논문 21-46-10-05 The Journal of Korean Institute of Communications and Information Sciences '21-10 Vol.46 No.10
https://doi.org/10.7840/kics.2021.46.10.1578

블라인드 채널 추정을 통한 전이중 통신 상황에서의 재밍 알고리즘

김 상 혁•, 강 준 혁°

Full-Duplex Jamming and Interception Algorithm Using Blind Channel Estimation

Sang-hyuk Kim•, Joon-hyuk Kang°

요 약

자체간섭 (SI) 수준이 낮은 전이중 (Full-Duplex, FD) 트랜시버 설계의 발전으로 인해 다양한 무선 통신 애플리케이션에서 전이중 통신장치를 통한 연구가 진행되었다. 본 논문에서는 물리 계층 보안과 관련된 연구 중 전이중 트랜시버를 사용하여 군통신 분야에서 적용하는 연구를 진행하였다. 기존에는 아군의 통신 성능을 보장하기 위해 보안용량을 높이는 것에 주력한 반면, 이 논문에서는 군용 전이중 라디오를 이용하여 공격적인 역할을 수행하는 연구를 진행한다. 본 시스템 모델은 적군 송신 신호를 가로채면서 동시에 수신기를 방해하여 상대의 전술적 통신 링크를 저해하는 상황을 다루었으며, 사전에 채널을 인지할 수 없는 특수상황을 고려하여 블라인드 채널 추정을 통해 교란신호를 전파하는 보완 알고리즘을 사용하였다. 보안 성능은 채널 중단 확률을 유도함으로써 이론적으로 수치화한다. 실험 결과를 통해 높은 SI 취소 성능이 보안 성능을 높일 수 있음을 제시한다.

키워드 : 전이중 통신, 블라인드 추정, 보안용량, 중단확률, 자체간섭
Key Words : Full-duplex, blind estimation, secrecy rate, outage probability, self-interference

ABSTRACT

Advances in the design of full-duplex (FD) transceivers with low self-interference (SI) levels have led to research with devices in a variety of wireless communications applications. In this paper, we study a military communication using a full-duplex transceiver among physical layer security area. Different from previous researches, we apply a FD transceiver as an offensive role by using a military full-duplex radio. This system model deals with the situation of intercepting the signal of the enemy transmitter node and at the same time interfering with the receiver node to hinder and eavesdrop on the opponent's tactical communication link. A Blind channel estimation algorithm is used to complement a wartime conditions. The security performance is theoretically quantified by deriving the outage probability of secrecy rate. Experimental results suggest that high SI cancellation performance can increase security performance.

※ 본 연구는 방위사업청과 국방과학연구소가 지원하는 미래전투체계 네트워크기술 특화연구센터 사업의 일환으로 수행되었습니다 (UD190033ED).
• First Author : Korea Institute of Science and Technology, starmoon13@kaist.ac.kr, 정회원
° Corresponding Author : Korea Institute of Science and Technology, jhkang@kaist.edu, 종신회원
논문번호 : 202103-070-A-RU, Received March 26, 2021; Revised May 11, 2021; Accepted June 12, 2021

Ⅰ. 서 론

무선 통신이 제공해야 하는 안전성을 강화하기 위한 대표적인 연구로 물리 계층 보안이 있다. 초기의 암호화 기술에 비하여 도청 기술과 계산 능력이 발전했기 때문에, 물리 계층에서 안전한 송수신을 보장하기 위해 강화된 물리 계층 보안 개념이 관심을 받고 있다[1]. 이 중 물리 계층 보안을 강화하는 한 가지 방법은 전이중 통신 기술이다. 전이중 통신기술은 무선 트랜시버가 동일한 주파수 대역에서 무선 정보를 동시에 송수신 할 수 있으므로 무선 네트워크의 스펙트럼 효율성이 두 배로 늘어나는 장점을 보인다[2]. 우수한 자체 간섭 제거 기능을 보유할 경우 전이중 양방향 통신이 가능하며, 자체 간섭 억제 기술을 보유할 경우에는 더 좋은 성능을 제공할 수 있다[3].

물리 계층 보안을 강화에 전이중 통신을 이용한 연구는 다양하게 진행되었다. 전이중 수신기를 이용하여 통신 상용 네트워크가 도청되는 것을 방지하는 연구[4], 기지국에서 안테나 선택 기법을 사용해 통신 신호를 보내고 수신기가 송신 데이터를 수신함과 동시에 재밍신호를 보내 보안용량을 높이는 연구[5]가 있다. [6]에서는 다수의 송/수신기 쌍과 도청자가 있는 ad-hoc 네트워크 환경에서 일부의 수신기는 반이중 통신을, 나머지 수신기는 전이중 통신을 적용하여 아군의 통신성능은 보장하면서 도청장치의 성능을 낮추는 연구를 진행하였다. 그 외에 무선 통신 신호와 전력을 동시에 보내는 전이중 통신에 대한 연구도 진행된 바 있다[7]. 다중 안테나 송신기는 전송된 신호를 수신기로 보내는 한편, 전이중 수신장치가 신호를 수신하는 동시에 재밍신호를 전파하여 도청기의 성능을 하락시키는 방법을 다루었다.

위에서 논의한 선행 연구의 대부분은 민감한 정보가 도청되는 것을 방지하기 위해 전이중 트랜시버를 방어적인 방식으로 사용하여 전송 노드에서 보안 수준을 향상시킨 연구이다. 반면, 전이중 트랜시버를 공격적인 측면으로 사용하는 것에 대한 연구는 잘 이루어지지 않았다. 따라서 군사 응용 프로그램 등의 경우에서 무선 데이터 보안을 다루는 연구 또한 미비한 편이다. 군사용으로 전이중 무선 라디오를 사용하면 전자전에서 상당한 이점을 얻을 수 있는데, 무선 통신 링크의 스펙트럼 효율성을 향상시켜 안전한 전술 통신을 가능하게 하거나 상대방의 신호를 가로채서 방해할 목적으로 수행될 수 있다. 따라서 전이중 트랜시버를 공격적인 측면으로 사용하는 연구는 군사 응용 분야에서 큰 잠재력이있을 것으로 예상된다[8].

