GPS 재밍 기법과 항재밍 GPS 기술

조인화 · 김형석 · 박태용

호원대학교

GPS Jamming Techniques and Anti-Jamming GPS Technologies

In-hwa Jo · Hyeong-suk Kim · Tae-yong Park

Howon University

E-mail : joeh0406@nate.com

요 약

위성을 이용한 측위 장치인 GPS는 위치를 구하는 용도 뿐 아니라 항법, 시간 정보 획득 등 다양한 분야에 활용되며, 특히 미사일 등 정밀 유도무기의 정밀도를 향상시키는데 중요한 역할을 하고 있다. 그러나 민간에 공개된 상용 코드(C/A 코드)를 사용하는 GPS는 대전자전 기능이 없다. 그러므로, 다양한 재밍 기법에 취약하고, 암호화된 군용 코드(P 코드)의 경우에도 인접한 곳에서 잡음 재밍 공격을 가할 경우 취약할 수 있다. 본 논문에서는 GPS의 재밍 기법과 과거 북한의 GPS 재밍 사례에 대해 조사하고, 항재밍 GPS에 적용되는 기술에 대해 설명하였다.

ABSTRACT

Positioning system using satellite GPS is used at positioning, navigation, acquisition time information and other various field and taking an important part precision guided weapon such as missile. But commercial code(C/A code) do not have ECCM. Therefore commercial code is vulnerable to various jamming techniques and noise jamming from near station can attack even the encrypted military code(P code) GPS. In this paper, GPS jamming techniques, North Korean GPS jamming cases and anti-jamming GP S technologies are surveyed and described.

키워드

GPS, 재밍, 항재밍 GPS, Anti-jamming GPS

Ⅰ. 서 론

평소 자동차 네비게이션 시스템, 스마트폰 위치 정보 등을 통해 친숙하게 접하고 있는 GPS(Global Positioning System)는 원래 미국이 군사용으로 활용하기 위해 개발한 체계이다. 민간 분야에서 GPS는 항공기, 선박, 차량 등의 항법장치에는 물론 휴대전화의 시간 동기, 토지 측량 등 광범위하게 활용되고 있다. 군사용으로는 함정 및 항공기의 항법장치에 활용되는 것은 물론 지상군 전투요원들의 개인 위치를 지휘소에 자동으로 전송해 주는 PRE(Position Reporting Equipment), 정밀유도무기체계의 정밀도 향상, 지휘통신체계의 통신 동기화를 위한 정확한 타이밍 정보 제공 등 다양한 용도로 활용되고 있다. 무기체계가 첨단화 될수록 GPS의 의존도는 높아지며, 따라서 미국에 대한 의존도를 낮추기 위해 러시아의 GLONASS, 유럽의 Galileo, 중국의 북두 등 몇몇 나라들은 독자적인 위성측위 시스템을 구축하고 있다. 우리군은 GPS에 많은 부분을 의존하고 있으며, 군사분야에서는 GPS에 제대로 작동하지 않을 경우 정밀유도무기 운용, 항법장비 운용 등에 제한을 받을 수 있다. 이러한 취약점을 노린 GPS 재밍 기법이 개발되어 있고, 실제 2011년 3월 4일 수도권 서북부 지역에서 발생한 GPS 전파 교란 현상의 진원지가 북한 개성 인근이라고 밝혀졌으며, 이때 민간 분야에서는 2G 이동통신망 혼선과 시각의 오차가 발생하였고, 군에서는 포병부대의 계산장비가 경미하게 영향을 받은 바 있다[1].

본 논문에서는 GPS의 개념에 대해 간략히 설명하고 GPS 재밍 기법과 재밍에 대응하기 위한 항재밍 기법에 대해 조사하여 기술하였다.

Ⅱ. GPS 개요

GPS는 최초의 위성항법 체계인 미 해군의 NNSS (Navy Navigation Satellite System) 이후 미 국방성의 주도하에 군사적 목적으로 1973년 연구개발에 착수하였으며, 1995년에 완성되었다. GPS는 원래 군용 항법시스템이지만, 민간용으로는 제한된 범위에서 사용 가능하게 한 위성항법 시스템으로 위성에서 수신기까지의 전파도달 시간을 측정하여 정확한 3차원 위치, 속도 및 시각 측정이 가능하며 무한의 이용자가 전 세계에서 24시간 이용 가능하다[2].

GPS 위성은 모두 24개이며, 고도 20,200km 상공에서 한 궤도에 4개의 위성이 60도 간격으로 떨어진 6개의 궤도를 따라 11시간 58분을 주기로 공전한다. GPS 측량의 기본 원리는 삼각 측량법으로, GPS 위성은 자신의 ID Code와 궤도 위치, 시간 정보를 송출하게 되고, GPS 수신기는 위성에서 발사하는 이들 정보를 수신하여 자신의 위치를 계산한다. 2개의 위성정보를 받으면 자신이 위치 가능한 선형 궤적을 유추할 수 있고, 3개의 위성정보를 받으면 평면상의 한 점으로 자신의 위치가 파악되며, 4개의 위성정보를 받으면 공간상의 한 지점으로 위치 식별이 가능해진다[3].

