http://dx.doi.org/10.7840/kics.2015.40.2.264

# 저피탐 위성항법 신호 설계를 위한 암호화된 확산부호의 상관 특성에 관한 연구

박 기 현•, 송 민 규*, 송 홍 엽°, 이 장 용**

# Correlation Property of Encrypted Spreading Code for Design of LPI Applied GNSS Signal

Ki-Hyeon Park•, Min Kyu Song*, Hong-Yeop Song°, Jang-Yong Lee**

요 약

본 논문에서는 저피탐 특성을 강화하기 위해 암호화된 수열을 확산부호로 사용하는 위성항법신호의 통계적 특성을 이론적으로 분석하고 간섭 저항 성능을 예측한다. 이를 위해 다양한 복소 단위원 심볼셋으로 암호화된 수열의 상관특성을 이론적으로 분석하고, 이를 토대로 기존의 Gold 코드나 Zadoff-Chu 코드와 암호화된 확산부호와의 간섭 저항 성능 차이를 이론적/실험적으로 분석하여 암호화된 확산부호의 적용으로 인한 신호 품질 열화 정도를 규명한다.

**Key Words :** spreading code, LPI, GNSS, GPS, galileo

ABSTRACT

In this paper, we analyze the statistical characteristic and describe the anti-interference performance of the signal for the LPI-applied GNSS using encrypted spreading code. To do this, we analyze the correlation property of encrypted sequences theoretically having various symbol sets over complex root of unity. We derive the degradation of anti-interference performance of encrypted sequences comparing with Gold and Zadoff-Chu sequences using theoretical and experimental methods.

## Ⅰ. 서 론

통신 사용자의 위치정보 제공을 위해 설계된 항법 신호는 실생활의 많은 곳에서 응용되고 있다. 특히 위치정보가 명확하고 측위반경이 넓은 위성을 이용한 전지구 위성항법시스템(Global Navigation Satellite System, GNSS)는 우리나라에서도 널리 쓰이는 미국의 GPS[1]를 비롯하여 유럽의 Galileo[2], 러시아의 GLONASS, 중국의 Beidou 등의 명칭으로 각국에서 활발하게 연구되는 분야이다. 최근 우리나라에서도 독자적 항법기술을  확보하기 위한 연구가 활발히 진행되고 있다.

가장 먼저 상용화된 미국의 GPS의 경우 신호탈취 및 변조에 의한 피해가 다수 보고되고 있으며[3], 재밍 신호를 통한 신호방해 공격은 우리나라에서도 수차례 보고되었을 만큼[3] 공격에 취약한 실정이다. 따라서

※ 본 연구는 방위사업청과 국방과학연구소가 지원하는 국방위성항법특화연구센터 사업의 일환으로 수행되었습니다.
• First Author : Yonsei University Department of Electrical and Electronic Engineering, kh.park@yonsei.ac.kr, 학생회원
° Corresponding Author : Yonsei University Department of Electrical and Electronic Engineering, hysong@yonsei.ac.kr, 종신회원
* Yonsei University Department of Electrical and Electronic Engineering, mk.song@yonsei.ac.kr
** Agency for Defence Development, flukelee@add.re.kr, 정회원
논문번호 : KICS2014-12-497, Received December 22, 2014; Revised February 11, 2015; Accepted February 11, 2015

상용화된 위성항법신호를 군용 항법시스템으로 도입하기 위해 항법신호를 보호하는 방법이 연구되기 시작하였고, 국내에서도 위성항법신호의 항재밍 성능 향상을 위한 다양한 시도가 이루어졌다[4]. 특히 기존에 레이더 신호 등에서 사용되던 저피탐 기법[5]에 대한 연구가 진행되었는데, 이는 신호의 탐지를 어렵게 하여 신호 생성 레벨에서 신호공격으로부터 신호를 보호하는 기술이다.

군사 목적으로 항법신호의 보호가 고려되어 설계된 GPS P(Y) 부호[1] 및 전문화된 군용 항법신호로 설계된 GPS M 부호[6]와 Galileo의 정부 서비스 신호인 Galileo E6[2]의 경우 항법신호의 확산부호에 암호화를 도입함으로써 공격자가 신호를 획득하기 어렵게 하고 있다. 하지만 실제 이렇게 암호화된 확산부호를 사용하는 경우 항법신호의 측위성능을 결정하는 확산부호의 자기/상호상관 특성은 상관특성을 극대화하여 설계된 Gold 부호 등을 사용하는 것에 비하여 상당히 감소하는 것으로 추측할 수 있다. 그러나 암호화에 따른 측위성능의 변화나 공격에 대한 내성 정도의 분석에 대한 국내 연구는 미비한 실정이다.

또한 항법신호를 위한 확산부호로 기존의 2진 수열이 신호가 아닌 복소수 값을 가지는 Zadoff-Chu 수열을 사용하는 시스템이 제시[7]되었고 다양한 후보코드간 간섭성능 분석에 대한 연구가 이루어졌다[7,8]. 하지만 복소수 수열을 기반으로 한 암호화된 확산부호의 성능에 대한 분석은 거의 이루어지지 않고 있다.

본 논문에서는 다양한 복소 단위원 심볼 환경에서 암호화된 확산부호가 적용된 항법신호의 상관특성을 기존 확산부호가 적용된 항법신호의 상관특성과 비교/분석하고 실제 암호화로 인한 측위성능 저하 정도를 이론적/실험적으로 규명한다.