전이중 트랜시버를 공격적인 측면에서 사용할 경우, 군용 통신환경 혹은 사이버 전자기전 환경에서 적군의 통신을 방해하는 측면에서 활용이 가능하다. 다만 이러한 경우, 전송 신호와 채널 등에 대한 사전 정보를 알고 있지 않은 상황에서 공격을 수행해야 한다. 따라서 수신되는 신호만을 바탕으로 적 통신망의 채널을 정확하게 추정하는 과정이 필요하고, 블라인드 채널 추정을 통해 적군 수신 단말 간 채널을 파악해 재밍하는 연구가 결합되어야 한다[9].

본 논문에서는 군통신 환경에서 사용되는 동기 코드 분할 다중 액세스 기술을 사용하는 환경에서의 채널추정을 다루는 한편[10], 주파수 분할 다중 액세스 환경의 확장 또한 가능함을 다루고자 한다. 여러 신호 구성 요소가 있는 경우에 적용이 가능한, 부분 공간 기반 블라인드 채널 추정기법을 다루고 이를 전이중 트랜시버에서 활용하도록 한다.

정리하면, 본 논문에서는 군용 전이중 통신 라디오를 이용하여 상대방의 수신기를 방해하면서 상대방의 신호를 가로채는 공격 전략을 다룬다. 적군이 상향링크 통신을 하는 동안 적군과의 채널을 부분 공간을 이용하여 블라인드 추정하고, 이를 바탕으로 효율적인 빔포밍을 산출하여 하향링크 시에 적군 수신기에게 재밍을 진행한다. 교란 및 도청 성능은 보안용량 값을 바탕으로 추정하며, 적군의 송신 파워와 아군의 자체 간섭 성능에 따른 보안용량 수치를 알아볼 것이다.

본 논문의 구성은 다음과 같다. 2.1장에서는 먼저 제안하는 통신 시스템 모델과 채널에 대해 살펴본다. 이를 통해 2.2장에서는 부공간 기반 블라인드 채널 추정 알고리즘에 대해 알아본다. 이를 바탕으로 보안용량과 중단확률값을 2.3장에서 산출한다. 3장에서는 시뮬레이션 결과 및 분석을 하고, 마지막으로 4장에서 본 논문의 결론을 맺는다.

Ⅱ. 시스템 모델

2.1 시스템 환경

본 논문에서는 그림 1과 같은 무선 통신 시스템을 고려한다. 반이중 통신을 사용하는 적군 기기 1, 2가 서로 정보를 주고받는 상황에서, 아군 기기가 전이중 통신을 사용해 도청과 교란을 동시에 수행한다. 적군 1이 적군 2에게 상향링크 통신을 하는 과정에서 채널 추정을 진행하며, 반대로 적군 2가 적군 1에게 신호를 보낼 때 도청 및 교란이 이루어진다. 이때 적군 2는 적군 1이 받는 수신 데이터 전송 속도를 최대화하기 위해 maximum ratio transmission (MRT)기법을 바탕

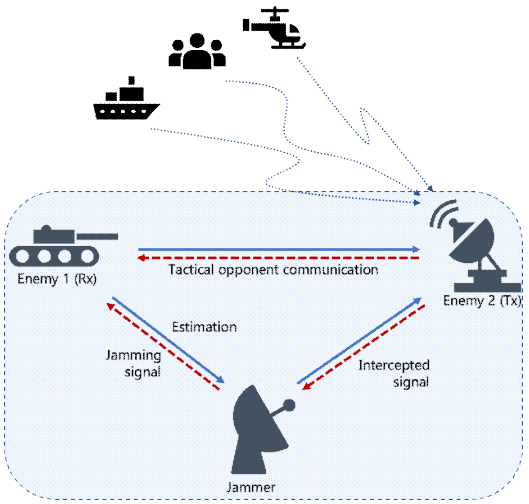

그림 1. 시스템 개요도
Fig. 1. Adopted system model

으로 빔포밍을 사용한다. 아군 도청기기는 추정한 채널 정보를 바탕으로 한 MRT 빔포밍을 진행한다.

2.1.1 채널 모델

적군 2는 N_{Tx}개의 다중 안테나를, 적군 1은 단일 안테나를 가지고 있는 MISO 환경이며, 아군 도청 기기는 N_J개의 안테나를 가지고 있다고 가정한다. 이후의 표기는 적군 1을 Rx, 적군 2를 Tx, 아군 기기를 Jammer (J)로 통일한다. 따라서 적군 1과 적군 2간의 채널이 $h_{Rx\to Tx}\in C^{N_{Tx}\times 1}$, 적군 1과 아군 기기 사이의 채널은 $h_{Rx\to J}\in C^{N_J\times 1}$, 적군 2와 아군 간의 채널은 $H_{Tx\to J}\in C^{N_J\times N_{Tx}}$로 표현된다. 군통신 환경에서는 UAV를 사용하지 않는 경우, 산지와 지형 등의 요인으로 LoS채널 형성되기 힘들다고 볼 수 있기에 채널의 모든 요소는 평균이 0, 분산이 1인 복소 레일리 분포를 따른다고 가정한다. 전이중 통신은 P_J의 재밍 파워로 송출하였을 때, β의 계수와 λ의 지수만큼 변화를 가지고 간섭을 일으킨다고 가정한다. 따라서 간섭식은 βP_J^{λ}로 표현한다.

2.1.2 채널 분포

채널 분포식을 파악하기에 앞서 적군 간의 채널, 그리고 적군과 아군 사이의 채널은 모두 채널 상호성을 만족시킨다고 가정한다. 따라서 적군 2와 적군 1 사이의 채널 $h_{Tx\to Rx}=h_{Rx\to Tx}^H\in C^{1\times N_{Tx}}$이며, 아군과 적군 간의 채널은 $h_{J\to Rx}\in C^{1\times N_J}$와 $h_{Tx\to J}\in C^{N_{Tx}\times N_J}$로 표현할 수 있다.

