS 재밍의 종류를 판단할 수 있는 방법을 제시하였다. 본 논문에서는 GPS 위성신호와 재밍 신호가 GPS 수신기에 어떤 신호세기로 수신되는지 신호세기 측면에서 분석하였다. 이러한 분석을 통해 각 채널에서 계산되는 위치정보에 대한 오차분포를 예상하였고, 오차분포로부터 인가되는 GPS 재밍의 종류를 탐지할 수 있는 방법을 제시하였다. 또한 제한적이지만 잡음과 기만 재밍 환경에서 재밍신호에 대한 탐지 가능성을 확인하였다. 이러한 탐지기술은 이동 플랫폼 또는 고정 주요시설에 사용되어 실시간으로 GPS 재밍의 인가 여부 및 종류를 탐지하는데 활용할 수 있다. 이를 통해 민간분야의 경우 교통 혼란, 충돌 방지를 위한 공지가 가능할 것으로 기대되며 국방 분야의 경우는 GPS 재밍상황의 인지 아래 안정적인 작전수행 등 GPS 재밍에 신속히 대처할 수 있고 GPS 재머의 위협변수 관리를 통해 체계적인 대응이 가능할 것으로 판단된다.

References

[1] Wei Quan, Jianli Li, Xiaolin Gong, and Jiancheng Fang, "INS/CNS/GNSS Integrated Navigation Technology", Beihang University, pp. 1-51, Jul. 2014.

[2] Schmid and Andreas, "Advanced Galileo and GPS receiver techniques : enhanced sensitivity and improved accuracy", Hauppauge, NY, pp. 1-10, Jan. 2009.

[3] "NAVSTAR GPS USER EQUIPMENT INSTRUCTION", Public Release Version, pp. 46, 103, Sep. 1996.

[4] S. K. Jeong, T. H. Kim, C. S. Sin, and S. U. Lee, "Technical Trends of Smart Jamming for GPS Signal", ETRI Electronics and Telecommunications Trends Vol. 27, No. 6, pp. 75-82, Dec. 2012.

[5] K. C Yoon, "GPS Jamming Countermeasures",

STC EW R&D Center, pp. 1-9, Feb. 2012

[6] SHOGHI COMMUNICATION company, https://www.shoghicom.com/electronic-warfare.php [Accessed: Apr. 02. 2018]

[7] A. El-Mowafy, "Kinermatic attitude determination from GPS, Department of Geomatrics Engineering", The univ. of Calagary, 1994.

[8] J. C. McMillan, D. A. G Arden, G. Lachalelle, and G. Lu, "Dynamic GPS performance using INS/GPS reference", Proceedings of ION GPS-94, pp. 2-7, Sep. 1994.

[9] H, Hu and N. Wei, "A study of GPS jamming and anti-jamming", in Proc. 2009 2nd Int. Conf. Power Electron. Intell. Transportation Syst. (PEITS), Shenzhen, China, pp. 388-391, Dec. 2009.

[10] YoungJoong Lee, JooRae Park, and JongKyu Kim, "An analysis on GPS jammer operational range against GPS receiver in sea environment", Journal of the KIMST, Vol. 14, No. 2, pp. 232-237, Apr. 2011

[11] YoungJoong Lee, InSeon Kim, JooRae Park, HyunKyu Kwak, and WookHyun Shin, "A study on evaluation of jamming performance on SAR satellite", Journal of the KIMST, Vol. 13, No. 2, pp. 252-257, Apr. 2010.

[12] Nathan A. White, Peter S. Maybeck, and Stewart L. Devilbiss, "Detection of Interference/Jamming and Spoofing in a DGPS-Aided Inertial System", IEEE Transactions on Aerospace and Electronic Systems, pp. 1208-1217, Oct. 1998.

[13] Alison Brown, Dale Reynolds, Capt. Darren Roberts, and Major Steve Serie, "Jammer and Interference Location System – Design and Initial Test Results", Proceedings of the ION GPS '99, pp. 1-6, Sep. 1999.

[14] Nathan A. White, Peter S. Maybeck, and Stewart L. DeVilbiss, "Detection of Interference/Jamming and Spoofing in a DGPS-Aided Inertial System", IEEE Transactions on Aerospace and Electronic Systems, Vol. 34, No. 4, pp. 1208-1217, Oct. 1998

[15] Todd E. Humphreys, Brent M. Ledvina, amd Mark L. Psiaki, "Assessing the Spooping Threat: Development of a Portable GPS Civilian Spoofer", Preprint of the 2008 ION GNSS Conference, pp. 1-12, Sep. 2008.

