통합의사잡음 신호를 사용한 GNSS의 재방송재밍 검출기법

A Novel Repeat-back Jamming Detection Scheme for GNSS using a Combined Pseudo Random Noise Signal

유 승 수, 염 동 진, 지 규 인, 김 선 용*

(Seungsoo Yoo¹, Dong-Jin Yeom², Gyu-In Jee¹, and Sun Yong Kim^{1,*})

¹Division of Electronics Engineering, Konkuk University

²Agency for Defense Development

Abstract: A repeat-back jamming signal is an intentionally re-broadcasted GNSS (Global Navigation Satellite System) interference. In this paper, a novel repeat-back jamming detection scheme is proposed. The proposed scheme uses a combined pseudo random noise signal (C-PRN) and is available for a generic GNSS receiver with a single antenna. The C-PRN signal is made by combining several received pseudo random noise signals that had been transmitted from the visible GNSS satellites. Through a Monte-Carlo simulation, the detection probability of a repeat-back jamming signal detected with the proposed scheme is presented.

Keywords: GNSS, repeat-back jamming, single antenna GNSS receiver, combined-PRN sequence, high resolution correlator, multipath mitigation

I. 서론

2000년대 이후 대표적인 GNSS (Global Navigation Satellite System)인 미국의 GPS (Global Positioning System)의 의도적 오차요소인 SA (Selective Availability) 신호가 제거되면서 GNSS 관련 연구개발이 본격적으로 진행되고 있다. 2011년 현재 GNSS 관련 시장은 매년 122.4억 달러씩 성장할 것으로 전망되며, 이 가운데 민간용 GNSS 장비와 응용제품 등은 매년 40%씩 지속적으로 성장할 것으로 예상되고 있다. 2014년 현재 GNSS는 금융, 농업, 환경, 항해, 재난대응 등 공공안전, 철도와 버스 등 대중교통제어, 각종 야외활동, 지형조사와 지도 제작 등 다양한 분야에서 활용되고 있다[1].

GPS 위성과 지상에 위치한 수신기의 가시성이 확보되는 야외 환경에서 수신되는 GPS L1 C/A (Coarse/Acquisition) 신호는 약 -130dBm 정도 수준인데 반해 C/A 신호의 중심 대역폭만을 수신하는 경우 열잡음은 약 -111dBm 정도로 C/A 신호에 비해 잡음이 약 19dB 더 강하게 수신된다. 그러나 이는 최적수신환경을 가정한 경우이며, 의도적 간섭(interference) 및 재밍(jamming)이 발생하는 경우 신호수신이 상당히 어렵거나 거의 불가능할 수 있다[1-3].

GNSS 재밍은 재밍의도의 수준에 따라 단순재밍, 재방송

(repeat-back)재밍, 기만재밍(spoofing) 등으로 구분된다. 단순재밍은 연속파재밍, 광대역 및 부분대역 정규잡음재밍, 펄스(pulse)재밍 등 단순한 형태를 갖는 신호를 생성해 수신기를 혼동시키는 재밍이다. 재방송재밍은 수신기에서 가까운 거리에 위치한 재방송재밍기에서 수신한 GNSS 신호를 단순히 재방송하는 재밍으로서, 희생 수신기의 위치해를 재방송재밍기의 위치 가까스로 오결정하도록 시도하는 재밍이다. 기만재밍은 기만기에서 수신한 GNSS 신호를 관찰한 후 수신기가 기만기의 의도된 위치해를 도출할 수 있도록 정교하게 처리된 기만신호를 이용해 수신기를 기만하는 재밍이다[2,4].

기만재밍에 대한 대표적인 해법은 GPS P(Y) (Precise) 신호 또는 M (Military) 신호처럼 암호화된 신호를 사용하는 것이다. 언급한 두 신호들은 모두 군사용으로 사용되는 신호로서 이를 해독할 열쇠 값(key value or sequence)을 갖지 못한 수신기는 해당 신호를 정확하게 역확산 할 수 없다[5]. 단순재밍에 대한 대표적인 해법은 단순재밍형태에 따라 다르다. 연속파재밍의 경우 고속푸리에변환과 같은 방법으로 연속파의 특징을 파악할 수 있으며, 간단한 대역제거 여파기(band rejection filter)를 사용해 쉽게 제거할 수 있다. 펄스재밍은 재밍신호가 수신되는 시간 동안 비정상적인 전력 수신 형태를 보이기 때문에 이를 감지한 후 해당 신호를 사용하지 않는 비움(blanking) 기법을 통해 쉽게 대응할 수 있다. 광대역 및 부분대역재밍은 잡음전력을 억제하기 위한 적산(integration) 기법을 사용해 일정 수준 완화할 수 있다[3].