랜덤한 변수 X가 레일리 분포를 따를 때, 변수 X^2은 지수분포를 따른다는 것이 알려져 있다[11]. 지수분포(λ)는 감마분포 중에서 모양변수와 크기변수가 $\left(1,\frac{1}{\lambda}\right)$인 경우와 동일한 분포이다. 따라서 채널 h가 레일리 분포를 따를 때, $|h|^2$은 감마분포 (1,1)을 따른다.

$$F_{|h|^2}(x)=1-e^{-\frac{x}{E[|h|^2]}} \tag{1}$$

$$f_{|h|^2}(x)=\frac{1}{E[|h|^2]}\cdot e^{-\frac{x}{E[|h|^2]}} =\Gamma(1,\frac{1}{E[|h|^2]}) \tag{2}$$

적군 1, 2 사이의 채널은 N_{Tx}개의 채널로 이루어져 있으므로 감마분포 $\Gamma(N_{Tx},1)$을 따른다.

$$f_Y(y)=\Gamma(N_{Tx},\frac{1}{E[X]}) \tag{3}$$

여기서 Y는 적군 2와 1 사이의 채널제곱 $|h_{Tx\to Rx}|^2$를, X는 레일리 단일 채널의 제곱 $|h|^2$을 나타낸다.

2.2 블라인드 채널 추정

블라인드 채널 추정은 적군 1이 적군 2에게 송신하는 과정에서 이루어진다. 그림 1과 같은 상황으로의 확장을 위해 총 P명의 유저가 신호를 보내는 상황을 다루어본다.

2.2.1 CDMA 기반 채널 추정 과정

먼저, 유저가 사용하는 코드를 다음과 같이 정의한다: $\{c(1),c(2),\cdots,c(L_c);c(k)=\pm 1\}$. 여기서 L_c는 코드의 길이를 말한다. 상승된 코사인 펄스 등의 칩-펄스 함수 $p(t)$와 정의된 코드를 사용하면 signature waveform을 다음과 같이 표현할 수 있다[10].

$$w(t)=\sum_{k=1}^{L_c}c(k)p(t-kT) \tag{4}$$

T는 칩-펄스 함수의 주기를 뜻한다. 실제 환경에서

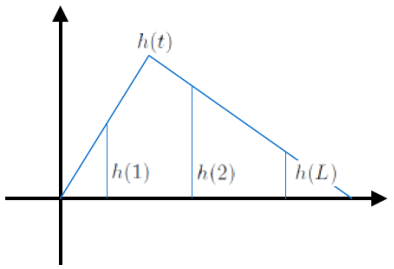

그림 2. 유한한 길이의 채널 h
Fig. 2. Finite impulse response channel h

는 신호가 다중경로를 통해 전파되고, 따라서 실제 채널은 경로의 수 L_d개의 칩-펄스 함수의 합으로 표현할 수 있다.

$$h(t)=\sum_{i=1}^{L_d}\alpha_i p(t-\tau_i) \tag{5}$$

여기서 α_i는 각각의 경로 별 감쇠를 고려한 복소계수를, τ_i는 경로 별 지연시간을 뜻한다. 채널의 길이는 L_d와는 무관하며, 주기 T를 고려하여 유한한 길이 L을 가진다고 가정한다($[0\ LT]$).

따라서 최대 지연 확산이 심볼 주기보다 작다는 가정 하에 식 (4)는 다음과 같이 변형된다.

$$w(t)=\sum_{k=1}^{L_c}c(k)h(t-kT) \tag{6}$$

식 (6)의 signature waveform을 이용하였을 때, 송수신 신호 간 관계식을 행렬식으로 표현할 수 있다. 송신 신호를 s라고 하였을 때, n번째 심볼주기에서 수신하는 신호와의 관계식은 다음과 같다.

$$y(n)=\begin{bmatrix} w(1) & w(L_c+1) \\ \vdots & \vdots \\ w(L-1) & w(L_c+L-1) \\ w(L) & 0 \\ \vdots & \vdots \\ w(L_c) & 0 \end{bmatrix}\begin{bmatrix} s(n) \\ s(n-1) \end{bmatrix} \tag{7}$$

signature waveform의 주기에 따라 심볼간 간섭이 일어날 수 있음을 알 수 있다. 이전 심볼의 영향을 받지 않는 부분만 추려 다시 정리하면 다음과 같은 관계식을 얻는다.

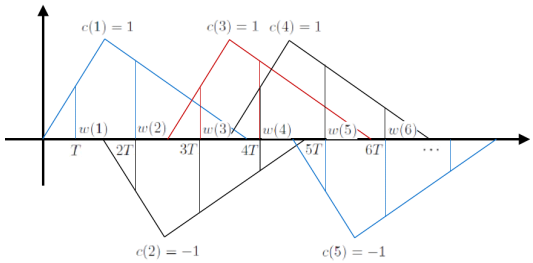

그림 3. 심볼간 간섭 예시
Fig. 3. Example of inter-symbol interference

$$\bar{y}(n)=\begin{bmatrix} y(n,L) \\ \vdots \\ y(n,L_c) \end{bmatrix}=\begin{bmatrix} w(L) \\ \vdots \\ w(L_c) \end{bmatrix}s(n)=\bar{w}s(n) \tag{8}$$

식 (8)에서 정리된 $\bar{w}$를 코드와 채널의 행렬 곱셈으로 표현하면 다음과 같다.

$$\bar{w}=\begin{bmatrix} c(L) & \cdots & c(1) \\ c(L+1) & \cdots & c(2) \\ \vdots & \vdots & \vdots \\ c(L_c) & \cdots & c(L_c-L+1) \end{bmatrix}h \tag{9}$$

식 (9)에서 코드로 이루어진 행렬을 kernel matrix로 명명하고, C로 정의한다.

$$C=\begin{bmatrix} c(L) & \cdots & c(1) \\ c(L+1) & \cdots & c(2) \\ \vdots & \vdots & \vdots \\ c(L_c) & \cdots & c(L_c-L+1) \end{bmatrix} \tag{10}$$

유저의 수가 P명이라면 각각의 유저가 서로 다른 코드를 이용하여 신호를 전송하기 때문에, 수신 신호가 다음과 같이 변형된다.

$$\bar{y}(n)=\sum_{i=1}^{P}\gamma_i\bar{w}_i s_i(n) \tag{11}$$

γ_i는 i번째 신호의 채널 이득값을 뜻한다. 식 (11)과 같이 표현할 경우, 유저별 채널 h_i의 크기를 모두 1로 고려할 수 있다.

