ETRI

2012
Electronics and
Telecommunications
Trends

스마트 미디어 시대의
방송통신 융합기술 특집

GPS 신호에 대한 스마트 재밍 기술 동향

Technical Trends of Smart Jamming for GPS Signal

정성균 (S.K. Jeong) 위성항법연구팀 선임연구원
김태희 (T.H. Kim) 위성항법연구팀 선임연구원
신천식 (C.S. Sin) 위성항법연구팀 책임연구원
이상욱 (S.U. Lee) 위성항법연구팀 팀장

* 본 연구는 방송통신위원회의 2011년도 방송통신 연구개발사업의 일환으로 수행하였음(2011-S-301-01, 다원화 항법 주파수 감시 및 이용 기술 개발)

이용 분야가 다양한 GPS(Global Positioning System) 신호는 지상에서의 수신 신호 세기가 매우 낮아 각종 전파교란 문제에 노출되어 있다. 최근 국내에서도 GPS 전파교란으로 인해 GPS 신호를 이용하는 이동통신 기지국, 항공기 및 선박 등의 분야에서 많은 피해 사례가 발생하였다. 이에 따라 GPS 전파교란에 대한 사회적 관심도가 높아지고 있고 보다 발전된 형태의 전파교란이 발생할 가능성도 높아지고 있다. 이와 같은 상황에서 본고에서는 GPS 전파교란 형태 중 항법수신기에서 잘못된 정보를 제공하게 하는 스마트 재밍에 대한 개념을 소개하고 이를 극복하기 위한 국내외 기술 동향에 대하여 기술하고자 한다.

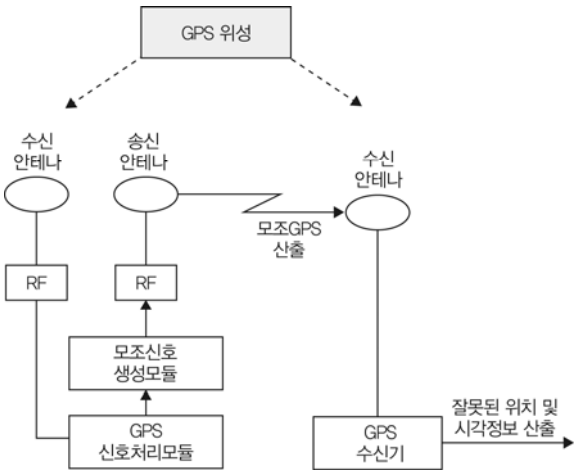
© 2012 한국전자통신연구원

Ⅰ. 서론

최근 차량 내비게이션을 비롯하여 스마트폰 등에서는 자신의 위치 정보와 시각 정보를 산출하는 데 있어 GPS(Global Positioning System) 신호를 사용하고 있다. 하지만 GPS 신호의 송출전력은 개방된 장소를 기준으로 했을 때 약 −160dBW로 매우 낮으며 이로 인해 GPS 신호를 수신할 때 각종 전파간섭이 발생할 가능성이 높다. 국내에서는 지난 2010년부터 최근까지 세 차례의 GPS 전파교란이 발생하였으며 이 때문에 통신 분야, 항공기 및 선박 등의 분야에서 많은 피해를 입기도 하였다.

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.

이 중 스마트 재밍은 GPS 신호의 모사신호를 만들어 실제 GPS 신호 세기보다 다소 높게 송출하는 것으로 수신기는 실제 GPS 신호가 아닌 모사 GPS 신호를 획득하고 추적하여 잘못된 위치 및 시각 정보를 산출하게 된다. 스마트 재밍에 대한 피해 사례는 다양한데 한 예로 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 시각 정보를 그대로 믿고 군사작전을 감행할 경우, 상당한 피해가 발생할 가능성이 높다고 할 수 있다. (그림 1)은 스마트 재밍의 예를 보여주고 있다. 따라서 본고에서는 GPS 전파교란 형태 중의 하나인 스마트 재밍에 대한 개념, 이를 극복하기 위한 기술개발 현황 및 전망에 대해 기술하고자 한다.



