위성항법 수신기에서의 기만 영향과 대응

■ 임성혁*, 지규인**
(*한국항공우주연구원, **건국대학교 전자정보통신공학과)

Ⅰ. 서론

위성항법 교란신호는 위성항법(GNSS : Global Navigation Satellite System) 신호를 무력화시킬 목적으로 사용되는 신호를 지칭한다. 교란신호는 크게 재밍(jamming), 기만(spoofing)과 미코닝(meaconing) 세가지로 분류할 수 있다. 재밍은 위성항법 신호보다 강한 세기를 신호를 수신기에 인가하여 위성항법 신호를 추적할 수 없게 만드는 반면 기만과 미코닝은 위성항법 신호와 유사하거나 동일한 신호를 송신하여 위성항법 신호의 추적을 교란하는 방법이다. 미코닝은 수신한 위성항법 신호를 증폭기를 이용하여 증폭한 후 그대로 전송하고 기만은 수신기를 속이기 위하여 실제 위성항법 신호와 동일한 신호 임의로 생성하여 전송하는 것으로 미코닝에 비해 작동이 복잡하나 위성항법 신호를 보다 효과적으로 교란할 수 있다.

최근 미국은 2006년 10월까지 새롭게 편성되는 군용 GPS 시스템에 SAASM (Selective Availability and Anti-Spoofing Module)을 탑재할 것을 권고하였다. 그만큼 기만은 GPS에 심각한 타격을 줄 수 있는 교란신호라는 점을 보여주는 예라 할 수 있다. 기만은 기만 신호를 이용하여 위성항법 수신기에 대한 교란을 행하는 방법으로 수신기가 각 위성으로부터 도달하는 위성항법 신호를 추적하는 과정을 효과적으로 기만하여 수신기가 기만 신호를 추적하도록 유도하여 결국에는 위성항법 수신기가 실제 위치해가 아닌 기만된 위치해를 도출하도록 한다. 또한 기존의 재밍신호는 고출력의 전파를 이용하여 위성항법 신호를 교란하는데 반해 기만은 위성항법 신호와 유사한 출력인 -160dBW 정도의 소량의 출력으로 위성항법 신호를 교란할 수 있어 기존 재밍이 지속시간이 짧은데 비해 장시간의 교란이 가능하다는 특징이 있다. 최근 ION GNSS 2008 학회에서 휴대용 GPS 기만장비가 1,000불 정도에 제작이 가능하다는 논문이 발표됨으로써 저가의 휴대형 GPS 기만장비의 생산이 가능함이 보여졌다 [4]. 또한 최근에 Todd E Hemphreys를 포함한 연구진은 무인헬기에 대한 기만시연을 통해 기만이 실제로 가능함을 확인시켰다. 따라서 기만에 대한 위협이 현실화됨으로써 정확도 및 정밀도를 생명으로 하는 위성항법을 이용하는 응용분야에 대한 항기만 기능의 탑재가 절실히 요구되고 있는 상황이다. 그러므로 항기만 기능 연구에 앞서 기만의 정의 및 형태 그리고 기만에 의해서 발생할 수 있는 위성항법 신호에 대한 영향의 분석 등이 선행될 필요가 있다.

그림 1은 민간 및 군 환경에서 처할 수 있는 GNSS 신호의 기만 상황을 묘사한 것이다. 그림에서와 같이 각종 기만 장비는 육상 및 공중에서 육상 및 공중 목표물에 대한 기만을 가할 수 있다. 일반적으로 사람이 직접 조정하는 이동체 보다는 무인이동체의 경우에 기만될 수 있는 가능성이 높다. 유인이동체는 인간의 조작이 포함되므로 지형지물 또는 운행경로의 상이함을 통해 기만여부에 대한 판단이 가능하다. 이와 유사하게 육상과 해상 및 공중의 경우에 육상에는 지형지물의 특징이 있으므로 이동경로와 기만에 의한 위성항법 수신기의 이상출력에 대한 비교가 가능하나 해상 및 공중에서는 환경적 특징의 비교가 거의 불가능하여 이상 여부에 대한 판단이 어렵게 된다.

다음 장에서 위성항법 신호의 특징과 이에 기반하여 위성항

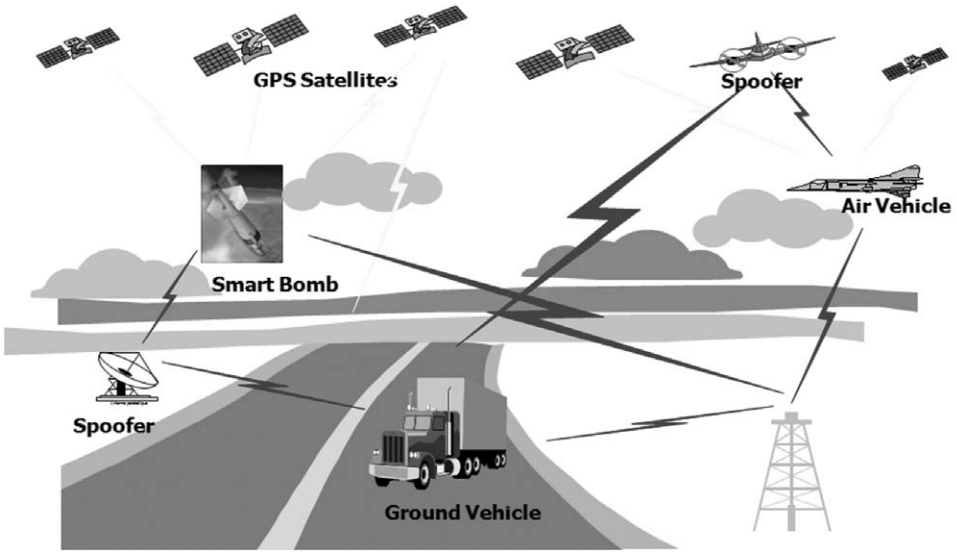
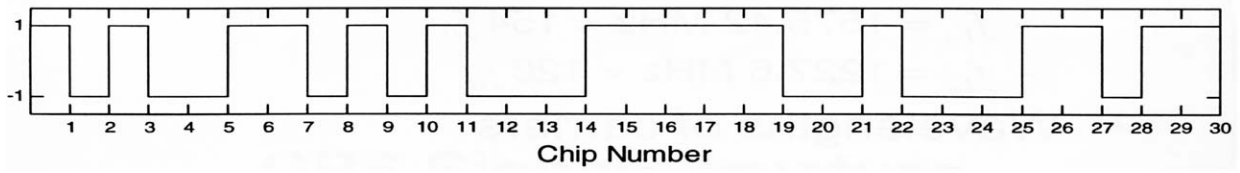
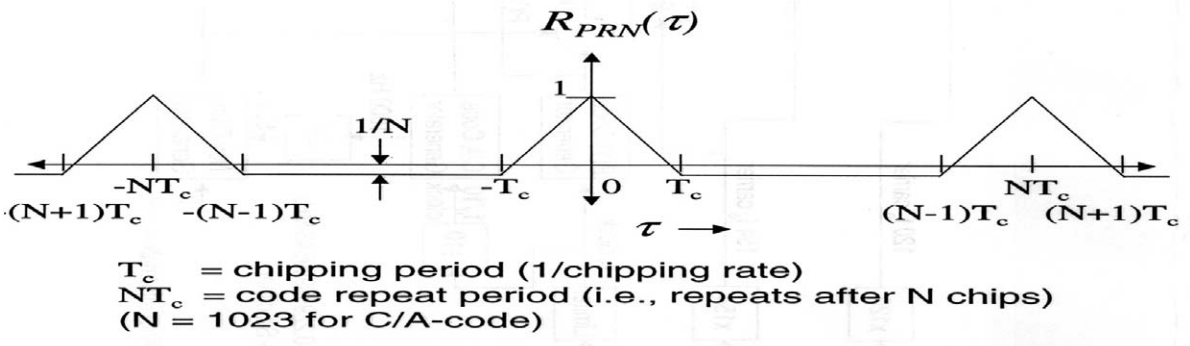


그림 1. 기만환경 예.