재방송재밍은 단순히 수신한 신호를 증폭기를 거쳐 재방송하기 때문에 [5]처럼 암호화된 항법신호를 사용해도 쉽게 극복하기 어렵다. 대표적인 재방송재밍 완화기법은 동기적 산(coherent integration)을 이용한 처리이득향상방법이다.

* Corresponding Author

Manuscript received June 5, 2014 / revised June 13, 2014 / accepted June 17, 2014

유승수, 지규인, 김선용: 건국대학교 전자공학부

(kelvin@konkuk.ac.kr/gijee@konkuk.ac.kr/kimsy@konkuk.ac.kr)

염동진: 국방과학연구소(djyeom@add.re.kr)

※ 본 논문은 방위사업청과 국방과학연구소가 지원하는 국방 위성항법 특화연구센터 사업, 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (2012R1A1A 2004944).

GPS L1 C/A 신호의 경우 항법정보의 비트 천이로 인해 특별한 기법 처리 없이 최대 20ms까지 동기적산이 가능하며, 이론적으로 역확산 이득을 포함해 최대 약 30dB의 이득향상이 가능하다. 그러나 이는 어디까지나 이론적인 경우이며, 수신기의 역동성(dynamic)이 큰 경우 동기적산에 큰 제약을 받기 때문에 제한적으로 적용된다[1,2]. 재방송재밍 검출과 완화를 함께 처리할 수 있는 대표적 기법은 적응형영점조정(adaptive null steering) 방법이다. 이 방법은 각기 아는 위치에 있는 다수의 배열안테나를 활용해 대부분 지표면 방향에서 수신되는 재방송재밍 신호의 신호 송출 방향을 추정하고, 해당 방향의 안테나 이득을 영점 조정해 재방송재밍을 효과적으로 완화하는 방법이다. 이 방법은 안정적 수신환경(static scenario)에서 약 40-50dB의 성능개선이 있다. 그러나 정밀한 위상동기 배열안테나가 필요하며, 배열안테나 사용에 따른 수신기의 부피가 상당히 큰 문제가 있다[6,7]. 또 다른 재방송재밍 완화방법은 여러 GNSS를 함께 사용하는 방법이다. 2014년 현재 지구 전역에서 활용 가능한 GNSS는 GPS를 비롯해, 러시아의 GLONASS (러시아어 Глобальная навигационная спутниковая система, 영어 GLObal NAVigation Satellite System, 2014년 5월 현재 몇 개의 위성이 정지되어 일시적으로 지구 전역 사용이 제한되고 있다[8]), 중국의 BDS (중국어 北斗卫星导航系统, 영어 BeiDou Navigation Satellite System, [9]) 등이 있으며, 유럽연합도 2020년 지구 전역운용을 목표로 Galileo 시스템 구축하고 있고, 인도와 일본 등 자국 등 일부 영역에서 위성항법을 제공할 수 있는 시스템을 보유 및 운용하고 있다. 재방송재밍을 비롯한 모든 재밍방법은 전파의 효과적인 방해로 인해 상당히 큰 전력량이 요구되어, 모든 GNSS를 재밍 하는 것은 상당히 어려운 일이다. 따라서 재밍의 효과적인 검출을 통해 재밍에 침해되는 GNSS를 찾고, 이를 회피해 다른 GNSS를 활용한다면 재방송재밍을 비롯한 거의 대부분 재밍에 효과적으로 대응할 수 있다. 그러나 이 기법은 효과적인 검출이 가능해야 적용할 수 있는 단점을 갖고 있다. 이 외에도 안테나의 물리적 조정을 통한 송수신방사각의 조정을 통한 재방송재밍 완화방법 등이 연구되고 있으나 아직까지 그 실효성에 대한 충분한 연구는 이루어지지 않고 있다[1,6].

본 논문은 재방송재밍 검출방법에 초점을 맞춘다. 특히 이 가운데서 [6]과 같이 단일 안테나를 사용하는 재방송재밍 검출방법을 제안한다. 이를 위해 본 서론에 이어 재방송재밍환경에서의 수신신호모형을 정리하고, 이를 바탕으로 새로운 단일안테나 기반 재방송재밍 검출기법을 제안한다. 제안한 기법은 통합의사잡음(combined pseudo random noise, C-PRN) 신호를 기반으로 구성한다. 이어 IV 장과 V 장에서는 모의실험을 통해 제안한 기법의 성능을 보이고, 이를 분석한 후 제안한 기법의 특징을 정리하고 맺는다.

