정보이론의 개념 및 응용

김진영 | 김윤현 | 허 준*
광운대학교, 고려대학교*

요 약

정보 이론은 최대한 많은 데이터를 매체에 저장하거나 채널을 통해 통신하기 위해 데이터를 정량화하는 응용 수학의 한 분야이다. 1948년 정보이론은 Shannon의 논문에서 발표되었으며 이 논문을 바탕으로 통신, 신호처리, 네트워크에의 데이터 처리 및 전송에 대한 획기적인 발전을 이루었다. 본 논고에서는 정보의 의미와 엔트로피, 채널 용량에 관한 내용을 다루어 정보이론의 기본 개념을 설명할 것이며, 또한 센서네트워크와 중계 채널 그리고 MIMO 시스템과 다른 분야에서 정보이론이 어떻게 적용되는지 그 응용분야에 대해 다뤄보고자 한다.

I. 서 론

정보 이론(Information theory)은 통신 시스템의 성능을 평가하는 다른 관점을 제시하고, 정보 이론에 대한 연구를 통하여 통신 시스템의 성능 특성에 대한 중요한 관점을 얻을 수 있다. 즉, 정보 이론은 메시지 신호에 포함된 정보의 정량적 측정량을 나타내며, 정보원으로부터 목적지로 이 정보를 전달하기까지의 시스템 용량을 결정할 수 있다. 정보이론의 주요 응용으로 부호화를 그 예로 들 수 있으며, 정보원 부호화의 사용으로 비체계적 리던던시(redundancy)는 채널을 최대 효율로 이용하기 위해 메시지 신호로부터 제거될 수 있다. 또한 부호화 사용을 통해 체계적 리던던시는 완전하지 않은 실제 채널들 때문에 발생하는 오류를 교정할 수 있는 전송 신호를 유도할 수 있다.

정보 이론은 이상적인 혹은 최적의 통신 시스템의 성능 특성을 제공한다. 이상적인 시스템의 성능은 실제 시스템과의 비교를 통해 중요한 기초를 제공한다. 이상적인 시스템의 성능 특성은 더욱 복잡한 전송과 검출을 수행함으로써 얻을 수 있는 성능에 대한 이득을 나타낸다. 다시 말해, 특정 시스템이 전송 또는 저장 가능한 최대 정보량을 이론적으로 계산 가능하게 하여, 실제 시스템에 적용 시 그 기준으로 이용할 수 있다. 또한 암호화 및 데이터 압축 및 전송 분야에도 널리 적용되어 사용된다.

정보 이론의 배경은 Shannon의 제 2정리라고 하는 Shannon의 부호이론 이다. "이것은 만약 정보원이 채널 용량보다 작은 정보율(information rate)을 가지고 있다면, 정보원의 출력이 임의의 작은 오류 확률을 가진 채널을 통하여 전송될 수 있는 부호화 과정이 존재한다는 것이다." 이것은 강력한 제안으로서 Shannon은 잡음이 존재함에도 불구하고 무시해도 좋은 오류가 있는 송신과 수신이 이루어질 수 있는 것을 우리에게 알려준다. 부호화라는 과정 그리고 통신 시스템의 설계와 성능에 대한 영향을 이해하기 위해서는 정보화 이론의 몇 가지 기본적인 개념들이 필요하다.

본 논고에서는 정보이론의 기본 개념과 채널 용량 및 정보이론의 응용에 관해 설명하고자 한다. 제 II장에서는 정보이론의 기본 개념에 대해 언급하고, 제 III장에서는 채널 용량 대하여 고찰할 것이고 정보이론을 응용하는 기술에 대하여 제 IV장에서 다루고, 제 V장에서 결론을 제시하고자 한다.

II. 정보 이론의 기본 개념

II. 1. 정 보

다음과 같은 조간 신문의 세 가지 머리기사를 생각해 보자.

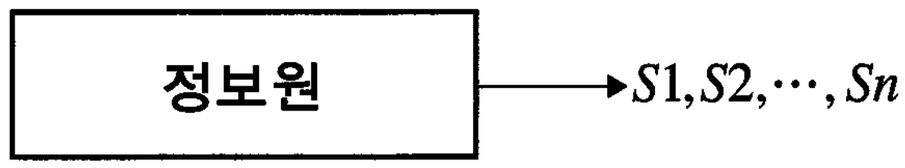
1. 내일은 해가 동쪽에서 뜰 것이다.
2. 미국이 쿠바를 침공하였다.
3. 쿠바가 미국을 침공하였다.

독자들은 첫 번째 머리기사에는 전혀 관심을 두지 않을 것이다. 아마 두 번째 기사는 아주 흥미 있어 할 것이다. 하지만 진짜로 독자들의 눈길을 끌어들이는 것은 세 번째이다. 이 항목은 이전 두 머리기사보다 훨씬 더 많은 관심을 끌 것이다. 일반 상식의 관점에서 보면, 첫 번째는 전혀 새로운 정보가 없고, 두 번째는 많은 정보를 가지고 있으며 세 번째는 더 많은 정보를 가지고 있다. 만일 우리가 이들 세 사건이 일어날 확률에 대해 생각한다면, 첫 번째 사건이 일어날 확률은 1 이며, 두 번째 사건의 확률은 아주 작고, 세 번째 사건의 확률은 거의 0 에 가깝다. 예상치 못했던 사건일수록 놀라움은 더 커지게 되며, 따라서 더 많은 정보를 내포한다. 한 사건이 일어날 확률은 그것의 의외성의 척도이며 정보의 양과 관계가 있다. 일반상식의 관점에서는 한 메시지로부터 얻는 정보의 양은 그것의 발생 확률의 역수에 관련이 있다. 만일 P가 한 메시지의 발생 확률이고 I가 그 메시지로부터 얻을 수 있는 정보라고 하면, 앞에서의 논의로부터 P→1 일 때, I →0이 되며 일반적으로 작은 에러 확률 P는 큰 정보 I를 갖게 한다는 것이 확실해 지며 다음과 같은 모델을 제시해 준다.