다중 안테나로 수신하게 되면, 채널의 변화에 따라 signature waveform가 바뀌고, 코드는 변하지 않는다. 따라서 M개의 수신 안테나를 고려하여 최종 표현식을 다음과 같이 표현할 수 있다.

$$\overline{y}(n)=\begin{bmatrix}\overline{y}^1(n)\\ \vdots\\ \overline{y}^M(n)\end{bmatrix},\ \overline{w}_i=\begin{bmatrix}\overline{w}_i^1\\ \vdots\\ \overline{w}_i^M\end{bmatrix},\ h_i=\begin{bmatrix}h_i^1\\ \vdots\\ h_i^M\end{bmatrix} \quad (12)$$

2.2.2 OFDMA 기반 채널 추정 과정

P명의 유저를 고려한 OFDMA 시스템을 고려한다. 총 N개의 부반송파를 가지며, 0부터 $D-1$까지의 D개의 부반송파가 데이터 전송에 사용되는데, 나머지 $N-D$개의 부반송파는 virtual carrier라고 불리며 변조되지 않은 부반송파를 의미한다. 이 OFDM 시스템은 Q개의 cyclic prefix를 가진다고 가정한다. 변조 전의 심볼은 다음과 같다.

$$\boldsymbol{s}(n,k)=\left[s_1(n,k),s_2(n,k),\cdots,s_P(n,k)\right]^T \quad (13)$$

$$\boldsymbol{s}_n=\left[\boldsymbol{s}(n,0)^T,\boldsymbol{s}(n,1)^T,\cdots,\boldsymbol{s}(n,D-1)^T\right]^T \quad (14)$$

여기서 $d_j(n,k)$는 j번째 유저가 전송한 n번째 OFDM 심볼의 k번째 부반송파에 실린 심볼을 의미한다. J개의 연속된 OFDM 심볼을 모으면 다음과 같다.

$$\boldsymbol{s}(n)=\left[\boldsymbol{s}_n^T,\boldsymbol{s}_{n-1}^T,\cdots,\boldsymbol{s}_{n-J+1}^T\right]^T \quad (15)$$

$w_N=e^{j2\pi/N}$이라고 할 때, 푸리에 역변환 과정을 행렬로 정의할 수 있다.

$$\boldsymbol{W}(i)=\frac{1}{\sqrt{N}}\left[1,w_N^i,\cdots,w_N^{i(D-1)}\right] \quad (16)$$

$$\boldsymbol{W}=\left[\boldsymbol{W}(N-1)^T,\ldots,\boldsymbol{W}(0)^T,\boldsymbol{W}(N-1)^T,\ldots,\boldsymbol{W}(N-P)^T\right]^T \quad (17)$$

$$\boldsymbol{\Gamma}=\boldsymbol{I}_J\otimes\boldsymbol{W}\otimes\boldsymbol{I}_P \quad (18)$$

OFDM 변조 후 전송되는 신호벡터는 다음과 같다.

$$\boldsymbol{x}(n,k)=\left[x_1(n,k),x_2(n,k),\ldots,x_{M_p}(n,k)\right]^T \quad (19)$$

$$\boldsymbol{x}_n=\left[\boldsymbol{x}(n,N-1)^T,\ldots,\boldsymbol{x}(n,0)^T,\boldsymbol{x}(n,N-1)^T,\ldots,\boldsymbol{x}(n,N-P)^T\right]^T \quad (20)$$

$$\boldsymbol{x}(n)=\left[\boldsymbol{x}_n^T,\boldsymbol{x}_{n-1}^T,\ldots,\boldsymbol{x}_{n-J+1}^T\right]^T \quad (21)$$

이 때, 변조 전 신호와 변조 후 신호는 식 (21)을 이용하여 다음과 같이 표현할 수 있다.

$$\boldsymbol{x}(n)=\boldsymbol{\Gamma s}(n) \quad (22)$$

송수신 안테나 사이의 이산 채널을 $P\times N_{Tx}$의 길이 L을 갖는 필터로 가정하면

$$\boldsymbol{h}(l)=\begin{bmatrix}h_{11}(l) & h_{12}(l) & \cdots & h_{1P}(l)\\ h_{21}(l) & h_{22}(l) & \cdots & h_{2P}(l)\\ \vdots & \vdots & \vdots & \vdots\\ h_{N_{Tx}1}(l) & h_{N_{Tx}2}(l) & \cdots & h_{N_{Tx}P}(l)\end{bmatrix} \quad (23)$$

여기서 $l=0,\cdots,L$이다. 식 (24)를 이용해 $J(N+Q-L)N_{Tx}\times J(N+Q)P$ 채널 행렬을 아래와 같이 정의하면,

$$\boldsymbol{\Omega}=\begin{bmatrix}\boldsymbol{h}(0) & \cdots & \boldsymbol{h}(L_h) & \boldsymbol{0} & \cdots & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{h}(0) & \cdots & \boldsymbol{h}(L_h) & \cdots & \boldsymbol{0}\\ \vdots & & \ddots & & \ddots & \\ \boldsymbol{0} & \cdots & \boldsymbol{0} & \boldsymbol{h}(0) & \cdots & \boldsymbol{h}(L_h)\end{bmatrix} \quad (24)$$

수신 신호 벡터를 채널 행렬을 이용하여 다음과 같이 표현할 수 있다.

$$\boldsymbol{y}(n)=\boldsymbol{\Omega x}(n)=\boldsymbol{\Omega\Gamma s}(n)=\boldsymbol{\Xi s}(n) \quad (25)$$