(그림 1) 스마트 재밍 예

Ⅱ. 스마트 재밍 기술

1. 스마트 재밍 원리

가. GPS 신호의 고의적인 방해 요소

GPS 신호를 방해하는 요소는 크게 재밍, 전파차단, 스마트 재밍, 재방송으로 나눌 수 있다. GPS 재밍은 GPS 신호와 같은 주파수 대역의 큰 신호 전력을 송신하는 재머를 이용하여 GPS 신호를 교란하는 것으로 비교적 쉽게 GPS 전파교란이 가능하다. 전파차단은 GPS 신호의 수신이 이루지지 못하도록 차단시키는 것으로 GPS 수신기 안테나를 결렬시키거나 금속 물체를 이용하여 안테나를 덮을 경우, 손쉽게 GPS 신호의 차단이 가능하다. GPS 재밍이나 전파차단이 발생하였을 경우 GPS 수신기가 GPS 신호에 대한 획득 및 추적 과정이 이루어지지 못하므로 GPS 신호에 대한 방해 여부를 비교적 손쉽게 인지할 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 일정 시간 동안 지연시킨 후 다시 수신기에 재송신함으로써 오차가 인가된 PVT(Positioning, Velocity, Timing) 정보를 산출하도록 하는 것이다[1].

스마트 재밍과 GPS 신호 재방송은 타깃 수신기가 거짓된 정보를 실제 GPS 신호라고 판단하고 신뢰하여 사용하도록 하므로 사용환경에 따라 더 치명적인 영향을 미친다. 스마트 재밍과 재방송은 모두 수신기의 동작불능이 아닌 사용자가 정확한 PVT 정보를 서비스 받지 못하도록 거짓된 정보를 전달하는 것이다. 이러한 점에서 재방송을 큰 범주의 스마트 재밍에 포함시킬 수 있다.

나. 스마트 재밍 신호의 목적

스마트 재밍은 GPS 신호와 동일한 구조를 가지나, 수신기가 정확한 PVT 정보를 서비스 받지 못하도록 거짓된 항법 데이터(위성 위치, 시각, 보정 관련 데이터의 기만) 또는 의사거리 정보를 포함하고 있다. GPS 기만기는 수신기가 GPS 신호가 아닌 거짓된 정보를 갖고 있는 기만신호를 획득하여 항법 시 오차를 유도함으로써 애플리케이션 환경에서 오류가 발생하도록 하기 위한 목적으로 거짓 정보를 송신한다. GPS 기만기 입장에서는 타깃 수신기에서 실제 GPS 신호와 비슷한 특성을 보이도록 기만신호를 생성하는 것이 관건이고, 수신기 입장에서는 각 위성 채널마다 기만 여부를 검출할 수 있는 기능을 추가하여 기만에 대응하는 것이 관건이다[1]. (그림 2)는 실험용으로 제작된 GPS 기만기와 방어기를 보여주고 있다.

(그림 2) GPS 기만기와 방어기[2]

스마트 재밍은 경제적인 목적, 테러 및 군사적 목적 등으로 이루어진다. 경제적인 스마트 재밍의 예는 어획량이 많은 어장에서 GPS를 기만하여 다른 어선들의 어획행위를 방해하거나 GPS로 오염물 처리 위치를 관리하는 지역에서 불법적인 위치에서 오염물을 처리가 가능하게 하는 것이다. 테러 및 군사적인 용도는 GPS로 동기를 맞추는 발전소에서 시간 오차를 발생시켜 손실을 가져오거나 항공교통에서 잘못된 정보로 항공기 충돌 사고를 유발시키는 것이다. 또한 위치 기반 무기나 무인기 등의 군사 장비를 무력화하기 위해 사용된다. 개인적인 용도로는 GPS 정보를 이용하여 접근 권한을 부여하는 프로그램의 보안을 해지시킬 때 사용되기도 한다.