(a)



(b)

그림 2. PRN 열(a)과 자기상관 함수(b).

법 수신기 기만을 위해서 기만신호가 만족시켜야 하는 조건에 대해 설명한다.

Ⅱ. 위성항법 신호의 특징

GPS L1 C/A 코드는 PRN (Pseudo-Random Noise)을 이용한 대역확산 신호이다. 잡음(noise)과 유사하게 설계된 2진의 의사잡음(pseudo random noise) 확산 시퀀스(sequence)는 잡음과 거의 유사하다. 생성된 확산 시퀀스는 그림 2(a)와 같고 그림 2(b)에서와 같은 자기상관 함수를 갖는다.

수신기가 위성신호를 수신하면서 정상적인 작동 즉 신호추적을 하고 있는 상황에서 GPS 기만신호는 위성으로부터 수신된 GPS 신호와 코드 지연이 약 1㎲(C/A code chip length) 이하인 경우에 GPS 신호를 교란할 수 있다. 그림 3은 기만신호에 의해

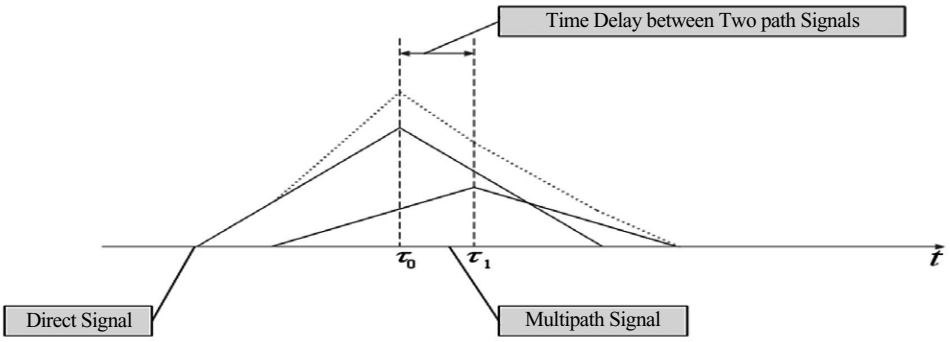


그림 3. 기만신호를 포함한 상관 형태(지연〈1 ㎲).

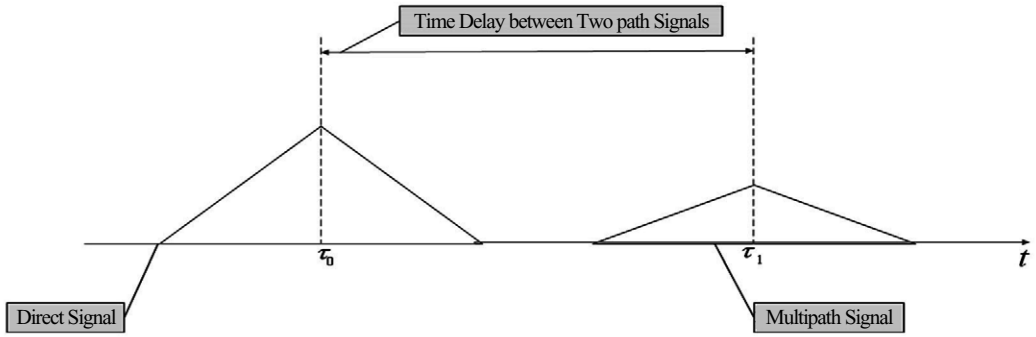


그림 4. 기만신호를 포함한 상관 형태(지연〉1 ㎲).

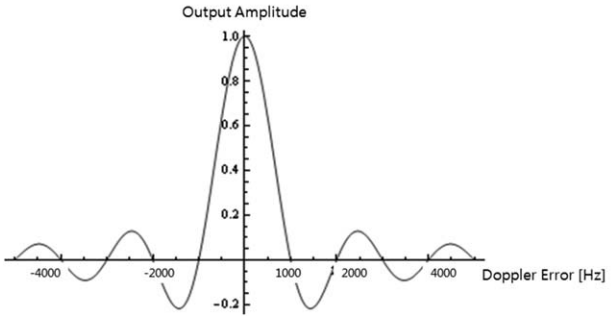


그림 5. 도플러 오차에 따른 전력 세기.

서 GPS 신호의 상관함수 값이 왜곡되는 상황을 나타낸다. 그러나 그림 4에서와 같이 GPS 신호와 기만신호 사이의 코드 지연이 1㎲ 이상인 경우에는 기만신호에 의해서 영향을 받지 않는다.

그림 5는 도플러 오차에 따른 출력 세기를 도식한 것이다. 그림에서와 같이 도플러 오차의 증가에 따라 수신기 내부 상관기의 출력 세기는 급격히 감소하게 된다. 특히 1000Hz에 가까워지게 되면 출력 세기는 '0' 이 된다.

그러므로 위성항법 수신기가 탑재된 항체에 기만 영향을 주기 위해서 기만장치는 항체의 위치에 대한 정보를 최소한 약 300미터 (1㎲=1chip) 이내로 추정하고 도플러는 1000Hz 이내로 추정하여 기만신호 발생기에 제공하여야 한다. 신호 대 잡음비를 고려하는 경우 기만장치는 항체의 위치 및 도플러에 대하여 보다 높은 추정 정확도를 필요로 하게 된다.

Ⅲ. 기만신호의 종류 및 특징

위성항법 신호에 대한 기만을 수행하기 위한 장치는 기만기(Spoofer)라고 지칭하며 표 1에서와 같이 능동형(Active) 기만기와 수동형(Passive) 기만기로 분류할 수 있다. 능동형 기만기는 목표물에 대한 추적기능(레이더 장비 이용)을 포함하여 정해진 목표물에 대한 기만을 수행하고 기만형태이고 수동형 기만기는 정해진 목표물에 대한 정보 없이 목표물의 예상 진로를 예측하여 예상 지역을 대상으로 기만을 수행한다. 일반적으로 능동형 기만기는 물체추적 장비의 추적 정확도의 낮음으로 인하여 실제적인 구현이 쉽지 않으므로 특정 지역을 대상으로 위성항법 기만 신호를 생성하여 기만하는 수동형 기만기가 많이 사용될 수 있으며 유도미사일, 비행체 또는 지상차량과 같이 개별적

