암호화된 PRN코드를 사용한 GNSS 신호의 저피탐 특성에 관한 분석

박기현, 김정현, 남미영, 박진수, 김인선, 이장용, 송홍엽

제 9회 국방기술학술대회

October 11, 2013

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

저피탐의 의미

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- **정보의 송수신 환경에서, 적합하지 않은 사용자가 통신 관련 정보를 얻기 어려운 상태**
- **두 가지 메인 정보의 은닉: Time and Frequency**
- **통신이 이루어진 시간의 은닉**
  - 신호의 송수신 여부를 은닉
  - 일반적인 의미에서의 저피탐은 통신이 이루어진 시간을 은닉하는 것을 의미
  - 주파수를 은닉하지 않으므로, 공격자가 송수신 대역을 안다고 가정
  - 은닉을 위해 낮은 파워로 송수신이 필요하여, 톤 재밍에 취약
- **통신이 이루어진 주파수의 은닉**
  - 신호의 송수신 대역을 은닉하여, 톤 재밍에 대항
  - 현재보다는 미래의 주파수 대역을 예측하지 못하게 하는 것이 중요

저피탐의 필요성

- **공격자가 신호의 정보를 알면, 공격 방향이 다양해지고 더욱 효과적인 공격이 가능해짐**
  - 공격자가 신호의 송수신 여부를 알 경우, 리플레이 공격 등이 가능해짐
  - 공격자가 신호의 대역을 알 경우, 톤 재밍 등을 통한 신호방해가 가능해짐
  - 위 두 가지 공격의 경우, 암호화를 통한 메시지 보호가 무의미함

- **저피탐 기법의 적용을 통해 신호의 송수신 여부 및 대역을 공격자가 관측하는 것이 어렵게 함**

저피탐 신호의 적용 사례

- **레이더 신호**
  - 저피탐 관점에서 가장 많은 연구결과를 가짐
  - 피 비행물체가 레이더 신호를 감지하면 자신의 위치가 노출되었음을 확인할 수 있게 됨
  - 피 비행물체를 감지하면서 상대에게 감지되었음을 알리지 않게 하기 위해, 저피탐 특성의 적용을 위한 많은 노력이 이루어짐
  - 낮은 파워, 넓은 대역을 사용
  - Chirp Pulse, Frequency Hopping, Spread Spectrum 기법 이용

- **대부분의 군 통신 기법이 저피탐 특성을 요구함**

위성항법 신호에서의 저피탐

- **GNSS신호는 항상 송수신된다고 가정되는 신호**

  ➔ 신호의 송수신 여부의 판별은 무의미하다고 여겨짐
- **GNSS신호는 예측이 가능**
  - 신호원인 위성의 위치는 GNSS 신호의 의존 없이, 다른 관측으로도 가능
  - 위성의 위치의 변화 또한 쉽게 예측이 가능
  - 송수신 포맷을 숨기기는 무척 힘들며, 따라서 시간대에 따른 수신신호 예측이 가능

- **GPS신호는 저피탐을 위한 노력을 특별히 하지 않음**

  ➔ 다양한 기만 공격 및 재밍 공격에 취약하다고 알려짐

탐지를 위한 공격자의 접근

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- **시간 관점에서의 접근**
  - 수신된 신호의 시간축에서의 분석
  - Matched filter를 가정하여 수신 시도
  - 가정의 범위가 좁은 신호에 유효
- **주파수 관점에서의 접근**
  - 수신된 신호의 주파수축에서의 분석
  - Fourier Transform, Spectral Density 등으로의 변환
  - 주파수 대역이 집중된 신호에 유효

- **저피탐 성능을 판별하기 위해, 시간 관점 및 주파수 관점에서의 신호 분석이 필요**

시간 관점에서의 접근 대응

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- 통신 신호 예측의 불확실성이 요구됨
- 동일 위치에서(동일 정보를) 보내는 위성의 통신 신호의 종류가 다양해야 함
- 넓은 key space를 바탕으로 암호화된 신호의 높은 엔트로피가 요구됨

주파수 관점에서의 접근 대응

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- **낮은 파워를 바탕으로 한 실질적인 은닉이 요구됨**
  - 노이즈 파워 레벨보다 신호 파워 레벨이 낮은 송수신
  - 항 재밍 능력의 저하 등으로 인해, 신호 파워 자체를 낮추는 것에는 한계가 있음 → 넓은 대역에 신호파워를 분산

- **주파수 특성이 대역 내에서 균일성을 유지하는 주파수 특성이 요구됨**
  - 여러 가지 확인 기법이 존재
  - Wigner-Wille Distribution, Ambiguity Function, Choi-Williams Distribution, Time-frequency distribution series, (Short-time) Fourier transform, Hough Transform, (Cyclostationary) Spectral Density
  - 이 중 **Spectral Density (신호의 Autocorrelation function의 Fourier transform) 이 가장 유효하다고 알려짐**

