논문 21-46-12-01 The Journal of Korean Institute of Communications and Information Sciences '21-12 Vol.46 No.12
https://doi.org/10.7840/kics.2021.46.12.2109

가산성 백색 가우시안 잡음 채널에서 은닉 통신 연구 동향

한 동 화◆, 이 남 윤°

A Survey of Covert Communication on AWGN Channels

Donghwa Han◆, Namyoon Lee°

요 약

본 논문에서는 은닉 통신 문제에 관한 기존 연구 결과들을 소개한다. 특히 가산성 백색 가우시안 잡음 (additive white Gaussian noise: AWGN) 채널 환경에서 독립적인 채널을 n번 사용할 때, 도청자가 통신의 여부를 탐지하지 못하게 하며 전송할 수 있는 정보 비트가 $o(\sqrt{n})$을 따른다는 은닉 통신의 정보 이론적 한계에 대한 기존 증명 과정을 상세히 설명하고 그 의미를 고찰하고자 한다. 또한 도청자가 채널의 잡음 분산을 정확히 알지 못하는 경우 양의 은닉 통신 전송률을 얻을 수 있다는 기존 이론에 대해 소개하고, AWGN 채널에서 은닉성을 유지하면서 상호 정보량을 최대화하는 최적의 송신 신호 분포에 대한 최신의 학계 연구 결과를 소개한다. 마지막으로 은닉 통신의 실용 방안을 살펴보기 위해 희소 중첩 코드 (sparse superposition codes: SPARCs)의 한 종류로 최근에 제안된 직교 희소 중첩 (orthogonal sparse superposition: OSS) 코드의 연속적 부호화 기법과 저 복잡도 복호 방식을 소개하고 은닉성에 대한 고찰을 한다.

Key Words : information-theoretic secrecy, covert communication, low probability of detection communication, channel coding, coded modulation

ABSTRACT

In this paper, we consider the problem of covert communication over additive white Gaussian noise (AWGN) channels and provide an overview of the information-theoretic limits on the amount of information that can be conveyed. No more than $o(\sqrt{n})$ bits can be sent reliably to the legitimate receiver in n independent channel uses while concealing from the warden the very existence of transmissions. A recent finding that a non-zero asymptotic rate can be obtained if the warden has noise variance measurement uncertainty is discussed. Results in the existing literature are presented, including the optimality of the Gaussian signaling in terms of maximizing the mutual information under the covert constraint. We then investigate the possibility of covert communication using orthogonal sparse superposition (OSS) codes, a new class of sparse superposition codes (SPARCs).

※ 이 논문은 2021년도 과학기술정보통신부의 재원으로 한국연구재단의 지원(2020R1C1C101338112, 차세대 이동통신 시스템을 위한 초거대 다중 안테나 시스템 연구)과 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (20210004670012000, 지능형 6G 무선 액세스 시스템).

◆ First Author : Pohang University of Science and Technology Department of Electrical Engineering, dhan92@postech.ac.kr, 학생회원
° Corresponding Author : Pohang University of Science and Technology Department of Electrical Engineering, nylee@postech.ac.kr, 종신회원

논문번호 : 202107-168-A-RU, Received July 11, 2021; Revised August 2, 2021; Accepted August 4, 2021

Ⅰ. 서 론

보안 통신(secure communication)은 허가 없이 통신을 탈취하는 도청자(eavesdropper/warden) 로부터 정보의 내용을 숨기는 것을 목적으로 한다. 이러한 정보 이론적 보안(information-theoretic secrecy)을 얻기 위해서는 정보를 담고 있는 메시지와 도청자가 감청하는 신호 사이의 상호 정보량(mutual information)을 0으로 만들어야 한다. 따라서 정보의 유출(leakage)로 보안 통신의 성능을 측정한다[1]. 특히 A. D. Wyner의 논문을 통해 도청자가 적법 송수신단 간의 이산 비기억 채널(discrete memoryless channel: DMC)보다 잡음이 더 심한 DMC를 통해 송신 신호를 탈취하는 경우, 적법 송수신단은 보안성을 유지하면서 양의(positive) 채널 용량(capacity)을 얻을 수 있다는 것이 증명되었다[2].

특정 상황의 경우 송신 정보의 유출을 방지하는 것보다 적법 송수신단 간 통신 여부의 탐지가 되지 않게 하는 것이 중요할 수 있다. 그 예로, 군용 통신에서 활성 전파 교란(active jamming)등의 행위는 악의를 가진 공격자가 통신 발생 여부를 탐지했다는 점에 입각해 수행된다[3]. 이를 막기 위해 원래의 메시지가 유발하는 수신 신호의 통계적 특성과 정보를 담고 있지 않은 신호를 보냈을 때의 특성을 비슷하게 만들어 도청자의 통신 여부 탐지 확률을 줄이는 스텔스 통신(stealth communication)이 연구되어 왔다[4]. 본 논문에서 다룰 은닉 통신(covert communication)이란 이러한 스텔스 통신의 특수한 종류로, 주요한 차이는 통신 탐지를 막기 위해 원래의 메시지와 통계적으로 유사한 혼란 신호(obfuscation signal)를 보내는 스텔스 통신과 달리 은닉 통신은 송신 자체를 하지 않는 다는 것이다.

특수한 목적의 군용 통신뿐 아니라 은닉 통신의 중요성은 다른 분야에서도 대두되고 있다. 특히, 최근에 각광받고 있는 IoT(internet of things)와 다가올 6G 차세대 무선통신에서 실현될 IoE(internet of everything)에서 네트워크에 연결된 수 많은 센서 및 웨어러블 디바이스(wearable device)가 민감한 개인 정보를 주고받는 문제가 있다. IoT 기기들의 한정된 연산 능력(computing power)과 출력을 고려해보면 종래의 공개키(public key)를 사용하는 암호화 방식은 송수신단의 부하를 증가시키고 오버헤드(overhead)가 심해지는 문제가 있다. 이러한 과제를 해결하기 위해 하이 레벨(high-level)에서의 접근이 아닌 통신 채널의 물리적 및 통계적 특성을 이용한 정보 이론적 보안 솔루션이 필요하다.

은닉 통신에 대한 정보 이론적 접근은 약 10년 전에 시작되었지만, 그 기원은 20세기로 올라간다. 제1차 세계대전 이후, 미국에서는 어뢰를 조종하는 전파 신호가 적군에 탐지되는 것을 막기 위해서 심볼을 전송할 때마다 반송 주파수(carrier frequency)를 변경하는 주파수 도약 대역 확산(frequency-hopping spread spectrum: FHSS) 기법을 개발하였다[5]. FHSS를 사용하여 송신하는 경우, 훨씬 더 넓은 대역폭을 사용하기 때문에 출력 신호의 스펙트럼 밀도가 낮아지게 되고 도청자는 수신한 신호를 잡음과 구분하기 어려워지게 된다. 따라서 통신의 탐지를 막을 수 있고, 최종적으로 적군의 활성 전파 교란 공격을 예방할 수 있다.

은닉 통신은 대역 확산 기법뿐 아니라 다른 통신 분야들과도 밀접한 관계가 있다. 한 예로 다른 메시지, 그림, 영상, 오디오 등의 은닉 매체(cover-text)에 원래의 메시지를 숨겨서 전송하는 기술인 스테가노그래피(steganography)가 있다[6]. 다른 예시로는 스펙트럼 센싱(spectrum sensing)을 통해 사용되고 있지 않은 대역을 찾아 할당하는 인지 무선 통신(cognitive radio) 네트워크에서 제2차 사용자의 존재를 스펙트럼에서 지워 간섭을 최소화하는 과제가 있다[7].

본론의 첫 번째 절에서는 SISO(single-input single-output) 가산성 백색 가우시안 잡음(additive white Gaussian noise: AWGN) 채널에서 은닉 통신의 모델링을 설명한다. 두 번째 절에서는 [8]에서 증명된 n번의 채널을 사용하는 동안 은닉성을 유지하면서 전달할 수 있는 정보 비트의 이론적 한계가 $o(\sqrt{n})$의 제곱근 법칙(square root law)을 따른다는 기존 결과의 증명 과정을 상세히 소개하고 그 의미에 대한 고찰을 한다. 이를 통해 은닉 통신의 정보 이론적 한계를 달성하기 위해서는 송신 출력이 $o\left(\frac{1}{\sqrt{n}}\right)$로 유지되어야 한다는 점을 알 수 있다. 세 번째 절에서는 도청자가 자신의 AWGN 채널의 잡음을 정확히 알지 못하는 특수한 경우에 양의 전송률을 얻을 수 있다는 [9]의 결과를 소개한다. 네 번째 절에서는 AWGN 채널에서 도청자의 탐지 오류 확률과 적법 송수신단 간의 상호 정보량을 최대화하는 최적의 송신 신호가 가우시안 분포를 따른다는 [10]의 결과를 서술한다. 은닉 통신에서는 블록 길이 n이 증가함에 따라 점근적으로(asymptotically) 0에 수렴하는 전송률로 통신이 이루어진다. 따라서, 긴 블록 길이의 코드 워드(codeword)를 보내 높은 전송률을 얻기 위한 목적으로 고안된 종래의 채널 코드를 사용하기보다는 낮은 전송률에서도

성능이 좋은 채널 코드를 활용하는 것이 효과적이다. 마지막 절에서는 한정된 블록 길이에서의 저전력 통신에 적합한 최근에 연구된 직교 희소 중첩(orthogonal sparse superposition: OSS) 코드 [11]를 소개하고 해당 코드의 은닉성에 대한 고찰을 한다.

Ⅱ. 본 론

2.1 시스템 모델

본 절에서는 우선적으로 시스템 모델을 설명하고, 해결하고자 하는 문제를 소개하도록 한다. 본 논문에서 고려하는 은닉 통신 환경은 그림 1과 같다. 송신단은 채널을 n번 사용해서 $\mathbf{x} = [x[1], \ldots, x[n]]^{\mathrm{T}} \in \mathbb{R}^n$를 전송한다. 그림 1에서 나타난 바와 같이 적법한 송수신단 앨리스(Alice)와 밥(Bob)은 충분한 길이의 비밀키(secret key)를 공유한다. 보안 통신에서의 비밀키는 도청자가 탈취한 메시지를 해독하지 못하게 하는 목적으로 사용되지만, 은닉 통신에서의 비밀키는 송수신단이 사용한 코드북(codebook)에 대한 정보를 숨기는 용도로써 사용한다. 적법 수신자 밥과 도청자가 받은 신호를 각각 $\mathbf{z}$와 $\mathbf{y}$로 표기할 때, 도청자는 코드북에 대한 정보의 부재로 n차원의 신호 $\mathbf{y}$의 정확한 분포는 알지 못하고 각 원소 $y[i]$가 독립 항등 분포(independent and identically distributed)를 따른다고 추정하게 된다. 최종적으로 도청자는 $\mathbf{y}$에 기반하여 적법한 송수신단 간에 통신이 이루어지고 있는지를 아래와 같은 가설 검정(statistical hypothesis testing)을 통해 탐지하게 된다:

$\mathcal{H}_0$: 통신이 이루어지고 있지 않음,
$\mathcal{H}_1$: 통신이 이루어지고 있음.