## Ⅱ. 항법신호의 확산부호와 저피탐

위성항법신호는 그림 1에서 볼 수 있듯 낮은 비트레이트의 항법메시지에 높은 비트레이트의 미리 정의된 확산부호를 더한 신호를 반송파에 실어 송출하는 구조로 되어 있다. 위성항법신호 중 가장 널리 쓰이는 GPS의 상용부호인 C/A부호[1]의 경우 약 50bps의 항법메시지를 사용하고, 항법메시지 1비트 당 20,460비트의 확산부호를 적용하여 송출한다. 이 20,460비트는 위성마다 서로 다르게 정의된 주기 1,023의 Gold 부호를 20주기만큼 반복하여 적용한다. 그리고 수신단에서는 각각의 위성들의 Gold 부호와 수신신호와의 상관값을 계측하여 항법신호의 송신원을 판별하고 송

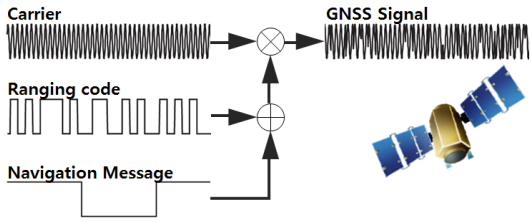


그림 1. 위성항법신호의 구조
Fig. 1. Structure of Navigation Satellite System Signal

수신 시간차를 계산하게 된다.

이 때, 송신원을 판별하는 데에 중요한 확산부호의 성질이 상호상관특성이며, 정확한 수신시간을 계측하여 측위를 수행하는 데에 중요한 성질이 자기상관특성이 된다. 신호 $a(t)$의 자기상관값 $R_a(\tau)$와 $b(t)$와의 상호상관값 $R_{a,b}(\tau)$는 각각 다음과 같이 계산된다[9].

$$R_a(\tau) = \int_{-\infty}^{\infty} a(t)a^*(t+\tau)dt \tag{1}$$

$$R_{a,b}(\tau) = \int_{-\infty}^{\infty} a(t)b^*(t+\tau)dt \tag{2}$$

GPS C/A 부호의 확산부호처럼 $a(t)$, $b(t)$가 각각 $N$을 주기로 갖는 주기수열 $a[n]$,$b[n]$으로 결정될 경우, (1)과 (2)는 다음과 같이 표현될 수 있다.

$$R_a(\tau) = \sum_{n=0}^{N-1} a[n]a^*[n+\tau] \tag{3}$$

$$R_{a,b}(\tau) = \sum_{n=0}^{N-1} a[n]b^*[n+\tau] \tag{4}$$

이 경우, 주어진 수열 $a[n]$, $b[n]$의 주기내 최대 자기 및 상호상관값 $|R_a|$ , $|R_{a,b}|$ 를 다음과 같이 정의할 수 있다.

$$|R_a| = \max_{\forall \tau \neq 0}(|R_a(\tau)|) \tag{5}$$

$$|R_{a,b}| = \max_{\tau}(|R_{a,b}(\tau)|) \tag{6}$$

이 때 $\tau=0$일 때의 $R_a(\tau)$값이 최대이므로, 특성으로서의 $|R_a|$ 는 $\tau=0$일 때를 제외하고 계산한다. $|R_a|$ 는 부정확한 시간의 신호에 의해 발생하는 간섭잡음의 세기를 결정하며, $|R_{a,b}|$ 는 의도하지 않은 위

성신호에 의해 발생하는 간섭 잡음의 세기를 결정한다. 따라서 $|R_a|$ , $|R_{a,b}|$ 값은 신호의 간섭저항 성능의 지표인 신호대 간섭비 (SIR, $E[SIR] = \frac{N^2}{E[|R_{a,b}|^2]}$ )를 결정하며 이 값이 낮은 수열들을 사용하는 것이 측위 성능에 유리하다고 할 수 있다.

저피탐 성능은 공격자의 신호 탐지 및 손상 공격에 대한 신호의 내성에 대한 지표로서, 본 논문에서는 동일 수준의 공격을 수행하기 위한 공격자의 비용으로 표현하기로 한다. 특히 확산부호 $a[n]$을 사용하는 신호를 공격자가 공격하기 위하여 $b[n]$이라는 확산부호를 사용할 때, 공격자가 수신하는 신호 파워 혹은 수신자가 느끼는 재밍 파워는 $|R_{a,b}|$ 값에 비례하게 된다. 즉 공격자는 $|R_{a,b}|$ 값을 크게 할 수 있는 $b[n]$을 찾음으로써 공격 비용을 낮출 수 있게 된다. 즉 공격자가 $a[n]$, 혹은 유사한 신호를 쉽게 추정하지 못하도록 신호를 설계하는 것이 저피탐 성능을 결정한다고 말할 수 있다.

공격자가 자신이 추정한 $b[n]$이 $a[n]$에 근접한지를 판별하기 위해서는 수신 신호와 자신이 추정한 수열의 상관값을 계산하여 기준치 근처의 첨점(peak)이 발생하는지를 조사함으로써 알 수 있다. 공격자는 다양한 $b[n]$을 선택하여 이러한 작업을 반복 수행함으로써 $a[n]$에 근접한 수열을 탐색하게 된다. 따라서 공격자가 선택하는 $b[n]$의 후보군의 개수가 저피탐 성능을 결정하는 중요한 요소로 작용하게 되는데 C/A의 부호의 경우 선택 가능한 확산부호의 가짓수가 1,025가지에 불과하기 때문에 공격자에 의해 쉽게 사용된 확산부호의 추정이 가능해진다. 따라서 공격자가 확산부호 후보군을 좁히지 못하게 하기 위해서는 가능한 많은 후보군을 가지는 확산부호를 사용하여야 한다.