$$I - \log\frac{1}{P}. \qquad (1)$$

II. 2. 정보원의 성질과 분류

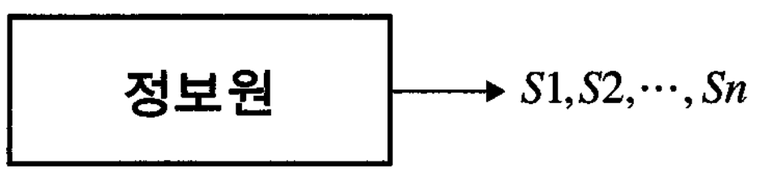
자연계에는 많은 정보원이 있다. 예를 들면 인간의 입에서 발생되는 언어, TV의 영상, 시시각각 변화하는 기온의 변화 등 무수히 많다. 그리고 이러한 정보원으로부터 정보가 발생 되는 데는 몇 가지의 기본적 성질이 있다. 이 중 특히 중요한 성질이 정보원의 마르코브성이다. 예를 들면 언어의 경우, 현재 발생되는 언어는 그 전의 발생된 언어에 상당한 영향을 받는다는 것이다. 이를 일반적인 개념으로 생각해보면, 그림 1과 같이 정보를 발생하는 정보원이 있어서 S1, S2, … Sn 까지의 부호가 발생했다고 하자.



조건부 확률 $P(sn \mid S1, S2, \cdots, Sn-1)$

(그림 1) 정보원

이 때, 다음에 발생하는 부호 Sn+1은 S1,…,Sn의 계열에 상당한 영향을 받음을 의미한다. 이와 같은 성질을 마르코브성이 있는 정보원이라 한다. 특히 영향을 받는 범위가 어느 정도까지 전의 부호에 의해 영향을 받는가에 의해 마르코브성을 분류할 수가 있다. 즉 다음에 발생하는 m개의 부호에 의해서만 영향을 받는 계열을 m차 마르코브성을 가진다고 한다. 따라서 1차, 2차,…, m차 마르코브 계열로 정의할 수 있다. 이와 같이 자연계에서 발생하는 계열에는 상호의존성이 높아 마르코브성이 있는 것이 보통이다. 여기에 대하여 특별한 예로써 0차의 마르코브, 즉 계열의 부호 사이에는 아무런 관계가 없는 경우인 (그림 2)를 생각해 보자.



조건부 확률 $P(sn \mid S1, S2, \cdots, Sn-1) = P(S_n)$

(그림 2) 무기억 정보원

정보원으로부터 부호 S1, S2, …가 순차로 발생하고 Si 가 발생할 확률은 P(Si)에 의해서만 정해지는 경우이다. 이러한 계열은 확률적으로 독립인 계열이라 하며, 정보원은 무기억 정보원(Memoryless information source)이라 한다.

II. 3. 엔트로피

각각의 확률 $P_1, P_2, \cdots, P_n$을 갖는 ($P_1+P_2+\cdots+P_n=1$) 메시지

$m_1, m_2, \cdots, m_n$을 발생하는 비기억 정보원 m을 생각해 보자. 비기억 정보원은 발생하는 각각의 메시지가 이전의 메시지와 독립적이라는 의미이다. 식 (1)에 의해서 메시지 m_i의 정보량 I_i는 다음과 같다.

$$I_i = \log \frac{1}{P_i}. \tag{2}$$

의 발생 확률은 이다. 따라서 정보원에서 발생하는 메시지당 평균 정보는 $\sum_{i=0}^{n} P_i I_i$ 비트가 된다. 정보원 m의 메시지당 평균 정보를 엔트로피라 하고 으로 표기한다.

$$\begin{aligned} H(m) &= \sum_{i=0}^{n} P_i I_i \\ &= \sum_{i=0}^{n} P_i \log \frac{1}{P_i} \\ &= -\sum_{i=0}^{n} P_i \log P_i. \end{aligned} \tag{3}$$

한 정보원의 엔트로피는 메시지 확률의 함수이다. 최대의 엔트로피를 갖게 하는 메시지의 확률 분포를 구해 보는 것도 흥미 있는 일이다. 엔트로피는 불확실성의 척도이기 때문에, 최대의 불확실성을 갖게 하는 확률 분포가 최대의 엔트로피를 갖는다. 따라서 모든 메시지의 발생 확률이 같으면 엔트로피는 최대가 되리라 예상할 수 있다.