그리고 이에 해당하는 이진 결정들을 다음과 같이 표기한다:

D_0 : 통신이 발생하지 않았다고 판단,
D_1 : 통신이 발생했다고 판단.

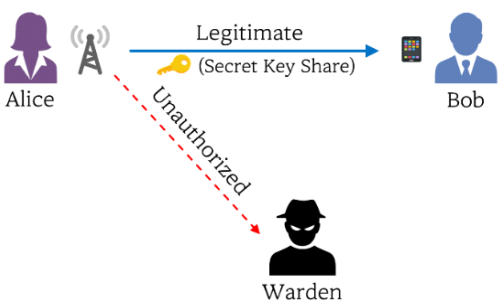


그림 1. 은닉 통신의 시스템 모델
Fig. 1. System model of covert communications.

위 가설 검정에서 귀무 가설(null hypothesis) $\mathcal{H}_0$이 참일 때 이를 거짓으로 판별하는 오 경보(false alarm) 확률을 $\mathbb{P}_{\mathrm{FA}} \triangleq \Pr(D_1|\mathcal{H}_0)$로, 대립 가설(alternative hypothesis) $\mathcal{H}_1$이 발생했을 때, D_0의 결정을 내릴 오 탐지(miss detection) 확률을 $\mathbb{P}_{\mathrm{MD}} \triangleq \Pr(D_0|\mathcal{H}_1)$로 각각 정의한다. $\mathcal{H}_0$이 참일 경우 도청자는 도청 채널의 잡음만 관찰하게 되고, 이때 $y[i]$의 확률 분포를 $\mathbb{P}_w$ 그리고 n번의 관찰 값 $\mathbf{y}$의 분포를 $\mathbb{P}_0 = \mathbb{P}_w^{\otimes n}$로 정의한다. 마찬가지로 $\mathcal{H}_1$이 참일 때 $y[i]$와 $\mathbf{y}$가 따르는 각각의 확률 분포를 $\mathbb{P}_s$와 $\mathbb{P}_1 = \mathbb{P}_s^{\otimes n}$로 정의한다. 도청자가 최적의 가설 검정 기법을 적용하였을 때 오류 확률의 합은 아래와 같이 나타난다: [12]

$$\xi = \mathbb{P}_{\mathrm{FA}} + \mathbb{P}_{\mathrm{MD}} = 1 - \mathcal{V}_T\left(\mathbb{P}_w^{\otimes n}, \mathbb{P}_s^{\otimes n}\right). \tag{1}$$

수식 (1)에서 $\mathcal{V}_T(\mathbb{P}, \mathbb{Q})$는 동일한 가측 공간(measurable space) $(\Omega, \mathcal{F})$에서 정의된 두 개의 확률 측도 $\mathbb{P}$와 $\mathbb{Q}$의 총 변동 거리(total variational distance)를 나타내고 다음과 같이 정의된다:

$$\begin{aligned}\mathcal{V}_T(\mathbb{P}, \mathbb{Q}) &\triangleq \min_{A \in \mathcal{F}} \left|\mathbb{P}(A) - \mathbb{Q}(A)\right| \\ &= \frac{1}{2}\|\mathbb{P} - \mathbb{Q}\|_1.\end{aligned} \tag{2}$$

은닉 통신이 가능하기 위해서는 수식 (1)의 도청자의 총 오류 확률 ξ이 1로 수렴해야 한다. 즉, 임의의 작은 값 ϵ에 대해 총 변동 거리를 다음과 같이 제한해야 한다:

$$\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1) \leq \epsilon. \tag{3}$$

하지만 두 개의 다차원 분포의 총 변동 거리를 계산하는 것은 수학적으로 복잡하다는 문제가 있다. 이때 핀스커 부등식(Pinsker's inequality)을 이용하면 다음과 같이 상대 엔트로피(relative entropy)로 총 변동 거리의 상한을 분석할 수 있다:

$$\mathcal{V}_T\left(\mathbb{P}_w^{\otimes n}, \mathbb{P}_s^{\otimes n}\right) \leq \sqrt{\frac{1}{2}\mathcal{D}_{\mathrm{KL}}\left(\mathbb{P}_w^{\otimes n} \| \mathbb{P}_s^{\otimes n}\right)}. \tag{4}$$

특히, 상대 엔트로피는 독립 항등 분포를 따르는 다차원 신호에 대해 연쇄 법칙(chain rule)을 아래와 같이 적용할 수 있다:

$$\mathcal{D}_{\mathrm{KL}}\left(\mathbb{P}_w^{\otimes n}\|\mathbb{P}_s^{\otimes n}\right)=n\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s). \tag{5}$$

수식 (1)-(5)을 종합하면 아래의 결과를 얻을 수 있다:

$$\xi\geq 1-\sqrt{\frac{n}{2}\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s)}. \tag{6}$$

수식 (6)에서 나타난 바와 같이 적법한 송수신단은 은닉성을 유지하기 위해 n이 증가함에 따라 감소하는 상대 엔트로피 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s)$를 유도하는 $\mathbb{P}_s$의 분포를 따르는 송신 신호로 통신해야 한다.

다음 절에서는 본 절에서 설명한 시스템 모델에서 수식 (3)의 은닉성 조건을 만족하면서 전송할 수 있는 최대 정보 비트를 정보 이론적 관점에서 분석한다.

2.2 은닉 통신의 정보 이론적 상한

본 절에서는 SISO AWGN 은닉 통신의 이론적 한계에 관한 기존 결과의 증명 과정을 자세히 서술한다.

2.2.1 SISO AWGN 채널에서 $o(\sqrt{n})$ 비트 전송의 가능성(achievability)

Theorem 1-1[8]: 도청 채널이 σ_w^2의 분산을 가지는 AWGN이며 송수신단이 충분한 길이의 비밀키를 공유하는 경우, 전송 가능한 최대 정보 비트는 $o(\sqrt{n})$를 따른다. 추가적으로, 송수신단이 도청 채널의 잡음 분산의 하한값 $\sigma_w^2\geq\ \hat{\sigma}_w^2>0$을 아는 경우, 전송 가능한 정보 비트는 $\mathcal{O}(\sqrt{n})$를 따른다.

송신단의 부호기가 길이 M의 비트 블록을 $R=\frac{M}{n}$의 비율로 n 차원의 코드 워드로 매핑하고 가우시안 랜덤 코딩 기법(Gaussian random coding argument)에 기반해서 2^{nR}개의 메시지 $\{W_k\}_{k=1}^{2^{nR}}$에 해당하는 코드 워드들 $\{\mathbf{c}(W_k):k=1,\ldots,2^{nR}\}$을 독립적으로 생성한다고 가정한다. 각 $\boldsymbol{x}[i]$의 출력을 P_x라고 표기하면, 도청자가 탐지하는 신호의 분포는 통신의 여부에 따라서 아래와 같이 나타나게 된다:

$$\mathbb{P}_w^{\otimes n}=\mathcal{N}(\mathbf{0},\sigma_w^2\mathbf{I}), \tag{7}$$

$$\mathbb{P}_s^{\otimes n}=\mathcal{N}(\mathbf{0},(P_x+\sigma_w^2)\mathbf{I}). \tag{8}$$

따라서 $\mathbb{P}_w$와 $\mathbb{P}_s$ 사이의 상대 엔트로피는 다음과 같이 계산할 수 있다:

$$\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s)=\frac{1}{2}\left[\log\left(1+\frac{P_x}{\sigma_w^2}\right)-\left(1+\left(\frac{P_x}{\sigma_w^2}\right)^{-1}\right)^{-1}\right]. \tag{9}$$

수식 (9)의 상대 엔트로피를 원점에서 P_x에 대한 테일러 정리(Taylor's theorem)를 이용해서 2차까지 정리하면 아래와 같다:

$$\begin{aligned}\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s)&=\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s)|_{P_x=0}+P_x\\&\quad\times\frac{\partial\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s)}{\partial P_x}|_{P_x=0}+\frac{P_x^2}{2!}\\&\quad\times\frac{\partial^2\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s)}{\partial P_x^2}|_{P_x=0}+\frac{P_x^3}{3!}\\&\quad\times\frac{\partial^3\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s)}{\partial P_x^3}|_{P_x=c}\\&=\frac{P_x^2}{2!}\times\frac{1}{2\sigma_w^4}+\frac{P_x^3}{3!}\times\frac{c-2\sigma_w^2}{(c+\sigma_w^2)^4}\\&=\frac{P_x^2}{4\sigma_w^4}+\frac{P_x^3(c-2\sigma_w^2)}{6(c+\sigma_w^2)^4}.\end{aligned} \tag{10}$$

위의 식에서 c는 0과 P_x 사이에 존재한다. 추가적으로 송신 출력 P_x가 P_x가 $P_x<2\sigma_w^2$를 만족할 때, 나머지 항(remainder term) $\frac{P_x^3(c-2\sigma_w^2)}{6(c+\sigma_w^2)^4}$이 항상 음수이기 때문에, 수식 (4)을 이용해 다음의 부등식을 얻을 수 있다:

$$\mathcal{V}_T(\mathbb{P}_0,\mathbb{P}_1)\leq\sqrt{\frac{n}{2}\frac{P_x^2}{4\sigma_w^4}}=\frac{P_x}{2\sigma_w^2}\sqrt{\frac{n}{2}}. \tag{11}$$

송신자가 도청 채널의 잡음 분산 σ_w^2에 대한 정보가 없는 경우, $f(n)=o(1)$과 $f(n)=\omega\left(\frac{1}{\sqrt{n}}\right)$을 만족하는 $f(n)$을 이용해 송신 출력을 $P_x\leq\frac{2\epsilon\sqrt{2}f(n)}{\sqrt{n}}$로 설정해 수식 (11)에 대입하면 수식 (3)의 은닉 조건을 만족함을 보일 수 있다. 만약 송수신단에서 도청 채널의 잡음 세기에 대한 부분 정보 $\sigma_w^2\geq\ \hat{\sigma}_w^2>0$가 있을 경우, 송신 출력을 $P_x\leq\frac{2\epsilon\sqrt{2}\hat{\sigma}_w^2}{\sqrt{n}}$로 설정하여 은닉성을 얻을 수 있다. 즉, 두 경우 모두에서 도청자의 통신 탐지 성능을 성공적으로 제한할 수 있다.