## Ⅲ. 암호화된 수열의 상관값 확률모델링

암호화된 수열을 확산부호를 사용하면 공격자가 탐색해야 할 확산부호 후보군이 $2^N$가지로 늘어나 사실상 전수 조사가 불가능하게 되기 때문에 저피탐 특성이 좋아진다. 암호화된 수열은 사용된 암호시스템이 이상적인 시스템에 가까울수록 출력수열이 이상적인 랜덤모델에 가까워지며, 수열의 특성에 대한 예측이 어려워진다. 안전한 키 관리 하에 이루어지는 암호시스템을 통하여 암호화된 수열을 확산부호 $a[n]$, $b[n]$으로 사용할 경우 $a[n]b^*[n+\tau]$의 확률분포함수 $p(a[n]b^*[n+\tau])$는 $n$과 $\tau$에 의존하지 않는 수식이 됨을 추측할 수 있다. 하지만, 이 확률분포함수는 수열 $a[n]$과 $b[n]$이 어떤 심볼셋을 사용하느냐에 따라서 달라지는데, 본 논문에서는 세 가지 경우를 고려하기로 한다.

첫 번째로, 두 수열 $a[n]$과 $b[n]$이 심볼 집합 $\{+1,-1\}$에서만 값을 가지는 수열인 경우이다. 이 경우 $a[n]b^*[n+\tau]$도 동일한 심볼 집합의 값을 가지는데, 본 논문에서는 이러한 심볼 집합에서 정의된 수열을 복소 2진, 혹은 2진 수열로 정의한다.

두 번째로, 두 수열 $a[n]$과 $b[n]$이 심볼 집합 $\{+1,-1,+j,-j\}$에서 값을 가지는 수열을 생각할 수 있다. 이 경우에도 $a[n]b^*[n+\tau]$이 동일한 심볼 집합의 값을 가지는데, 본 논문에서는 이러한 심볼 집합에서 정의된 수열을 (복소) 4진 수열로 정의한다.

일반적으로 보면 두 수열 $a[n]$과 $b[n]$이 실수 $\theta$에 대해 심볼 집합 $\left\{e^{j\frac{2m\pi}{M}} \mid 0 \le m < M\right\}$에서 값을 가지는 수열을 생각할 수 있는데, 우리는 이러한 심볼 집합에서 정의된 수열을 (복소) $M$진 수열로 정의한다.

그림 2는 세 가지 경우의 심볼셋의 분포를 복소 평면에서 나타낸 것이다. 2진 수열은 4진 수열에, 4진 수열은 $M$진 수열에 포함되는 관계이지만 각각의 심볼셋 환경에서 암호화가 이상적으로 적용되었다고 가정하면, 각 수열 $a[n]$과 $b[n]$은 심볼셋 내의 모든 심볼을 동일한 확률로 가지게 되므로 암호화된 수열은 세 경우의 특성이 각각 달라지게 된다.

### 3.1 2진 수열의 경우

암호화된 2진 수열의 경우 $a[n]$과 $b[n]$은 각각 1/2의 확률로 +1, -1을 가지게 되며, 따라서 $a[n]b^*[n+\tau]$도 마찬가지로 1/2의 확률로 +1, -1을 가지게 된다.

**정의 1**: $p_B(N,h)$는 $N$을 주기로 가지며 동일한 확률로 $\{+1,-1\}$ 값을 갖는 주기수열 $a[n]$, $b[n]$의 특정 위치에서의 상호상관값 $R_{a,b}(\tau)$의 절대값이 $h$일 확률의 확률분포함수로 정의한다.

정의 1에서 $p_B(N,h)$는 $N$개의 슬롯에서 +1이 나오는 위치의 개수가 $\frac{N-h}{2}$이거나 $\frac{N+h}{2}$일 확률이

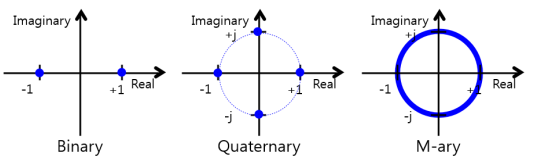


그림 2. 수열에 따른 심볼셋의 분포
Fig. 2. Symbol Set Distribution of each Sequences

되며, 이 둘의 확률은 같으므로 식 (8)과 같이 구할 수 있다.

$$p_B(N,h)=\begin{cases}\binom{N}{\frac{N-h}{2}}0.5^{N-1} & \text{if } N\geq h>0 \text{ and } N-h \text{ is even}\\ \binom{N}{\frac{N}{2}}0.5^{N} & \text{if } N\geq 0 \text{ is even and } h=0\\ 0 & \text{otherwise}\end{cases} \quad (8)$$

식 (8)의 모양은 상당히 복잡한 편인데, 수열의 주기 $N$이 충분히 크다고 가정할 경우 중심극한정리를 이용하여 확률분포함수를 가우시안 함수의 변형으로 표현할 수 있다. 여기서 $a[n]b^*[n+\tau]$의 평균이 0, 분산이 1이라는 것은 쉽게 알 수 있으므로, 이러한 통계적 특성을 가지는 랜덤변수의 $N$개 합으로 표현되는 상호상관값의 절대값의 확률분포는 확률밀도함수인 식 (9)처럼 표현할 수 있게 된다.