$H(m)$이 확률 $P_1, P_2, \cdots, P_n$의 함수이므로 $H(m)$의 최대값은 모든 $i=1,2,\cdots,n$에 대하여 $dH(m)/dP_i=0$ 으로부터 구할 수 있다. 단,

$$P_n = 1 - (P_1 + P_2 +_n \cdots + P_{-1}). \tag{4}$$

왜냐하면,

$$H(m) = -\sum_{i=0}^{n} P_i \log P_i, \tag{5}$$

이므로, $-P_i \log P_i$ 와 $-P_n \log P_n$ 항만 고려하면 된다. 따라서,

$$\begin{aligned} \frac{dH(m)}{dP_i} &= \frac{d}{dP_i}(-P_i \log P_i - P_n \log P_n) \\ &= -P_i(\frac{1}{P_i})\log e - \log P_i + P_n(\frac{1}{P_n})\log e + \log P_n \\ &= \log \frac{P_n}{P_i} \end{aligned} \tag{6}$$

이것은 $P_i = P_n$일 때 0이 된다. 이것은 모든 i에 대하여 사실이므로 다음과 같은 결론이 된다.

$$P_1 = P_2 = \cdots = P_n = \frac{1}{n}. \tag{7}$$

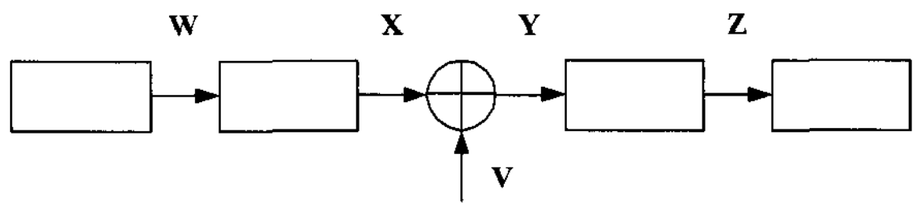
식 (6)이 $H(m)_{\min}$이 아니라 $H(m)_{\mathrm{mix}}$를 구하는 것이라는 점을 보이기 위해 예를 들어보면, $P_1 = 1$이고 $P_2 = \cdots P_n = 0$이면, $H(m) = 0$이 되고 식 (7)의 확률을 가지면 $H(m)$은 다음과 같은 값을 갖는다.

$$\begin{aligned} H(m) &= -\sum_{i=1}^{n} \frac{1}{n} \log \frac{1}{n} \\ &= \log n. \end{aligned} \tag{8}$$

III. 채널 용량

III. 1. 통신의 모델과 정보량

통신에 있어서 정보량의 관점에서 본 통신 모델을 아래의 (그림 3)과 같이 나타낼 수 있으며 5종류의 확률변수를 생각할 수 있다.



(그림 3) 통신의 모델

여기서 H(W), H(X), H(Z)는 평균 정보량이며 H(V), H(Y)는 평균 정보량이라고도 하지만 보통 엔트로피라고 명한다. H(X|Y)는 X의 사후 평균 정보량, H(Y|X)는 채널 잡음의 엔트로피라 한다. 통신 모델에 있어서 정보의 흐름은 W → X → Y → Z 이지만 수신 신호 Y는 X에 대하여 직접적으로 영향을 받으나 W에 의해서는 직접적인 영향은 없다. Z에 대해서도 마찬가지로, 이에 대해 다음과 같은 평균 상호 정보량 사이의 부등식이 성립한다.

$$\bar{I}(X;Y) \geq \bar{I}(W;Y) \geq \bar{I}(W;Z). \tag{9}$$

통신 모델에 있어서 평균 상호 정보량 $\bar{I}(X;Y)$ 를 X에서 Y까지의 전송 정보량이라 한다. 위의 (그림 3)을 토대로 상호

정보량을 살펴보면 정보원에서 수신기까지의 전송 정보량 $\bar{I}(X;Y)$ 는 다른 어떤 전송 정보량보다 적다. 이는 도중 경로의 전송 정보량 이상의 정보는 전송 할 수 없다는 의미이다. 극단적인 예로써 통신로의 전송 정보량 $\bar{I}(X;Y)$ 가 0이면 많은 정보를 가진 정보원 일지라도 전송 정보량 $\bar{I}(X;Y)$ 이 0이 되어 수신기에게는 아무런 정보도 전송되지 않는다.

통신 모델을 생각할 때 단위 시간당 전송 정보량이 문제가 된다. 이를 정보 전송 속도 또는 전송 속도라 하며 bit/sec 단위로 표시한다. 본 논고에서 다루는 정보원의 정보량과, 채널을 통해 전송되는 전송 정보량은 모두 정상 무기억 정보원과 통신로로 가정한다. 정상이라 함은 특성이 시간적으로 변화하지 않음을 의미한다.

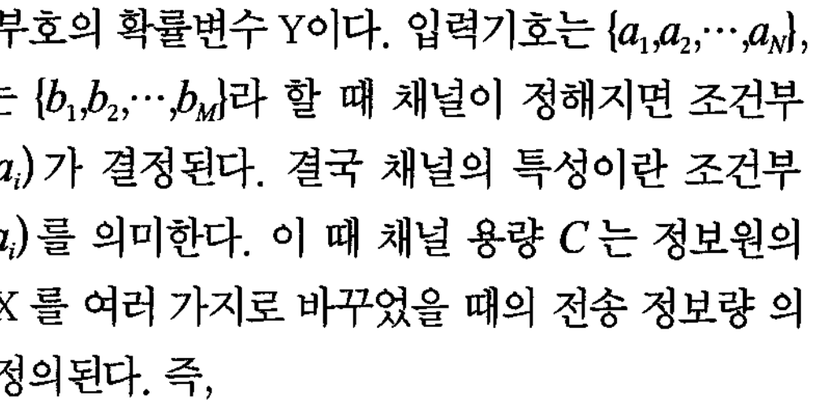
Ⅲ. 2. 채널 용량

모든 채널은 전송할 수 있는 정보량의 한계가 있다. 잡음이 많은 통신로는 잡음이 적은 통신로보다 전송 할 수 있는 정보량이 작다. 이러한 사실을 정량적으로 나태내기 위하여 채널 용량의 도입이 필요하다. (그림 3)의 통신 모델에서 채널 부분을 보면 입력은 송신 부호의 확률변수 X이고 출력은 수신 부호의 확률변수 Y이다. 입력기호는 $\{a_1,a_2,\cdots,a_N\}$, 출력기호는 $\{b_1,b_2,\cdots,b_M\}$라 할 때 채널이 정해지면 조건부 확률 $P(b_j|a_i)$가 결정된다. 결국 채널의 특성이란 조건부 확률 $P(b_j|a_i)$를 의미한다. 이 때 채널 용량 C는 정보원의 확률변수 X 를 여러 가지로 바꾸었을 때의 전송 정보량 의 최대치로 정의된다. 즉,

$$\begin{aligned} C &= \max_{P(X)} \bar{I}(X;Y) \\ &= \max_{P(X)} \{H(X) - X(X|Y)\}, \end{aligned} \tag{10}$$

가 된다.