한편, 적법 송수신단에서는 위 방법에 따라서 송신 출력을 조절할 때 복호 오류 없이 안정적으로 전송할 수 있는 최대 정보 전송량을 유도해야 한다. 코드 워

드 $\mathbf{c}(W_k)$가 전송되었을 때 수신 신호 $\mathbf{z}$가 다른 코드 워드 $\mathbf{c}(W_i)$, $i \neq k$와의 유클리드 제곱 거리가 더 가까운 오류 사건을 $E_i(\mathbf{c}(W_k))$라고 표기하고, 코드북 전체에 대해 평균을 취한 복호 오류 확률을 다음과 같이 계산할 수 있다:

$$\begin{aligned}\mathbb{P}_e &= \mathbb{E}_{\mathbf{c}(W_k)}\left[\Pr\left(\bigcup_{i=1,i\neq k}^{2^{nR}} E_i(\mathbf{c}(W_k))\right)\right] \\ &\leq \sum_{i=1,i\neq k}^{2^{nR}} \mathbb{E}_{\mathbf{c}(W_k)}\left[\Pr\left(E_i(\mathbf{c}(W_k))\right)\right].\end{aligned} \tag{12}$$

각 코드 워드는 가우시안 랜덤 코딩 기법에 따라 얻어지므로 $\mathbf{d} \triangleq \mathbf{c}(W_k) - \mathbf{c}(W_i)$라고 정의할 때, 코드 워드간 사이의 유클리드 제곱 거리 $\|\mathbf{d}\|_2^2$는 n의 자유도를 갖는 카이제곱(chi-square)분포 $U \sim \chi_n^2$로 표현할 수 있다:

$$\|\mathbf{d}\|_2^2 = 2P_x U. \tag{13}$$

따라서 송신 출력을 $P_x = \frac{2\epsilon\sqrt{2}f(n)}{\sqrt{n}}$로 가정하고, 부등식 $Q(x) \leq \frac{1}{2}e^{-\frac{x^2}{2}}$을 이용해서 수식 (12)의 피가수(summand)의 상한을 아래와 같이 구할 수 있다:

$$\begin{aligned}&\mathbb{E}_{\mathbf{c}(W_k)}\left[\Pr\left(E_i(\mathbf{c}(W_k))\right)\right] \\ &= \mathbb{E}_U\left[Q\left(\sqrt{\frac{P_f U}{2\sigma_b^2}}\right)\right] \\ &\leq \mathbb{E}_U\left[\exp\left(-\frac{2\epsilon\sqrt{2}f(n)U}{4\sqrt{n}\sigma_b^2}\right)\right] \\ &= 2^{-\frac{n}{2}\log_2\left(1+\frac{2\epsilon\sqrt{2}f(n)}{2\sqrt{n}\sigma_b^2}\right)}.\end{aligned} \tag{14}$$

위의 식에서 σ_b^2은 적법한 AWGN 통신 채널의 잡음 분산을 나타낸다. 수식 (14)을 (12)에 대입하여 아래의 최종 형태를 얻을 수 있다:

$$\mathbb{P}_e \leq 2^{n\left(R-\frac{1}{2}\log_2\left(1+\frac{2\epsilon\sqrt{2}f(n)}{2\sqrt{n}\sigma_b^2}\right)\right)}. \tag{15}$$

수식 (15)에 따르면 전송률 R이 $\rho < 1$인 상수 ρ에 대해 $R = \frac{\rho}{2}\log_2\left(1+\frac{2\epsilon\sqrt{2}f(n)}{2\sqrt{n}\sigma_b^2}\right)$일 때, n이 증가하면서 $\mathbb{P}_e$는 0에 수렴한다. 따라서 적법 송수신단이 채널을 n번 사용해서 보낼 수 있는 비트 nR의 상한을 다음과 같이 계산할 수 있다:

$$\begin{aligned}nR &= n\frac{\rho}{2}\log_2\left(1+\frac{2\epsilon\sqrt{2}f(n)}{2\sqrt{n}\sigma_b^2}\right) \\ &\leq n\frac{\rho}{2}\frac{2\epsilon\sqrt{2}f(n)}{2\sqrt{n}\sigma_b^2\log 2} \\ &= \frac{\rho\epsilon f(n)}{\sqrt{2}\sigma_b^2\log 2}\sqrt{n}.\end{aligned} \tag{16}$$

수식 (16)은 $f(n) = o(1)$인 송신 출력 $P_x = \frac{2\epsilon\sqrt{2}f(n)}{\sqrt{n}}$를 이용해서 $o(\sqrt{n})$ 정보 비트를 은닉 조건을 만족하면서 송신 가능하다는 것을 의미한다. 만약 도청자의 잡음의 세기의 하한을 알아서 $f(n) = \hat{\sigma}_w^2$로 설정할 경우 전송 가능한 정보 비트는 $O(\sqrt{n})$을 따르게 된다. 이는 은닉 통신의 정보 이론적 한계에 해당하고 제곱근 법칙이라고 명명한다[8].

2.2.2 SISO AWGN 채널에서 제곱근 법칙의 역(converse)

본 항에서는 은닉성을 유지하면서 제곱근 법칙 이상의 정보 비트를 전송할 수 없다는 결과를 소개한다.

Theorem 1-2[8]: 도청 채널이 AWGN이며 송수신단이 $w(\sqrt{n})$의 정보 비트를 송신하는 경우, 블록 길이 n이 ∞로 증가함에 따라 도청자가 낮은 오류 확률 ξ로 통신의 여부를 탐지하게 되거나, 적법 수신단의 복호 에러 확률이 0으로 수렴하지 않는다.

위 정리의 증명은 크게 두 가지 단계로 나누어진다. 우선 송신 출력이 $w\left(\frac{1}{\sqrt{n}}\right)$을 따를 때, 도청자가 낮은 오류 확률을 가지고 통신 탐지에 성공함을 보인다. 송신자가 임의의 코드북 $\{\mathbf{c}(W_k), k = 1, \ldots, 2^{nR}\}$을 이용하고, 도청자가 평균 출력 $S = \frac{\mathbf{y}^{\mathrm{T}}\mathbf{y}}{n}$을 검정 통계량(test statistic)으로 사용한다고 가정한다. 가설 $\mathcal{H}_0$이 참일 때 S는 자유도 n의 카이제곱 분포를 따르고 다음의 평균과 분산을 가진다:

$$\mathbb{E}[S] = \sigma_w^2, \tag{17}$$

$$\mathrm{Var}[S] = \frac{2\sigma_w^4}{n}. \tag{18}$$

반면, 메시지 에 해당하는 코드 워드 $\mathbf{c}(W_k) = \{x^{(k)}[i]\}_{i=1}^n$이 전송된 경우, 도청 수신 신호 벡터의 원소 $y^{(k)}[i] \sim \mathcal{N}(x^{(k)}[i], \sigma_w^2)$의 제곱은 비중심(noncentral) 카이제곱 분포를 따른다. 편의를 위해 인덱스 표기를 생략하고, $(y^{(k)}[i])^2$의 평균과 분산을 구하면 아래와 같다:

$$\begin{aligned}\mathbb{E}\left[\left(y^{(k)}\right)^2\right] &= \mathbb{E}\left[\sigma_w^2 V^2 + 2\sigma_w x^{(k)} V + \left(x^{(k)}\right)^2\right] \\ &= \sigma_w^2 + \left(x^{(k)}\right)^2,\end{aligned} \tag{19}$$

$$\begin{aligned}\mathrm{Var}\left[\left(y^{(k)}\right)^2\right] &= \mathbb{E}\left[\left(y^{(k)}\right)^4\right] - \left(\mathbb{E}\left[\left(y^{(k)}\right)^2\right]\right)^2 \\ &= \left[3\sigma_w^4 + 6\sigma_w^2\left(x^{(k)}\right)^2 + \left(x^{(k)}\right)^4\right] \\ &\quad - \left[\sigma_w^4 + 2\sigma_w^2\left(x^{(k)}\right)^2 + \left(x^{(k)}\right)^4\right] \\ &= 4\left(x^{(k)}\right)^2\sigma_w^2 + 2\sigma_w^4.\end{aligned} \tag{20}$$

수식 (19)에서 V는 $\mathcal{N}(0,1)$를 따르는 임의의 확률변수이다. 최종적으로 $\mathcal{H}_1$이 참일 때, 코드 워드의 평균 출력을 $P_k = \frac{\mathbf{c}(W_k)^{\mathrm{T}}\mathbf{c}(W_k)}{n}$로 표기하면 S의 평균과 분산은 다음과 같다:

$$\mathbb{E}[S] = \sigma_w^2 + P_k, \tag{21}$$

$$\mathrm{Var}[S] = \frac{4P_k\sigma_w^2 + 2\sigma_w^4}{n}. \tag{22}$$

위에서 구해진 S의 통계적 정보에 기반하여 도청자는 특정한 임계치(threshold) t를 설정하고 다음의 가설 검정을 수행한다:

$$S \underset{D_0}{\overset{D_1}{\gtrless}} \sigma_w^2 + t. \tag{23}$$

$\mathcal{H}_0$이 참일 때의 도청자의 수신 신호 벡터의 분포를 $\mathbb{P}_0$라고 할 때 오 경보 확률은 아래와 같다:

$$\begin{aligned}\mathbb{P}_{\mathrm{FA}} &= \Pr(S \geq \sigma_w^2 + t | \mathcal{H}_0) \\ &= \mathbb{P}_0(S \geq \sigma_w^2 + t).\end{aligned} \tag{24}$$

수식 (24)에 체비셰프의 부등식(Chebyshev's inequality)을 적용하면 다음의 결과를 얻을 수 있다:

$$\begin{aligned}\mathbb{P}_{\mathrm{FA}} &\leq \mathbb{P}_0(|S - \sigma_w^2| \geq t) \\ &\leq \frac{\mathrm{Var}_{\mathbb{P}_0}[S]}{t^2} = \frac{2\sigma_w^4}{nt^2}.\end{aligned} \tag{25}$$

수식 (25)에 따르면 도청자가 특정한 오 경보 확률 값 $\mathbb{P}_{\mathrm{FA}}^*$을 얻기 위해서는 임계치 t를 다음과 같이 설정해야 한다:

$$t = \frac{\sqrt{2}\sigma_w^2}{\sqrt{\mathbb{P}_{\mathrm{FA}}^*}}\frac{1}{\sqrt{n}}. \tag{26}$$

만약 $\mathbf{c}(W_k)$이 전송되었을 때의 분포를 $\mathbb{P}_1^{(k)}$라고 표기하면, 수식 (23)-(25)와 같은 과정을 통해 아래의 오 탐지 확률을 얻을 수 있다:

$$\begin{aligned}\mathbb{P}_{\mathrm{MD}}^{(k)} &= \mathbb{P}_1^{(k)}(S < \sigma_w^2 + t) \\ &\leq \mathbb{P}_1^{(k)}(|S - \sigma_w^2 - P_k| \geq P_k - t) \\ &\leq \frac{4P_k\sigma_w^2 + 2\sigma_w^4}{\left(\sqrt{n}P_k - \sqrt{n}t\right)^2}.\end{aligned} \tag{27}$$

이 때 수식 (26)을 임계치로 사용하고 송신 출력이 $P_k = w\left(\frac{1}{\sqrt{n}}\right)$일 경우 $\lim_{n\to\infty}\mathbb{P}_{\mathrm{MD}}^{(k)} = 0$이 되어서 도청자가 성공적으로 가설 검정을 수행함을 알 수 있다.