$$p_B(N,h)\cong\frac{2}{\sqrt{2\pi N}}exp\left(-\frac{h^2}{2N}\right)\ (h\geq 0) \quad (9)$$

### 3.2 4진 수열의 경우

4진 수열 $a[n]$과 $b[n]$은 각각 1/4의 확률로 $\pm 1$이나 $\pm j$값을 가지게 되며, 따라서 $a[n]b^*[n+\tau]$도 마찬가지로 1/4의 확률로 $\pm 1$ 혹은 $\pm j$값을 가지게 된다. 이 경우 상호상관값 $R_{a,b}(\tau)$는 복소수 형태로 나타나게 되며, 이는 복소수가 나타내는 신호위상에서 상관값의 크기가 $|R_{a,b}(\tau)|$ 가 나타남을 의미한다. 따라서 $|R_{a,b}(\tau)|$ 가 $h$일 확률은 $R_{a,b}(\tau)$의 실수부의 절대값이 $i$일 확률과 허수부의 값이 $\sqrt{h^2-i^2}$일 확률을 구하고 이를 가능한 모든 $i$에서 구하여서 각각의 확률을 더한 값, 즉 식 (10)과 같이 표현할 수 있게 된다.

$$\sum_{i=0}^{Z}p_B(Z,i)p_B(N-Z,\sqrt{h^2-i^2}) \quad (10)$$

식 (10)에서 $Z$ ($Z\leq N$)는 실수값이 나오는 위치의 개수이다. $a[n]b^*[n+\tau]$가 실수값이 나오는 경우는 두 신호 $a[n]$, $b^*[n+\tau]$가 모두 $\pm 1$이거나 $\pm j$일 경우이며, 그렇지 않은 경우는 허수값이 나오게 된다.

**정의 2**: $p_Q(N,h)$는 $N$을 주기로 가지며 동일한 확률로 $\{+1,-1,+j,-j\}$ 값을 갖는 주기수열 $a[n]$, $b[n]$의 특정 위치에서의 상호상관값 $R_{a,b}(\tau)$의 절대값이 $h$일 확률의 확률분포함수로 정의한다.

따라서 $p_Q(N,h)$는 실수값이 $Z$만큼 나올 확률과 식 (10)의 곱을 가능한 모든 $Z$에서 더한 형태로 표현되며, 따라서 식 (11)과 같이 구할 수 있다.

$$p_Q(N,h)=\sum_{Z=0}^{N}\binom{N}{Z}0.5^N\sum_{i=0}^{Z}p_B(Z,i)p_B(N-Z,\sqrt{h^2-i^2}) \quad (11)$$

여기서 $p_Q(N,h)$는 정수의 제곱근에서 값을 가질 수 있는 확률분포함수이다.

### 3.3 복소 $M$진 수열의 경우 ($M\gg 4$)

Zadoff-Chu 수열과 같은 다중위상부호는 단위원상에서 $M$등분된 집합을 심볼로 사용한다. 이 때, 일반적으로 매우 큰 $M$일 때는 균등하게 분포된 단위원상에서의 한 점을 심볼값으로 가진다고 가정할 수 있다. 이러한 수열을 사용하는 경우 $a[n]$과 $b[n]$은 $\sqrt{x^2+y^2}=1$을 만족하는 $x+yi$라는 복소수 형태로 표현된다. 이를 다시 표현하면 어떤 위상 $\theta$에 대해 $\cos\theta+i\sin\theta$형태로 표현할 수 있다.

**정의 3**: $p_M(N,h)$는 $N$을 주기로 가지며 위상 $\theta$가 $0\leq\theta<2\pi$의 범위에서 동일한 확률을 가지면서 $\{\cos\theta+j\sin\theta\}$ 값을 갖는 주기수열 $a[n]$, $b[n]$의 특정 위치에서의 상호상관값 $R_{a,b}(\tau)$의 절대값이 $h$일 확률의 확률밀도함수로 정의한다.

$a[n]$의 위상을 $\theta$로, $b^*[n+\tau]$의 위상을 $\psi$로 표현하면 $a[n]b^*[n+\tau]$의 위상은 $\theta+\psi$가 되고, $\theta$와 $\psi$가 0과 $2\pi$ 사이에서 균등한 분포를 가지므로 $\theta+\psi$ 또한 0과 $2\pi$ 사이에서 균등한 분포를 가지게 된다. 또한 균등 확률분포를 가지는 랜덤변수 $\theta$에 대해 $\cos\theta$와 $\sin\theta$는 평균 0, 분산 0.5의 값을 가지는 랜덤변수가 된다. 이를 토대로 $p_M(N,h)$를 구하기 위해서는 삼각함수로 표현되는 랜덤변수를 합산해야 하며, 매우 복잡한 형태로 표현되게 된다. 따라서 랜덤변수의 통계적 특성을 이용하여 각각의 수열의 주기 $N$이 충분히 길다고 가정하고, 2진 수열 모델을 간략화한 것과 같이 중심극한정리를 적용한다. 이 경우 두 수열의 상관값은 평균 0, 분산 $0.5N$의 정규분포를 따르는 랜덤변수 $s$, $t$에 대해 $R_{a,b}(\tau)=s+ti$의 형태로 표현될 수 있다. 이 두 변수의 결합 확률밀도함수는 2차원 정규분포형태의 식 (12)와 같다.