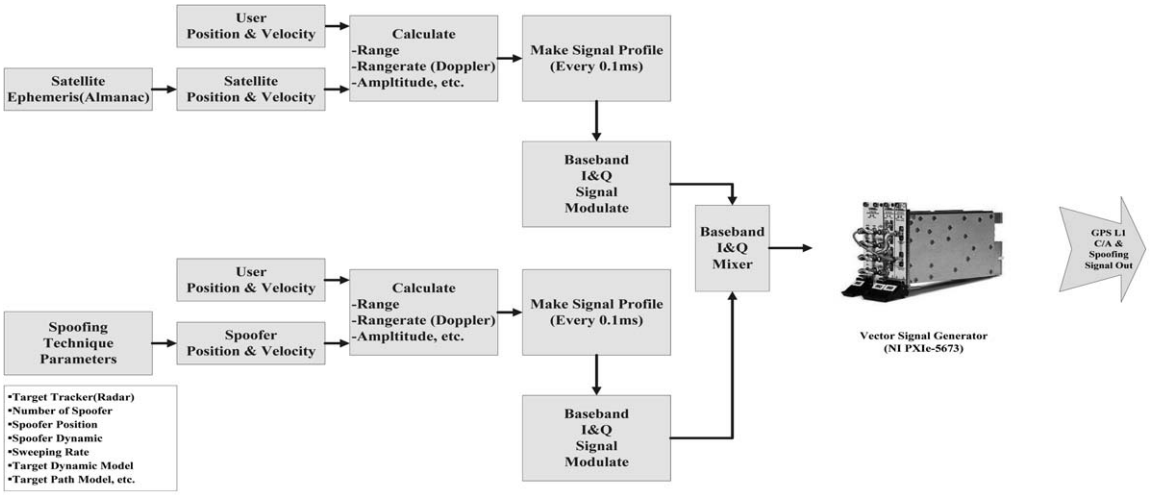


그림 6. 위성항법/기만 신호 발생기 구조.

표 1. 기만기 구분.

구분			장점	단점
기만기	추적기능	능동형 기만기	효과적인 기만 가능 (모든위성신호 기만)	기만지역 협소, 구현이 어려움 (추적장비 필요)
		수동형 기만기	광역 기만 가능	인지 및 제거 용이
	이동여부	고정형 기만기	고출력 가능	기만지역 제한
		이동형 기만기	과업위지역 기만가능	출력 제한

표 2. 기만 전략.

구분	내용
경로/동특성 탐색형 기만	- 대상 항체가 지나가는 모든 경로를 찾기 위해서 코드 및 도플러를 변경하며 탐색하여 기만한다. - 일반적으로 기만신호의 탐지가 쉽고 모든 위성신호를 기만할 수 없지만 넓은 지역에 대한 기만이 가능하다.
경로/동특성 대기형 기만	- 특정 동특성을 가진 대상 항체가 지나가는 특정 경로를 지정하여 코드 및 도플러 값을 설정하여 그 지역을 지나가는 유도무기가 기만되도록 함 - 기만 탐지가 쉽지 않으며 모든 위성신호에 대해서 기만이 가능하지만 좁은 지역에 대한 기만이 가능하다.

인 기만이 가능한 경우에 한해서 능동형 기만기의 사용이 용이할 수 있다. 마찬가지로 기만기의 형태를 고정형과 이동형 기만기로 분류할 수 있다. 고정형의 경우에는 지상으로부터 위성항법 기만 신호를 발사하여 목표물을 기만하는 형태이며 이동형은 비행체(또는 이동체)나 Buoy 등을 이용하여 기만 신호를 방사하는 형태이다.

수동형 기만기의 경우에는 기만전략(spoofing strategy)이 중요하다. 그 이유는 위성항법 신호의 특성과 기만 목표의 움직임에 의해서 특정시간 및 특정지역에서의 의사거리와 도플러가 결정되게 되기 때문이다. 그러므로 효과적인 기만을 위해서는 고도로 설계된 기만전략을 필요로 한다. 기만전략을 크게 두 가지로 나누면 표 2와 같이 정리할 수 있다.

결과적으로 위성항법 신호의 기만은 위성항법 신호를 사용하는 장치를 기만하기 위해서는 위성항법 신호와 가장 유사한 신호를 사용하는 것이 기만효과를 극대화하는 방법이다. 그러므로 위성항법 신호의 기만을 위해서는 앞의 2장에서 설명한 위성항법 신호의 일반적인 특성에 대하여 정확한 이해가 필요하다. 바꾸어 말하면 기만대응을 위해서는 위성항법 신호의 특성에 대한 이해를 통해서 기만가능성에 대해 연구한 후 취약부분을 보완함으로써 기만을 피할 수 있다.

Ⅳ. 기만기 시뮬레이터

일반 상용 위성항법 수신기에 대한 기만신호에 의한 영향을 분석은 RF레벨의 위성항법 및 기만 신호생성 및 처리 장치를 통해서 가능하다. 실제 위성항법 신호와 동일한 수준의 신호를

생성할 수 있는 소프트웨어 기반의 위성항법 신호 생성기와 National Instrument 사의 RF 신호 발생기와의 결합을 통하여 소프트웨어 기반의 위성항법 신호 생성기를 통해 발생된 기저대역 위성항법/기만 신호를 RF 대역으로 변환하여 송출하도록 하여 기만기 시뮬레이터를 구축할 수 있다.

그림 6은 기만실험을 위한 GPS/Spoofing 신호 발생장치이다. 기만신호 발생장치는 목표물의 위치/속도와 기만기의 위치 정보를 이용하여 위성항법 신호 기저대역 신호를 생성한 후 National Instrument 사의 PXIe-5673(RF Genenrator)로 인가하여 위성항법 RF 신호를 생성한다.

그림 7은 위성항법/기만 신호 발생기의 성능 평가를 위해서 기만 신호가 존재하지 않는 상황에서 상용 수신기인 Novatel 사의 OEM-V3와 Ublox 사의 LEA-4T에 인가하여 사용된 위성항법 수신기가 개발된 시뮬레이터를 통해 생성된 위성항법 신호에 대한 위치해 정확도를 평가하는 실험 사진이다. 그림을 통해서 생성된 신호를 위성항법 수신기가 정상적으로 추적하여 위치해를 제공함을 확인할 수 있다.

Ⅴ. 단일 위성 신호 기만 영향 분석

GPS 신호는 기만신호의 코드 위상과 반송파 도플러 및 GPS 신호 대 기만신호의 세기 비에 따라 받는 영향의 정도가 달라진다. 3가지 기만신호의 특성에 대한 수신기 신호추적루프에서의 영향을 분석한다. 수신기 신호추적루프 출력값 중에서 기만여부, 주파수 추적오차, 코드 추적오차와 신호대 잡음비에 대해 기만기 시뮬레이터를 이용하여 분석을 수행한다

1. 단일 위성 신호 기만 영향 분석 모의실험 변수 설정

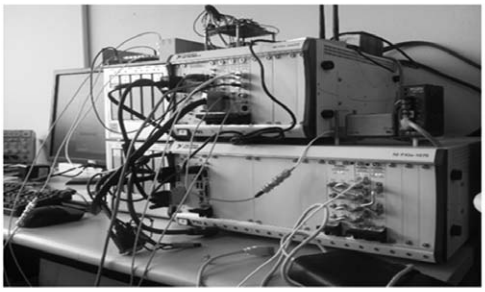
표 3은 기만신호 설정 변수를 나타낸 것이다. 앞에서 언급한 바와 같이 기만신호를 정의하는 변수는 도플러 오프셋(offset) 및 코드검색 속도와 GPS 신호와 기만신호의 세기로 분류할 수 있고 각각의 조정값은 신호추적루프의 설정값을 고려하여 선택하였다. 표 4는 모의실험에 사용된 소프트웨어 수신기의 Front-end 및 신호추적루프의 설정값을 나타낸 것이다. 직관적

표 3. 기만신호 설정 변수.