채널은 입출력의 정보 성질에 의해 분류되는데 입출력 정보가 모두 이산일 경우를 이산 통신로라 하며, 입출력 정보 모두가 연속일 경우 연속 통신로라 한다. 본 논고에서는 이산 통신로의 경우를 가정한다. 송 수신 기호는 0과 1인 2원(binary)신호이고, 0의 발생 확률을 라 하면 1의 발생 확률은 가 되는 (그림 4)와 같은 2원 대칭 통신로를 가정한다.



(그림 4) 2원 대칭 통신로

위의 그림에서 입력신호의 발생확률, 즉 $P_r(X=1)$, $P_r(X=0)$을 $P_x(a_1)$, $P_x(a_2)$ 하자.

즉,

$$\begin{aligned} &Px(a_1) = Px(1) = 1 - P_0 \\ &Px(a_2) = Px(0) = P_0 \\ &P(b_1|a_1) = P(b_2|a_2) = 1 - P \\ &P(b_2|a_1) = P(b_1|a_2) = P. \end{aligned} \tag{11}$$

또 수신기호의 발생확률 $P_r\{y=b_i\}$ 를 $Py(b_j)$로 나타내면,

$$\begin{aligned} Py(b_1) &= P_x(a_1)P(b_1|a_1) + P_x(a_2)P(b_1|a_2) \\ &= Py(1) = P_0P + (1+P_0)(1-P) \\ Py(b_2) &= P_x(a_1)P(b_2|a_1) + P_x(a_2)P(b_2|a_2) \\ &= Py(0) = P_0(1-P) + (1-P_0)P, \end{aligned} \tag{12}$$

이며, 수신측의 엔트로피는 다음과 같이 구해진다.

$$\begin{aligned} H(Y) &= -\sum_Y P(b)\log P(b) \\ &= -Py(0)\log Py(0) - Py(1)\log Py(1). \end{aligned} \tag{13}$$

식 (10)과 (12)를 이용하여 다음과 같이 조건부 엔트로피를 구할 수 있다.

$$\begin{aligned} H(Y|X) &= -\sum_{i=1}^{2}\sum_{j=1}^{2} Px(a_i)P(b_j|a_i)\log P(b_j|a_i) \\ &= -P\log P - (1-P)\log(1-P) \end{aligned} \tag{14}$$

따라서 평균 상호 정보량 $\bar{I}(X;Y)$ 은

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= H_N(Py(0)) - H_N(P) \\ where, H_N(X) &= -X\log X - (1-X)\log(1-X), \end{aligned} \tag{15}$$

이며 최종적으로 채널 용량은 다음과 같이 구할 수 있다.

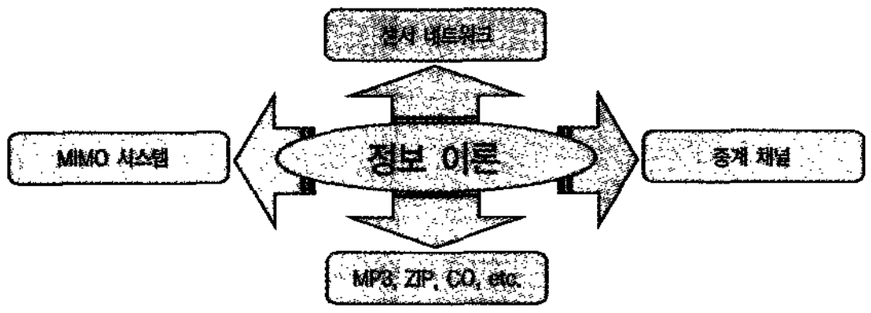
$$C = \max_{P(X)} \bar{I}(X;Y)$$
$$= \max_{P(X)} \{H_N(Py(0)) - H_N(P)\}$$
$$= \max_{P(X)} \{H_N(Py(0))\} - H_N(P). \quad (16)$$

즉, 는 송신기호화는 무관하며, 채널에 의해서만 정해진다. 따라서 $\bar{I}(X;Y)$를 최대로 하기 위해서는 $H_N(Py(0))$가 최대가 되어야 하며 이는 엔트로피 성질에 의해 $Py(0) = 1/2$일 때 최대가 된다. 따라서 식 (15)의 최대 채널 용량은 다음과 같이 구해진다.