$$p_N(s,t) = \frac{1}{\sqrt{\pi N}} exp\left(-\frac{s^2}{N}\right) \frac{1}{\sqrt{\pi N}} exp\left(-\frac{t^2}{N}\right) = \frac{1}{\pi N} exp\left(-\frac{s^2+t^2}{N}\right) \quad (12)$$

직교좌표계 $(s,t)$를 원좌표계 $(r,\theta)$로 바꾸게 되면, 식 (12)는 식 (13)과 같이 바꿀 수 있다.

$$p_N(r,\theta) = \frac{1}{\pi N} exp\left(-\frac{r^2}{N}\right) \quad (13)$$

식 (13)은 $r$에 관한 함수인데 $h = r$이라는 사실에서 확률밀도함수 $p_M(N,h)$는 모든 $\theta$에 대한 $p_N(h,\theta)$의 적분합이라는 것을 알 수 있으며, 따라서 식 (14)와 같이 구할 수 있다.

$$p_M(N,h) \cong \int_{-\pi}^{\pi} p_N(h,\theta) d\theta = \frac{2h}{N} exp(-h^2/N) \quad (h \geq 0) \quad (14)$$

한편, 4진 수열 또한 실수부와 허수부의 랜덤변수가 각각 평균 0, 분산 0.5의 분포를 가지므로 통계적 특성이 (14)와 유사할 것으로 예측할 수 있다.

그림 3은 이 세 확률분포함수 $p_B(N,h)$, $p_Q(N,h)$, $p_M(N,h)$를 도식한 것이다. 4진 수열을 비롯한 $M$진 수열의 경우 $a[n]b^*[n+\tau]$의 분산이 2진 수열에 비해 낮기 때문에 일반적으로 상관특성이 2진 수열보다 낮을 것으로 예측할 수 있는데, 그림을 보면 실제로도 $M$진 수열이 2진 수열보다 상관값이 낮게 분포함을 알 수 있다.

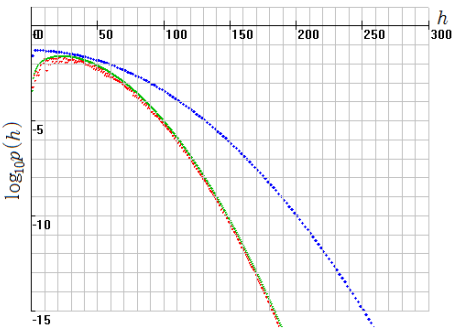


그림 3. $p_B(1000,h)$, $p_M(1000,h)$, $p_Q(1000,h)$ 그래프 (위쪽부터)
Fig. 3. Graph of $p_B(1000,h)$, $p_M(1000,h)$, and $p_Q(1000,h)$ (From up to down)

### 3.4 상관값의 평균 및 파워

식 (9)와 (14)를 사용하여 상호상관값의 평균과 파워를 정리 1과 같이 구할 수 있다.

**정리 1**: 주기가 $N$이고 심볼값의 평균이 0, 분산이 1인 실수 심볼로 표현된 두 암호화된 수열의 상호상관값의 절대값을 $h_N$이라 하면 확률밀도함수 $p_B(N,h_N)$는 식 (9)와 같다. 또한 상호상관값 평균 $E[h_N]$과 파워 $E[h_N^2]$는 각 식 (15), (16)과 같다.

$$E[h_N] = \sqrt{2N/\pi} \quad (15)$$

$$E[h_N^2] = N \quad (16)$$

또한 주기가 $N$이고 심볼값의 실수부와 허수부의 평균이 0, 분산이 0.5인 복소수 값으로 표현된 두 암호화된 수열의 상호상관값의 절대값을 $h_N$이라 하면 확률밀도함수 $p_{MPSK}(N,h_N)$는 식 (14)와 같다. 상호상관값 평균 $E[h_N]$과 파워 $E[h_N^2]$는 각 식 (17), (18)과 같다.

$$E[h_N] = \sqrt{\pi N}/2 \quad (17)$$

$$E[h_N^2] = N \quad (18)$$

증명: $a[n]$과 $b[n]$이 실수이고 값의 평균이 0, 분산이 1인 인 경우 $a[n]b^*[n+\tau]$도 마찬가지로 실수이며, 두 랜덤변수가 독립적일 경우 평균은 0, 분산값은 1이 된다. 따라서, 식 (9)와 동일한 형태로 중심극한정리를 이용하여 확률밀도함수를 구할 수 있다. 식 (15)의 증명은 가우시안 함수의 1차 절대값 모멘트의 식을 이용하며 다음과 같다.

$$E[h_N] = \int_0^{\infty} h\, p_B(N,h) dh = \int_{-\infty}^{\infty} \frac{|h|}{\sqrt{2\pi N}} exp\left(-\frac{h^2}{2N}\right) dh = \sqrt{\frac{2N}{\pi}}$$

식 (16)의 증명은 가우시안 함수의 2차 모멘트의 식을 이용하며 다음과 같다.

$$E[h_N^2] = \int_0^{\infty} h^2 p_B(N,h) dh = \int_{-\infty}^{\infty} \frac{h^2}{\sqrt{2\pi N}} exp\left(-\frac{h^2}{2N}\right) dh = N$$

$a[n]$과 $b[n]$이 복소수이고 심볼값의 평균이 0, 실수부와 허수부의 분산이 0.5인 인 경우 $a[n]b^*[n+\tau]$도 마찬가지로 복소수이며, 두 랜덤변수가 독립적일 경우 평균은 0, 실수부와 허수부 각각의 분산값은 0.5가 된다. 따라서, 식 (14)와 동일한 형태로 중심극한정리를 이용하여 확률밀도함수를 구할 수 있다. 식 (17)과 (18)도 마찬가지로 가우시안 함수의 2차 및 3차 절대값 모멘트의 식을 이용하여 구할 수 있다.