기만신호 설정 변수	값
도플러 오프셋(Hz) : GPS신호와의 주파수 차	0, 25, 50, 100, 200, 250, 500, 1000
코드검색 속도(chip/sec)	1, 2, 3, 5, 10
GPS 신호 대 기만신호 세기 비(dB)	-5, -3, 0, 3, 5

표 4. 소프트웨어 수신기 Front-end 및 추적루프 변수 설정.

설정 변수	값
샘플링 주파수	22MSps
중간 주파수	8.58MHz
양자화 비트수	1.5비트
위성신호의 최대 전력	40 dB/Hz
코드추적루프 구조	반송파 도움 1차 루프
코드/주파수 추적루프 대역폭	1Hz/12Hz



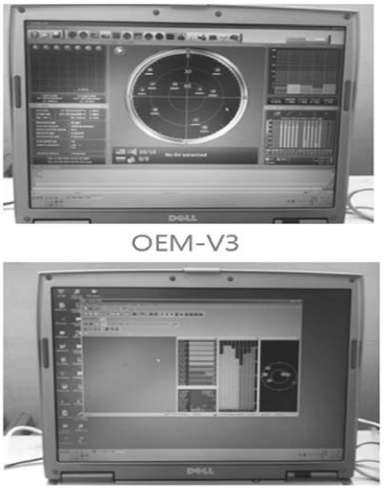


그림 7. 위성항법/기만 신호 발생기 성능 평가.

으로 대역폭이 1Hz의 추적루프를 사용하는 경우 코드의 경우 초당 약 1칩(chip)의 코드 순간이동의 추적이 가능하며, 반송파의 경우 초당 약 1Hz의 주파수 순간이동의 추적이 가능함을 의미한다. GPS 신호는 C/A코드에 의해서 의사거리가 결정되고 이를 바탕으로 위치를 결정하게 된다. 그러므로 코드추적오차는 거리로 환산하여 미터로 표기하였다.

그러나 일반적으로 GPS 수신기에 도달하는 GPS 신호에 대한 정보를 완벽히 알 수 없기 때문에 검색을 통한 기만을 수행하게 되며, 검색하는 속도를 코드검색 속도(code sweep rate)라 한다.

2. 단일 위성 신호 기만 영향 분석 모의실험 결과 및 분석

모의실험 결과의 분석은 기만성공 여부와 코드추적 오차 및 주파수추적 오차 세 가지로 수행하였다.

표 5는 기만성공 여부를 나타낸다. 표에서 보는 바와 같이 대부분의 경우에서 기만성공이 이루어지지 않았으며 코드 검색 속도가 코드 추적루프 대역폭(=1Hz)과 같은 1cps이고 GPS 신호대 기만신호의 비가 3dB보다 크고 도플러 오프셋이 250Hz보다 작은 경우와 GPS 신호대 기만신호의 비가 5dB이고 도플러 오프셋이 500Hz보다 작은 경우에만 기만성공이 이루어졌다.

코드검색 속도가 1cps인 경우에 기만신호는 약 2초간에 걸쳐 초당 1chip 이동하므로 완전한 기만이 가능하다. 하지만 코드검색 속도가 2cps 이상인 경우 초당 2chip 이상으로 이동하므로 대역폭이 1Hz인 코드추적루프가 기만신호를 추적하지 못하여 기만되지 않는다.

표 5. 기만 변수에 따른 기만 성공 여부(성공: ○, 실패: ×).

	sweep rate = 1cps					sweep rate = 2cps					sweep rate = 3cps				
\JSR	-5	-3	0	3	5	-5	-3	0	3	5	-5	-3	0	3	5
0Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
25Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
50Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
100Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
200Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
250Hz	×	×	×	○	○	×	×	×	×	×	×	×	×	×	×
500Hz	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×
1KHz	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

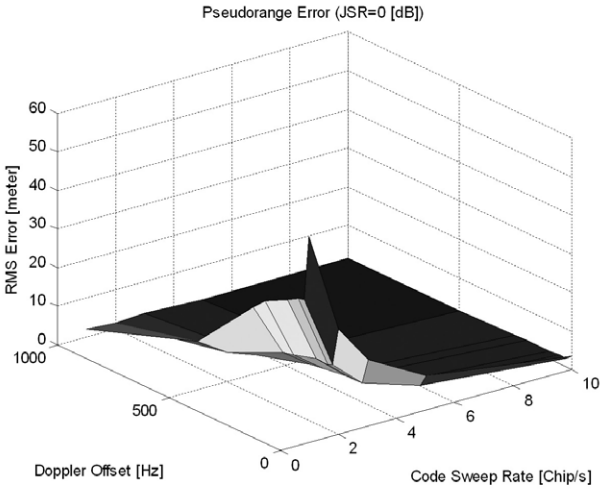


그림 8. 코드추적 오차(JSR=0dB).

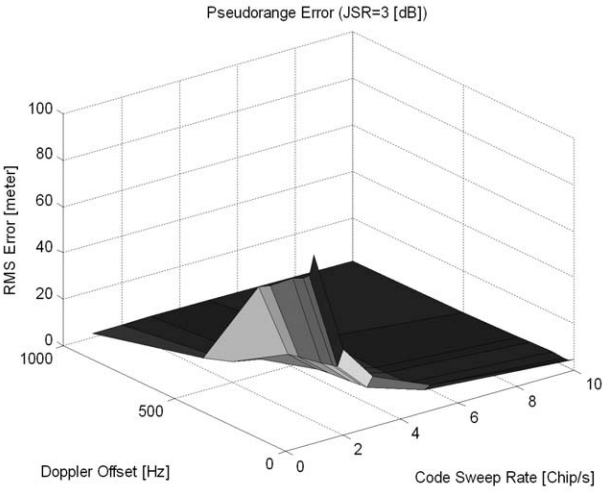


그림 9. 코드추적 오차(JSR=3dB).

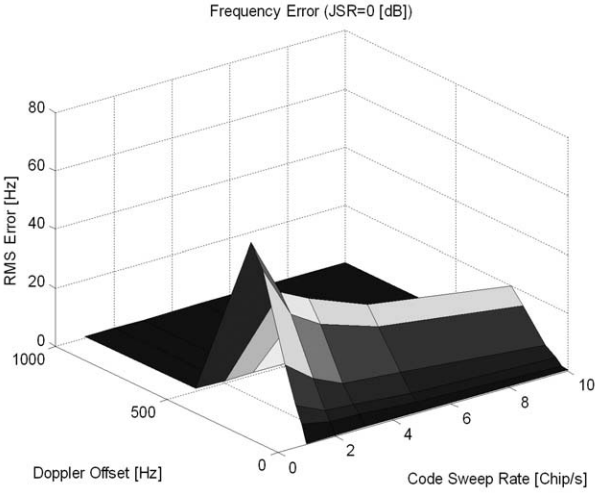


그림 10. 주파수추적 오차(JSR=0dB).