2.2.3 수신 신호 기반 블라인드 추정 알고리즘

블라인드 추정 과정은 부공간을 기반으로 하여 진행한다. 잡음의 크기는 랜덤성을 가지므로, 이를 평균화하기 위해 여러 번의 데이터를 수신하여 추정한다. 총 N번의 데이터를 수신하는 경우 공분산행렬은 다음과 같이 나타난다.

$$\hat{R}=\frac{1}{N}\sum_{j=1}^{N}\overline{y}(j)\overline{y}(j)^H \quad (26)$$

식 (26)에 사용된 $\overline{y}(j)$는 CDMA 상황에서의 수신 신호를 의미하며 다음을 나타낸다.

$$\overline{y}(j)=\begin{bmatrix}\overline{y}_j^1(n)\\ \vdots\\ \overline{y}_j^M(n)\end{bmatrix}+\begin{bmatrix}\overline{n}_j^1\\ \vdots\\ \overline{n}_j^M\end{bmatrix} \quad (27)$$

공분산행렬은 고윳값 분해를 진행한다[12]. 대각행렬

을 내림차순으로 정렬하였을 때, 순서대로 P개를 제외한 나머지 값은 이론적으로 0이 나온다. 실제로는 잡음이 들어있기에 0이 나오지는 않지만, 신호 대 잡음비에 따라 상위 P개의 값이 상대적으로 큰 값을 가지므로 분류가 가능하다.

$$\hat{R} = \begin{bmatrix} \hat{U}_s & \hat{U}_n \end{bmatrix} \begin{bmatrix} \hat{\Lambda}_s & 0 \\ 0 & \hat{\Lambda}_n \end{bmatrix} \begin{bmatrix} \hat{U}_s^H \\ \hat{U}_n^H \end{bmatrix} \tag{28}$$

$\hat{\Lambda}_n$에 해당하는 고유벡터들이 모인 부공간 $\hat{U}_n$은 신호부공간 $\hat{U}_s$와 직교한다는 성질을 가진다. 따라서 잡음부공간과 signature waveform 또한 직교하는 성질을 가지며, 단일 수신의 경우에는 $\hat{U}_n^H C_i h_i = 0$을, 다중 수신의 경우에는 아래의 식을 만족하게 된다[9].

$$\hat{U}_n^H \begin{bmatrix} C_i & & 0 \\ & \ddots & \\ 0 & & C_i \end{bmatrix} h_i = 0 \tag{29}$$

C_i는 i번째 유저의 코드를 의미한다.

블라인드 채널 추정은 식 (29에서 나타나는 성질을 역으로 이용하여 추정이 이루어진다. 파악하고 있는 kernel matrix와 수신 신호를 바탕으로 구한 $\hat{U}_n$를 이용하여, 직교성을 만족하는 채널을 추정한다.

$$\hat{h} = \mathrm{argmin}_t \, t^H \left[\sum_{i=1}^{P} (C_i)^H \hat{U}_n \hat{U}_n^H C_i \right] t \tag{30}$$

전수조사를 통해 채널을 추정할 경우, 계산복잡도가 기하급수적으로 증가하므로 바람직하지 않다. 따라서 $Z^T \hat{U}_n \hat{U}_n^H Z$의 고윳값 중 최소값에 해당하는 고유벡터를 구하는 방법을 이용한다.

$$Z^T = \begin{bmatrix} C_1^T & \cdots & C_P^T \end{bmatrix} \tag{31}$$

2.2.4 채널 식별성

식 (30)에서 알 수 있듯이, 채널 h를 추정하는 마지막 단계는 $\hat{U}_n$과 직교하는 $C\hat{h}$를 찾는 과정이다. 이는 $\hat{U}_s$의 부공간과 $C\hat{h}$의 교집합을 찾는 과정과 동치이다. 따라서 유일한 채널 추정값을 얻기 위해서는 이론적으로 다음과 같은 조건들이 충족되어야 한다.

① Z의 벡터공간과 U_s의 벡터공간의 교집합이 1차원을 가질 것

② Kernel matrix C_i가 모두 세로 벡터에 대해 full rank일 것

해당 조건을 만족할 경우, 채널을 추정할 수 있는데, 여기서 h_0가 추정 결과인 경우, 임의의 복소 스칼라 변수 ϕ에 대해 ϕh_0또한 모든 조건을 만족하는 결과이다. 따라서 이러한 위상 모호성을 해결하여야 하며, 본 논문에서는 적군이 사용하는 파일럿 신호를 정확하게 알지 못하더라도, 그 종류의 풀을 알고있다고 가정한다. 따라서 적군이 서로의 송수신기 간의 채널을 파악하기 위해 파일럿 신호를 사용할 때, 보유한 신호의 후보 중에서 파일럿 신호를 파악하고 이를 바탕으로 위상 모호성을 보완한다.

2.3 보안 용량 및 중단 확률

적군 1의 상향링크 통신을 통해 사전에 채널 추정을 진행하였습니다. 이를 바탕으로 보안 용량을 구하고 채널 중단 확률에 대해 알아보겠습니다. 먼저 신호의 전송률을 구하기 위한 신호 대 잡음비는 다음과 같습니다.

2.3.1 신호 대 잡음비

(1) 단일 입력 단일 출력

아군 도청기기와 적군 Rx는 모두 적군 Tx가 송신한 신호의 세기 P_{Tx}를 거리와 채널이 반영된 만큼 받는다. 아군 기기의 경우 자체 간섭이 발생하고, 적군 수신기의 경우는 아군의 교란 신호를 추가적으로 받는다.

$$\gamma_{Jammer} = \frac{P_{Tx} d_{Tx \to J}^{-\alpha_{Tx \to J}} \left| h_{Tx \to J} \right|^2}{\sigma_J^2 + \beta P_J^{\lambda}} \tag{32}$$

$$\gamma_{Rx} = \frac{P_{Tx} d_{Tx \to Rx}^{-\alpha_{Tx \to Rx}} \left| h_{Tx \to Rx} \right|^2}{\sigma_{Rx}^2 + P_J d_{J \to Rx}^{-\alpha_{J \to Rx}} \left| h_{J \to Rx} \right|^2} \tag{33}$$

$d_{A \to B}$는 A와 B사이의 거리를, $\alpha_{A \to B}$는 exponent를 나타낸다.