다음으로 송신 출력을 $\mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$로 유지할 때, $w(\sqrt{n})$의 정보 비트를 송신하게 되면 적법 수신단의 복호 에러 확률이 0으로 수렴하지 않는 다는 결과를 서술한다. 송수신단에서 도청자의 오류 확률을 $\xi = \mathbb{P}_{\mathrm{FA}} + \mathbb{P}_{MD} \geq \zeta > 0$로 설정하기 위해서는 코드북이 낮은 출력의 코드 워드들을 포함하고 있어야 한다. 송신 출력이 $P_{\mathcal{U}} = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$를 따르는 코드 워드들의 코드북 대비 비율을 γ라고 정의하고, 해당 코드 워드들의 부분 집합을 $\mathcal{U} \subset \{\mathbf{c}(W_k)\}_{k=1}^{2^{nR}}$라고 정의한다. 이 때 수신단에서의 복호 오류 확률 $\mathbb{P}_e$는 다음과 같이 나타낼 수 있다:

$$\begin{aligned}\mathbb{P}_e &= \mathbb{P}_e(\mathcal{U})\Pr(\mathbf{c}(W \in \mathcal{U}) \text{ sent}) \\ &\quad + \mathbb{P}_e(\mathcal{U}^c)\Pr(\mathbf{c}(W \in \mathcal{U}^c) \text{ sent}) \\ &\geq \gamma\mathbb{P}_e(\mathcal{U}).\end{aligned} \tag{28}$$

수식 (28)에서 $\mathbb{P}_e(\mathcal{U})$는 $\mathcal{U}$에 포함된 메시지가 전송되었을 때의 평균 복호 오류 확률을 의미한다:

$$\mathbb{P}_e(\mathcal{U}) = \frac{1}{|\mathcal{U}|}\sum_{W\in\mathcal{U}}\Pr\left(\mathbf{c}(\widehat{W}) \neq \mathbf{c}(W)\right). \tag{29}$$

전송된 메시지 W가 다른 메시지 W_j로 복호되는 사건을 E_j라고 정의하고 부분 집합 $\mathcal{U}$의 앙상블(ensemble)에 대한 복호 오류 확률 $\mathbb{P}_e^{(\mathcal{U})}$를 아래와 같이 정의한다:

$$\mathbb{P}_e^{(\mathcal{U})} \triangleq \Pr\left(\bigcup\nolimits_{W_j\in\mathcal{U}\setminus\{W\}} E_j\right). \tag{30}$$

파노의 부등식(Fano's inequality)을 사용하여 메시지 추정값 $\widehat{W}$에 대한 조건부 엔트로피(conditional entropy)의 상한을 해당 앙상블에서 다음과 같이 구할

수 있다.[13]

$$H(W|\widehat{W}) \le H_b\left(\mathbb{P}_e^{(\mathcal{U})}\right) + \mathbb{P}_e^{(\mathcal{U})}\log_2|\mathcal{U}| \le 1 + \mathbb{P}_e^{(\mathcal{U})}\log_2|\mathcal{U}|. \quad (31)$$

수식 (31)에서 $H_b\left(\mathbb{P}_e^{(\mathcal{U})}\right)$는 $\mathbb{P}_e^{(\mathcal{U})}$의 이진 엔트로피(binary entropy)를 의미한다. 모든 메시지 W가 동일한 확률을 가지기 때문에 $\mathcal{U}$의 앙상블에서 W의 엔트로피에 대한 다음의 관계식을 얻을 수 있다:

$$\begin{aligned} H(W) &= \log_2|\mathcal{U}| \\ &= I(W;\widehat{W}) + H(W|\widehat{W}) \\ &\le I(\mathbf{x};\mathbf{z}) + 1 + \mathbb{P}_e^{(\mathcal{U})}\log_2|\mathcal{U}| \\ &= H(\mathbf{z}) - H(\mathbf{n}_b) + 1 + \mathbb{P}_e^{(\mathcal{U})}\log_2|\mathcal{U}| \\ &\le \sum_{i=1}^{n}\left(H(z[i]) - H(n_b[i])\right) + 1 \\ &\quad + \mathbb{P}_e^{(\mathcal{U})}\log_2|\mathcal{U}| \\ &\le \sum_{i=1}^{n}\frac{1}{2}\log_2\left(1+\frac{P_{\mathcal{U}}}{\sigma_b^2}\right) + 1 \\ &\quad + \mathbb{P}_e^{(\mathcal{U})}\log_2|\mathcal{U}| \\ &\le \frac{n}{2}\cdot\frac{P_{\mathcal{U}}}{\sigma_b^2} + 1 + \mathbb{P}_e^{(\mathcal{U})}\log_2|\mathcal{U}|. \end{aligned} \quad (32)$$

위의 식에서 $n_b[i]$은 적법 AWGN 채널의 잡음을 의미하고 σ_b^2의 출력을 가진다. $|\mathcal{U}| = \gamma 2^{nR}$이고, 수식 (32)을 $\mathbb{P}_e^{(\mathcal{U})}$에 대해 정리하면 다음의 부등식을 얻을 수 있다:

$$\mathbb{P}_e^{(\mathcal{U})} \ge 1 - \frac{\frac{nP_{\mathcal{U}}}{2\sigma_b^2}+1}{\log_2|\mathcal{U}|} = 1 - \frac{\frac{nP_{\mathcal{U}}}{2\sigma_b^2}+1}{\log_2\gamma + nR}. \quad (33)$$

$w(\sqrt{n})$의 정보 비트를 송신할 경우, 전송률은 $R = w\left(\frac{1}{\sqrt{n}}\right)$가 된다. 하지만 출력이 $P_{\mathcal{U}} = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$이기 때문에 수식 (33)에서 n이 ∞로 증가함에 따라 복호 오류 확률 $\mathbb{P}_e^{(\mathcal{U})}$가 0에 수렴하지 않음을 알 수 있다. 또한 집합 $\mathcal{U}$에 포함된 메시지가 전송되었다는 정보가 있는 경우, 수신단은 더 적은 수의 코드 워드들을 비교하게 되므로 복호 오류 확률을 줄일 수 있다. 따라서 다음의 부등식이 성립한다:

$$\Pr\left(\mathbf{c}(\widehat{W}) \ne \mathbf{c}(W)\right) = \Pr\left(\bigcup_{j=1, W_j \ne W}^{2^{nR}} E_j\right) \ge \mathbb{P}_e^{(\mathcal{U})}. \quad (34)$$

최종적으로 $\gamma > 0$이기 때문에, 수식 (28)-(34)를 종합하면 $\mathbb{P}_e$가 0에 수렴하지 않는 것을 알 수 있다. 이어서 다음 절에서는 0이 아닌 양의 전송률을 얻을 수 있는 특수한 경우에 대해 논한다.

2.3 0이 아닌 전송률의 가능성

번의 채널을 사용해서 $o(\sqrt{n})$ 또는 $\mathcal{O}(\sqrt{n})$의 정보 비트를 전송하게 되면 이 무한히 커질수록 전송률은 0으로 수렴하게 된다. 본 절에서는 [14]에서 정의한 SNR_{wall} 기법을 이용해 도청자가 도청 채널의 잡음 분산 σ_w^2을 정확히 알지 못할 때 0이 아닌 전송률을 얻을 수 있다는 것을 보인 [9]의 결과를 기술한다.

고정된 SNR값에서 $0 < \mathbb{P}_{\mathrm{FA}} < 0.5$와 $0 < \mathbb{P}_{\mathrm{MD}} < 0.5$를 만족하는 어떠한 $(\mathbb{P}_{\mathrm{FA}}, \mathbb{P}_{\mathrm{MD}})$ 짝을 얻지 못하는 경우, 검출 알고리즘이 견뢰하지 않다고(non-robust) 정의한다. 특정 검출 알고리즘이 임의의 임계치인 SNR_t보다 낮은 모든 SNR 범위에서 견뢰성을 얻지 못한다고 할 때, 이러한 임계치의 최대값을 SNR_{wall}이라고 정의한다[14]. 도청자가 검출 알고리즘으로 우도 비율 검정(likelihood ratio test: LRT)을 사용할 경우, 아래와 같이 표현할 수 있다:

$$T(\mathbf{y}) = \frac{1}{n}\mathbf{y}^{\mathrm{H}}\mathbf{y} = \frac{1}{n}\sum_{i=1}^{n}|y[i]|^2 \underset{D_0}{\overset{D_1}{\gtrless}} \Lambda. \quad (35)$$

도청자가 σ_w^2을 알고 있는 경우, 중심극한정리(central limit theorem)에 따라서 각 가설에서의 검정 통계량은 다음의 분포를 따르게 된다:

$$T(\mathbf{y})|\mathcal{H}_0 \sim \mathcal{N}\left(\sigma_w^2, \frac{1}{n}2\sigma_w^4\right), \quad (36)$$

$$T(\mathbf{y})|\mathcal{H}_1 \sim \mathcal{N}\left(P_x + \sigma_w^2, \frac{1}{n}2(P_x+\sigma_w^2)^2\right). \quad (37)$$

이 때 오 경보와 오 탐지 확률은 각각 아래와 같이 구해진다:

$$\mathbb{P}_{\mathrm{FA}} = \Pr(T(\mathbf{y}) > \Lambda|\mathcal{H}_0) = Q\left(\frac{\Lambda - \sigma_w^2}{\sqrt{\frac{2}{n}}\sigma_w^2}\right), \quad (38)$$

$$\mathbb{P}_{\mathrm{MD}} = \Pr(T(\mathbf{y}) < \Lambda|\mathcal{H}_1) = 1 - Q\left(\frac{\Lambda - (P_x+\sigma_w^2)}{\sqrt{\frac{2}{n}}(P_x+\sigma_w^2)}\right). \quad (39)$$

도청자가 자신의 채널이 겪는 잡음 분산에 대해 정확히 알 지 못하는 경우 다음의 범위를 고려할 수 있다:

$$\sigma_w^2 \in I \triangleq \left[\frac{1}{\rho}\sigma_n^2, \rho\sigma_n^2\right]. \tag{40}$$