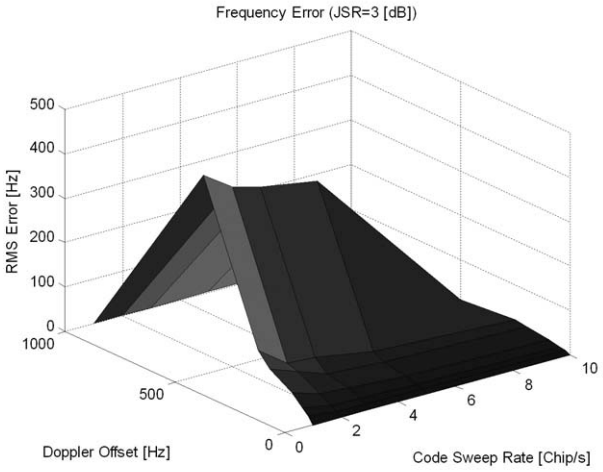


그림 11. 주파수추적 오차(JSR=3dB).

표 6. 기만 변수에 따른 코드추적 RMS 오차 (단위 : meter).

	sweep rate = 1cps					sweep rate = 2cps					sweep rate = 3cps				
\JSR	-5	-3	0	3	5	-5	-3	0	3	5	-5	-3	0	3	5
0Hz	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1
25Hz	1	2	6	14	22	1	2	4	9	10	1	1	4	7	8
50Hz	1	1	12	28	41	1	1	7	16	20	1	1	6	13	16
100Hz	1	3	24	50	106	1	3	17	31	37	1	2	12	26	30
200Hz	2	30	53	81	130	1	19	34	57	70	1	11	29	35	56
250Hz	1	2	60	111	405	1	2	41	66	90	1	21	35	61	70
500Hz	1	1	1	447	454	1	1	1	405	413	1	1	1	387	389
1KHz	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

표 7. 기만 변수에 따른 주파수 추적 RMS 오차 (단위 : Hz).

	sweep rate = 1cps					sweep rate = 2cps					sweep rate = 3cps				
\JSR	-5	-3	0	3	5	-5	-3	0	3	5	-5	-3	0	3	5
0Hz	30	38	54	81	126	17	21	27	37	46	11	13	17	22	26
25Hz	13	20	37	71	134	7	10	17	29	39	5	7	11	16	21
50Hz	13	20	36	69	143	7	10	17	28	38	4	6	11	16	20
100Hz	12	18	34	67	143	7	10	17	27	36	4	7	10	15	20
200Hz	10	15	31	59	118	6	8	15	25	34	4	6	10	14	19
250Hz	10	15	28	56	176	5	8	15	24	32	4	5	9	14	18
500Hz	5	7	13	14	17	3	4	8	9	11	2	3	5	7	16
1KHz	1	1	2	2	3	1	1	1	2	2	1	1	2	2	3

GPS의 주요 성능지표는 항법해의 정확도이다. 그러므로 앞에서와 같이, 완전한 기만은 이루어지지 않았지만 GPS 신호추적 루프가 기만신호에 의해서 영향을 받아 신호추적 오차가 증가할 수 있다. 이 오차는 항법해 오차의 원인인 의사거리 오차와 반송파 적산 오차를 발생시킨다. 의사거리 오차와 반송파 적산 오차는 각각 코드추적 루프 오차와 주파수추적 루프 오차에 의해서 발생한다.

그림 8~11과 표 6~7은 표 3에서 제시된 설정 변수에 따른 코드추적 및 주파수추적 오차를 나타낸 것이다. 그림 8과 9는 코드 검색속도와 도플러 오프셋에 따른 코드추적 오차를 GPS신호보다 기만신호가 0dB와 3dB 큰 경우를 도식한 것이다. 두 그래프에서 코드 검색속도가 증가할수록 오차가 작아짐을 확인할 수 있다. 또한 도플러 오프셋이 커짐에 따라 코드추적 오차가 감소함을 확인할 수 있다. 그림 10과 11은 코드 검색속도와 도플러 오프셋에 따른 주파수추적 오차를 그림 8과 9와 동일하게 0dB와 3dB 인 경우에 대해서 도식한 것이다. 주파수추적 오차는 도플러 오프셋이 커짐에 따라 증가하다가 감소하는 경향을 나타낸다. 기만신호의 도플러 오프셋이 1kHz 이상인 경우에는 오차가 발생하지 않음을 알 수 있다.

시뮬레이션 결과를 통해 기만신호가 GPS 신호와 유사할수록 미치는 영향이 커짐을 확인할 수 있다. 특히 코드 검색속도는 신호추적 루프 오차를 결정하는 주요한 요인이다. 그러나 코드 검색속도가 느린 경우에는 GPS 신호에 영향을 줄 수 있는 범위가 감소하게 된다. 또한 기만신호의 세기가 기만대상이 되는 GPS 신호보다 큰 경우에만 기만이 성공적으로 이루어지며 기만신호의 세기가 감소할수록 영향은 감소하게 된다. 기만신호의 세기가 큰 경우에는 검출이 용이해진다. 일반적인 GPS 수신기는 코드위상 측정값(의사거리)만으로 항법해를 결정한다. 따라서 주파수추적 오차가 항법해에 반영되는 것은 코드추적 오차가 반영되는 것에 비하여 상대적으로 작다.

표 6과 7은 그림 8~11에서 도식된 결과를 표로 나타낸 것이다. 시뮬레이션은 총 10초간 100회씩 수행되었으며 RMS오차는 10초간 발생한 오차의 평균을 의미한다.

Ⅵ. 이동체에 대한 기만 영향 분석

1. 기만기가 목표물의 위치를 정확히 알고 있는 기만상황

위성항법 신호를 기만하기 위해서는 기만하고자 하는 대상의 위치에 대한 정보가 필수적이다. 모의실험을 위해서 최초 기만신호는 기만대상의 위치를 탐지하지 못한 상태에서 시작하

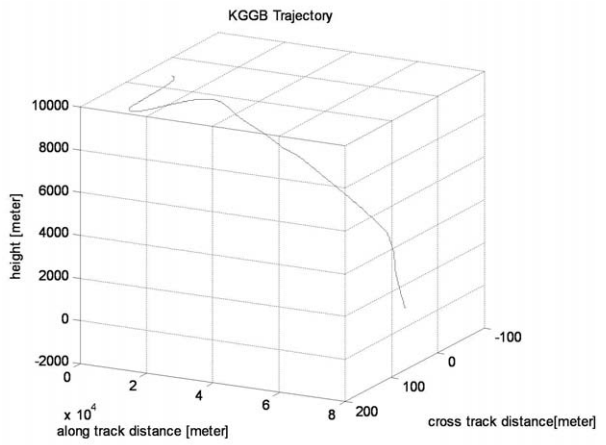


그림 12. 항체의 진행 경로.

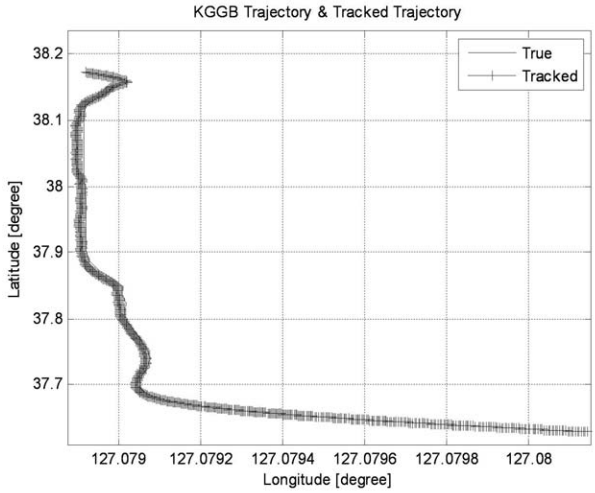


그림 13. 항체 및 수신기 출력 수평면 위치(기만 없는 경우).