다. 스마트 재밍 신호의 조건

스마트 재밍 신호는 GPS 신호와 동일한 구조 및 형태가 요구되고, 사용자의 수신 안테나에 GPS 신호와 비슷한 신호 전력 레벨로 수신되어야 하며, 실제 GPS 위성으로부터 수신기까지의 신호 전달 시간을 고려한 측정치 정보를 포함하고 GPS 신호와 동일한 구조와 형태로 신호를 모사해야 한다. 수신 전력은 기만기와 타깃 수신기 간의 거리와 주변 환경에 따라 민감하게 변하므로 타깃 수신기 근처에 기만기와 네트워크로 연결된 별도의 수신기를 위치시켜 조정하여야 한다. 따라서 타깃 위치를 매 순간 파악하는 것은 매우 어려우므로 일정한 타깃 범위 안의 수신기를 기만하는 것이 일반적이다. 사용자의 위치가 고정된 환경이나 공항, 항구, 공사장과 같이 사용자의 이동 패턴이 일정한 지역이 신호기만의 주요

타깃이 된다[1].

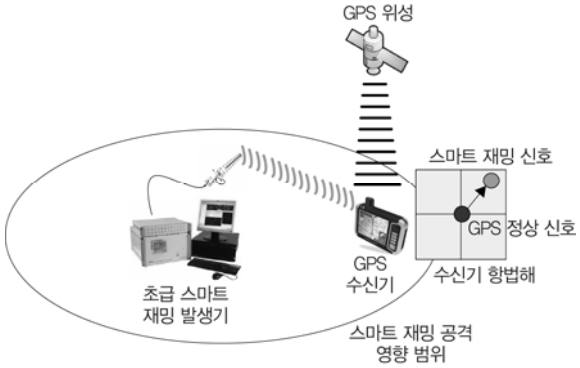
2. 스마트 재밍 발생 기술

가. 초급 스마트 재밍 발생

스마트 재밍 발생 기술의 가장 단순한 형태로 GPS 신호를 생성할 수 있는 신호생성 시뮬레이터를 이용한 스마트 재밍 방법이다. 이러한 방법은 2002년에 미국 Argonne 국립 연구소에서 GPS 신호생성 시뮬레이터와 전력증폭기를 연결하여 GPS 수신기로 스마트 재밍 RF 신호를 방출하여 GPS 수신기를 공격하는 데 성공하였다[3]. (그림 3)은 Spirent사의 RF 신호 생성기를 이용한 초급 스마트 재밍 발생 장치이다.

초급 기만 방법을 이용한 스마트 재밍 공격은 단순하고 쉬운 방법임에도 불구하고 몇 가지 단점을 가지고 있다. 첫 번째로 비용적 측면이다. 현재 RF 신호생성 시뮬레이터의 가격은 40만 달러 정도의 높은 가격대를 형성하고 있다. 두 번째 단점은 크기이다. 대부분의 GPS 신호생성 시뮬레이터는 무겁고 복잡한 구조의 장치이다. 만약 가까운 거리에서 스마트 재밍 공격을 수행할 경우 해당 장비의 크기로 인해 쉽게 눈에 띌 것이다[4].