$$E[h_N]=\int_0^\infty h\,p_M(N,h)\,dh$$
$$=\sqrt{\frac{\pi}{N}}\int_{-\infty}^{\infty}\frac{h^2}{\sqrt{\pi N}}exp\left(-\frac{h^2}{N}\right)dh=\frac{\sqrt{\pi N}}{2}$$
$$E[h_N^2]=\int_0^\infty h^2 p_M(N,h)\,dh$$
$$=\sqrt{\frac{\pi}{N}}\int_{-\infty}^{\infty}\frac{|h|^3}{\sqrt{\pi N}}exp\left(-\frac{h^2}{N}\right)dh=N$$

■

암호화된 수열 $a[n]$의 자기상관값 $a[n]a^*[n+\tau]$또한 $\tau=0$일 때를 제외하면 정리 1과 같은 확률분포, 평균 및 파워를 가짐을 쉽게 알 수 있다.

한편, 각 확률밀도함수의 누적확률밀도함수를 $N$제곱한 것이 최대 상호상관값 $|R_{a,b}|$ 의 누적확률밀도함수가 된다는 점으로부터 식 (9), (14)를 사용하여 수열의 주기 $N$에 대해 $|R_{a,b}|=H$가 될 확률의 확률밀도함수 $P_B(N,H)$ 및 $P_M(N,H)$를 식 (19), (20)과 같이 유도할 수 있다.

$$P_B(N,H)=\frac{d}{dH}\left[\int_0^H p_B(N,h)\,dh\right]^N$$
$$=Np_B(N,H)\left[\int_0^H p_B(N,h)\,dh\right]^{N-1} \quad (19)$$
$$=\frac{1}{(2N)^{N/2}\sqrt{\pi}}exp\left(-\frac{H^2}{2N}\right)\left[erf\left(\frac{H}{2\sqrt{N}}\right)\right]^{N-1}$$

$$P_M(N,H)=Np_M(N,h)\left[\int_0^H p_M(N,h)\,dh\right]^{N-1}$$
$$=\frac{2^N H}{N^{N-1}}exp\left(-\frac{H^2}{N}\right)\left[\int_0^H h exp\left(-\frac{h^2}{N}\right)dh\right]^{N-1} \quad (20)$$

식 (19)나 (20)을 사용하여 각 경우에서의 최대 상호상관값 평균인 $E[H_N]=\int_0^\infty HP(N,H)\,dH$ 와 파워 $E[H_N^2]=\int_0^\infty H^2P(N,H)\,dH$ 를 구할 수 있다. 이를 간단한 수식으로 표현하는 것은 어려우나, 평균 상관값의 통계적 특성과의 연관성을 고려한다면, $E[H_N]$는 $N$이 커질수록 $E[h_N]\sim\sqrt{N}$에서 멀어질 거라는 추측에서 대략 $E[H_N]\approx cN^{0.5+\epsilon}$의 형태로, $E[H_N^2]$는 마찬가지로 $N$이 커질수록 $E[h_N^2]\sim N$에서 멀어질 거라는 추측에서 대략 $E[H_N^2]\approx cN^{1+\epsilon}$의 형태로 근사시킬 수 있을 것이라고 추측할 수 있다.

## Ⅳ. 상관값 시뮬레이션을 통한 간섭성능 계산

그림 4는 주기 1000의 다양한 심볼셋을 가진 수열들을 1억회 씩 반복 시뮬레이션을 수행하여 각각의 확률분포를 통계적으로 도식한 것이다. 그림 3에서 16QAM은 크기가 고정되지 않는 크기 16인 심볼셋 $\{a+jb\}$ (여기서 $a,b\in\{k,-k,3k,-3k\}$이고 $k=10^{-0.5}$) 중 하나의 값을 갖는 수열을 사용한 시뮬레이션이며, 64QAM은 크기가 고정되지 않는 크기 64인 심볼셋 $\{a+jb\}$ (여기서 $a,b\in\{l,-l,3l,-3l,5l,-5l,7l,-7l\}$이고 $l=42^{-0.5}$) 중 하나의 값을 갖는 수열을 사용한 시뮬레이션이다. 두 경우 모두 실수부와 허수부의 평균이 0이고 분산은 0.5가 된다. 상관값이 소수로 나오는 경우 내림을 하여 정수 상관값의 확률에 포함시킴으로써 확률밀도함수와 스케일을 일치시켰다.

그림 4를 보면 2진, 4진, $M$진 수열의 경우 3장에

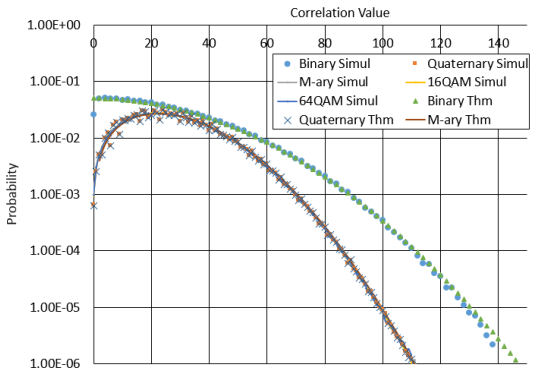


그림 4. $N=1000$일 때 각 수열의 상관값 확률 시뮬레이션
Fig. 4. Simulation result about absolute correlation value of each sequences at $N=1000$

서 구한 이론치와 시뮬레이션으로 구한 확률분포가 거의 일치함을 볼 수 있으며, 2진 수열의 결과를 제외한 복소평면상의 신호셋을 사용하는 나머지 수열의 상관값은 모두 정리 1에서 예측한 것과 같이 동일한 확률분포를 가짐을 확인할 수 있다.