$$C = 1 + P\log P + (1-P)\log(1-P). \quad (17)$$

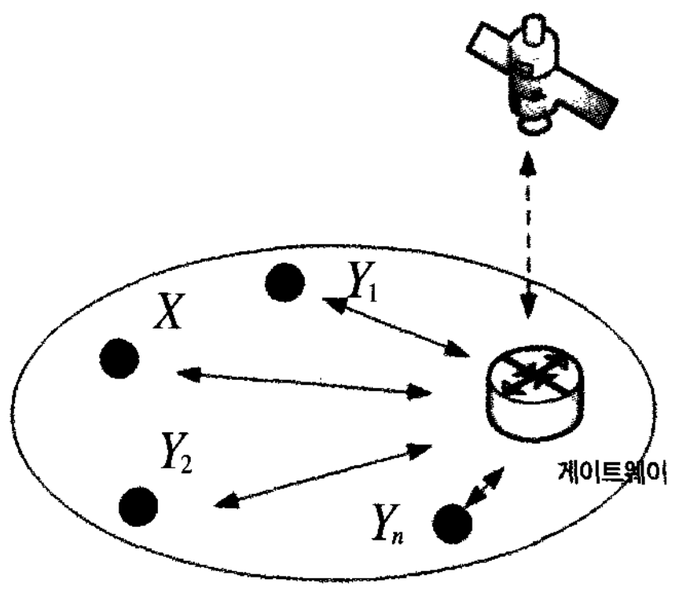
Ⅳ. 정보 이론의 응용

정보이론을 탐구하는 가장 큰 이유는 바로 그것이 정보 전송시스템을 설계하는 기준을 제공해 준다는 점일 것이다. 정보와 전송에 대한 명확한 개념을 개발함으로써 기술의 목표와 한계를 더 확실히 이해할 수 있다. 이런 이해로 말미암아 좀 더 효율적인 방향으로 연구와 개발이 진행될 수 있고, 이것이 바로 정보이론의 가장 중요한 성공분야로 간주된다. 정보이론의 여러 가지 응용분야 중에서도 가장 중요한 것은 통신의 제반 문제에 관련된 것이다. 현재 잡음 채널상에서 일반적인 최적 데이터 전송방식은 알려져 있지 않다. 특히 데이터의 정보율이 채널의 정보 용량보다 더 클 경우 왜곡이나 변형 없이 데이터를 전송한다는 것은 불가능하다. 즉 채널 용량과 송신 데이터의 정보량, 엔트로피의 개념을 도입함으로써 정보이론은 통신시스템의 최적 성능을 정확하게 판단할 수 있게 해준다. 덧붙여 최적 시스템을 합리적으로 설계할 수 있는 방안도 제시하여준다. 센서 네트워크, 중계채널, MIMO 시스템등과 같은 디지털 통신시스템에서는 현재 신호 파형을 더 이상 한번에 한 비트씩 송수신 하지 않고, 더 많은 비트열에 해당하는 파형을 전송하는 좀 더 복잡하고 발전된 형태를 사용하고 있다. 정보이론은 이런 앞서 나가는 방식들의 개발에 지침을 마련해주고 또 얼마나 많은 개선의 여지가 있는가를 알려준다.



(그림 5) 정보 이론의 응용 분야

Ⅳ. 1. 센서 네트워크



(그림 6) 다중 노드 센서 네트워크 시스템

(그림 5)와 같은 정보원 X와 Y_i의 다중 센서 네트워크 시스템을 고려해보자. 다중의 노드들 중 하나의 노드가 정보를 생성해 내면 나머지 노드들은 정보원의 정보에 대한 상관 정보들을 생성한다. 게이트웨이에서는 유입된 정보를 채널 상황에 맞게 적절한 부호화 과정을 수행하게 된다.

각 노드들 사이에 가우시안 분포를 형성하고 있다고 가정하면 다음과 같은 공분산 행렬이 결정된다.

$$\begin{bmatrix} \sigma_X^2 & \rho_{XY_1}\sigma_X\sigma_{Y_1} & \cdots & \rho_{XY_n}\sigma_X\sigma_{Y_n} \\ \rho_{XY_1}\sigma_X\sigma_{Y_1} & \sigma_{Y_1}^2 & \cdots & \rho_{Y_1X}\sigma_{Y_1}\sigma_{Y_n} \\ \vdots & \cdots & \ddots & \vdots \\ \rho_{XY_n}\sigma_X\sigma_{Y_n} & \rho_{Y_1X}\sigma_X\sigma_{Y_1} & \cdots & \sigma_{Y_n}^2 \end{bmatrix} \quad (18)$$

식 (18)의 공분산 행렬을 이용하여 가우시안 채널 상에서의 다중 노드 센서 네트워크 시스템의 채널 용량의 범위는 다음과 같이 결정된다.

$$C_X \geq \frac{1}{2}\log\left\{\frac{\sigma_X^2}{D_X}\left[\prod_{k=1}^{n}\left(1-\rho_{XY_k}^2+\rho_{XY_k}^2\cdot 2^{-2R_k}\right)\right]^{1/n}\right\} \quad (19)$$

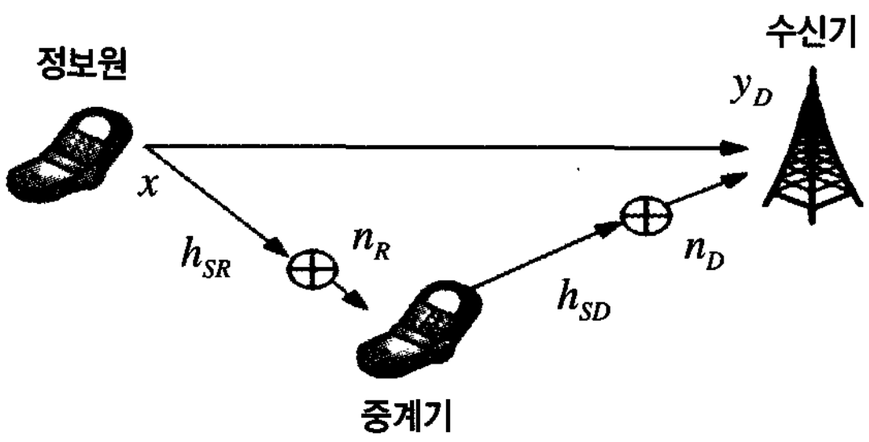
$$where\begin{cases}R_k : Admissible\ rate\\ D_X : Distortion\ rate\ by\ Gaussian\end{cases}.$$

$$y_D = \sqrt{\frac{E_{SR}E_{RD}}{|h_{SR}|^2 E_{SR}+n_S n_D}}h_{SR}h_{RD}x + \sqrt{\frac{E_{SR}E_{RD}}{|h_{SR}|^2 E_{SR}+n_S n_D}}h_{RD}n_R + n_D. \quad (20)$$