항법신호 비인가 탐지 시나리오

비인가 사용자	신호 탐지 방법
• 주파수 대역 • 신호 파형 • Spreading Code PSD 특성	• 수신 신호의 PSD 계산을 통한 관측 ➔ Spreading code 유추 등의 복잡한 공격은 하지 않는 것으로 가정

정상사용자

- 주파수 대역
- 신호 파형
- 정확한 Spreading Code 정보

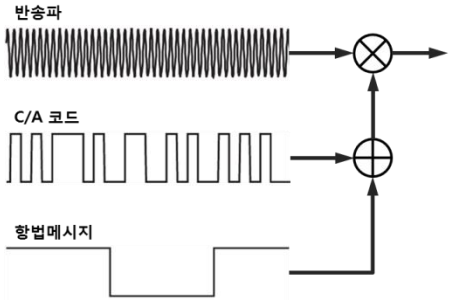
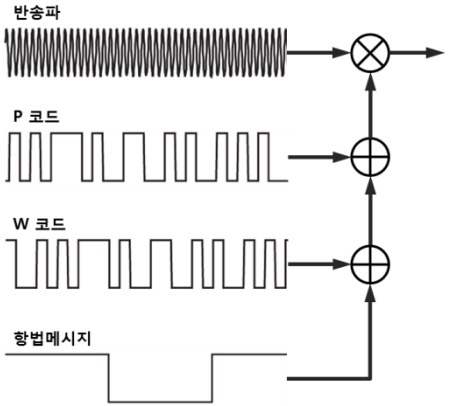
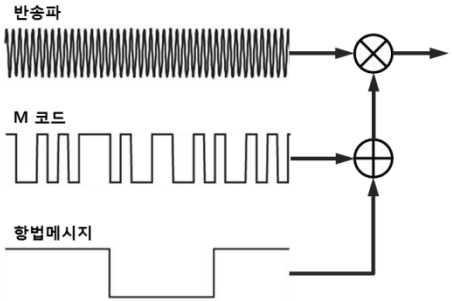
항법신호의 PSD 최대값 > 수신 노이즈 파워 평균
= 신호 탐지 성공으로 판단

정상사용자

비인가사용자

GPS PRN 코드

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

	C/A 코드	P 코드	M 코드
사용주파수	1.023 MHz	10.23 MHz	?
코드길이	1,023 chip	6.1871E12 chip	?
항법메시지 Spreading	1,023 * 20 chip	10,230 * 20 chip	?
암호화 기능	없음	옵션 P ⊕ W = P(Y) (or Y)	자체기능
신호구조			

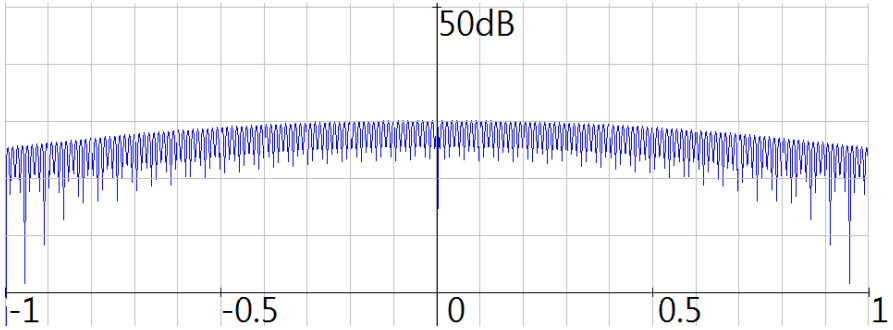
- 신호가 갖는 특성 : Pseudo Random Number, Pseudo Random Noise
- 코드생성 시 역할 : Spreading Code
- 시스템에서의 역할 : Ranging Code

조사 대상 수열

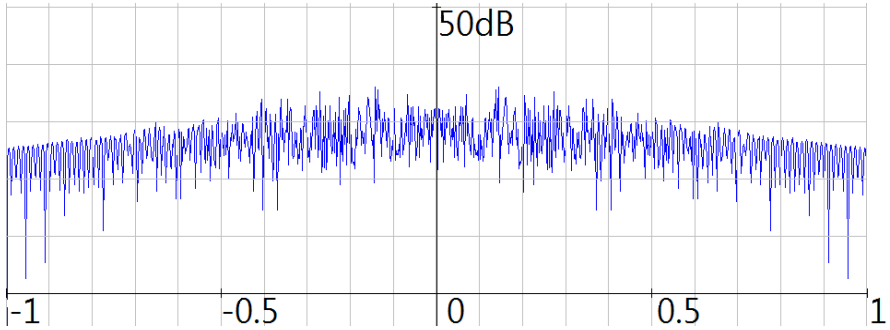
- **M-sequence**
  - 수학적으로 특성이 증명된 시퀀스
  - 가장 높은 자기상관 특성을 가짐
  - 상호상관 특성은 다소 떨어짐
  - 동일 길이에서 선택의 폽이 매우 좁음
- **Gold Code**
  - m-sequence로부터 생성
  - 가장 높은 상호상관 특성을 가짐
  - 동일 길이에서 선택의 폭이 좁음
  - 실제 GPS 시스템의 C/A 에서 사용
- **랜덤 시퀀스**
  - 난수 발생기를 통해 임의로 생성시킨 수열
  - 상관특성 및 저피탐 특성이 가변적임
  - 통계적 특성의 조사가 쉬우나 실제로 사용할 수는 없음
- **암호화된 시퀀스**
  - 랜덤 시퀀스와 비슷한 경향을 보일 것으로 생각되는 수열
  - 동일 길이에서 선택의 폭이 넓음