σ_n^2는 실제 잡음 분산 그리고 ρ는 불확실성의 정도(degree of uncertainty)를 나타낸다. 이 경우 $(\mathbb{P}_{\mathrm{FA}}, \mathbb{P}_{\mathrm{MD}})$는 아래와 같이 표현될 수 있다:

$$\begin{aligned}\mathbb{P}_{\mathrm{FA}} &= \max_{\sigma_w^2 \in I} Q\left(\frac{\Lambda - \sigma_w^2}{\sqrt{\frac{2}{n}}\sigma_w^2}\right) \\ &= Q\left(\frac{\Lambda - \rho\sigma_w^2}{\sqrt{\frac{2}{n}}\rho\sigma_w^2}\right),\end{aligned} \tag{41}$$

$$\begin{aligned}\mathbb{P}_{\mathrm{MD}} &= 1 - \min_{\sigma_w^2 \in I} Q\left(\frac{\Lambda - (P_x + \sigma_w^2)}{\sqrt{\frac{n}{2}}(P_x + \sigma_w^2)}\right) \\ &= 1 - Q\left(\frac{\Lambda - \left(P_x + \frac{1}{\rho}\sigma_w^2\right)}{\sqrt{\frac{2}{n}}\left(P_x + \frac{1}{\rho}\sigma_w^2\right)}\right).\end{aligned} \tag{42}$$

수식 (41), (42)를 n에 대해서 정리하면 아래의 결과를 얻을 수 있다:

$$n = \frac{\rho Q^{-1}(\mathbb{P}_{\mathrm{FA}}) - \left(\frac{P_x}{\sigma_n^2} - \frac{1}{\rho}\right) Q^{-1}(1 - \mathbb{P}_{\mathrm{MD}})}{\left[\frac{P_x}{\sigma_n^2} - \left(\rho - \frac{1}{\rho}\right)\right]^2}. \tag{43}$$

수식 (43)으로부터 SNR = P_x/σ_n^2 값이 $\left(\rho - \frac{1}{\rho}\right)$에 접근할수록 n이 ∞에 가까워진다는 점을 알 수 있다. 즉, $P_x \le \left(\rho - \frac{1}{\rho}\right)\sigma_n^2$의 경우 도청자가 아무리 채널을 오랫동안 관찰하더라도 LRT 검출 알고리즘이 견뢰하지 않음을 의미한다. SNR_{wall}을 이용한 분석을 통해 도청자가 자신의 잡음 분산을 모르는 경우 양의 전송률을 얻을 수 있음을 아래의 정리를 통해 보일 수 있다.

Theorem 2[9]: 도청자가 도청 AWGN 채널의 잡음 분산을 정확히 알지 못하는 경우 다음의 전송률을 얻을 수 있다:

$$R_{pr} = \log_2\left(1 + \left(\rho - \frac{1}{\rho}\right)\frac{\sigma_n^2}{\sigma_b^2}\right). \tag{44}$$

송신 신호가 가우시안 분포를 따를 때, 적법 AWGN 채널의 용량이 최대화되므로 송신 신호와 각 채널의 잡음이 다음의 분포를 따른다고 가정한다:

$$x[i] \sim \mathcal{CN}(0, P_x), \tag{45}$$

$$n_b[i] \sim \mathcal{CN}(0, \sigma_b^2), \tag{46}$$

$$n_w[i] \sim \mathcal{CN}(0, \sigma_w^2). \tag{47}$$

이 때 분산 σ_w^2은 범위 $I \triangleq \left[\frac{1}{\rho}\sigma_n^2, \rho\sigma_n^2\right]$에 균등하게 분포해 있다. 도청자가 LRT 알고리즘을 사용해 검출하는 경우, 다음과 같이 정리할 수 있다:

$$\begin{aligned}&\frac{\mathbb{P}_1 \triangleq \prod_{i=1}^n f(y[i]|\mathcal{H}_1)}{\mathbb{P}_0 \triangleq \prod_{i=1}^n f(y[i]|\mathcal{H}_0)} \underset{D_0}{\overset{D_1}{\gtrless}} 1, \\ &\Leftrightarrow \prod_{i=1}^n \left[\frac{1}{\pi(P_x + \sigma_w^2)} \exp\left\{-\frac{|y[i]|^2}{P_x + \sigma_w^2}\right\}\right] \\ &\qquad \underset{D_0}{\overset{D_1}{\gtrless}} \prod_{i=1}^n \left[\frac{1}{\pi\sigma_w^2} \exp\left\{-\frac{|y[i]|^2}{\sigma_w^2}\right\}\right], \\ &\Leftrightarrow -n\log\left(\pi(P_x + \sigma_w^2)\right) - \frac{1}{P_x + \sigma_w^2}\sum_{i=1}^n |y[i]|^2 \\ &\qquad \underset{D_0}{\overset{D_1}{\gtrless}} -n\log(\pi\sigma_w^2) - \frac{1}{P_x}\sum_{i=1}^n |y[i]|^2, \\ &\Leftrightarrow T(\mathbf{y}) \underset{D_0}{\overset{D_1}{\gtrless}} \Lambda.\end{aligned} \tag{48}$$

위 수식에서 검정 통계량 $T(\mathbf{y})$와 임계치 값 Λ는 다음과 같다:

$$T(\mathbf{y}) = \frac{1}{n}\mathbf{y}^{\mathrm{H}}\mathbf{y} = \frac{1}{n}\sum_{i=1}^n |y[i]|^2, \tag{49}$$

$$\Lambda = \frac{(P_x + \sigma_w^2)\sigma_w^2}{P_x} \cdot \log\left(\frac{P_x + \sigma_w^2}{\sigma_w^2}\right). \tag{50}$$

각 가설에서 $T(\mathbf{y})$가 자유도 $2n$의 카이제곱 분포를 따르기 때문에 오 경보 확률 $\mathbb{P}_{\mathrm{FA}}$과 탐지 확률 $\mathbb{P}_{\mathrm{D}}$은 아래와 같고,

$$\begin{aligned}\mathbb{P}_{\mathrm{FA}} &\triangleq \Pr(T(\mathbf{y}) > \Lambda | \mathcal{H}_0) \\ &= \Pr\left(\frac{1}{n}\cdot\frac{\sigma_w^2}{2}\sum_{i=1}^{2n} V_i^2 > \Lambda\right) \\ &= Q_{\chi^2_{2n}}\left(\frac{2n\Lambda}{\sigma_w^2}\right),\end{aligned} \tag{51}$$

$$\begin{aligned}\mathbb{P}_{\mathrm{D}} &\triangleq \Pr(T(\mathbf{y}) > \Lambda | \mathcal{H}_1) \\ &= \Pr\left(\frac{1}{n}\cdot\frac{P_x+\sigma_w^2}{2}\sum_{i=1}^{2n} V_i^2 > \Lambda\right) \\ &= Q_{\chi^2_{2n}}\left(\frac{2n\Lambda}{P_x+\sigma_w^2}\right),\end{aligned} \tag{52}$$

다음의 극한값을 취한다:

$$\lim_{n\to\infty}\mathbb{P}_{\mathrm{FA}} = \begin{cases}0, & \text{if} \quad \Lambda > \sigma_w^2 \\ 1, & \text{if} \quad \Lambda < \sigma_w^2\end{cases}, \tag{53}$$

$$\lim_{n\to\infty}\mathbb{P}_{\mathrm{D}} = \begin{cases}0, & \text{if} \quad \Lambda > P_x+\sigma_w^2 \\ 1, & \text{if} \quad \Lambda < P_x+\sigma_w^2\end{cases}. \tag{54}$$

수식 (51)과 (52)에서 V_i는 $\mathcal{N}(0,1)$을 따르는 독립 항등 확률변수이다. 도청자의 오류 확률의 합 ξ을 1로 수렴시키면서 출력 P_x를 최대화하기 위해서는 $\mathbb{P}_{\mathrm{FA}}$를 1로 만들거나 $\mathbb{P}_{\mathrm{D}}$를 0으로 만들어야 한다. $\Lambda \geq \rho\sigma_n^2$라고 가정하면, $P_x < \left(\rho - \frac{1}{\rho}\right)\sigma_n^2$의 조건 아래서 $\sigma_w^2 = \frac{1}{\rho}\sigma_n^2$ 값이 $\mathbb{P}_{\mathrm{D}}$을 0으로 만드는 것을 알 수 있다. 즉 $\frac{P_x}{\sigma_n^2} = \left(\rho - \frac{1}{\rho}\right)$가 SNR_{wall}이 되고 송신 출력이 $\left(\rho - \frac{1}{\rho}\right)\sigma_n^2$ 보다 낮을 때 다음의 전송률을 얻을 수 있다:

$$\begin{aligned}R_{pr} &= \lim_{n\to\infty}\log_2\left(1+\frac{P_x}{\sigma_b^2}\right) \\ &= \log_2\left(1+\left(\rho-\frac{1}{\rho}\right)\frac{\sigma_n^2}{\sigma_b^2}\right).\end{aligned} \tag{55}$$

위의 정리에서 유의할 점은 도청자가 불확실한 잡음 분산 정보를 가지고 있을 때, LRT가 최적의 검출 알고리즘이 아닐 수 있다는 것이다. 즉 수식 (55)의 전송률 R_{pr}은 채널 용량 C_{pr}과는 다른 값으로 생각해야 한다. 다음으로 상호 정보량 관점에서의 최적의 송신 신호 분포에 대해서 논한다.

2.4 송신 신호 최적화

본 절에서는 상대 엔트로피의 비대칭성에서 유도되는 두 개의 다른 은닉 제약(constraint)을 분석하고 은닉성을 유지하면서 적법 송수신단 간의 상호 정보량을 최대화하는 최적의 송신 신호 분포를 연구한 [10]과 [15]의 결과를 소개한다.