II. 수신신호모형

N 개의 가시위성과 단일 재방송재밍기가 있는 재방송재밍 상황은 그림 1과 같다. 그림 1에서 SV_1 - SV_N 은 각 궤도에 위치한 가시 GNSS 위성, RBJ 는 재방송재밍기(repeat-

그림 1. 가시 GNSS 신호가 수신될 때 단일 재방송재밍 상황.

Fig. 1. A single repeat-back jamming scenario when some visible GNSS signals are being received.

back jammer), V 는 재방송재밍기에 의해 공격을 당하는 수신기(victim receiver), τ_i, f_i, θ_i 와 $\tilde{\tau}_i, \tilde{f}_i, \tilde{\theta}_i$ 는 i 째 가시 GNSS 위성으로부터 수신기와 재방송재밍기에 수신되는 GNSS 항법신호의 전파지연, 주파수편이, 위상편이 ($i = 1, 2, \dots, N$), τ_j, f_j, θ_j 는 재방송재밍기에 의해 야기되는 재방송재밍기와 수신기 사이의 전파지연, 주파수편이, 위상편이를 뜻한다.

재방송재밍은 기만재밍과는 다르게 수신한 GNSS 신호를 별도로 처리하지 않고 단순히 재방송하는 형태의 재밍으로서, 수신기가 정상적인 동작을 하고 있는 도중에 재방송재밍기에 의해 공격을 받는 경우 재방송재밍기의 공격이 유효하기 위해서는 재방송재밍기는 일반적인 수신기의 부호 동기추적 범위인 $1.0T_c$ 이내에 재방송재밍 신호가 수신될 수 있는 곳에 위치해야 한다[1,6]. 여기서 T_c 는 공격하고자 하는 GNSS 확산신호의 칩(chip) 주기이며, GPS L1 C/A 신호의 경우 약 997ns, 거리로 환산하면 약 300m 정도이다. 이 경우 지상에서 약 20,200km 상공에 위치한 GPS 위성에 비해 재방송재밍기와 수신기 사이의 거리는 극히 짧아 수신기와 재방송재밍기에 수신되는 GNSS 항법신호의 전파지연, 주파수편이, 위상 편이는 거의 같다. 따라서 본 논문에서는 $\tilde{\tau}_i = \tau_i, \tilde{f}_i = f_i$ 로 가정한다. 또한 재방송재밍기와 수신기 사이의 전파지연, 주파수편이, 위상 편이는 재방송재밍기에 의해 재방송되는 모든 GNSS 항법신호에 동일하게 적용된다.

이상과 같이 일반적인 재방송재밍 상황을 고려했을 때 기저대역 수신신호모형은 식 (1)과 같다. 식 (1)에서 N 은 가시 GNSS 위성 수, S_i 는 i 째 GNSS 위성으로부터 수신된 항법신호의 수신전력, $d_i(t)$ 는 i 째 GNSS 위성의 항법정보, $c_i(t)$ 는 i 째 GNSS 위성의 의사 잡음(PRN: Pseudo Random Noise) 신호, J 는 재방송재밍신호의 수신전력, $n_f(t)$ 는 재방송재밍기에 유입된 복소가산정백색정규잡음(complex

additive white Gaussian noise), $n(t)$ 는 수신기에서 유입된 복소가산성백색정규잡음을 각각 뜻한다.

$$r(t) = \sum_{i=1}^N \sqrt{S_i} d_i(t - \tau_i) c_i(t - \tau_i) \cos(2\pi f_i t + \theta_i) + \sqrt{J} \left[\sum_{i=1}^N \sqrt{S_i} d_i(t - \tau_i - \tau_J) c_i(t - \tau_i - \tau_J) \cos(2\pi(f_i + f_J)t + \tilde{\theta}_i + \theta_J) + n_J(t) \right] + n(t) \quad (1)$$

그림 1과 식 (1)처럼 수신기에서 유효한 위치에 재방송재밍이 한 개만 있는 경우 J , τ_J , f_J , τ_J 는 재방송하는 모든 GNSS 신호에 공통적으로 적용되는 값으로서 각 GNSS 위성에서 송신된 신호가 수신기에 도달할 때 각기 다른 전파경로로 인해 각각의 전파지연, 주파수편이, 위상 편이가 발생하고, 각각의 다중경로신호가 수신되는 반면, 재방송재밍신호는 이에 공통된 전파지연, 주파수편이, 위상 편이가 더해지는 형태이다. 본 논문에서는 표현의 단순화를 위해 다중경로신호는 고려하지 않는다.