여 위치 탐지가 완벽하여 기만신호를 기만대상으로 접근시킨 후 일정시간이 경과한 다음 기만기가 원하고자 하는 위치에 대한 정보를 담은 기만신호를 생성하여 항체에 탑재된 위성항법 수신기의 위치해 출력을 벗어나도록 유도한다.

그림 12는 기만대상 항체의 목표 궤적의 한 예를 나타낸다.

항체가 출발한 후 기만기는 항체 경로의 진행방향(along track)과 교차방향(cross track)으로 각각 750미터의 오차를 갖는 위성항법 기만 신호를 생성하여 150초가 되는 순간 항체와 일치하는 위치에 대한 기만 신호를 생성하고 250초부터 기만기는 위성항법 기만 신호를 항체의 진행 경로의 교차방향 우측으로 위치해를 도출하도록 기만 신호를 생성한다.

기만신호와 위성항법 신호의 전력비(JSR)는 0dB와 5dB 각각에 대해 모의실험을 실시하였다.

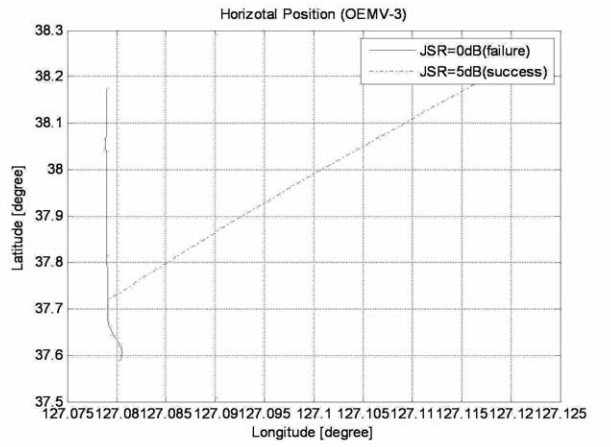


그림 14. 수평면 위치해(OEMV-3) : 파란색 실선-기만실패, 붉은색 점섬-기만성공.

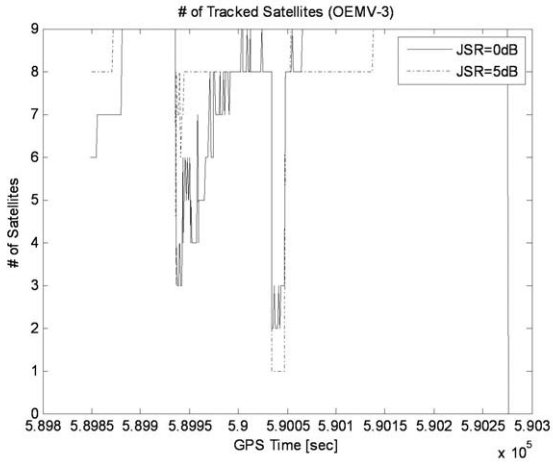


그림 15. 추적 위성 수(OEMV-3) : 파란색 실선-기만실패, 붉은색 점섬-기만성공.

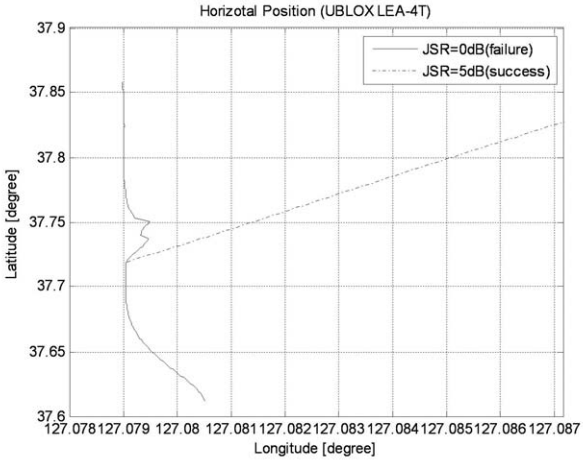


그림 16. 수평면 위치해(LEA-4T) : 파란색 실선-기만실패, 붉은색 점섬-기만성공.

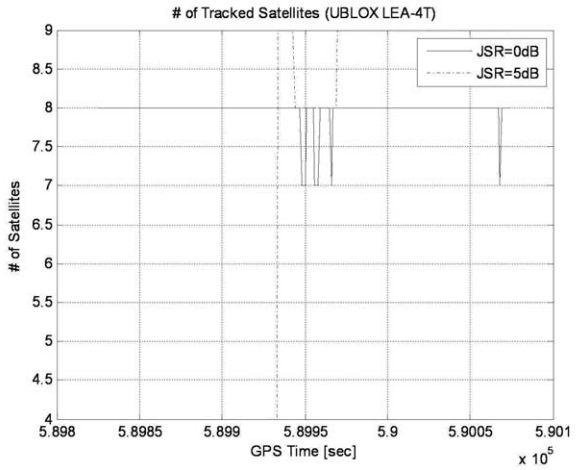


그림 17. 추적 위성 수(LEA-4T) : 파란색 실선-기만실패, 붉은색 점선-기만성공.

기만신호가 인가되지 않는 경우에는 그림 13에서와 같이 실제 목표 궤적과 수신기가 출력하는 궤적의 정보가 일치함을 확인 할 수 있다.

그림 14~17은 기만신호를 인가한 후 각각의 위성항법 수신기가 출력한 결과를 비교한 것이다.

그림 15와 17에서와 같이 기만신호가 위성항법 신호에 영향을 주는 시점과 영향이 사라지는 시점에서 급격한 신호의 산란(fading)에 의해서 위성항법 신호를 잃는 경우가 발생하게 된다. 이는 기만 성공 여부와 상관없이 발생하며, 기만신호 대 위성항법 신호의 비가 같은 경우 위성신호를 잃은 후에 다시 위성항법 신호를 추적하게 되고 기만신호가 위성항법 신호보다 5dB가 큰 경우에는 위성신호를 잃은 후에 기만신호를 추적하여 완전히 기만되는 것을 확인할 수 있다.

그림 14와 16은 기만신호에 의해 영향을 받은 위성항법 수신기가 출력하는 수평면 궤적을 나타낸 것이다. 기만신호가 위성항법 신호보다 5dB 큰 경우에는 완전히 기만되어 붉은 점선과 같이 기만궤적을 출력하는 것을 확인할 수 있다. 또한 기만이 되지 않더라도 그림 16의 파란색 실선과 같이 기만신호에 의한 다중경로오차 발생으로 인하여 저가형 상용 위성항법 수신기는 위치오차가 증가하는 것을 확인할 수 있다.