Ⅳ. 2. 중계 채널

기존의 기간망이 존재하는 시스템에서, 특히 최근 이슈가 되고 있는 IEEE 802.16j 시스템에서 중계국은 셀 커버리지를 확장하고 정보 전송률을 증가시키기 위한 역할을 수행한다. 중계 채널은 정보 이론에서 채널 용량을 분석하기 위한 가상적인 채널 모델로 등장하였다. 일반적으로 두 개의 단말이 통신하는 것에 비하여 세 개의 단말이 통신을 함으로써 채널 용량을 증가시킬 수 있다는 사실이 밝혀지면서 그것의 채널 용량을 구하는 많은 연구가 진행되었다.

Ⅳ. 2. 1. 증폭-전송 (AF) 기법



(그림 7) 증폭-전송 기법

증폭-전송 기법은 릴레이에서 수신되는 신호의 파워만 증폭시켜 재 전송하는 기법이다. 수신 신호의 파워를 정규화하고 이를 릴레이에서 전송할 수 있는 파워 레벨로 증폭시켜 전송하는 것으로 구현 측면에서는 간단하나 부가된 잡음이 증폭되는 단점을 지니고 있다. 정보원으로부터 전송된 신호를 x 라 할 때 증폭-전송 기법을 이용하는 릴레이를 통하여 수신기에 수신된 신호는 다음과 같이 표현된다.

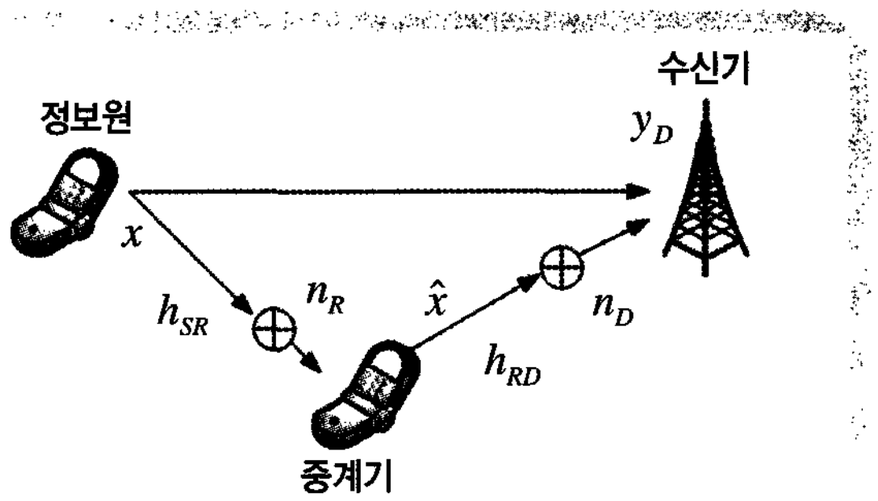
여기서 h_{SR}과 h_{RD}는 각각 정보원과 릴레이, 그리고 릴레이와 수신기사이의 채널이고, n_R과 n_D는 각각 릴레이와 수신기에 부가되는 잡음으로 동일한 분포를 가지나 서로 독립관계이다. 식 (20)에서 수신 신호의 유효 SNR, ρ_{eff}는 다음과 같다.

$$\rho_{eff} = \frac{\rho_{SR}\cdot\rho_{RD}}{1+\rho_{SR}+\rho_{RD}}. \quad (21)$$

위 식을 이용하여 증폭-전송 기법의 채널 용량은 다음과 같이 구할 수 있다.

$$C_{AF} = \frac{1}{2}\log_2\left(1+\frac{\rho_{SR}\cdot\rho_{RD}}{1+\rho_{SR}+\rho_{RD}}\right). \quad (22)$$

Ⅳ. 2. 2. 복호-전송 (DF) 기법



(그림 8) 복호-전송 기법

앞서 언급한 증폭-전송 기법이 아날로그 신호 처리 기법인 반면, 복호-전송 기법은 수신 신호를 비트 단위까지 복호화하고 이를 다시 부호화 및 변조하여 재 전송하는 기법이다. 증폭-전송 기법에 비해 연산량 측면에서 복잡한 기법이나 대부분의 통신 단말에 변복조기와 부호/복호화기가 탑재되어 있음을 가만하면 현실적으로 구현 가능한 기법이다. 복호-전송 기법을 이용하는 중계기는 수신한 신호를 복호화하

고 재 부호화 및 변조한 신호를 수신기에 전송하며, 이 때, 수신된 신호는 다음과 같다.