III. 새로운 재방송재밍 검출기법

앞 장에서 언급한 것처럼 GNSS 위성으로부터 수신기에 직접 수신되는 신호는 각 위성별로 별도의 전파지연, 주파수편이, 위상 편이가 적용되는 반면, 재방송재밍신호는 이에 공통된 전파지연, 주파수편이, 위상 편이가 더해지는 형태이다. 따라서 수신기가 정상동작 중에 재방송재밍 공격이 이루어지는 경우 공격이 시작되는 시점에서 수신기는 각 GNSS 위성의 전파지연, 주파수편이, 위상편이, 항법정보 등을 알고 있다고 가정할 수 있다. 일반적인 경우 전파지연, 주파수편이, 위상편이, 항법정보 등 주요정보 추정에 따른 오차가 있으나 본 논문에서 제안하는 기법을 뚜렷하게 보이기 위해 우선 각 주요정보의 추정은 정확하다고 가정하며, 이에 오차가 있는 경우는 추후 연구에서 다룰 예정이다.

일반적으로 고려되는 재방송재밍 신호의 전력은 GNSS 신호 전력에 비해 상당히 세계 전송하기 어렵다. 상당히 센 재방송신호를 송출할 경우 재방송을 위해 자체적으로 수신하려고 하는 GNSS 신호에 재방송재밍 신호가 함께 수신되는 자기간섭효과(self interference effects)가 크게 일어나 상당히 왜곡된 신호를 전송하기 쉽다[6]. 수신기도 간단한 반송파 대 잡음신호 전력 비(carrier-to-noise power ratio)의 관측을 통해 재방송재밍 여부를 판정할 수 있다[1,2]. 따라서 본 논문에서는 재방송재밍 신호 전력 대 GNSS 신호전력의 비(repeat-back jamming power to GNSS signal power ratio, JSR)가 크지 않은 상황만을 고려한다.

제안한 기법에 대해 설명하기에 앞서 제안한 기법의 핵심 구성요소인 C-PRN 신호에 대해 설명한다. C-PRN 신호는 재방송재밍 직전에 수신기에서 가시 GNSS 위성으로부터 수신한 신호를 처리한 정보를 바탕으로 얻은 전파지연, 주파수편이, 위상편이, 항법정보를 각 가시 GNSS 위성의 PRN 신호에 적용한 후 이를 하나로 결합한 새로운 PRN 신호이다.

표 1. 임의의 한 C-PRN 신호의 세부 사양.

Table 1. Specifications of a combined pseudo random noise signal.

SVID of SV_i	1	9	15	21
f_i [Hz]	-127	1286	-2512	257
τ_i [chip]	16.125	440.125	-259.625	-30.875
θ_i [rad]	-0.87	+1.25	+2.35	+0.02

그림 2. PRN 번호가 각각 (a) 1, (b) 9, (c) 15, (d) 21인 GPS 위성 신호가 수신된 때와 (e) 이에 대한 C-PRN 신호를 사용했을 때 정규화된 상관 값.

Fig. 2. Normalized correlation values when GPS satellite vehicle signals, whose PRN numbers are (a) 1, (b) 9, (c) 15, and (d) 21, respectively, are received, and (e) using C-PRN signal from the received signal.