2. 기만기가 알고 있는 목표물의 위치에 오차가 존재하는 기만상황

현실적으로 목표물의 위치와 속도를 정확히 추정하는 것은 어렵다. 그러므로 위치에 대한 오차가 존재하는 기만상황에 대해 모의 실험을 실시하였다. 위치는 3차원이지만 3차원에 대해

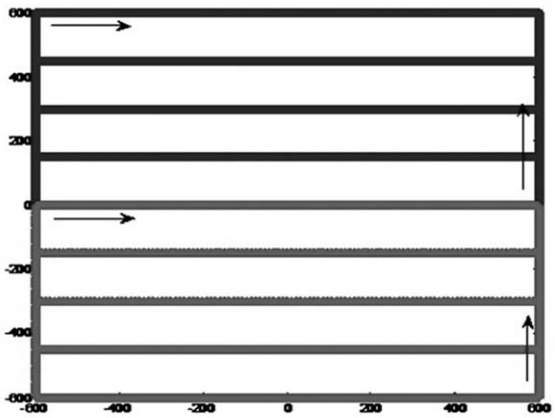


그림 18. 기만 신호 인가 형태.

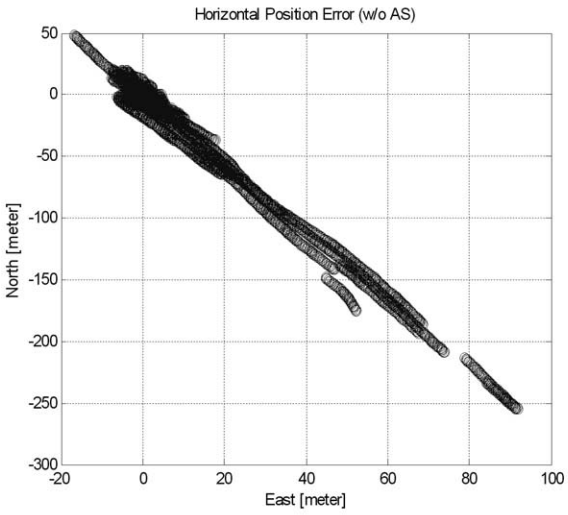


그림 19. 수평면 위치 오차.

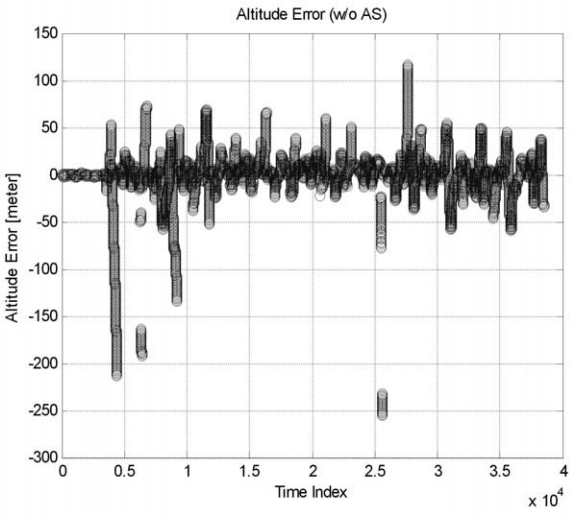


그림 20. 수직 위치 오차.

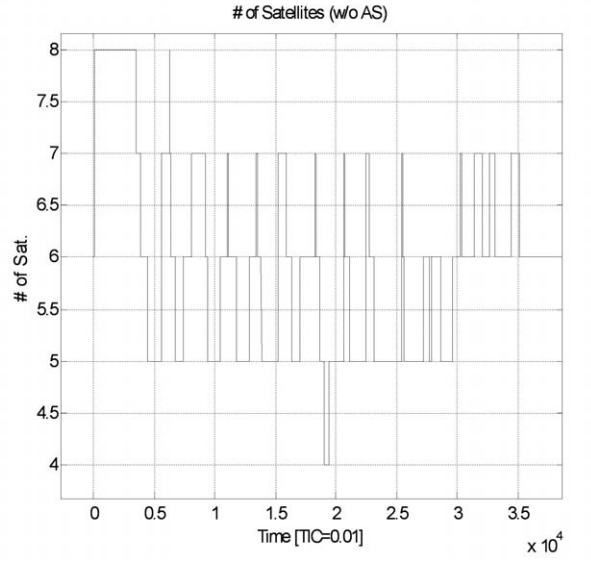


그림 21. 추적된 위성 수.

표 8. 위성항법 수신기 위치 오차.

구분	East [meter]	North [meter]	Altitude [meter]
오차	8.96	24.66	23.86

모두 모른다고 가정하는 경우 기만할 수 있는 경우는 복잡해지므로 단순화를 위하여 항체의 진행방향에 대해서는 정확이 안다고 가정하고 항체의 진행방향의 교차방향으로 각각 ±600미터의 기만기의 목표물에 대한 위치추정 오차가 존재한다고 가정하였다.

그림 18은 2대의 기만기가 목표물의 진행방향에 대한 교차방향에 대해서 지그재그로 기만신호를 인가하는 교차방향 위치에서 나타낸 것이다.

그림 19와 20은 각각 수평면 위치 오차와 고도 오차를 나타낸 그림이다. 두 가지의 기만 신호는 그림 18과 같이 항체의 진행방향의 교차방향에 대해서 초당 300미터로 진행하게 된다. 그러므로 수초마다 위성항법 신호는 기만 신호에 노출되게 된다.

기만에 의해서 일부 위성이 영향을 받음에 따라 수평면과 수직 위치오차가 발생하게 된다. 표 8은 기만에 의해서 발생된 위성항법 수신기에서의 오차를 나타낸 것이다.

Ⅶ. 기만 대응

위성항법 신호는 항법 신호로서 일정한 규칙성과 제한을 내재한다. 내재한 특성 중의 중요한 것이 항법 데이터와 위성신호

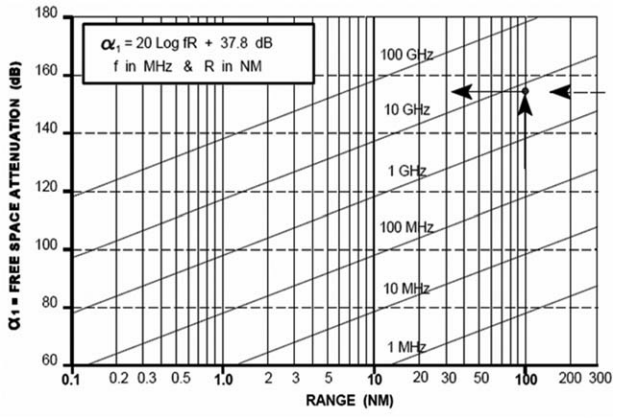


그림 22. 거리에 따른 신호 세기.

표 9. 기만 대응 기법.