(그림 3) 초급 스마트 재밍 발생 장치(Spirent사)



(그림 4) 초급 스마트 재밍 발생 방법

(그림 4)는 초급 스마트 재밍 발생 방법을 예시적으로 보여주고 있다. 시뮬레이터 기반 스마트 재밍 공격으로 인한 위협은 공격 대상 수신기에서 쉽게 공격을 감지할 수 있다. 공격 대상 수신기에서는 GPS 위성의 동기된 신호를 처리하기 때문에 시뮬레이터를 이용한 스마트 재밍 신호가 GPS 위성과 동기가 이루어지지 않은 상태이면 보다 쉽게 스마트 재밍 신호를 감지할 수 있는 것이다. 시뮬레이터를 이용한 단순한 스마트 재밍의 경우 대상 수신기가 스마트 재밍 신호를 수신할 때 일반 재밍 신호로 받아들여 lock을 잃어버리게 되며, 다시 신호를 획득할 때 신호생성 시뮬레이터에서 전송한 스마트 재밍 신호를 처리하게 함으로써 단순 스마트 재밍 공격을 수행하게 된다. 이러한 GPS 신호와 동기화되지 않은 스마트 재밍 공격은 공격 대상 수신기의 시간을 변화시킬 수 있다. 물론 공격 대상 수신기에서 GPS와 동기가 이루어지지 않은 이러한 스마트 재밍 공격은 쉽게 감지할 수 있다. 그러나 현재의 보통 수신기에서는 이렇게 단순한 스마트 재밍 공격조차도 방어할 수 있는 대책을 제공하고 있지 않은 상태이다.

나. 중급 스마트 재밍 발생

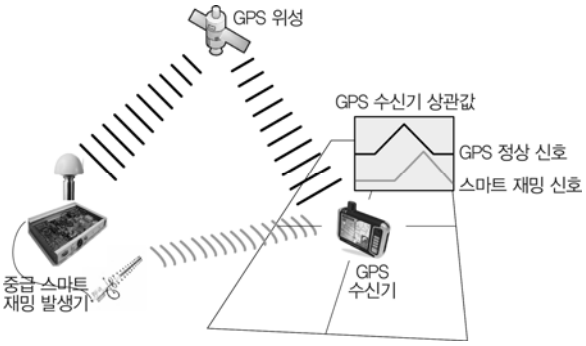
중급 스마트 재밍은 공격 대상의 정확한 위치 및 속도 정보를 획득하여 실제 GPS 신호와 동기된 스마트 재밍 신호를 생성하여 수신기를 기만하는 방법이다. 이러한 방법은 GPS 수신기와 스마트 재밍 발생기로 구성되며 공격 대상 수신기에 근접하면서도 눈에 띄지 않을 만큼 소형화할 수 있는 장점이 있다. 따라서 스마트 재밍 발생기가 공격 대상에 근접한 위치에서 공격할 수 있으므로 공격 대상 수신기가 GPS 위성으로부터 수신하는 GPS 신호와 유사한 스마트 재밍 신호를 발생하여 대상을 공격할 수 있게 된다[4].

(그림 5) 중급 스마트 재밍 발생 장치[4]

또한 중급 스마트 재밍의 장점은 공격 대상 수신기를 원하는 방향으로 제어하여 공격할 수 있다는 것이다. 일반적으로 수신기는 각 채널별로 실제 GPS 신호를 수신하여 상관을 수행하여 신호를 추적하게 된다. 따라서 중급 스마트 재밍 발생기에서 공격 대상의 수신기가 GPS 신호를 처리하여 생성한 상관값과 유사한 상관값을 생성할 수 있는 신호를 제공할 경우 공격 대상 수신기는 실제 GPS 위성신호가 아닌 스마트 재밍 신호를 추적하게 된다. 이는 스마트 재밍 공격을 수행하는 입장에서 공격 대상 수신기를 제어하면서 공격을 수행할 수 있게 되는 것이다[4]. (그림 5)는 중급 스마트 재밍 발생 장치이다.