(2) 다중 입력 단일 출력

송신 안테나가 여러 개인 경우에는 빔포밍을 수행해야 한다. 앞서 언급한 바와 같이 MRT 기법을 사용하는데, Tx에서 수행하는 송신 빔포밍은 Rx와의 채널만을 고려한 빔포밍을 뜻한다. 아군 도청장치는 추정한 채널로부터 생성할 수 있는 빔포밍을 진행한다.

$$\gamma_{Jammer} = \frac{P_{Tx} d_{Tx\to J}^{-\alpha_{Tx\to J}} \| H_{Tx\to,J\omega_{Tx\to Rx}} \|^2}{\sigma_J^2 + \beta P_J^{\lambda} \left| \hat{\omega}_{J\to Rx} \right|^2} \quad (34)$$

$$\gamma_{Rx} = \frac{P_{Tx} d_{Tx\to Rx}^{-\alpha_{Tx\to Rx}} \left| h_{Tx\to Rx} \omega_{Tx\to Rx} \right|^2}{\sigma_{Rx}^2 + P_J d_{J\to Rx}^{-\alpha_{J\to Rx}} \left| h_{J\to Rx} \hat{\omega}_{J\to Rx} \right|^2} \quad (35)$$

2.3.2 통신 채널 중단 확률

도청과 교란의 복합적 성능을 검증하기 위해서는 아군의 rate과 적군 수신기의 rate을 모두 고려해야 한다. 따라서 도청기 측면에서의 통신 채널 중단 확률을 별도로 정의하여 분석한다.

통신 채널 중단 확률을 구하기 위해서는 먼저 아군 도청장치의 rate과 적군 1의 rate을 알아야 한다. 다중 입력 단일 출력 환경에서의 신호 대 잡음비를 바탕으로 각각의 rate을 다음과 같이 구할 수 있다.

$$R_J = B\log_2(1+\gamma_J) \quad (36)$$

$$R_{Rx} = B\log_2(1+\gamma_{Rx}) \quad (37)$$

여기서 B는 아군 도청기기와 적군 수신기 사이의 대역을 뜻한다. 위에서 구한 두 개의 전송률을 바탕으로 보안 전송률을 다음과 같이 식으로 표현할 수 있다.

$$\begin{aligned} R &= \max\{0, R_J - R_{Rx}\} \\ &\approx B\log_2(1+\gamma_J) - B\log_2(1+\gamma_{Rx}) \\ &= B\left(\log_2\left(\frac{1+\gamma_J}{1+\gamma_{Rx}}\right)\right) \\ &= B\left(\log_2\left(\frac{1+\frac{P_{Tx} d_{Tx\to J}^{-\alpha_{Tx\to J}} \| H_{Tx\to,J\omega_{Tx\to Rx}} \|^2}{\sigma_J^2 + \beta P_J^{\lambda}}}{1+\frac{P_{Tx} d_{Tx\to Rx}^{-\alpha_{Tx\to Rx}} \left| h_{Tx\to Rx} \omega_{Tx\to Rx} \right|^2}{\sigma_{Rx}^2 + P_J d_{J\to Rx}^{-\alpha_{J\to Rx}} \left| h_{J\to Rx} \hat{\omega}_{J\to Rx} \right|^2}}\right)\right) \end{aligned} \quad (38)$$

따라서, 보안 중단 확률은 다음과 같이 정리할 수 있다.

$$\begin{aligned} P_{out} &= P\{R < R_{Threshold}\} \\ &= P\left\{\frac{1+\gamma_J}{1+\gamma_{Rx}} < 2^{\frac{R_{Threshold}}{B}}\right\} \\ &= P\left\{\frac{1+\frac{P_{Tx} d_{Tx\to J}^{-\alpha_{Tx\to J}} \| H_{Tx\to,J\omega_{Tx\to Rx}} \|^2}{\sigma_J^2 + \beta P_J^{\lambda}}}{1+\frac{P_{Tx} d_{Tx\to Rx}^{-\alpha_{Tx\to Rx}} \left| h_{Tx\to Rx} \omega_{Tx\to Rx} \right|^2}{\sigma_{Rx}^2 + P_J d_{J\to Rx}^{-\alpha_{J\to Rx}} \left| h_{J\to Rx} \hat{\omega}_{J\to Rx} \right|^2}} < 2^{\frac{R_{Threshold}}{B}}\right\} \\ &= P\left\{\left(\left(1-2^{\frac{R_{Threshold}}{B}}\right) + \frac{P_{Tx} d_{Tx\to J}^{-\alpha_{Tx\to J}} \| H_{Tx\to,J\omega_{Tx\to Rx}} \|^2}{\sigma_J^2 + \beta}\right.\right. \end{aligned} \quad (39)$$

$R_{Threshold}$ 는 미리 지정된 값으로 해당 rate보다 낮을 경우 중단이 발생하는 값을 뜻한다. 2.1장에 의해 $\left|h_{Tx\to Rx}\right|^2$은 감마분포를 따르기 때문에 중단확률을 아래와 같이 요약할 경우,

$$P_{out} = P\left\{K < \left|h_{Tx\to Rx}\right|^2\right\} \quad (40)$$

중단확률 값은 감마함수의 누적밀도함수를 통해 얻을 수 있다.

$$P_{out} = F(K) = E_{H_{Tx\to J}, h_{J\to Rx}}\left[\frac{1}{\Gamma(N_{Tx})}\gamma(N_{Tx}, K)\right] \quad (41)$$

여기서 K는 식 (40)의 확률함수 안에 있는 좌변을 뜻하며, $K = f_1 f_2 f_3 f_4$로 계산한다.