표 1과 같은 조건 하에서 GPS L1 C/A 신호의 각각에 대한 PRN 신호를 사용한 경우와 C-PRN 신호를 사용한 경우 정규화된 비동기 자기상관값은 그림 2와 같다. 그림 2(a)부터 그림 2(d)까지는 표 1과 같은 개별 PRN 신호에 대한 상관 값이며, 그림 2(e)는 C-PRN 신호를 사용한 상관 값이다. 그림 2에서 C-PRN 신호에 대한 부호동기시점을 0으로 맞추기 위해 나머지 PRN 신호는 상대적으로 회전해 표현하였다. 그림 2처럼 개별 PRN 신호의 상관 값의 경우 각 신호의 상호상관 및 재방송재밍 신호로 인한 신호 왜곡이 나타난다. 그림 2(e)의 C-PRN 신호의 정규화된 비동기(non-coherent) 자기상관값을 확대해 다시 그리면 그림 3과 같다. 그림 3에서 오른쪽 위의 작은 그림은 상관 값의 첨두 주변을 확대한 그림이다. 표 1처럼 신호를 결합한 경우 비동기 자기상관값의 첨두값 대 근제곱평균값의 비(peak to root mean square noise power ratio)는 16.9900dB이다. 해당 C-PRN 신호를 생성하기 위해 사용한 9번 GPS 위성의 PRN 신호의 비동기 자기상관값의 첨두값 대 근제곱평균값의 비는 16.9747dB로서 관찰한 C-PRN 신호와 임의의 PRN 신호의 비동기 자기상관특성은 크게 다르지 않으며, 가장 중요한 성능지표 가운데 하나인 처리이득도 유사함을 확인할 수 있다. 이는 [1]처럼 PRN 신호의 기본 성질 가운데 하나로써 임의의 두 PRN 수열을 더해 새롭게 합성한 PRN 수열도 역시 PRN 수열의 특성을 갖는 성질에 기인한다. 따라

그림 3. 임의의 한 C-PRN 신호의 정규화 된 비동기 자기상관 값.
Fig. 3. Normalized non-coherent auto-correlation values for a combined pseudo random noise signal.

그림 4. 재방송재밍 신호에 의해 왜곡된 수신신호의 비동기 상관 값.
Fig. 4. Non-coherent correlation values of a distorted received signal caused by a repeat-back jamming signal.

서 본 논문에서는 재방송재밍 검출을 위한 새로운 PRN 신호로서 C-PRN 신호를 사용한다.

C-PRN 신호를 사용하는 경우 재방송재밍신호는 한 상관 채널에서의 단일 다중경로신호성분과 그 특성이 같으며, 기존에 제안된 많은 다중경로영향 검출 및 완화기법을 활용해 재방송재밍신호를 검출/식별/완화할 수 있다. C-PRN 신호기반 재방송재밍 검출채널에서 $JSR = -3\text{dB}$, $\tau_J = 0.5 T_C$, $f_J = 79\text{Hz}$ 인 재방송재밍신호가 함께 수신된 경우 정확한 동기시점에서 정규화 된 상관 값의 개형은 그림 4처럼 왜곡된다. 본 논문에서는 재방송재밍기와 수신기는 역동성(dynamic)이 없거나 상당히 작은 경우만을 고려하며, f_J 는 $[-100\text{Hz} + 100\text{Hz}]$ 에서 균등분포를 갖는 확률변수로 설정하였다. 그림 4처럼 설정한 재방송재밍신호가 수신기에 유입된 경우 [11]에서 보인 단일 다중경로신호에 의한 상관 값의 왜곡과 유사한 형태를 보이는 것을 확인할 수 있다. 이는 C-PRN 신호가 다수의 PRN 신호를 결합해 만들었기 때문에 각각의 위성수신경로의 다중경로신호는 그 지연이 각기 다르지만 C-PRN 신호를 통해 확인한 재방송재밍신호의 지연이 모든 GNSS 위성 PRN에 대해 동일하기 때문에 C-PRN 신호를 이용한 비동기 상관에서 재방송재밍신호는 일반적인 다중경로신호에 의한 왜곡과 유사한 경향을 보이는 것이다.

그림 5. 재방송재밍 신호가 인가되지 않았을 때 WELP와 NELP의 정규화 된 판별 값.

Fig. 5. Normalized discrimination values of WELP and NELP when no repeat-back jamming signal is received.

그림 6. 재방송재밍 신호가 수신되었을 때 WELP와 NELP의 정규화 된 판별 값 ($JSR = 0\text{dB}$, $\tau_J = 0.5 T_C$, and $f_J = 79\text{Hz}$).

Fig. 6. Normalized discrimination values of WELP and NELP when a repeat-back jamming signal is received ($JSR = 0\text{dB}$, $\tau_J = 0.5 T_C$, and $f_J = 79\text{Hz}$).

II 장에서 언급한 신호모형과 앞서 언급한 C-PRN 신호 설정 하에서 재방송재밍 신호가 없을 때와 $JSR = 0\text{dB}$ 의 재방송재밍신호가 인가되었을 때 [9]의 HRC (High Resolution Correlator)의 판별기(discriminator)와 유사한 WELP (Wide Early-minus-Late Power)와 NELP (Narrow Early-minus-Late Power) 판별기의 정규화 된 판별값은 각각 그림 5와 그림 6과 같다. 두 판별기의 이른-늦은 상관 전력 값의 표본 차이는 각각 $1.00 T_C$ 와 $0.25 T_C$ 로 설정하였다. 식 (1)에서 고려한 신호와 잡음의 전력은 일반적인 실외 수신환경을 고려해 반송파 신호 전력 대 잡음 전력의 비가 44dB-Hz 인 환경을 고려했다.