방법	검출 통계	Spoofer의 특징	제한 조건
1	절대 신호전력	위성신호에 비해 신호전력 큼	안테나 자세변화
2	신호전력 변화율	신호전력의 변화율 큼	안테나 자세변화
3	위성간 상대 신호세기	위성간 신호세기 균일	이온층오차 영향
4	의사거리 변화율	의사거리 변화율 큼	GPS 수신기의 이동성
5	도플러 변이	위성간 도플러 변이 동일	·
6	상관 크기	L1/L2의 상관값 비교	Y코드에서 낮은 성능
7	항법데이터 제거 신호	GPS 신호를 복구하여 비교	GPS 신호의 세기
8	L1/L2 의사거리 차분	L1/L2의 의사거리 차이	L1/L2 수신기 필요
9	위성력 정보	Ephemeris 데이터 검증	·
10	신호의 세기와 데이터	신호의 순간적인 변화 비교	·

의 세기이며 마지막으로 위성과 수신기간의 상대운동이다. 위성항법 데이터는 4시간 또는 6시간마다 변경되는 시점을 제외하고는 변화가 없기 때문에 예측가능하고 모조가 가능하다. 하지만 위성신호의 세기와 상대운동의 경우에는 항법위성과 지상 또는 공중에 배치된 기만장치와 현격한 차이를 발생한다. 위성신호의 세기는 위성과 지상의 거리가 멀지만 기만장치와 위

성항법 수신기간의 거리는 상대적으로 짧다. 그림 22는 거리에 따른 신호세기의 변화를 나타내는 그림이다. 그림에서와 같이 위성과 위성항법 수신기간의 거리는 멀기 때문에 거리 변화에 따른 신호의 크기 변화가 거의 없지만 기만장치와 위성항법 수신기간의 거리는 상대적으로 짧아 조그만 거리변화에도 큰 신호세기의 변화를 겪게 된다.

또한 항법위성과 위성항법 수신기의 움직임에 의해서 의사거리의 변화율과 도플러가 결정되게 된다. 그러므로 위성항법 수신기가 움직이고 있는 경우에 기만신호가 인가되기 전의 의사거리 변화율과 도플러와 기만에 의한 의사거리 변화율과 도플러는 차이가 발생할 수 있다. 그러므로 위에서 언급한 중요한 3가지 측정값 이외에도 위성항법 신호가 내재한 특성을 이용하여 표 9에서와 같이 Spoofing의 인지 및 제거가 가능하다.

그러나 기존의 기만대응 연구는 개별적인 위성신호에 대한 기만에 대응하고 인지된 기만 신호는 사용을 배제하는 형태로 진행되어 왔지만 앞서 언급한 능동형 기만의 경우에는 위성항법 신호를 100%에 가깝게 모사할 수 있기 때문에 GPS L1 C/A신호에 국한된 경우에는 기존 기만대응 방법으로 인지가 불가능하고 모든 위성 신호에 대해서 기만이 인가되고 있기 때문에 사용을 배제할 수 없다.

표 9에서의 기만대응 기법 중에서 L1 C/A 코드 수신기에서 사용 가능한 방법은 1, 2, 3, 4, 5, 7, 9, 10번이다. 기존의 기만대응 방법은 기만의 인지를 통해 해당 위성 신호의 배제를 목적으로 구상되었으나 앞서 언급된 능동형 기만에 의해서 기만되는 경우에는 모든 위성신호에 대해서 기만이 가해지므로 기만을 회피하는 동시에 기존의 신호를 복구할 수 있어야 한다.

Ⅷ. 결론

기만에 대해 정의하고 위성항법 신호를 기만할 수 있는 조건에 대해서 알아보았다. 모의 실험을 통해서 기만될 수 있는 몇 가지 상황에 대한 결과를 보였다. 일반적으로 기만은 재밍장치보다 복잡하지만 기만의 성공 가능성은 재밍보다는 낮다. 그러나 낮은 가능성에 비해 기만에 의한 영향은 재밍보다 큰 피해를 줄 수 있다. 위성항법 신호는 이미 공공에 알려져 있어 그 특성에 대해서 많은 연구가 이루어져 있으며 그 만큼 기만신호와 같은 모조신호에 취약할 수 있다. 가장 근본적인 기만신호에 대한 해결책은 보안된 항법신호 사용을 통한 기만에 대한 원천적인 차단이라 할 수 있다. 하지만 이와 같은 보안된 항법신호 사용은 위성항법시스템을 운영하는 미국, EU, 중국 및 일본과 같은 나라에서 가능하며 모든 국가에 공개된 항법신호는 기만에 취약할 수 밖에 없다. 한국에서의 보안신호 사용은 한국형 SBAS(Satellite Based Augmentation System)에 C/A 코드와 함께 보안된 위성항법 신호 설계하여 동일 대역에 전송함으로써 인증된 사용자는 보안된 위성항법 신호를 이용하여 기만여부에 대한 파악이 가능하도록 할 수 있다.

마지막으로 기만에 대응하는 가장 첫 번째는 효과적인 기만기에 대한 연구를 수행하는 것이다. 효과적인 기만에 대한 연구를 통해 위성항법 신호의 기만에 대한 취약성을 연구한 후 이에 대한 대응책을 마련하는 것이다. 무엇보다도 중요한 것은 기만 이후에 대한 대응보다는 보안된 위성항법 신호를 이용한 기만에 대한 원천적 차단이 최선의 방법이다.

참고문헌

[1] B.W. Parkinson, J. J. Spilker Jr, *GPS Positioning System : Theory and Application*, AIAA, 1996.

[2] Kaplan E. D., *Understanding GPS : Principles and Applications*, Artech House Publisher, Norwood, MA, 1996.

[3] Jame Bao-Yen Tsui, *Fundamentals of Global Positioning System Receivers : A Software Approach*, John Willey&Sons INC., 2000.

[4] Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O' Hanlon, and Paul M. Kintner, Jr., "Assessing the Spoofing Threat : Development of a Portable GPS Civilian Spoofer," *ION GNSS 2008*, 2008.

[5] Sung-Hyuck Im, Gyu-In Jee, Sang-Do Cho, and Sun-Jun Ko," A Novel Software GPS Receiver Architecture Using Partial Down Conversion," *ION 2007 National Technical Meeting*, 2007.

[6] Jon S. Warner, Roger G. Johnston, " GPS Spoofing Countermeasures," *Homeland Security Journal*, December 12, 2003.

[7] 임성혁, 임준혁, 지규인, 백승욱, 이인원, 이대열, "GPS L1 C/A 신호추적루프에서의 기만에 의한 영향," *한국항행학회 논문지*, 15 권, 1호, p32-38, 2011.

[8] 임성혁, 지규인, "맵 기반의 부분시간 공통 중간주파수 제거 방식을 이용한 GNSS 신호의 상관 기법," *제어로봇시스템학회 논문지*, 제14권 제7호, p695-701, 2008.

[9] 임성혁, 지규인, "소프트웨어 기반의 GNSS IF(intermediate frequency) 신호 및 관성항법장치(IMU : inertial measurement unit) 데이터 발생기 구현," 12차 GNSS Workshop, 2005.

저 자 약 력

임 성 혁

· 2003년 건국대학교 전자정보통신공학과 졸업.
· 2005년 건국대학교 전자정보통신공학과(공학석사).
· 2011년 건국대학교 대학원 전자정보통신공학과(공학박사),
· 2011년~현재 한국항공우주연구원 선임연구원.
· 관심분야 : 실시간 고성능 컴퓨팅기반 GNSS 수신기 신호 처리 및 생성, GNSS anti-jamming/spoofing, GNSS 신호처리, 복합센서 결합 항법.

지 규 인

· 1959년 11월 24일생.
· 1982년 서울대학교 제어계측공학과(공학사).
· 1984년 서울대학교 제어계측공학과(공학석사).
· 1989년 Case Western Reserve Univ. System and Control Engineering(공학박사).
· 1992년~현재 건국대학교 전자정보통신공학과 교수.
· 관심분야 : GPS/INS 결합항법, GPS 수신기 신호처리, 무선측위, 소프트웨어 GPS, GPS anti-jamming, 무인자동차 자율주행.