$$f_1 = \frac{\sigma_{Rx}^2\left(1-2^{\frac{R_{Threshold}}{B}}\right)}{2^{\frac{R_{Threshold}}{B}} P_{Tx} d_{Tx\to Rx}^{-\alpha_{Tx\to Rx}}} \quad (42)$$

$$f_2 = \frac{P_J d_{J\to Rx}^{-\alpha_{J\to Rx}}\left(1-2^{\frac{R_{Threshold}}{B}}\right)}{2^{\frac{R_{Threshold}}{B}} P_{Tx} d_{Tx\to Rx}^{-\alpha_{Tx\to Rx}}} \left|h_{J\to Rx}\hat{w}_{J\to Rx}\right|^2 \quad (43)$$

$$f_3 = \frac{\sigma_{Rx}^2 P_{Tx} d_{Tx\to J}^{-\alpha_{Tx\to J}}}{\sigma_J^2 + \beta P_J^{\lambda}} \| H_{Tx\to J} w_{Tx\to Rx} \|^2 \quad (44)$$

$$f_4 = \frac{P_J d_{J\to Rx}^{-\alpha_{J\to Rx}}\left(1-2^{\frac{R_{Threshold}}{B}}\right)}{2^{\frac{R_{Threshold}}{B}} P_{Tx} d_{Tx\to Rx}^{-\alpha_{Tx\to Rx}} (\sigma_J^2 + \beta P_J^{\lambda})} \left|h_{J\to Rx}\hat{w}_{J\to Rx}\right|^2 \quad (45)$$

Ⅲ. 실 험

2.3장에서 보안용량과 중단 확률의 성능을 분석하기 위해 적군 송신기의 SNR과 아군의 자체 간섭 성능을 변화시켜가며 적군 수신기의 SNR 변화로 인한 채널 중단 확률의 그래프를 구해보았다. 시뮬레이션에 적용한 환경은 1MHz의 대역을 사용하고, 거리별 손실 계수를 2.3으로 설정하였습니다. 전이중 통신장치의 자체 간섭 지수는 0.3으로 설정하였으며, 채널 중

단을 결정하는 rate의 경계값은 초당 100비트를 지정하였다.

적군 1은 단일 안테나, 적군 2는 3개의 안테나를 가지고 있다고 가정하고, 3개의 안테나를 가진 아군 기기가 도청 및 교란을 하는 상황을 다루었다. 거리와 잡음의 크기는 적군간 거리를 600m, 적군 수신기와 아군 기기의 거리를 200m, 적군 송신기와 아군 기기의 거리를 1000m로 설정하였다. 적군 수신기의 잡음은 -70dB를, 아군 기기의 수신 잡음은 -80dB로 설정 후 진행하였다. 블라인드 채널 추정 과정에서는 1000번의 수신을 통해 평준화 후 채널 추정을 진행하였고, 블라인드 채널 추정에서 발생하는 phase ambiguity의 값을 파악하였다고 가정하였다.

첫 번째로 도청 기기의 자체 간섭에 따른 중단 확률의 변화를 알아보기 위해, 자체 간섭 크기 변수를 변화시켜가며 확률의 변화를 살펴보았다. 총 5가지 다른 교란신호 세기마다 시뮬레이션을 진행하였고, 각 과정에서는 100000번씩 반복하여 신뢰성을 높였다. 그림 4에서 확인할 수 있듯이 5개의 그래프 모두 점진적으로 증가하여 최종적으로는 1에 도달하는 것을 확인할 수 있다. 기존의 정의에 따르면 β와 λ가 작을수록 자체 간섭 제거 능력이 더 높다는 것을 의미하는데, 이는 반대로 β가 커짐에 따라 자체 간섭이 잘 발생하여 outage가 잘 발생함을 의미한다. 따라서 점차 증가하고, 최종적으로는 1에 도달하는 결과는 매우 타당하다. 그래프 간의 값을 상대적으로 비교하였을 때에는, 동일한 β에 대해, 재밍 파워가 더 낮은 경우의 그래프가 더 낮은 중단 확률을 보인다. 교란 파워가 낮으면 적군 수신율이 높은 값을 가지기 때문에, outage가 더 잘 일어나는 결과를 확인할 수 있었다.

두 번째로는 고정된 자체 간섭 성능에서 적군 송신 신호의 세기에 따른 중단 확률의 변화를 알아보기 위해 -40dB부터 20dB까지 변화시켜가며 확률을 구해보았다. 이때, 실험은 총 5가지 서로 다른 β에 대해 이루어졌다. 실험 결과로부터 β가 낮은 경우, 즉, 도청 기기가 자체 간섭 제거 성능이 매우 뛰어난 경우에, 송신 신호가 낮은 영역에서도 뛰어난 교란 성능을 기반으로 낮은 중단확률을 보임을 알 수 있었다. 반대로 β가 높은 경우에는 아주 높은 세기로 적군이 송신을 하더라도 채널 중단 확률이 1에 근접한 결과를 보임을 통해 뛰어난 자체 간섭 제거 성능이 야기하는 교란 및 도청의 성능을 실제로 확인해볼 수 있었다.

Ⅳ. 결 론

본 논문에서는 전이중 통신 장치를 이용한 군 통신 시스템에서 전이중 장치의 자체 간섭 제거 성능에 따른 교란과 도청의 성능을 알아보는 연구를 진행하였다. 적군이 통신을 할 때, 아군 전이중 트랜시버가 도청과 교란을 동시에 진행하는 상황을 다루었다. 교란 신호는 부공간을 기반으로 한 블라인드 추정기법으로 적군의 채널을 추정하여 진행하였다.