그러나 현재 중급 스마트 재밍을 위해 수신기와 스마트 재밍 신호 발생기가 결합된 형태의 공격이 발생하지 않았기 때문에 이러한 수신기와 결합된 스마트 재밍 발생 장치는 판매되지 않고 있다. 그럼에도 불구하고 최근 소프트웨어 GPS 수신기의 출현으로 이러한 장벽이 서서히 무너지고 있다. 중급 스마트 재밍 발생기의 하드웨어는 규격화된 모듈을 조합하여 구성할 수 있으며 이를 구동하는 소프트웨어가 복잡하게 구성될 것이다. GPS 신호에 대한 정의가 ICD(Interface Control Document)에 나와 있는 상태이므로 이를 이용한 소프트웨어 개발이 누군가에 의해 이루어지고 이를 인터넷과 같은 곳에서 쉽게 얻을 수 있다면 이러한 공격이 활성화될 가능성도 있다.

이동이 가능한 수신기가 결합된 스마트 재밍 발생기



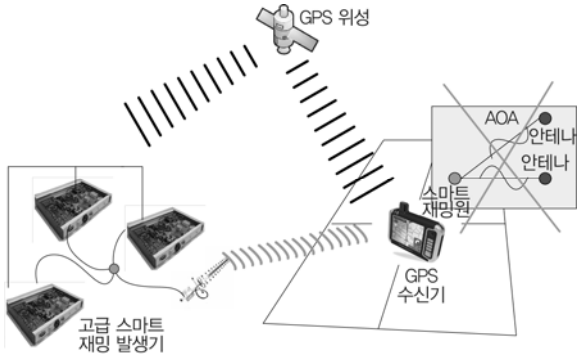
(그림 6) 중급 스마트 재밍 발생 방법

의 공격은 단순 스마트 재밍 공격과 달리 공격 대상 수신기에서 감지되기 어려운 특성을 가지고 있다. 수신기가 결합된 형태이기 때문에 현재 GPS 신호에 대한 처리를 통해 GPS 신호와 동기를 유지한 스마트 재밍 신호를 생성할 수가 있다[4]. (그림 6)은 중급 스마트 재밍 발생 방법을 보여주고 있다.

그러나 이러한 공격 또한 하나의 안테나를 통해 스마트 재밍 신호가 송출되므로 공격 대상 수신기에서 angle of arrival(AOA) 방식을 통하여 스마트 재밍 발생 시작 위치를 구별할 수 있게 된다[4].

다. 고급 스마트 재밍 발생

고급 스마트 재밍은 AOA로 방어를 할 수 있는 수신기에게 다수의 수신기가 결합된 스마트 재밍 발생기를 이용하여 공동으로 공격하는 방식이다. 이러한 방식에서는 스마트 재밍 발생 장치가 공통의 기준 오실레이터를 이용하여 동기를 유지하여 스마트 재밍 공격을 수행할



(그림 7) 고급 스마트 재밍 발생 방법

경우 AOA 방어를 수행하는 수신기에서도 스마트 재밍 신호원을 검출할 수 없을 것이다[4]. (그림 7)은 고급 스마트 재밍 발생 방법을 보여주고 있다.

Ⅲ. 스마트 재밍 극복 기술 동향

1. 스마트 재밍 검출 기술

GPS의 취약성을 지적한 후 스마트 재밍에 대한 연구는 2001년 Volpe Center의 보고서[5]에서 본격적으로 시작되었으며 Warner 외[3]는 시뮬레이터에서 생성된 스마트 재밍 신호를 검출하는 방법으로 수신된 위성신호 세기 감시, 위성 번호 감시, 시각 감시 등의 방법을 제시하였다[6]. Warner 외가 제시한 방법은 측정치, 신호 세기, 항법 메시지를 기반으로 한 방법을 포괄하고 있으며 다음과 같은 검출 기법들이 사용된다.