GPS 위성에서는 반송파, PRN(Pseudo-Random Number) 코드, 항법메시지를 지상으로 송신한다. 반송파는 L-밴드 대역의 주파수를 사용하며, L1(1,575.42MHz), L2(1,227.6MHz) 두 가지의 주파수에 PRN코드와 항법메시지를 변조하여 보낸다. PRN코드에는 두 가지가 있는데, 그 하나는 C/A코드(Coarse Acquisition Code)이고, 다른 하나는 P코드(Precise Code)이다. 민간 사용자는 L1 반송파만 사용하므로 C/A코드만 수신할 수 있으며, 1,023비트로 이루어졌고, 1msec마다 반복된다. P코드는 자격을 갖춘 특정한 사용자만 사용할 수 있도록 암호화하여(암호화된 P코드를 Y코드라 한다) 군용으로 쓰이는데, 10.23MHz의 주파수를 가지며, L1과 L2 반송파에 동시에 실린다. L1과 L2 반송파가 이온층을 통과하는 시간차를 이용하여 이온층 지연시간을 계산하여 의사거리를 보다 정확히 계산할 수 있으므로 C/A코드보다 정확도가 높다[4].

Ⅲ. GPS 재밍 기법 및 주요 적용 사례

GPS와 같이 위성을 사용하는 모든 GNSS(Global Navigation Satellite System)의 단점은 약 2만 킬로미터 상공에서 운행 중인 위성에서 보내온 신호를 사용하기 때문에 그 신호의 크기가 굉장히 약해 우발적이거나 악의적인 간섭에 취약하다. 태양 활동에 의한 자연적 간섭현상에서부터 우발적인 발신 장치 오작동이나 신호 반사, 악의적인 신호 교란에 이르기까지 다양한 형태로 발생된 교란에 취약하다[1].

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 시각 정보를 산출토록 하는 기만(Spoofing), 즉 스마트 재밍(Smart Jamming)으로 나눌 수 있다. 스마트 재밍은 GPS 기만기를 이용하여 이루어지는데, GPS 기만기는 공개된 GPS 신호 구조를 이용하여 오차가 인가된 거짓 GPS 신호를 생성하여 목표로 삼은 수신기에 송신함으로써 수신기가 잘못된 시각과 위치를 계산하도록 한다. 스마트 재밍을 위해 GPS 기만기는 GPS 신호를 수신하고 이를 처리할 수 있는 장비를 이용하여 임의 위성신호에 대해 오차가 삽입된 정보를 생성하고 이를 실제 GPS 신호보다 다소 높게 송출함으로써 목표로 삼은 수신기가 실제 GPS 신호가 아닌 기만기가 송출한 신호를 획득, 추적하도록 한다. GPS 신호를 수신하고 단순히 재방송하는 형태의 전파교란인 재방송은 수신기가 TOA(Time of Arrival) 정보를 사용하여 위치를 계산하는 점을 이용해 수신한 GPS 신호를 일정시간 동안 지연시킨 후 다시 수신기에 재송신함으로써 오차가 인가된 PVT(Positioning, Velocity, Timing) 정보를 산출하도록 하는 것이다[5].

북한은 1990년대 말 러시아로부터 GPS 교란 장비를 수입한 뒤 이를 개량한 독자 장비를 만든 것으로 알려졌다. 2006년 6월 미 하원 군사위원회 청문회에서도 북한이 GPS로 유도되는 정밀 타격무기를 교란하기 위한 재밍 능력을 갖췄다는 발언도 있었으며, 2010년 국정감사에서 김태영 전 국방장관은 북한이 러시아에서 수입한 차량 탑재 장비로 50-100km의 범위에서 GPS 전파 교란을 할 수 있다는 첩보가 있다고 확인한 바 있다고 언론에 보도된 바 있다[1].

과거 언론에 보도된 내용을 종합하면 북한은 2010년에만 8월, 11월, 12월에 총 세 차례 전자전 도발을 가해왔다. GPS 전파수신이 간헐적으로 중단되는 현상이 2010년 8월 23일~25일 전라남도 홍도에서 충청남도 안흥만까지 이르는 서해안 일부지역에서 수 시간 동안 발생했고, 국방부와 방송통신위원회는 교란신호 발신지를 북한으로 추정했다. 2010년 11월 23일 연평도 포격 당시에도 전파교란(Jamming)을 가하여 연평도의 대포병 레이더가 초기에 모두 작동이 안 되었고, 같은 해 12월 20일에는 연평도 상공을 비행 중인 우리 군의 무인정찰기에 GPS 재밍을 가하였다[7]. 또한 2011년 3월 4일에는 수도권 서북부 지역에서 GPS 전파 교란 현상이 발생하여 2G 이동통신 시스템에서 오작동이 발생하고, 포병부대의 계산장비가 경미한 영향을 받았는데, 이 교란 전파는 북한 개성 인근에서 발생한 것으로 알려졌다[1]. 미국의 경우 이라크 및 아프가니스탄 지역 등에서 진행 한 군사작전 중에 유도무기 일부가 당초 목표했던 장소가 아닌 지역에 떨어져 민간인 피해가 발생한 적이 있다[5].