또한 주기 $N$에 따른 $E[|R_{a,b}|]$ 및 $E[|R_{a,b}|^2]$ 값을 구하기 위해 다양한 $N$에서 시뮬레이션을 수행하였고, $E[|R_{a,b}|] \approx cN^{0.5+\epsilon}$ 가 시뮬레이션 결과값과 일치하도록 하는 $c$, $\epsilon$값을 반복 대입을 통하여 추적하였다. 그 결과 최대값 평균은 2진 수열에서는 $c=2.25$, $\epsilon=0.0625$에서, $M$진 수열에서는 $c=1.75$, $\epsilon=0.0625$에서 가장 시뮬레이션 결과와 비슷한 값을 도출하는 것을 확인하였고, $E[|R_{a,b}|^2] \approx cN^{1+\epsilon}$ 는 2진 수열에서는 $c=5.1$, $\epsilon=0.125$에서, $M$진 수열에서는 $c=3.1$, $\epsilon=0.125$에서 가장 시뮬레이션 결과와 비슷한 값을 도출하는 것을 확인하였다. 각 길이에서 1천 회 반복 수행을 통하여 평균을 구한 시뮬레이션 결과와 도출된 상수를 사용하여 추정한 결과의 비교 그래프가 그림 5에 나타나 있다.

표 1은 두 가지 서로 다른 심볼셋 집합을 사용하는 네 가지 서로 다른 확산부호 모델에서 $E[h_N]$과 파워 $E[h_N^2]$, $E[|R_{a,b}|]$ , 그리고 신호대 간섭비를 정리한 것이다. Gold는 여러 통신시스템에서 널리 쓰이는 상관특성이 뛰어난 2진 수열 확산부호이며, Zadoff-Chu는 상관특성이 뛰어난 $M$진 수열 확산부호이고 각각의 상관특성은 이론적으로 잘 알려져 있다 표 1의 Gold 부호 관련 수식의 경우 비교를 용이하게 하기 위해 정확한 값이 아닌 대략적인 값을 사용하였는데, 주기 $N=2^n-1$에서 $n$이 홀수일 때와 짝수일 때의 서로

표 1. Gold 부호 및 암호화된 2진 수열과 Zadoff-Chu 부호 및 암호화된 $M$진 수열의 특성 비교
Table 1. Comparison of Gold code, encrypted binary sequence, Zadoff-Chu sequence and encrypted complex sequence

| Symbol | Binary Sequence | | $M$-ary Sequence | |
|---|---|---|---|---|
| Sequence | Gold | Encrypted | Zadoff-Chu | Encrypted |
| $E[h_N]$ | $\sqrt{\frac{N}{2}}, \frac{\sqrt{N}}{2}$ | $\sqrt{\frac{2N}{\pi}}$ | $\sqrt{N}$ | $\frac{\sqrt{\pi N}}{2}$ |
| $E[h_N^2]$ | $N$ | $N$ | $N$ | $N$ |
| $E[\|R_{a,b}\|]$ | $\sqrt{2N}, 2\sqrt{N}$ | $2.25N^{9/16}$ | $\sqrt{N}$ | $1.75N^{9/16}$ |
| $E[SIR]$ | $\frac{N}{2}, \frac{N}{4}$ | $\frac{N^{7/8}}{5.1}$ | $N$ | $\frac{N^{7/8}}{3.1}$ |

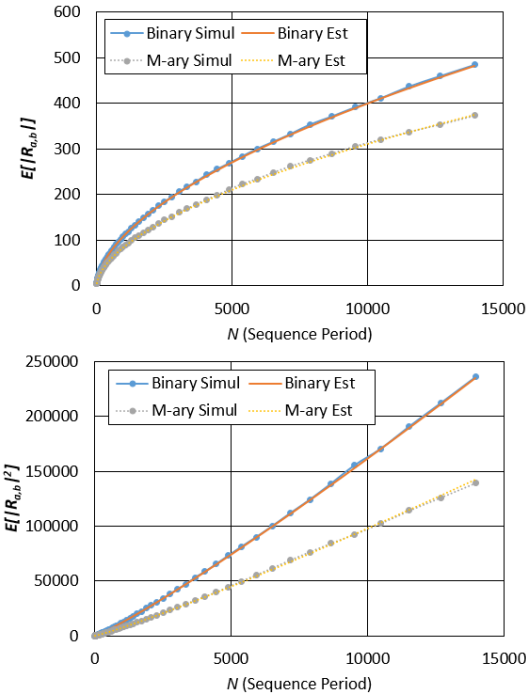


그림 5. 2진/$M$진 수열에서 주기 $N$에 따른 암호화된 수열의 $E[|R_{a,b}|]$ 및 $E[|R_{a,b}|^2]$ 시뮬레이션 및 추정치(Est) 그래프
Fig. 5. Graph of simulation result and estimated value of $E[|R_{a,b}|]$ and $E[|R_{a,b}|^2]$ of encrypted sequence of length $N$ at the binary/quaternary symbol

다른 상관특성으로 인한 서로 다른 값을 각각 홀수일 때, 짝수일 때로 표시하였다.