상대 엔트로피의 비대칭성 때문에 각 가설에 해당하는 분포도 $\mathbb{P}_0 = \mathbb{P}_w^{\otimes n} = \mathcal{N}(\mathbf{0}, \sigma_w^2\mathbf{I})$, $\mathbb{P}_1 = \mathbb{P}_s^{\otimes n} = \mathcal{N}(\mathbf{0}, (P_x+\sigma_w^2)\mathbf{I})$에 대해서 다음 두 개의 다른 상대 엔트로피를 구할 수 있다:

$$\begin{aligned}\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_0\|\mathbb{P}_1) = \frac{n}{2}\Bigg[&\log\left(1+\frac{P_x}{\sigma_w^2}\right) \\ &-\left(1+\left(\frac{P_x}{\sigma_w^2}\right)^{-1}\right)^{-1}\Bigg],\end{aligned} \tag{56}$$

$$\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_1\|\mathbb{P}_0) = \frac{n}{2}\left[\frac{P_x}{\sigma_w^2} - \log\left(1+\frac{P_x}{\sigma_w^2}\right)\right]. \tag{57}$$

두 개의 상대 엔트로피의 차이를 출력 P_x에 대한 함수 $f(P_x)$로 아래와 같이 정의하고:

$$\begin{aligned}f(P_x) &\triangleq \mathcal{D}_{\mathrm{KL}}(\mathbb{P}_1\|\mathbb{P}_0) - \mathcal{D}_{\mathrm{KL}}(\mathbb{P}_0\|\mathbb{P}_1) \\ &= \frac{n}{2}\left[\frac{P_x}{\sigma_w^2} - \left(\frac{P_x}{\sigma_w^2}+1\right)^{-1} + 1\right],\end{aligned} \tag{58}$$

$f(P_x)$을 P_x에 대해 미분하면 다음의 결과를 얻을 수 있다:

$$\frac{\partial f(P_x)}{P_x} = \frac{n}{2\sigma_w^2} + \frac{n}{2\sigma_w^2\left(\frac{P_x}{\sigma_w^2}+1\right)^2} \geq 0. \tag{59}$$

최종적으로 아래의 관계식이 유도된다[10]:

$$\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_0\|\mathbb{P}_1) \leq \mathcal{D}_{\mathrm{KL}}(\mathbb{P}_1\|\mathbb{P}_0). \tag{60}$$

$\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_0\|\mathbb{P}_1)$와 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_1\|\mathbb{P}_0)$ 모두 수식 (4)의 핀스커 부등식을 만족하기 때문에 수식 (3)의 은닉 조건을 상대 엔트로피를 사용해 다음과 같이 표현할 수 있다:

$$\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_0\|\mathbb{P}_1) \leq 2\epsilon^2, \tag{61}$$

$$\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_1\|\mathbb{P}_0) \leq 2\epsilon^2. \tag{62}$$

2.4.1 가우시안 분포의 최적성

우선 첫번째 항에서는 수식 (62)의 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_1\|\mathbb{P}_0) = \mathcal{D}_{\mathrm{KL}}(\mathbb{P}_s\|\mathbb{P}_{\mathrm{w}}) \leq 2\epsilon^2$을 은닉성 제약으로 사용했을 때, 적법 송수신단 간의 상호 정보량을 최대화하는 송신 신호의 분포가 가우시안을 따른다는 정리를 소개한다.

Theorem 3[10]: $\mathbb{P}_w = \mathcal{N}(0, \sigma_w^2)$이고 $\mathbb{P}_s$의 분산이 $P_x + \sigma_w^2$일때, 상대 엔트로피 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_s \| \mathbb{P}_w)$을 최소화하는 확률 분포 $\mathbb{P}_s$는 $\mathcal{N}(0, P_x + \sigma_w^2)$을 따른다.

위 정리를 최적화 문제로 표현하면 다음과 같다:

$$\arg\min_{\mathbb{P}_s} \ \mathcal{D}_{\mathrm{KL}}(\mathbb{P}_s \| \mathbb{P}_w), \tag{63-1}$$

$$\text{subject to} \quad \mathbb{E}[|y[i]|^2] = P_x + \sigma_w^2, \tag{63-2}$$

$$\int_{-\infty}^{\infty} f_s(y[i])\, dy = 1, \tag{63-3}$$

$$f_s(y[i]) \geq 0. \tag{63-4}$$

위 문제에서 $f_s(y)$는 $\mathbb{P}_s$의 확률 밀도 함수를 나타낸다. 편의를 위해 $y[i]$에서 인덱스 표기를 생략하고, 라그랑주 방법(Lagrangian method)을 사용했을 때 다음의 식을 얻을 수 있다:

$$\begin{aligned} &\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_s \| \mathbb{P}_w) + \lambda \left[\int_{-\infty}^{\infty} f_s(y) dy - 1 \right] \\ &\qquad + \nu \left[\int_{-\infty}^{\infty} y^2 f_s(y) dy - (P_x + \sigma_w^2) \right] \\ &= \int_{-\infty}^{\infty} \mathcal{L}(y, f_s(y), \lambda, \nu) dy - [\lambda - \nu(P_x + \sigma_w^2)]. \end{aligned} \tag{64}$$

범함수(functional) $\mathcal{L}(y, f_s(y), \lambda, \nu)$에 대한 최적화 컨디션(optimality condition) $\frac{\partial \mathcal{L}(y, f_s(y), \lambda, \nu)}{\partial f_s(y)} = 0$을 계산하면 $f_s(y)$를 $\mathbb{P}_w$의 확률 밀도 함수인 $f_w(y)$와 라그랑주 승수들 λ, ν의 식으로 표현할 수 있다:

$$f_s(y) = f_w(y) e^{-\nu y^2 - \lambda - 1}. \tag{65}$$

제약 (63-3)과 (63-2)를 계산하면 라그랑주 승수들을 아래와 같이 나타낼 수 있다:

$$e^{-\lambda - 1} = \sqrt{1 + 2\nu\sigma_w^2}, \tag{66}$$

$$\nu = -\frac{1}{2\sigma_w^2} + \frac{1}{2(P_x + \sigma_w^2)}. \tag{67}$$

수식 (66), (67)을 (65)에 대입하면 최종적으로 다음의 결과를 얻을 수 있다:

$$f_s(y) = \frac{1}{\sqrt{2\pi(P_x + \sigma_w^2)}} e^{\frac{y^2}{2(P_x + \sigma_w^2)}}. \tag{68}$$

고정된 분산에 대해서 엔트로피를 최대화하는 확률변수가 가우시안 이라는 점[13]을 이용해서 정리 3에서 다음의 정리가 유도된다.

Theorem 4[10]: $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_s \| \mathbb{P}_w) \leq 2\epsilon^2$을 은닉 조건으로 사용할 때, 적법 송수신단 간의 상호 정보량 $I(\mathbf{x}; \mathbf{z})$을 최대화하는 0의 평균을 가지는 가우시안 송신 신호의 출력 P_x^*은 아래의 수식을 만족한다:

$$\frac{1}{2}\left(\frac{P_x^*}{\sigma_w^2} + \log \frac{\sigma_w^2}{P_x^* + \sigma_w^2} \right) = 2\epsilon^2. \tag{69}$$

가우시안 송신 신호를 가정하고, $P_y \triangleq P_x + \sigma_w^2$라고 정의하면 $\frac{\partial \mathcal{D}_{\mathrm{KL}}(\mathbb{P}_s \| \mathbb{P}_w)}{\partial P_y} = \frac{1}{2}\left(\frac{P_y - \sigma_w^2}{P_y \sigma_w^2} \right) \geq 0$이므로 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_s \| \mathbb{P}_w)$가 P_y, 나아가 P_x에 대해서 단조증가(monotonically increase)함을 알 수 있다. 아래의 수식을 만족하는 P_x의 특정한 값을 P_x^ϵ라고 표기한다:

$$\frac{1}{2}\left[\frac{P_x^\epsilon}{\sigma_w^2} - \log\left(1 + \frac{P_x^\epsilon}{\sigma_w^2} \right) \right] = 2\epsilon^2. \tag{70}$$

은닉 조건이 없을 경우 $I(\mathbf{x}; \mathbf{z})$ 역시 송신 출력 P_x에 대해 단조증가 하기 때문에, $P_x^* = P_x^\epsilon$ 임을 알 수 있다. 즉 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_s \| \mathbb{P}_w) \leq 2\epsilon^2$을 은닉 조건으로 사용하는 경우 수식 (70)을 만족하는 송신 출력을 가지는 가우시안 신호가 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_s \| \mathbb{P}_w)$을 최소화 하면서 동시에 $I(\mathbf{x}; \mathbf{z})$을 최대화하는 최적의 송신 기법이라는 것을 알 수 있다[10].

2.4.2 가우시안 분포의 비최적성

수식 (61)의 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w \| \mathbb{P}_s) \leq 2\epsilon^2$를 은닉 조건으로 사용할 경우 위의 정리들과는 상반된 결과를 얻게 된다.

Theorem 5[15]: $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w \| \mathbb{P}_s) \leq 2\epsilon^2$이 은닉 조건일 때, 송신 신호가 평균 μ_x와 분산 σ_x^2을 가지는 가우시안 분포를 따르면 송수신단 간의 최대 상호 정보량을 얻을 수 없다.

송신 신호의 확률 분포의 밀도 함수를 $f(x)$라고 할 때, 위의 정리는 $f(x) = \mathcal{N}(0, P_x)$가 아래의 최적화 문제의 답이 아닌 것을 의미한다:

$$\arg\max_{f(x), P_x} \ I(\mathbf{x}; \mathbf{z}), \tag{71-1}$$

$$\text{subject to} \quad \mathbb{E}[\|\mathbf{x}\|_2^2] = P_x, \tag{71-2}$$

$$\int_{-\infty}^{\infty} f(x) dx = 1, \tag{71-3}$$

$$f(x) \geq 0, \tag{71-4}$$

$$\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w \| \mathbb{P}_s) \leq 2\epsilon^2. \tag{71-5}$$

$\sigma_w^2 = \sigma_b^2$의 특별한 경우를 고려했을 때, 가설 $\mathcal{H}_1$이 참일 경우 $\mathbf{z}$와 $\mathbf{y}$는 동일한 분포를 따르게 된다. $I(\mathbf{x};\mathbf{z}) = h(\mathbf{z}) - h(\mathbf{z}|\mathbf{x}) = h(\mathbf{z}) - h(\mathbf{n}_b) = h(\mathbf{y}) - h(\mathbf{n}_w)$ 때문에, $I(\mathbf{x};\mathbf{z})$를 최대화하는 밀도 함수 $f(x)$를 찾는 것은 $h(\mathbf{y})$를 최대화하는 를 찾는 것과 동등하다. 따라서 아래의 동등한 최적화 문제를 고려할 수 있다:

$$\arg\max_{f_s(y[i])} \; h(y), \tag{72-1}$$

$$\text{subject to} \int_{-\infty}^{\infty} f_s(y[i])dy = 1, \tag{72-2}$$

$$\mathbb{E}[\|\mathbf{y}\|_2^2] = P_y, \tag{72-3}$$

$$\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w \| \mathbb{P}_s) \le 2\epsilon^2, \tag{72-4}$$

$$f_s(y[i]) \ge 0. \tag{72-5}$$

위의 문제에서 $P_y = P_x + \sigma_w^2$이고 라그랑주 방법을 이용해 다음의 범함수를 얻을 수 있다:

$$\begin{aligned}\mathcal{L}(y, f_s(y), \lambda_1, \lambda_2, \lambda_3) &= f_s(y)\log\frac{1}{f_w(y)} + \lambda_1 f_w(y)\log\frac{f_w(y)}{f_s(y)} \\ &+\lambda_2 f_s(y) + \lambda_3 y^2 f_s(y).\end{aligned} \tag{73}$$

수식 (73)을 $f_s(y)$로 미분하면 다음의 최적화 조건을 얻을 수 있다:

$$\log\frac{1}{f_s(y)} - 1 - \lambda_1\frac{f_w(y)}{f_s(y)} + \lambda_2 + \lambda_3 y^2 = 0. \tag{74}$$

만약 은닉 조건이 없을 경우, (71-2)-(71-4)의 제약들을 만족하는 원래의 최적화 문제 (71)의 답은 0의 평균과 P_y의 분산을 가지는 가우시안 분포이다. 따라서 $f_s(y) \sim \mathcal{N}(0, P_y)$는 아래의 조건을 충족해야만 한다:

$$-\log\frac{1}{f_s(y)} - 1 + \nu_1 + \nu_2 y^2 = 0. \tag{75}$$

수식 (74)와 (75)를 비교하면 $f_s(y)$에 대한 다음의 표현식을 얻을 수 있다:

$$f_s(y) = \frac{\lambda_1 f_w(y)}{(\lambda_2 - \nu_1) + (\lambda_3 - \nu_2)y^2}. \tag{76}$$

위 식에서 $\mathbb{P}_s$가 가우시안을 따르면서 $f_s(y)$가 (72-2)의 제약을 만족하려면 다음의 두 식이 성립해야만 한다:

$$\lambda_3 - \nu_2 = 0, \tag{77}$$

$$\frac{\lambda_1}{\lambda_2 - \nu_1} = 1. \tag{78}$$

하지만 이 경우 $\mathbb{P}_s$의 분산이 σ_w^2와 동일해지기 때문에 출력에 대한 조건을 만족하지 못한다. 따라서 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w \| \mathbb{P}_s) \le 2\epsilon^2$의 은닉 조건 아래에서는 상호 정보량 $I(\mathbf{x};\mathbf{z})$을 최대화하는 최적의 송신 신호 분포가 가우시안이 아닌 것을 알 수 있다.