Spread Spectrum 특성 분석 (10^3 길이)

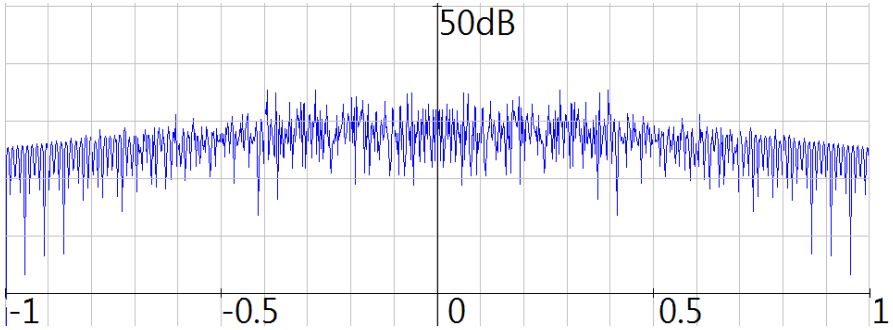
1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111



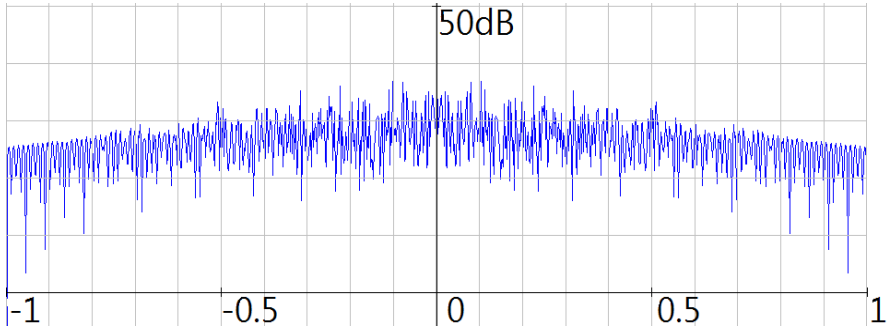
m-sequence



random sequence



Gold-sequence



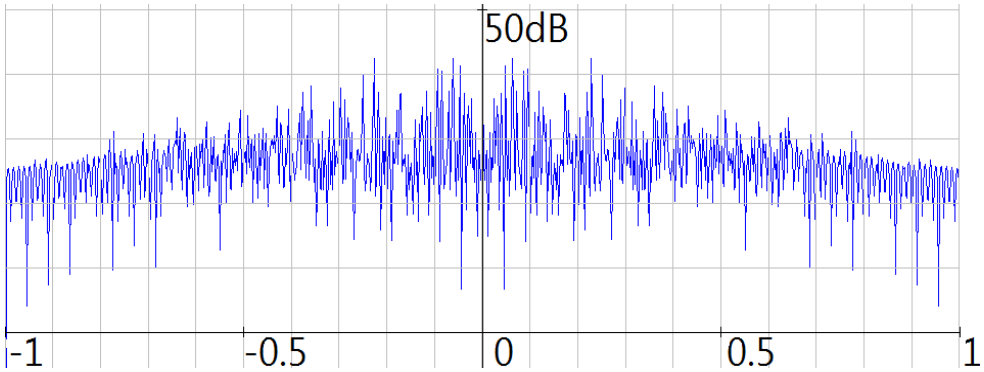
AES-encrypted sequence

- 주파수 특성 관점에서 최적으로 알려진 m-sequence를 제외하면 동일한 경향
- AES는 128 비트 단위로 랜덤 수열을 랜덤 고정 키를 통해 ECB로 암호화여 실험

동일 포맷의 암호화

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

- M-코드는 Ranging code 을 위해 일정 형식의 메시지를 암호화한 것을 Spreading code로 사용한다고 알려짐
- 동일 포맷의 암호화를 가정하기 위해 랜덤 수열이 아닌 All-zero 수열의 암호화를 가정



- 포맷이나 암호화 방식에 따라 저피탐 특성이 매우 나빠질 수 있음

결 론

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

- 랜덤 수열 및 암호화된 수열은 GPS C/A 코드인 Gold Code와 저피탐 특성에서 성능차이가 거의 없음

- 암호화된 수열은 원본 수열의 형태 및 암호화 방식에 따라 저피탐 성능이 확연히 나빠질 수 있음을 확인