Ⅳ. 항재밍 기법

GPS 재밍으로부터 보호하는 기법을 항재밍(Anti-jamming) 기법이라 한다.

위성항법 수신기로 유입되는 간섭 및 재밍신호를 효율적으로 제거 또는 억압하기 위한 항재밍 기술들은 크게 안테나 기술, 프론트 엔드(Front-End) 필터링 기술, AGC(Automatic Gain Control) 기술, 디지털 항재밍 신호처리 기술, 코드/반송파 추적 루프 기술 등이 있다. 안테나 기술은 적응형 안테나 어레이를 사용하는 기술로서 위성 신호 방향에 매우 좁은 펌폭의 빔을 형성하여 이득을 높이는 빔조향 어레이 기술과 재밍 신호 방향에 널(null)을 형성하여 재밍 신호를 억압하는 널 조향 기술 등이 있다. 프론트 엔드 필터링 기술은 수신기에 강하게 유입되는 재밍 전력을 차단하는 기술로서 위성항법 신호 대역 이외의 재밍 신호를 억압하고 위성항법 신호만을 통과시키는 sharp cut-off 특성을 가지는 대역 필터를 사용하는 방법이다. AGC 기술은 J/N(Jamming to Noise Power Ratio)를 측정하여 J/N이 기준 임계값 이상이 되면 재밍이 인가되고 있음을 인지하고 수신기로 가는 신호를 차단하는 방법이다. GPS 위성으로부터 수신되는 신호는 수신기의 열잡음보다 낮기 때문에 이보다 높은 전력이 검출될 경우 재밍 환경임을 판단할 수 있다. 디지털 항재밍 신호처리 기술은 대표적인 전처리 항재밍 위성항법시스템 기술로 위성항법 수신신호가 복조되기 전에 디지털화된 신호 샘플들을 이용하여 재밍 및 간섭신호를 제거하는 기술이다. 코드/반송파 추적 루프 기술은 위성항법 수신기의 보조를 받는 기술로, 외부의 관성항법장치 등의 속도 정보 등을 활용하여 추적 루프의 대역폭을 정확히 선정할 수 있게 되어 최적의 설계가 가능하다[6]. P코드를 사용하는 군사용 GPS의 경우 미군이 사용하는 암호장비를 통해서만 코드를 해독할 수 있기 때문에 스마트 재밍에 대해서는 안전하다고 할 수 있으나, 잡음 재밍에 대해서는 안테나 기술 등의 항재밍 기법이 필요할 것으로 판단된다.

Ⅴ. 결 론

GPS는 실생활에서는 물론 첨단 무기체계의 운용에 있어서도 매우 중요한 장비이다. 그러나 고도 2만킬로미터 이상에서 송신하는 GPS 신호는 수신기의 열잡음보다 미약하게 수신되며, 이에 따른 취약점도 존재하고 있고, 군사적으로 적대 관계에 있는 국가에서는 다양한 교란 수단을 보유하고 실재로 운용하고 있다. 우리 군에서도 이에 대한 심각성을 인지하고 항재밍 GPS를 개발에 성공하여 스마트 폭탄 키트인 한국형 유도폭탄 KGGB(Korean GPS Guided Bomb)에 장착한 바 있다. 무기체계가 첨단화될수록 정확한 항법장치와 타이밍 정보에 대한 의존도가 높아지게 됨을 감안할 때, 재밍 등 GPS의 운용이 제한되는 상황에서도 무기체계를 성능 저하 없이 운용할 수 있는 방안에 대한 연구가 필요하다.

참고문헌

[1] 허노정, “GPS 재밍 공격 대응 방안 비교 연구,” 제어로봇시스템학회 합동학술대회 논문집, vol.1, no.1, pp.270-278, 2011. 07

[2] 고광섭, 최창묵, “GPS를 이용한 선박의 방위 정보 향상에 관한 연구,” 한국정보통신학회 논문지, vol.9, no.3, pp.528-533, 2005. 06

[3] 최기주, 장정아, 심상우, “SA 해제 이후 GPS 데이터의 교통정보수집 적용가능성 평가,” 한국지형공간정보학회지, vol.12, no.1, pp.11-20, 2004. 03

[4] 지규인, 이영재, “Global Positioning System (GPS) : 원리와 응용,” 제어로봇시스템학회지, vol.2, no.2, pp.10-18, 1996. 03

[5] 정성균 외 3명, “GPS 신호에 대한 스마트 재밍 기술 동향,” ETRI전자통신동향분석, vol.27, no.6, pp.75-82, 2012. 12

[6] 김기윤, “위성항법시스템을 위한 항재밍 기술 분석,” 한국통신학회논문지, vol.38, no.12, pp.1216-1227, 2013. 12

[7] 코나스넷, “북한의 전자전 공격에 대비해야 -김성만 전 해군작전사령관,” 2011. 03. 08 (http://www.konas.net/article/article.asp?idx=24776)