표 1에서 보듯, 정상수신 환경에서의 간섭세기인 $E[h_N^2]$는 모든 수열에서 동일한 값이 나옴을 알 수 있다. 하지만 $E[SIR]$을 비교해 보면 먼저 2진 수열을 사용하는 Gold 부호에 비해 암호화된 2진 수열은 대략 $3+0.125\log N$ dB 가량의 SIR 손실이 발생하는 것을 알 수 있으며, $M$진 수열을 사용하는 Zadoff-Chu Code에 비해 암호화된 $M$진 수열은 대략 $4.8+0.125\log N$ dB 가량의 SIR 손실이 발생하는 것을 알 수 있다. 하지만 암호화된 $M$진 수열은 암호화된 2진 수열에 비해서는 대략 2.23dB 정도의 SIR 이득을 얻을 수 있음을 알 수 있다.

## V. 결 론

GPS M부호 및 Galileo E6 등에서 사용되는 암호화된 확산부호는 공격자의 확산부호 추정이 어렵기 때문에 신호에 대한 탐지 및 재밍 공격이 어려워진다

는 장점이 있지만 상관특성이 최적화된 확산부호를 사용하는 기존 시스템에 비해 다소 열화된 측위성능을 보일 수 있다는 단점이 있다.

본 논문은 실제 측위성능 열화 정도를 이론적/실험적으로 확인하였고 구체적인 SIR 손실량을 계산하였다. 특히 서로 다른 심볼셋의 수열이라도 동일하게 실수 집합의 심볼셋인 경우나 복소 집합의 심볼셋인 경우에 상관특성은 거의 일치함을 확인하였다. 이는 필요에 따라 심볼셋을 바꾸어도 암호화된 확산부호를 거의 측위성능의 차이 없이 사용할 수 있음을 의미한다.

또한 기존의 2진 수열이 아닌 복소 $M$진 수열을 사용한 경우의 상관 특성을 계산함으로써 암호화된 수열의 상관특성을 개선할 수 있다는 것을 확인하였다.

## References


[1] IS-GPS-200G, *Global positioning systems directorate systems engineering & integration interface specification*, 2012.

[2] Ebner, H., *Galileo Overall Architecture Definition: SIS Frequency Characteristics*, GALA-ASTR-DD-019, issue 5.0, Nov. 2000.

[3] C. S. Sin, “Technologies to counter the GPS jamming,” *TTA J.*, vol. 149, pp. 92-99, 2013.

[4] K. Kim, “Analysis of anti-jamming techniques for satellite navigation systems,” *J. KICS*, vol. 38C, no. 12, pp. 1216-1227, 2013.

[5] G. D. Weeks, J. K. Townsend, and J. A. Freebersyser, “A method and metric for quantitatively defining low probability of detection,” *IEEE Military Commun. Conf. (MILCOM 98),* vol. 3, pp. 821-826, Boston, MA, Oct. 1998.

[6] B. C. Barker, J. W. Betz, J. E. Clark, J. T. Correia, J. T. Gillis, S. Lazar, K. A. Rehborn, and J. R. Straton, “Overview of the GPS M code signal,” in *Proc. 2000 National Technical Meeting of The Inst. Navi.*, pp. 542-549, Anaheim, CA, Jan. 2000.

[7] J. Kim and J. M. Ahn, “Acquisition performance of tiered polyphase code based GNSS signal,” *J. KICS*, vol. 38A, no. 11, pp. 970-972, 2013.

[8] M. H. Jin, H. H. Choi, K. J. Kim, C. Park, J.-M. Ahn, and S. J. Lee, “The design method of GNSS signal using the analysis result of receiver performance,” *J. KICS*, vol. 37C, no. 06, pp. 502-511, 2012.

[9] K. Fazel and S. Kaiser, *Multi-Carrier and Spread Spectrum Systems: From OFDM and MC-CDMA to LTE and WiMAX*, 2nd Ed., NY: Wiley, 2008.



**박 기 현** (Ki-Hyeon Park)

2007년 2월 : 연세대학교 전기전자공학과 졸업

2009년 2월 : 연세대학교 전기전자공학과 석사

2009년 3월~현재 : 연세대학교 전기전자공학과 박사과정

<관심분야> 통신공학, 정보이론, 암호이론, 이산수학

**송 민 규** (Min Kyu Song)

2011년 2월 : 건국대학교 전자공학과 졸업

2013년 2월 : 연세대학교 전기전자공학과 석사

2014년 3월~현재 : 연세대학교 전기전자공학과 박사과정

<관심분야> 통신공학, 정보이론, 암호이론, 이산수학

**송 홍 엽** (Hong-Yeop Song)

1984년 2월 : 연세대학교 전자공학과 졸업

1986년 5월 : University of Southern California Dept. of EE. System 석사

1991년 12월 : University of Southern California Dept. of EE. System 박사

1995년 9월~현재 : 연세대학교 전기전자공학과 전임교수

<관심분야> 통신공학, 정보이론, 부호이론, 암호이론, 이산수학

**이 장 용** (Jang-Yong Lee)

1995년 2월 : 전남대학교 전자공학과 졸업
1997년 2월 : 전남대학교 전자공학과 석사 졸업
2007년 2월~현재 : 국방과학연구소 재직
<관심분야> 통신공학, 위성항법, 재밍대응, 의사위성