다음 절에서는 앞서 논의되었던 AWGN 채널에서 은닉성을 얻을 수 있는 실용적인 채널 코딩 기법에 대해 논한다.

2.5 OSS 코드

본 논문의 마지막 절에서는 희소 중첩 코드(sparse superposition codes: SPARCs)의 한 종류로 최근에 제안된 OSS 코드에 대해 소개한다. SPARCs의 코드워드는 희소한 메시지 벡터의 0이 아닌 원소 인덱스에 해당하는 사전 행렬(dictionary matrix)의 열 벡터들을 선형 결합하여 생성된다[16]. SPARCs는 AWGN 채널에서 새넌의 한계(Shannon-limit) 용량을 달성하나, 길이가 짧아질수록 복호 성능이 저하된다는 단점이 있다. OSS 코드 역시 사전 행렬의 열 벡터들의 중첩으로 코드 워드들을 생성한다는 공통점이 있으나, 사전 행렬로 유니테리 행렬(unitary matrix)을 사용하고 각 부분 코드 워드들이 서로 직교(orthogonal)하는 특성이 있다[11].

2.5.1 OSS 코드의 순차적 직교 부호와 저 복잡도 복호 방식

L개의 층으로 이루어진 OSS 코드의 부호기는 그림 2와 같다. 부호기는 각 층에서 순차적으로 $N \in \mathbb{Z}^+$의 길이를 가진 희소 부분 부호 벡터들 $\{\mathbf{x}_\ell\}_{\ell=1}^{L}$을 만든다. 첫 번째 층에서 0이 아닌 원소들이 선택될 수 있는 인덱스 후보 집합 $\mathcal{N}_1 = [N] = \{1, 2, \ldots, N\}$을 정의한다. 이

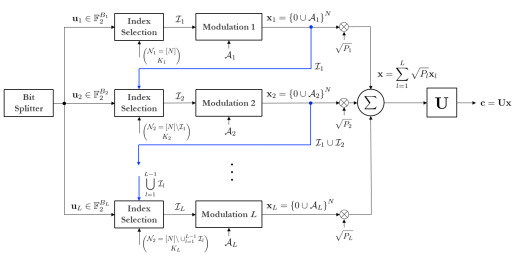


그림 2. OSS 코드의 순차적 직교 부호기
Fig. 2. Successive orthogonal encoder of OSS codes.

집합에서 K_1개의 인덱스를 무작위로 추출해 인덱스 서포트 집합 $\mathcal{I}_1 = \{i_{1,1}, i_{1,2}, \dots, i_{1,K_1}\}$을 만들고 원소 $\{x_{1,n}: n \in \mathcal{I}_1\}$에 성상도 $\mathcal{A}_1$의 값들을 균등하게 할당해 준다. 다음 층에서는 이전 층에서 사용되었던 인덱스를 배제하기 위하여 새로운 인덱스 후보 집합 $\mathcal{N}_2 = [N]\backslash\mathcal{I}_1$에서 K_2개를 선택해 $\mathcal{A}_2$의 값들을 할당하여 $\mathbf{x}_2$를 생성한다. 마지막 L번째 층에서 만들어지는 $\mathbf{x}_L$은 $\mathcal{N}_L = [N]\backslash\left(\cup_{\ell=1}^{L-1}\mathcal{I}_\ell\right)$에서 선택된 K_L개의 0이 아닌 값들을 가지게 된다. 이러한 연속적인 부호화 방식을 통해 생성된 부분 벡터 $\mathbf{x}_\ell$들은 이전 층에서 사용된 인덱스를 제외한 위치에서만 0이 아닌 값을 할당받는다. 따라서, $\mathcal{I}_\ell \cap \{\cup_{k=1}^{\ell-1}\mathcal{I}_k\} = \phi$로 서로 다른 층에서 생성된 부분 벡터들은 직교성을 띠게 된다:

$$\mathbf{x}_i^{\mathrm{T}}\mathbf{x}_j = 0, \quad i \neq j \in [L]\ . \tag{79}$$

최종적으로 채널에 보내지는 부호 워드 $\mathbf{c} \in \mathbb{R}^N$는 L개의 부분 벡터 $\mathbf{x}_\ell$들의 가산 중첩 $\mathbf{x} = \sum_{\ell=1}^{L}\sqrt{P_\ell}\mathbf{x}_\ell$과 직교 행렬 $\mathbf{U} \in \mathbb{R}^{N\times N}$의 곱으로 생성된다:

$$\mathbf{U} = \begin{bmatrix} | & | & & | \\ \mathbf{u_1} & \mathbf{u_2} & \cdots & \mathbf{u_N} \\ | & | & & | \end{bmatrix}, \tag{80}$$

$$\mathbf{c} = \mathbf{U}\mathbf{x} = \sum_{j\in\mathcal{J}=\{n:x_n\neq 0\}} \mathbf{u}_j\mathbf{x}_j\,. \tag{81}$$

이때 $\sqrt{P_\ell}$는 각각의 부분 벡터의 출력 컨트롤 계수를 나타내고, $\mathbf{u}_j$는 사전 행렬 $\mathbf{U}$의 j번째 열 벡터를 의미한다. ℓ번째 층에서 $\binom{|\mathcal{N}_\ell|}{K_\ell}$개의 인덱스 조합이 가능하기 때문에 부호화 되는 정보 비트는 다음과 같다:

$$B = \sum_{\ell=1}^{L}\left\lfloor \log_2\left(\binom{|\mathcal{N}_\ell|}{K_\ell}\cdot|\mathcal{A}_\ell|^{K_\ell}\right)\right\rfloor. \tag{82}$$

따라서 채널을 N번 사용할 때 전송되는 부호율은 아래와 같다:

$$R = \frac{\sum_{\ell=1}^{L}\left\lfloor \log_2\left(\binom{|\mathcal{N}_\ell|}{K_\ell}\cdot|\mathcal{A}_\ell|^{K_\ell}\right)\right\rfloor}{N}. \tag{83}$$

층의 개수 L과 ℓ번째 층에서의 희소도 $K_\ell \triangleq \|\mathbf{x}_\ell\|_0$ 그리고 성상도 을 조정할 수 있기에, OSS 코드는 부호율을 유연하게 정할 수 있다는 강점이 있다.

다음으로 연속적 서포트 집합 소거를 통한 원소 별 최대 사후 확률 복호(element-wise maximum a posteriori decoding with successive support set cancellation) 방법을 소개한다. 연쇄 법칙을 이용해서 동시 사후 확률은 다음과 같이 표현할 수 있다:

$$\Pr(\mathbf{x}|\mathbf{y}) = \prod_{\ell=1}^{L}\mathrm{P}(\mathbf{x}_\ell|\mathbf{y}, \mathbf{x}_{\ell-1}, \dots, \mathbf{x}_2, \mathbf{x}_1)\,. \tag{84}$$

$\mathcal{I}_{\ell-1}, \mathcal{I}_{\ell-2}, \dots, \mathcal{I}_2, \mathcal{I}_1$가 $\mathbf{x}_l$를 복호 하는 데 필요한 충분한 정보를 갖고 있기 때문에, 수식 (84)는 아래처럼 표현될 수 있다.

$$\Pr(\mathbf{x}|\mathbf{y}) = \prod_{\ell=1}^{L}\mathrm{P}(\mathbf{x}_\ell|\mathbf{y}, \mathcal{I}_{\ell-1}, \dots, \mathcal{I}_2, \mathcal{I}_1)\,. \tag{85}$$

제안하는 반복적인 복호 방식은 각 층 ℓ에서 사용된 인덱스 서포트 집합 $\hat{\mathcal{I}}_\ell$을 추정하고 다음 단계를 위해 사전 분포를 업데이트 한다. $\ell-1$번의 반복 후 $\hat{\mathcal{I}}_{\ell-1}, \dots, \hat{\mathcal{I}}_1$를 정확하게 추정했다는 가정하에 복호기는 $\hat{\mathcal{I}}_\ell$을 찾기 위해 원소 별 최대 사후 확률 복호를 한다. 이전 단계에서 배제되지 않은 후보 인덱스의 조합을 $\widehat{\mathcal{N}}_\ell = [N]\backslash\cup_{k=1}^{\ell-1}\hat{\mathcal{I}}_k$라고 정의하면 $\mathbf{x}_\ell$의 조건부 사후 확률은 아래와 같다:

$$\begin{aligned}&\Pr(\mathbf{x}_\ell|\boldsymbol{y}, \mathcal{I}_{\ell-1}, \dots, \mathcal{I}_2, \mathcal{I}_1)\\ &= \prod_{n\in\widehat{\mathcal{N}}_\ell}\frac{\Pr(y_n|x_{\ell,n})\Pr(x_{\ell,n})}{\Pr(y_n)}\mathbf{1}_{\left\{\sum_{n\in\widehat{\mathcal{N}}_\ell}\mathbf{1}_{\{x_{\ell,n}\in\mathcal{A}_\ell\}}=K_\ell\right\}}.\end{aligned} \tag{86}$$

사후 확률 값이 가장 큰 원소 인덱스를 찾기 위해 복호기는 y_n이 주어졌을 때 사건 $\{n \in \mathcal{I}_\ell\}$의 조건부 확률을 계산한다:

$$\begin{aligned}&\Pr(n \in \mathcal{I}_\ell|y_n)\\ &\quad= \frac{\Pr(y_n|x_{\ell,n}\in\mathcal{A}_\ell)\Pr(x_{\ell,n}\in\mathcal{A}_\ell)}{\Pr(y_n)}.\end{aligned} \tag{87}$$