가. 신호 전력의 절대적인 크기 감시

일반적으로 GPS 수신 신호 전력은 L1 채널의 P(Y) 코드에 대해서는 −155.5dBW, C/A 코드에 대해서는 −153dBW, L2 채널의 모든 신호에 대해서는 −158dBW를 초과하지 않을 것으로 예상된다. 이들 숫자가 모든 수신기에 대해서 신호 전력의 상한값이라 할 수는 없다. 그 이유는, 안테나 형태 및 장착, 다중경로 같은 환경 효과가 수신 신호 전력을 극적으로 변화시킬 수 있기 때문이다. 그럼에도 불구하고, 최대 전력값을 설정하여 스마트 재밍 신호 전력의 한계로 정할 수 있다. 왜냐하면, 스마트 재밍 신호는 적어도 3dB 이상은 신호 전력을 증가시켜 공격하기 때문이다[7].

나. 신호 전력의 변화율 감시

GPS 위성은 지구로부터 2만km 떨어져있기 때문에, 지구 표면 근처의 어떠한 위치 변화에 대해서도 신호 전력이 급격하게 변하지 않는다. 하지만, 다중경로, 안테나 자세 등과 같은 환경에 따라서 수신 전력이 변화하므로, 이 방법은 고정점에서의 관측을 통한 검출에만 적용할 수 있다. 위성 앙각이 수신 신호 전력에 영향을 주므로, 위성 앙각이 상수로 유지되는 시간 구간 동안 사용이 가능하다[7].

다. 상대적인 신호 세기 감시

L1 주파수의 최저 수신 RF 신호 전력을 P(Y) 코드의 경우 −163.0dBW, C/A 코드의 경우 −160dBW이며 L2 주파수의 최저 신호 전력 세기는 −166dBW로 제시되어 있다. 상식적인 전력 비율의 3dB 아래에 위치한다. GPS 신호는 상대적으로 고정 전력 비율을 가진다. 따라서 상대적인 전력 비율을 확인하면서, 모든 주파수, 모든 신호 항목(L1/L2 및 modernized L5)에서 스마트 재밍을 쉽게 검출 가능하다. 이 방법의 장점은 안테나 자세에 의해 영향을 받지 않지만, 전리층 반사는 서로 다른 주파수의 전력 비율에 영향을 줄 수 있다[7].

라. 코드와 반송파의 변화율 비교

GPS 기만기가 고정된 수신기의 위상 측정치를 기만하는 것이 쉬울 지라도, 움직이는 수신기의 위상 측정치는 기만기가 제어하기 쉽지 않다. 만일 기만기가 반송파 측정치가 코드 측정치에 일치하기를 원한다면, 두 개의 변화값을 일치시켜 기만하여야 한다. 만약 이것이 어렵다면 위상 측정치는 코드 측정치와 동일하게 변화하지 않을 수 있다. 따라서, 코드와 반송파 측정치 변화율을 비교함으로써 이상 검출이 가능하고, 변화율의 경계를 지정하여 스마트 재밍을 검출하는 메커니즘을 구현할 수 있다[7].

마. 도플러 변화량 검사

GPS 수신기는 위치해를 계산할 뿐만 아니라 위성 위치도 계산할 수 있다. 따라서, 각 GPS 위성에 대한 수신기의 상대적인 속도도 유도가 가능하다. 단일 송신기를 사용하는 기만기는 모든 위성에 대해서 도플러 변화량

을 얻는 것은 불가능하다. 왜냐하면, 도플러 변화량은 반송파 주파수에 대해서 변화하고 서로 다른 PRN (Pseudo Random Noise) 코드를 갖는 CDMA 신호들이 반송파로 변조되기 전에 합해짐에도 불구하고, 기만신호는 도플러 시험을 피하기 위해 서로 다른 반송파에 변조되어야만 하기 때문이다. 따라서, 기만기는 각각의 기만 위성마다 하나의 송신기를 가져야만 한다. 도플러 변화량을 활용하여 스마트 재밍 신호를 검출할 수 있다[7].

바. L1-L2 측정치 비교

GPS L1과 L2로부터 측정된 측정치는 서로 연관 관계가 있으며 L1과 L2사이의 측정치의 차이는 전리층 효과에 의해서 유발된다. 스마트 재밍 신호는 대류층만 통과하므로 전리층 지연을 갖는 실제 신호와는 다른 양상을 보인다[7].