본 연구에서는 도청 장치의 rate과 적군 수신기의 rate의 차를 바탕으로 한 채널 중단 확률을 이용하여 전이중 통신 기기의 교란 성능을 확인해보았다. 먼저 고정된 교란 신호의 세기별로 자체 간섭 제거 변수의 변화에 따른 중단 확률을 살펴보았고, 자체 간섭 계수가 유의미한 영향을 미치는 영역에서 중단 확률이 가파르게 상승하는 것을 확인하였다. 교란 신호의 세기가 커질수록 자체 간섭으로 인해 아군 도청장치의

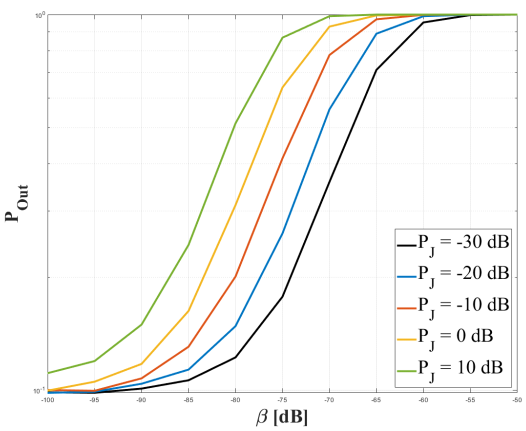

그림 4. 자체 간섭 성능 (β)에 따른 중단 확률
Fig. 4. Outage probability versus self-interference factor β

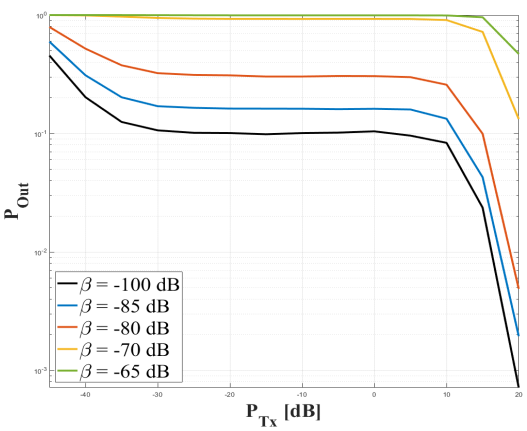

그림 5. 적군 송신 전력에 따른 중단 확률
Fig. 5. Outage probability versus transmission power

rate이 영향을 받는데, 이로 인해 채널 중단 확률이 더 높고, 더 빠르게 확률 1에 수렴하는 것을 확인할 수 있었다. 다음으로, 적군 송신 신호의 세기에 따른 채널 중단 확률을 알아보았다. 적군 송신 신호의 세기가 증가함에 따라 채널 중단 확률이 감소하는 것을 알 수 있었는데, 교란이 유의미한 영향을 끼치면 송신 빔포밍이 증가하더라도 도청률이 더 크게 상승함을 알 수 있었다.

그림 4에서 주어진 환경 β가 -80dB 이상인 경우부터 중단 확률이 급격히 증가한다는 사실을 알 수 있었다. β값의 크기에 따라 중단 확률이 차이를 보이는 것을 알 수 있는데, 그림 5의 결과로부터 SI 취소 성능이 높을수록 보안 성능을 높일 수 있는 결과까지 확인할 수 있다.

References

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

[2] V. Syrjala, M. Valkama, L. Anttila, T. Riihonen, and D. Korpi, "Analysis of oscillator phase-noise effects on self-interference cancellation in fullduplex ofdm radio transceivers," *IEEE Trans. Wirel. Commun.,* vol. 13, no. 6, pp. 2977-2990, 2014.

[3] D. Korpi, M. Heino, C. Icheln, K. Haneda, and M. Valkama, "Compact inband full-duplex relays with beyond 100 db self-interference suppression: Enabling techniques and field measurements," *IEEE Trans. Antennas and Propag.*, vol. 65, no. 2, pp. 960-965, 2017.

[4] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Sign. Process.*, vol. 61, no. 20, pp. 4962-4974, Oct. 2013.

[5] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Info. Forensics and Secur.*, vol. 12, no. 5, pp. 1195-1206, May 2017.

[6] T. Zheng, H. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/halfduplex receiver deployment strategy," *IEEE Trans. Wirel. Commun.*, vol. 16, no. 6, pp. 3827-3839, Jun. 2017.

[7] X. Tang, Y. Cai, Y. Deng, Y. Huang, W. Yang, and W. Yang, "Energy-constrained swipt networks: Enhancing physical layer security with fd self-jamming," *IEEE Trans. Info. Forensics and Secur.*, vol. 14, no. 1, pp. 212-222, Jan. 2019.

[8] T. Riihonen, D. Korpi, M. Turunen, T. Peltola, J. Saikanmaki, M. Valkama, and R. Wichman, "Tactical communication link under joint jamming and interception by same-frequency simultaneous transmit and receive radio," in *IEEE MILCOM 2018*, pp. 1-5, 2018.

[9] W. Kang and B. Champagne, "Subspace-based blind channel estimation: generalization and performance analysis," *IEEE Trans. Sign. Process.*, vol. SP-53, no. 3, pp. 1151-1162, Mar. 2005.

[10] H. Liu and G. Xu, "A subspace method for signature waveform estimation in synchronous CDMA systems," *IEEE Trans. Commun.*, vol. 44, pp. 1346-1354, Oct. 1996.

[11] M. Abughalwa, L. Samara, M. O. Hasna, and R. Hamila, "Full-duplex jamming and interception analysis of uav-based intrusion links," *IEEE Commun. Lett.*, 2020.

[12] S. Kim, Y. Jang, J. Ahn, and J. Kang, "Subspace-based blind channel estimation in MIMO environment," in *Proc. Symp. KICS*, pp. 267-268, Jeju Island, Korea, Jun. 2018.

김 상 혁 (Sang-hyuk Kim)

2017년 8월 : 한국과학기술원 수리과학과 졸업
2019년 8월 : 한국과학기술원 전기및전자공학부 석사
2019년 9월~현재 : 한국과학기술원 전기및전자공학부 박사과정

<관심분야> 무선통신, 통신공학, 신호처리 등
[ORCID:0000-0001-8897-5627]

강 준 혁 (Joon-hyuk Kang)

1991년 : 서울대학교 제어계측공학과 졸업
1993년 : 서울대학교 제어계측공학과 석사
2002년 : The University of Texas at Austin 전자컴퓨터공학과 박사
2003년~2009년 : ICU 부교수
2009년~현재 : 한국과학기술원 전기및전자공학부 정교수
<관심분야> 무선통신, 신호처리, 인지무선통신,실내위치인식 등
[ORCID:0000-0003-2933-5528]