그림 5처럼 재방송재밍 신호가 인가되지 않았을 때 NELP와 WELP 출력은 정확한 동기시점($\tau = 0$)에서 영점을 지난다(zero-crossing). 이는 [1]에서 언급한 일반적인 비동기 이른-늦은 상관 전력차 판별기의 출력과 유사한 결과이다. 그러나 고려한 재방송재밍 신호가 인가되는 경우 그림 6처럼 NELP와 WELP 판별값 모두에 왜곡이 나타나며, 영점을 교차하는 시점이 정확한 동기시점을 크게 벗어난다. 또한

그림 5에서 본 바와 같이 NELP는 침두 주변, WELP는 이보다 훨씬 넓은 간격을 갖고 설계되기 때문에 왜곡되는 정도, 즉 영점을 지나는 시점이 각각 다르다. 본 논문에서는 이를 고려하여 식 (2)가 성립하는 경우 재방송재밍 신호가 수신되었음을 검파하는 새로운 재방송재밍 검출기법을 제안한다.

$$|D_W^{-1}(\tau_{J,W}=0) - D_N^{-1}(\tau_{J,N}=0)| > \gamma \quad (2)$$

여기서 $D_W^{-1}(\tau)$ 와 $D_N^{-1}(\tau)$ 는 식 (3)과 식 (4)와 같은 WELP와 NELP 판별식의 역함수, $\tau_{J,W}$ 와 $\tau_{J,N}$ 은 WELP와 NELP로 추정된 재방송재밍신호의 부호위상, γ 는 재방송재밍 검출을 위한 문턱 값이다. γ 는 식 (1)에서 재방송재밍기가 잡음만을 재방송할 때 설정한 오경보 확률 (false-alarm probability)로부터 얻을 수 있다.

$$D_W(\tau) = R\left(\tau - \frac{\Delta_W}{2}\right) - R\left(\tau + \frac{\Delta_W}{2}\right) \quad (3)$$

$$D_N(\tau) = R\left(\tau - \frac{\Delta_N}{2}\right) - R\left(\tau + \frac{\Delta_N}{2}\right) \quad (4)$$

여기서, $R(\cdot)$ 는 식 (5)와 같은 비동기 상관 함수, Δ_W 와 Δ_N 은 각각 WELP와 NELP 판별기의 이른-늦은 상관 전력 값의 표본 차이이다.

$$R(\tau) = \left| \frac{1}{LT_C} \int_0^{LT_C} r(t) C(t+\tau) dt \right| \quad (5)$$

여기서, L 은 확산신호의 길이, $C(t)$ 는 식 (6)과 같은 C-PRN 신호이다.

$$C(t) = \sum_{i=1}^N \hat{d}_i(t - \hat{\tau}_i) c_i(t - \hat{\tau}_i) \cos(2\pi \hat{f}_i t + \hat{\theta}_i) \quad (6)$$

여기서 $\hat{d}_i(t)$, $\hat{\tau}_i$, $\hat{f}_i$, $\hat{\theta}_i$ 는 각각 수신기에서 재방송재밍이 야기되기 직전 추정된 항법정보, 부호위상, 주파수편이, 위상 편이이다. 본 논문에서는 이들 정보의 추정이 정확하다고 가정한다.

이상의 개념을 바탕으로 한 제안한 기법은 그림 7처럼 구성된다. 그림 7에서 I&D (Integration and Dump)는 상관적

산 후 상관주기에 따른 상관 값 출력함수, $C_{W,E}$, $C_{W,L}$, $C_{N,E}$, $C_{N,L}$ 은 각각 WELP와 NELP 구성을 위한 각각의 C-PRN 신호이다. 그림 7처럼 제안한 기법은 WELP와 NELP를 사용해 재방송재밍 신호로 인한 각 부호위상 추정 값을 도출하고, 그 차이로부터 재방송재밍을 검출한다.