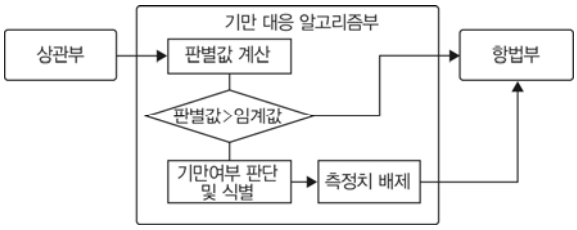
사. 위성 궤도력 검사

위성 위치 계산에 사용된 수신 위성 궤도력 데이터와 기만되기 전의 위성 궤도력 데이터를 비교하여 스마트 재밍 신호를 검출할 수 있다. 이 방법은 기만기가 스마트 재밍 신호에 잘못된 메시지를 삽입하여 전송하는 것을 검출하는 것이다.

아. 점프 검출

모든 측정치에 대하여 급격한 변화를 감시하는 방법이다. 측정치, 신호 세기에 있어서 특별한 점프 현상이 발생한 다면 이것은 스마트 재밍 공격이라 생각할 수 있다. 정상 지역에서 기만된 지역으로 이동한 수신기는 아주 긴 거리를 횡단하는 것과 같은 효과가 발생한다[7].

이상의 방법들에서 볼 수 있듯이 스마트 재밍은 GPS 수신기가 수집한 측정치, 신호 세기, 메시지 등으로 확인할 수 있으며 신호 추적과 획득의 과정에서도 GPS 신호의 이상 여부를 판별할 수 있다.



(그림 8) 스마트 재밍 PRN 제거 방법

2. 스마트 재밍 극복 기술

가. 스마트 재밍 PRN 제거 방법

스마트 재밍 극복 기술로 스마트 재밍 PRN에 대한 제거 방법이 있다. 스마트 재밍 공격 대상 수신기에서는 스마트 재밍을 감지하기 위하여 신호 처리를 수행하고 신호 처리 결과 및 항법 데이터를 이용하여 스마트 재밍 신호에 해당하는 PRN 정보를 얻을 수 있다. 이때 스마트 재밍을 극복하기 위한 간단한 방법으로 수신기에서는 스마트 재밍의 공격을 받은 PRN의 신호 처리 결과를 항법해 산출에 반영하지 않고 제거하면 스마트 재밍 공격을 방어할 수 있게 된다. (그림 8)은 스마트 재밍 PRN 제거 방법을 도식적으로 보여주고 있다. 그러나 일반적으로 상용 수신기에서 스마트 재밍 극복을 위한 스마트 재밍 PRN에 대한 제거와 관련된 알고리즘이 적용되지 않는 상태이므로 수신기의 수정이 요구되는 단점을 가지고 있다.

나. 스마트 재밍 RF 신호 상쇄 방법

스마트 재밍 RF 신호 상쇄 방법은 스마트 재밍 PRN을 검출한 후 해당 PRN에 대한 역 위상신호를 생성하여 스마트 재밍이 혼합된 신호와 결합하면 스마트 재밍 신호만 상쇄되어 사라지고 나머지 정상적인 신호를 수신 처리할 수 있는 스마트 재밍 극복 기술이다. 스마트 재밍 RF 신호 상쇄를 위한 구성은 스마트 재밍 신호 처리 모듈과 신호 처리 모듈에서 추출한 신호 추적 파라미터를 이용한 스마트 재밍 대응 신호생성 모듈로 구성된

다. 신호생성 모듈에서는 스마트 재밍된 PRN에 대해 신호를 획득하고 추적하여 코드 위치, 도플러, 신호 세기를 생성한다. 스마트 재밍 대응 신호생성 모듈에서 수신 처리된 결과를 이용하여 반송파가 180도 반전된 위상을 갖는 신호를 생성하여 RF 신호로 변환한 후 안테나에서 수신된 RF 신호와 합성하여 스마트 재밍 신호만을 상쇄하는 기술이다. 이러한 스마트 재밍 극복 기술의 장점은 기존의 상용 GPS 수신기의 수정 없이 안테나와 수신기 사이의 RF 부분에 장착함으로써 스마트 재밍을 극복할 수 있게 한다.