[16] Yuting Ng and Grace Xingxin Gao, "Mitigating Jamming and Meaconing Attacks Using Direct GPS Positioning", Proceedings of the IEEE/ION Position, Location and Navigation Symposium, PLANS 2016, pp. 1021-1026, May 2016.

[17] Z. Ahmad, M. Thahir, and I. Ali, "Analysis of beamforming algorithms for antijam", in Proc. 2013 Int. Seminar/Workshop Direct Inverse Problems Electromagn. Acoust. Wave Theory (DIPED), Lviv, Ukraine, pp. 89-96, Sep. 2013.

[18] Ki-Yun Kim, "Analysis of Anti-Jamming Techniques for Satellite Navigation Systems", Journal of KICS, Vol. 38C, No. 12, pp. 1216-1227, Dec. 2013.

[19] Anindya Kundu and Soham Ghosh, "Development of Smart Antenna Array Signal Processing Algorithm for Anti-Jam GPS Receiver", Progress In Electromagnetics Research Symposium, Hangzhou, China, pp. 125-131, Mar. 2008.

[20] YoungJoong Lee, GilJae Lee, YangWon Park, DongKeun Lee, and ByumJun Park, "GPS jamming detection equipment design using multiple GPS receiver channel", Conference of the KIMST 2016, pp. 514-515, Jun. 2016

[21] Young-Joong Lee and Sung-Woong Ra, "A Study on Estimation of Detection and Identification Types of GPS Jamming", Conference Proceedings, Seoul International Conference on Engineering and Applied Sciences, pp. 384-387, Feb. 2017

[22] "Digital Integrated GPS Anti-jam Receiver (DIGAR) brochure", Rockwell Collins homepage [Accessed: Apr. 02. 2018]

[23] "DIGAR-300 GPS anti-jam antenna electronics

brochure", Rockwell Collins homepage [Accessed: Apr. 02. 2018]

[24] "Airborne SAASM Receiver brochure", Rockwell Collins homepage [Accessed: Apr. 02. 2018]

[25] Hugo Fruehauf, "A better way of life for PPS users. GPS SAASM and P(Y)-direct, the new wave of military receiver technology for the PPS navigation and time and frequency user", Zyfer, Inc., 31st annual precise time and time interval(PTTI) meeting, pp. 347-356, 1999.

[26] Lamont V. Blake, "Ray Height Computation for a Continuous Nonlinear Atmospheric Refractive-Index Profile", Radio Science, Vol. 3, No. 1, pp. 85-92, Jan. 1968.

[27] Ralph M. Schmalenberger, and Michael G. Edrich, "Channel Modelling for Wideband Data Communication in a Maritime Mobile Environment", Eurocomm 2000, Information systems for enhanced public safety and security, IEEE/AFCEA, May 2000.

[28] D. E. Kerr, "Propagation of Short Radio Waves", M.I.T. Radiation Laboratory Series, Vol. 13, McGraw-Hill, 1951

[29] Young-Joong Lee, In-Seon Kim, and Joo-Rae Park, "A study on estimation of VHF datalink range in the sea", Journal of the KIMST, Vol. 11, No. 6, pp. 55-62, Dec. 2008.

[30] Young-Joong Lee, In-Seon Kim, and Joo-Rae Park, "A study on estimation and factors of VHF datalink range", Journal of the KIMST, Vol. 13, No. 3, pp. 413-420, Jun. 2010.

[31] Filippo Neri, "Introduction to Electronic Defense Systems", Artech House, 1991.

[32] Young-Joong Lee and Sang-Yeol Lee, "Jamming signal generation using DRFM", ADD, IEDC-517-011144, Nov. 2001

[33] SangYeol Lee, "ALQ-X system jamming technique", ADD, IEDC-517-011141, Nov. 2001.

[34] "Radio communication principle and jamming technique", ROKAF, 2005.

저자소개

이 영 중 (Young-Joong Lee)

1996년 2월 : 전북대학교 전자공학과(공학사)
1998년 2월 : 전북대학교 전자공학과(공학석사)
1998년 2월 ~ 현재 : 국방과학연구소 선임연구원
관심분야 : 디지털 신호처리, GPS/SAR 재밍/재밍탐지, 전자전장비

나 성 웅 (Sung-Woong Ra)

1976년 2월 : 서울대학교 전기공학과(공학사)
1978년 2월 : 한국과학기술원 전기 및 전자공학과(공학석사)
1992년 8월 : 한국과학기술원 전기 및 전자공학과(공학박사)
1980년 ~ 현재 : 충남대학교 전자전파정보통신공학과 교수
관심분야 : 통신, 디지털 신호처리, 영상처리