IV. 모의실험 및 분석

이번 장에서는 모의실험을 통해 제안한 기법의 검파성능을 분석한다. 모의실험을 위해 재방송재밍기의 자기간섭은 없고, $\hat{d}_i(t)$, $\hat{\tau}_i$, $\hat{f}_i$, $\hat{\theta}_i$ 은 이상적으로 추정되었고, 단일 재방송재밍을 고려하며, 재방송재밍기와 수신기 사이의 상대적 운동은 없거나 거의 없다고 가정한다. 그리고 재방송재밍기와 수신기 잡음 발생을 위해 반송파 전력 대 잡음 전력의 비를 일반적인 GPS L1 C/A 신호의 실외 수신환경과 같이 44dB-Hz, 검파확률 도출을 위한 오경보확률은 10^{-3} 으로 설정하였다.

$\tau_J = 0.5 T_C$ 일 때, 가시위성의 수 N 에 따른 JSR 대비 검파확률은 그림 8과 같다. 그림 8처럼 제안한 기법의 전체적인 검파확률은 점차 높아지다 JSR 약 5dB 이후 낮아지는 개형을 갖는다. GPS L1 C/A 신호의 일반적인 수신환경처럼 수신기와 재방송재밍기 모두에서 8개의 가시위성신호가 수신될 때, JSR -6dB의 경우 검파확률이 약 0.5이다. JSR -6dB 이하의 경우에는 재방송재밍신호가 미약해 C-PRN 신호의 상관 값에 크게 영향을 주지 않기 때문에 제안한 재방송재밍검파기는 재방송재밍여부를 검출하기 어렵다. 그러나 해당 영역은 재방송재밍신호가 최종 측위해에 큰 영향을 미치지 않을 것으로 쉽게 예상할 수 있다. 마찬가지로 JSR +16dB인 경우 검파확률이 약 0.5가 된다. 이는 C-PRN 신호의 상관 값에 신호가 큰 영향을 주지 못하고, 재방송재밍신호에 의한 상관 값이 거의 이상적인 C-PRN 신호의 자기상관개형과 유사하기 때문이다. 그러나 JSR +10dB 이상의 영역은 반송파 신호 전력 대 잡음 전력의 비의 관측만으로도 일반적인 수신 상태가 아님을 판정할 수 있으므로 재방송재밍에 따른 관심영역이 아니다. 그림 8에서 흥미로운 또 한 가지는 가시위성의 수 N 에 따른 검파확률의 개형이다. C-PRN 신호를 생성하기 위한

그림 7. 제안한 기법의 구성도.

Fig. 7. Configuration of the proposed scheme.

그림 8. 가시위성의 수 N 에 따른 JSR 대비 검파확률.

Fig. 8. Jamming-to-signal power ratio versus the detection probability according to the number of visible satellites.

그림 9. 재방송재밍신호의 위상지연에 따른 JSR 대비 검파확률.
Fig. 9. Jamming-to-signal power ratio versus the detection probability according to the code phase of a repeat-back jamming signal.

PRN 신호의 수가 늘어날수록 전반적으로 검파성능이 향상됨을 확인할 수 있으며, 이는 C-PRN 신호의 전력이 향상되어 더욱 뚜렷한 상관 값을 얻을 수 있음을 의미한다.

$N=12$ 일 때, τ_j 에 따른 검파확률은 그림 9와 같다. 그림 9처럼 τ_j 가 클수록, 즉 재방송재밍기와 수신기 사이의 물리적 거리가 멀거나, 재방송재밍기의 재방송처리지연이 큰 경우 제안한 기법의 검파성능이 크게 향상됨을 확인할 수 있다.

V. 결론

본 논문에서는 재방송재밍 환경에서 C-PRN 신호를 활용한 효과적인 재방송재밍신호 검출기법을 제안하였으며, 모의실험을 통해 검파확률을 분석하였다. 제안한 기법은 수신기에 재방송재밍이 가해질 때 수신기 보유 정보를 최대한 활용해 C-PRN 신호를 생성하고, 이를 사용해 재방송재밍신호와 GNSS 신호가 함께 수신되는 경우 단일 다중경로환경에서의 부호동기추적오차 발생 문제와 재방송재밍 문제가 유사해짐을 보였으며, 이때 효과적인 재방송재밍신호 검출을 위해 기존에 다중경로영향 완화 기법 가운데 하나인 이중 이른-늦은 상관전력 차 기반 부호동기위상 판별기를 응용한 새로운 재방송재밍신호 검출기법을 제안하였다. 제안한 기법은 [6]과 더불어 단일 안테나를 사용하는 모바일 항법단말에 효과적인 재방송재밍 검출방법 가운데 하나로 활용될 수 있다. 본 논문에서는 제안한 기법의 개념을 효과적으로 설명하기 위해 많은 오차 성분들과 다양한 다중경로영향 완화 기법 등을 고려하지 않았다. 추후에는 이들을 종합적으로 고려해 효과적인 재방송재밍 검출/식별/완화 기법에 대해 연구할 예정이다.