Ⅳ. 결론

GPS 신호를 활용하는 분야가 점차 다양화됨에 따라 GPS 신호의 이용에 장애를 유발하는 GPS 전파교란의 형태 역시 다양화되고 있는 추세이다. GPS 신호에 대한 특성, 코드 정보 등이 개방된 이후, GPS 신호에 대한 전파교란을 야기하는 형태 및 종류 또한 연구 개발되어 GPS 재밍 장치에 대한 설계 도면은 물론 상용제품까지도 인터넷 사이트 등을 통해 구매가 가능한 상황이 되었다. 이와 같은 상황하에서 국외 및 국내에서도 GPS 전파교란으로 인한 피해가 발생되고 있어 관련 기술개발에 대한 관심도가 높아지고 있다. 본고에서는 이와 같은 점을 고려하여 GPS 전파교란의 형태 중 항법수신기가 전파교란을 감지하지 못하고 잘못된 위치와 시각 정보를 계산하게 하는 스마트 재밍 기술에 대한 동향과 이에 대응할 수 있는 기술에 대해 수록하였다. 본고에서 살펴본 자료를 바탕으로 향후 스마트 재밍에 대한 기술개발의 관심도를 높이는 동시에 스마트 재밍으로 인해 발생될 수 있는 피해에 대한 대처능력 확보에 기여할 것으로 판단된다. 스마트 재밍으로 인한 문제를 근본적으로 해결할 수 있는 해결책은 아직까지 제시되지 않았으나 지속적인 연구 개발로 진화하는 스마트 재밍에 대한 대응이 가능할 것으로 짐작된다.

용어해설

GPS Jamming GPS 주파수 대역에 큰 신호 전력을 송신하여 GPS 수신기가 GPS 위성신호를 수신하지 못하게 하는 공격

GPS Spoofing GPS 위성신호보다 약간 높은 신호로 GPS 신호와 비슷한 위조된 정보를 방송하여 GPS 수신기가 잘못된 위치와 시각을 계산하도록 하는 공격

약어 정리

AOA	Angle of Arrival
GPS	Global Positioning System
ICD	Interface Control Document
PRN	Pseudo Random Noise
PVT	Positioning, Velocity, Timing
RF	Radio Frequency
TOA	Time of Arrival

참고문헌

[1] 신미영 외 “GPS 신호기만의 특성 및 수신기에 미치는 영향 분석,” 한국군사과학기술학회지, vol. 13, no. 2, 2010. 4, pp. 296-303.

[2] The University of Texas at Austin. http://radionavlab.ae.utexas.edu

[3] J. Warner and R. Johnston, “A Simple Demonstration That the Global Positioning System (GPS) is Vulnerable to Spoofing,” *J. Security Administration*, vol. 25, 2002. pp. 5-8.

[4] T.E. Humphreys et al., “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,” *ION GNSS Conf.*, 2008.

[5] John A. Volpe National Transportation Systems Center, “Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System : Final Report,” Department of Transportation, USA, 2001, pp. 73-54.

[6] 조성룡 외, “의사거리 측정치를 이용하는 기만신호 검출 기법의 성능 비교,” 한국군사과학기술학회지, vol. 13, no. 5, 2010. 10, pp. 793-800.

[7] H. Wen et al., “Countermeasures for GPS Signal Spoofing,” *Proc. 18th Int. Tech. Meeting Satellite Div. Inst. Navigation*, 2005. 9, pp. 1285-1290.