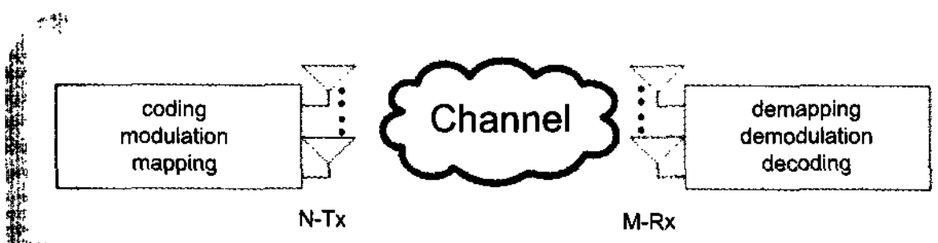
$$y_D = h_{RD}\hat{x} + n_D. \tag{23}$$

여기서 $\hat{x}$은 복호-전송에 의해 재 부호화 및 변조된 중계기에서의 송신 신호이다. 복호-전송 기법이 적용된 시스템의 채널 용량은 정보원과 중계기 그리고 중계기와 수신기간의 두 채널 중 SNR이 작은 쪽의 채널 용량이 되며 다음과 같이 표현할 수 있다.

$$C_{DF} = \min\left\{\frac{1}{2}\log_2(1+\rho_{SR}), \frac{1}{2}\log_2(1+\rho_{RD})\right\}. \tag{24}$$

두 채널의 유효 SNR이 동일할 경우, 증폭-전송 기법과 비교할 경우 채널 용량이 3dB 이득이 있음을 알 수 있다.

Ⅳ. 3. MIMO 시스템



(그림 9) MIMO 시스템 개념도

본 절에서는 (그림 9)와 같은 MIMO 시스템에서의 이론적인 채널 용량에 대해 살펴보고자 한다. 수신기에서는 채널에 대한 정보를 정확히 알고 있고, 전체 시스템이 쓸 수 있는 송신전력은 송신 안테나의 개수에 상관없이 일정하게 제한되어 있다고 가정한다. 이 때, MIMO시스템의 채널 용량은 다음과 같이 주어짐을 보일 수 있다.

$$C = \log_2 \det\left(\mathbf{I}_N + \frac{1}{\rho^2}\mathbf{H}\mathbf{K}_\mathbf{X}\mathbf{H}^\mathbf{H}\right). \tag{25}$$

여기서 $\mathbf{I}_N$은 $N\times N$ 항등행렬을, $\mathbf{K}_\mathbf{X}$는 송신신호 벡터의 공분산 행렬을 뜻하며, $(\bullet)^H$연산은 Hermitian 연산을 나타낸다. 위에서 주어진 채널용량은 송신기에서 채널 정보를 알 수 없는 경우와 알 수 있는 경우에 따라, 각각 개루프 방식, 폐루프 방식에서의 용량으로 나누어 생각해 볼 수 있고, 그 값 또한 다르다. 만약 채널 종보를 송신기에서 알 수 있다면 최적화된 신호처리를 통해 주어진 MIMO 채널의 최대 용량을 달성할 수 있게 된다.

이제 개루프 방식에서의 용량을 살펴보면, 이 경우는 송신기에서 채널 정보를 알지 못하므로, 각 전송신호마다 단순히 주어진 전체 송신전력을 균등하게 할당하여 전송하게 되고 따라서 다음과 같이 주어짐을 보일 수 있다.

$$C_{OPEN} = \log_2 \det\left(\mathbf{I}_N + \frac{P_T}{M\cdot\rho^2}\mathbf{H}\mathbf{H}^\mathbf{H}\right). \tag{26}$$

다음으로, 폐루프 방식에서의 용량을 살펴보면, 이는 채널 행렬 H를 SVD(Singular Value Decomposition) 시킨 결과를 이용하여 송수신기에서 서로 교차되는 다중 입출력 채널의 시스템을 여러 개의 평행한 단일 입출력 부채널들이 존재하는 시스템으로 변환한 뒤, 각 단일 입출력 부채널에 최적의 송신전력을 할당함으로써 얻어지게 된다. 따라서 송신기에서는 이러한 최적의 신호처리과정을 수행하기 위해 주어진 채널에 대한 정보가 반드시 필요하게 된다. 폐루프 방식의 채널 용량은 다음과 같이 주어짐을 보일 수 있다.

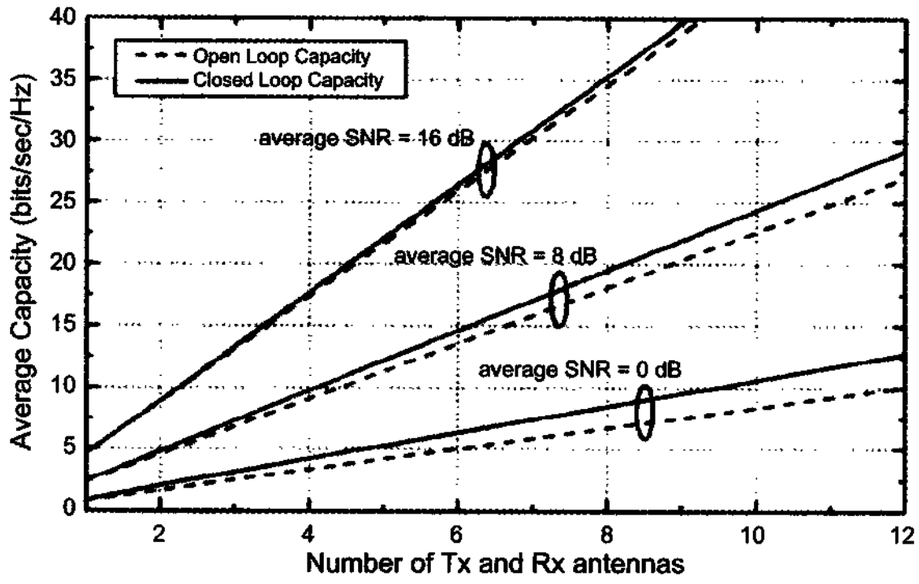
$$C_{CLOSED} = \sum_{i=1}^{\min(M,N)} \log_2\left(1+\frac{\lambda_i}{\sigma^2}p_i\right). \tag{27}$$

여기서 λ_i는 행렬 $(\bullet)^H$의 고유값들을 나타내며 p_i는 다음과 같이 주어진다.

$$p_i = \begin{cases} \nu - \dfrac{\sigma^2}{\lambda_i}, & if\ \lambda_i \geq \dfrac{\sigma^2}{\nu} \\ 0, & else \end{cases}. \tag{28}$$

여기서 ν는 전체 송신전력 제한조건 $\sum_{i=1}^{\min(M,N)} P_i = P_T$ 을 만족시키도록 주어진다.