REFERENCES

- [1] J. Coffed, "The threat of GPS jamming: The risk to an information utility," *Report of EXELIS*, Jan. 2014. Online Available: http://www.exelisinc.com/solutions/signalsentry/Documents/ThreatOfGPSJamming_February2014.pdf
- [2] E. D. Kaplan and C. J. Hegarty, *Understanding GPS Principles and Applications, 2nd Edition*, Artech House,

Norwood, MA, 2006.

- [3] B. W. Parkinson, J. J. Spilker Jr., P. Axelrad, and P. Enge, *Global Positioning System: Theory and Applications*, vol. 1, AIAA, Reston, VA, 1996.
- [4] D. W. Lim, J. M. Kang, and M. B. Heo, "Hybrid TDOA/AOA localization algorithm for GPS jamming," *Journal of Institute of Control, Robotics and Systems (in Korean)*, vol. 20, no. 1, pp. 101-105, Jan. 2014.
- [5] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronics Systems*, vol. 49, no. 2, pp. 1073-1090, Apr. 2013.
- [6] J. Nielsen, A. Broumandan, and G. Lachapelle, "GNSS spoofing detection for single antenna handheld receivers," *Navigation: Journal of The Institute of Navigation*, vol. 58, no. 4, pp. 335-344, Winter 2011.
- [7] A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Spoofing countermeasure for GNSS receivers - A review of current and future research trends," *Proc. on the 4th Intern Colloquim on Scientific and Fundamental Aspects of the Galileo Programme*, pp. 1-8, Praha, Czech Republic, Dec. 2013.
- [8] D. Lu, R. Wu, P. Li, and Z. Su, "GPS smart jammer suppressin algorithm based on spatial apes," *Proc. of 2007 International Symposium on Intelligent Signal Processing and Communication Systems*, pp. 88-91, Xiamen, China, Nov.-Dec. 2007.
- [9] R. B. Langley, "GLONASS loses control again," *GPS World: The Business and Technology of GNSS*, Apr. 2014. Online Available: <http://gpsworld.com/glonass-loses-control-again/>
- [10] China Satellite Navigation Office, Report on the Development of BeiDou (COMPASS) Navigation Satellite System (V2.2), Dec. 2013. Online Available: <http://www.beidou.gov.cn/attach/2013/12/26/20131226fed336adf2184d52843d5bf81832e82c.pdf>
- [11] G. McGraw and M. Braasch, "GNSS multipath mitigation using gated and high resolution correlator concept," *Proc. of the 1999 National Technical Meeting of The Institute of Navigation*, pp. 333-342, San Diego, CA, Jan. 1999.

유 승 수

2003년 건국대학교 전자정보통신공학부 졸업. 2005년 동 대학원 공학석사. 2010년 동 대학원 공학박사. 2010년~2011년 건국대 2단계 BK21 위성항법시스템 수신기 기술 연구팀 박사후 연구원. 2011년~현재 건국대학교 전자정보통신공학부 조교수. 관심분야는 통계학적 신호처리, GNSS 수신기 신호처리, GNSS 항재밍 신호처리 등.

염 동 진

1991년 충남대학교 전자공학과 졸업.
1993년 동 대학원 공학석사. 1993년~
현재 국방과학연구소 책임연구원. 관
심분야는 능동 위상배열 레이더 시스
템, 신호처리 등.

지 규 인

1982년 서울대 제어계측공학과 졸업.
1984년 동 대학원 제어계측공학과 공
학석사. 1989년 Case Western Reserve
University 공학박사. 1992년~현재 건국
대학교 전자정보통신공학부 교수. 관
심분야는 GPS/INS 결합방법, GPS 수

신기 신호처리, 무선측위, Software GPS, GPS 항재밍 신호
처리 등.

김 선 용

1990년 한국과학기술원 전기 및 전자
공학과 졸업(최우등). 1993년 동 대학
원 공학석사. 1995년 동 대학원 공학
박사. 1996년~2001년 한림대학교 정보
통신공학부 조교수. 2001년~현재 건국
대학교 전자정보통신공학부 교수. 관

심분야는 통계학적 신호처리, 이동통신시스템, 통신이론,
GPS 항재밍 신호처리 등.