수식 (87)에서 $x_{\ell,n}$의 확률 함수는 다음과 같고

$$\Pr(x_{\ell,n}\notin\mathcal{A}_\ell) = 1 - \frac{K_\ell}{|\widehat{\mathcal{N}}_\ell|}, \tag{88}$$

$$\Pr(x_{\ell,n}\in\mathcal{A}_\ell) = \frac{K_\ell}{|\widehat{\mathcal{N}}_\ell|}, \tag{89}$$

우도 함수는 아래의 수식으로 표현할 수 있다:

$$\begin{aligned}&\Pr\left(y_n|x_{\ell,n}\in\mathcal{A}_\ell\right)\\&=\frac{1}{|\mathcal{A}_\ell|}\sum_{\ell=1}^{|\mathcal{A}_\ell|}\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{\left|y_n-a_{\ell,j}\right|^2}{2\sigma^2}\right).\end{aligned}\tag{90}$$

수식 (87)-(90)을 이용하여 $\Pr(y_n)$을 계산할 수 있다:

$$\begin{aligned}\Pr(y_n)&=\Pr\left(y_n|x_{\ell,n}\in\mathcal{A}_\ell\right)\Pr\left(x_{\ell,n}\in\mathcal{A}_\ell\right)\\&\quad+\Pr\left(y_n|x_{\ell,n}\notin\mathcal{A}_\ell\right)\Pr\left(x_{\ell,n}\notin\mathcal{A}_\ell\right)\\&=\sum_{j=1}^{|\mathcal{A}_\ell|}\frac{1}{|\mathcal{A}_\ell|}\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{|y_n-a_{\ell,j}|^2}{2\sigma^2}}\left(\frac{K_\ell}{N-\sum_{i=1}^{\ell-1}K_i}\right)\\&\quad+\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{|y_n|^2}{2\sigma^2}}\left(1-\frac{K_\ell}{N-\sum_{i=1}^{\ell-1}K_i}\right).\end{aligned}\tag{91}$$

$\mathbf{x}_\ell$의 희소성 조건 $\sum_{n\in\hat{\mathcal{N}}_\ell}\mathbf{1}_{\{x_{\ell,n}\in\mathcal{A}_\ell\}}=K_\ell$을 만족하기 위해서 복호기는 집합 $\hat{\mathcal{N}}_\ell$에서 중 사후 확률 값이 가장 큰 K_ℓ 원소들을 오더링(ordering) 해서 $\hat{\jmath}_\ell$의 추정 값을 얻는다:

$$\hat{\jmath}_\ell=\left\{\hat{\imath}_{\ell,1},\hat{\imath}_{\ell,2},\dots,\hat{\imath}_{\ell,K_\ell}\right\}.\tag{92}$$

마지막으로 추정된 $\hat{\jmath}_\ell$을 가지고 성상도를 찾기 위해 원소 별로 최대 사후 확률 복호를 진행한다:

$$\begin{aligned}\hat{x}_{\ell,n}&=\arg\max_{a_{\ell,j}\in\mathcal{A}_\ell}\ \Pr\left(x_{\ell,n}=a_{\ell,j}|y_n,x_n\in\hat{\jmath}_\ell\right)\\&=\arg\min_{a_{\ell,j}\in\mathcal{A}_\ell}\ \left|y_n-a_{\ell,j}\right|^2.\end{aligned}\tag{93}$$

위의 과정을 순차적으로 진행하여 총 L개의 부분 부호 벡터들을 검출할 때까지 반복한다.

2.5.2 OSS 코드의 은닉성

본 항에서는 OSS 코드를 사용할 때 은닉 통신이 가능하다는 것을 보인다. 부호기에서 단위 행렬 $\mathbf{I}$를 유니테리 사전 행렬로 사용한다고 가정하면, 최종적으로 채널에 전송되는 코드 워드는 $\mathbf{c}=\mathbf{x}$가 된다. ℓ번째 층에서 성상도 $\mathcal{A}_\ell=\{a_{\ell,1},\dots,a_{\ell,K_\ell}\}$를 사용할 때 부분 메시지 벡터 및 코드 워드 $\mathbf{x}_\ell$의 출력은 다음과 같다:

$$\mathbb{E}[\|\mathbf{x}_\ell\|_2^2]=\frac{1}{N}\left[K_\ell\left(\frac{\sum_{i=1}^{|\mathcal{A}_\ell|}|a_{\ell,i}|^2}{|\mathcal{A}_\ell|}\right)\right].\tag{94}$$

모든 부분 코드 워드가 직교성을 유지하기 때문에, 최종 코드 워드의 평균 출력을 P_c이라고 표기하고 아래와 같이 계산할 수 있다:

$$\begin{aligned}P_{\mathrm{c}}&=\mathbb{E}[\|\mathbf{x}\|_2^2]=\sum_{\ell=1}^{L}\mathbb{E}[\|\mathbf{x}_\ell\|_2^2]\\&=\sum_{\ell=1}^{L}\frac{1}{N}\left[K_\ell\left(\frac{\sum_{i=1}^{|\mathcal{A}_\ell|}|a_{\ell,i}|^2}{|\mathcal{A}_\ell|}\right)\right].\end{aligned}\tag{95}$$

수식 (95)의 출력 P_c를 수식 (11)의 P_x에 대입하면 수식 (3)의 은닉성 조건을 만족하는 것을 보일 수 있다.

Ⅲ. 결 론

본 논문에서는 AWGN 채널에서 은닉 통신 문제의 수학적인 모델링과 전송 가능한 비트의 정보 이론적 한계인 제곱근 법칙에 대한 관련 연구 결과를 기술하였다. 주요한 점은 전송 가능한 비트가 $o(\sqrt{n})$을 따르나 도청 채널의 잡음 레벨(noise level)에 대한 부분 정보가 있는 경우 $\mathcal{O}(\sqrt{n})$을 달성할 수 있다는 결과이다. 또한 도청자가 채널 잡음을 정확히 모르는 특수한 경우, 점근 영역(asymptotic regime)에서 0이 아닌 전송률을 얻을 수 있다는 연구를 소개하였다. 추가로, 상호 정보량을 최대화하는 최적의 송신 신호 분포가 은닉 조건에 따라 상이하다는 결과를 서술하고 최근에 제안된 은닉성을 만족하는 부호화 변조(coded modulation) 기법인 OSS 코드를 소개하였다.

은닉성을 유지하기 위해서는 도청자의 가설 검정 성능을 제한하기 위해 블록 길이가 증가할수록 $\mathcal{D}_{\mathrm{KL}}(\mathbb{P}_w\|\mathbb{P}_s)$이 감소해야 한다. 직관적으로 이는, 통신의 여부에 따른 각 가설의 확률 분포 $\mathbb{P}_w$와 $\mathbb{P}_s$가 거의 동일해져야 한다는 것을 의미하고, 송신 신호가 잡음에 잘 섞일 수 있게 출력이 낮아져야 함을 알 수 있다. 출력을 낮추기 위해 [8]에서는 $\mathcal{O}(\sqrt{n})$의 출력을 따르는 코드 워드들을 포함한 코드북을 역의 증명에 이용하였다. 비슷한 이유로 FHSS 기법에서는 넓은 대역폭을 사용해서 출력을 낮추었다. 이러한 점을 OSS 코드의 구조에 빗대어 생각해보면 은닉이라는 특성이 희소성에 의해서 유도됨을 알 수 있다.

앞으로 다양한 채널 및 통신 환경에서의 은닉 통신 문제와 $o(\sqrt{n})$의 한계를 달성하면서 낮은 복잡도의 복호기를 가진 실용적인 새로운 부호 기법에 관한 활발한 연구가 기대된다.

References

[1] M. Bloch, et al., "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas in Info. Theory*, vol. 2, no. 1, pp. 5-22, Mar. 2021.

[2] A. D. Wyner, "The wire-tap channel," *The Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proc. 6th ACM Int. Symp. Mob. Ad Hoc Netw. Comput.*, 2005.

[4] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," *2014 IEEE Int. Symp. Info. Theory*, 2014.

[5] R. Price, "Further notes and anecdotes on spread-spectrum origins," *IEEE Trans. Commun.*, vol. 31, no. 1, pp. 85-97, Jan. 1983.

[6] C. Cachin, "An information-theoretic model for steganography," *Info. and Comput.*, 2004.

[7] W. Ren, A. Swami, and Q. Zhao, "Coexistence, connectivity and delay in heterogeneous networks," *Proc. 27th Army Sci. Conf.*, 2011.

[8] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas in Commun.*, vol. 31, no. 9, pp. 1921-1930, Sep. 2013.

[9] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics in Sign. Process.*, vol. 9, no. 7, pp. 1195-1205, Oct. 2015.

[10] S. Yan, Y. Cong, S. V. Hanly, and X. Zhou, "Gaussian signalling for covert communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3542-3553, Jul. 2019.

[11] Y. Nam, S. Hong, and N. Lee, "Orthogonal sparse superposition codes," *2020 ISITA*, 2020.

[12] E. Lehmann and J. Romano, *Testing Statistical Hypotheses*, 3rd Ed., Springer, 2005.

[13] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd Ed., John Wiley & Sons, 2002.

[14] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Sel. Topics in Sign. Process.*, vol. 2, no. 1, pp. 4-17, Feb. 2008.

[15] L. Sun, S. Yan, R. Chen, and F. Shu, "On likelihood functions to minimize KL divergence in binary hypothesis testing," *2020 14th ICSPCS*, 2020.

[16] A. Joseph and A. R. Barron, "Least squares superposition codes of moderate dictionary size are reliable at rates up to capacity," *IEEE Trans. Info. Theory*, vol. 58, no. 5, pp. 2541-2557, May 2012.

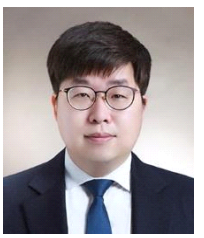
한 동 화 (Donghwa Han)

2020년 5월 : University of Rochester 전기컴퓨터공학 학사

2020년 9월~현재 : 포항 공과대학교 석사과정

<관심분야> 채널 코딩, 은닉 통신

이 남 윤 (Namyoon Lee)



2006년 2월 : 고려대학교 전파통신공학 학사

2008년 2월 : 한국과학기술원 전자공학 석사

2014년 12월 : The University of Texas at Austin 박사

2008년 2월~2011년 6월 : 삼성종합기술 연구원/선임연구원

2014년 11월~2015년 5월 : NOKIA Research Center, Berkeley, USA 선임연구원

2015년 5월~2016년 2월 : Intel Labs, Santa Clara, USA Researcher Scientist

2016년 2월~현재 : 포항공과대학교 조교수, 부교수

<관심분야> 차세대 MIMO 송/수신기, 기계학습 기반 통신 네트워크 설계

[ORCID:0000-0003-4321-4108]