앞서 살펴본 결과를 토대로 안테나의 수에 따른 각 방식의 채널 용량을 비교하면 다음과 같이 보여진다.



(그림 10) 안테나 수에 따른 평균 용량 비교

Ⅳ. 4. Other Fields

정보이론의 개념은 암호화 이론에 적용될 수 있다. Shannon은 암호화된 문장의 본래의 형식의 리던던시 기법을 토대로, 한 문장의 암호문을 해석하기 위해 필요한 최소 암호문자를 계산해 내었다. 또한 데이터 무손실 압축(ZIP 파일)또는 데이터 손실 압축(MP3)기법, 그리고 채널 부호화 분야에 적용되어 전송 또는 저장하려는 정보의 최대치 또는 그 한계를 계산하는데 이용된다.

Ⅴ. 결 론

앞서 언급한 것처럼, 통신 시스템의 목적은 통신 채널을 통해 한 장소에서 다른 장소로 정보를 얼마나 빨리, 얼마만큼의 신뢰도를 가지고 전송할 수 있는가 이다. 이 질문의 대답은 각각 신호원의 엔트로피와 채널 용량에 있다. 본 고에서는 정보 이론을 이해함에 있어서 기초가 되는 정보와 그 정보의 엔트로피, 그리고 채널 용량에 관해 다루었다. 또한 개념적으로 접근한 정보 이론이 실제 시스템에 어떻게 적용되는지 센서 네트워크와 중계 채널을 그 예로 들어 살펴보았다. Shannon이 언급한 채널 용량의 제한에 근접하는 알고리즘이 현재 계속 개발되고 있으며, 그 알고리즘들이 보다 쉽게 구현되면서 좋은 성능을 보이도록 연구원들의 부단한 노력이 필요하다.

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp.623-656, 1948.

[2] D. Slepian, Ed., Key Papers in Developmentof Information Theory: New York, IEEE Press, 1973.

[3] C. E. Shannon, "Prediction and entropy of printed gnglish," *Bell Syst. Tech. J.*, vol. 30, pp.50-64, 1951.

[4] A. Kolmogorov, "Logical basis for information theory and probability theory," *IEEE Trans., Inform., Theory*, vol. IT-14, pp. 662-664, 1968.

[5] T. L. Fine, Theories of Probability : New York, Academic Press, 1973.

[6] A. D. Wyner, "Recent results in Shannon theory," *IEEE Trans., Inform., Theory*, vol. IT-20, pp. 2-10, 1974.

[7] A. D. Wyner, "The capacity of he band-limited Gaussian channel," *Bell Syst. Tech. J.*, vol. 45, pp.359-371, March. 1965.

[8] D. Drajic, D. Bajic, "Information theory 증폭-전송ter," *TELSIKS' 97, Nis.*, pp. 5-12, Oct. 1997.

[9] J. Hagenauer "The impact of information theory on communicatins," *IEEE Inf., Theory, Society Newsletter*, Special Golden Jubilee Issue, Summer 1998, pp. 6-8.

[10] G. J. Pottie et. al., "Wireless sensor networks", *Inform., Theory, Workshop Proc.*, Killamey, Ireland, June 22-24, 1998.

[11] T. S. Han and K. Kobayashi, "A unified achievable rate region for a general class of multi-terminal source coding systems," *IEEE Trans., on Inform., Theory*, vol. IT-26, pp. 277-288, May 1980.

[12] C. E. Shannon, "Two-way communications channels," *in Proc., 4th Berkeley Symp., Math, Stat., Prob.*, 1, Univ. California Press, pp. 611-644, 1961.

[13] A. El Gamal, "The capacity of the deterministic relay channel," pres-ented at the 1979 *IEEE Int. Symp. Information Theory*

약 력

1998년 서울대 전자공학과 (공학박사)
1998년 ~ 2000년 미국 Princeton University, Research Associate
2000년 ~ 2001년 SK텔레콤 네트워크 연구원 책임연구원
2001년 ~ 현재 광운대학교 전파공학과 부교수
관심분야 : 디지털 통신, 신호처리, 채널 부호화

김 진 영

2008년 광운대학교 전파공학과 (공학석사)
2008년 ~ 현재 광운대학교 전파공학과 박사과정 재학중
관심분야 : 이동통신, 디지털통신, MIMO, OFDM.

김 윤 헌

2002년 미국 University of Southern California 공학박사
1991년 ~ 1997년 LG전자 중앙연구소 선임연구원
1997년 ~ 1998년 미국 Stanford University 객원연구원
2001년 ~ 2002년 미국 Trellisware Inc. Senior Engineer
2003년 ~ 2007년 건국대학교 정보통신공학부 조교수
2007년 ~ 현재 고려대학교 전기전자전파공학부 조교수
관심분야 : 채널 부호화, 디지털 통신

허 준