심볼-단위 재밍 공격 감쇄를 위한 적응형 수신 빔포밍 기법의 성능 분석

송용진, 이영석, 정방철

충남대학교

yjsong@o.cnu.ac.kr, yslee@o.cnu.ac.kr, bcjung@cnu.ac.kr

Performance Analysis of Adaptive Receive Beamforming Technique for Mitigating Symbol-level Jamming Attacks

Yong-Jin Song, Young-Seok Lee, Bang Chul Jung

Chungnam National University

요 약

본 논문에서는 공인 송신기와 동일한 변조 및 채널 부호를 사용하는 심볼-단위 재밍(symbol-level jamming: SLJ) 공격이 존재하는 통신 환경에서 그 영향을 효과적으로 감쇄할 수 있는 적응형 수신 빔포밍 기술을 제안하고 비트 당 오류율(bit-error-rates: BER) 성능을 수학적으로 분석한다. 구체적으로, 본 논문에서 다중안테나 수신기는 에너지 탐지를 통해 SLJ의 공격을 탐지하고 SLJ 공격이 탐지된 심볼에 대해 방향탐지를 적용하여 재머의 가시선(line-of-sight: LoS) 채널을 추정한다. 다중안테나 수신기는 SLJ 공격 유무에 따른 심볼에 대해 서로 상이한 수신 빔포밍을 수행함으로써 SLJ 공격을 완화할 수 있으며 이때의 BER 성능을 수학적으로 분석한다. 모의실험을 통해 본 논문에서 제안하는 적응형 수신 빔포밍 기법이 SLJ 공격의 영향을 효과적으로 완화할 수 있음과 수학적으로 분석한 BER 성능이 실제 모의실험 결과를 잘 나타내는 것을 검증한다.

Ⅰ. 서 론

차세대 이동통신에서 인공지능(artificial intelligence: AI)을 활용한 통신 시스템의 성능 개선 연구가 학계 및 산업계에서 활발히 진행되고 있다 [1]. 그러나, AI 기술의 발전은 송수신기 간 주파수 대역, 채널 부호 기법, 변복조 기법 등 물리 계층 보안과 관련한 다양한 통신 파라미터를 추정하는 데 도움을 줄 수 있어 재밍(jamming)과 같은 의도적 전파 간섭 공격에 취약해질 수 있는 문제가 있다 [2]. 이러한 AI 기술을 기반으로 재머가 공인 송신기가 사용하는 변조 및 채널 부호 기법을 똑같이 적용하여 신호를 생성하고 전송함으로써 수신기를 무력화할 수 있는 심볼-단위 재밍(symbol-level jamming: SLJ) 공격은 수신기가 전파 간섭 공격을 탐지 및 완화하는데 까다로울 수 있어 매우 심각한 통신 성능 저하가 발생할 수 있다 [3, 4].

따라서, 본 논문에서는 SLJ 공격이 존재하는 통신 환경에서 SLJ 신호가 존재하는 심볼을 탐지하고 해당 심볼에 대해 다중안테나 수신기가 방향탐지를 통해 재머의 채널을 추정하는 과정과 SLJ 공격의 유무에 따라 서로 상이한 수신 빔포밍을 적용함으로써 SLJ 공격을 완화할 수 있는 적응형 수신 빔포밍 기법을 제안한다. 또한, 본 논문에서는 반복 부호(repetition code: RC)와 길쌈 부호(convolutional code: CC)를 적용할 때의 SLJ 신호 영향 저감을 비트 당 오류율(bit-error-rates: BER) 관점에서 수학적으로 분석한다. 모의실험을 통해, 본 논문에서 제안하는 적응형 수신 빔포밍 기법의 SLJ 신호 감쇄 성능을 확인하고 수학적으로 분석한 BER 성능이 실제 모의실험 결과를 잘 표현하는 것을 검증한다.

Ⅱ. SLJ 공격 감쇄를 위한 적응형 수신 빔포밍 기법

본 논문에서는 그림 1과 같이 M개의 안테나를 갖는 수신기와 단일 안테나를 갖는 공인 송신기와 재머가 존재하는 통신 환경을 고려한다. 재머는 기지국과 가시선(line-of-sight: LoS) 경로를 확보하였다고 가정하였으며 공인 송신기가 사용하는 변조 및 부호 방식(modulation and coding scheme: MCS)을 정확히 추정하였다고 가정한다. 이때, 다중안테나 수신기는 공인 송신기와의 채널 상태 정보(channel state information: CSI)만 알고 있다고 가정하였다. 본 논문에서 재머는 공인 송신기의 MCS 정보를 추정한 후 SLJ 신호를 송신하기 때문에 채널 부호를 위한 인터리빙(interleaving)을 고려할 때 전체 N개의 심볼을 포함하는 패킷에서 SLJ 신호가 존재하는 심볼 수의 비율로써 재밍 확률을 정의할 수 있다. 따라서, $i(\in\{1,\cdots,N\})$째 심볼에 대한 수신 신호 $\mathbf{y}_i\in\mathbb{C}^M$는 재밍 확률 α에 따라 다음과 같이 표현할 수 있다.

$$\mathbf{y}_i=\begin{cases}\sqrt{E}x_i\mathbf{h}_i+\mathbf{w}_i, & \text{with probability } \alpha,\\ \sqrt{E}x_i\mathbf{h}_i+\beta\sqrt{E}e^{j\phi}z_i\mathbf{a}+\mathbf{w}_i, & \text{w.p. } 1-\alpha,\end{cases}$$

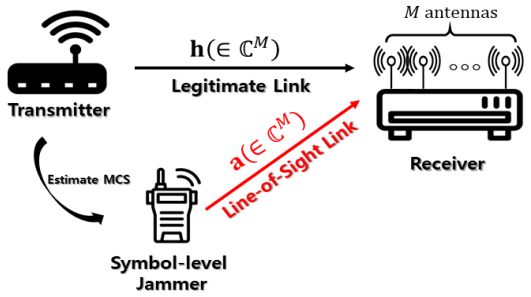

그림 1. 다중 안테나 기반 적응형 수신 빔포밍 기법의 시스템 모델

여기서, E는 심볼 에너지를 나타내며 x_i는 공인 송신기가 전송한 i째 변조 심볼을 나타내고 z_i는 동일한 MCS 방식을 적용하여 재머가 생성한 임의의 심볼을 나타낸다. 이때, β와 ϕ는 공인 송신기가 전송한 신호 대비 재머가 송신한 SLJ 신호의 크기 비율 및 위상 오차를 나타낸다. 또한, $\mathbf{w}_i(\in\mathbb{C}^M)$는 수신기에서 발생하는 부가 열잡음 벡터를 의미하며 본 논문에서 모든 잡음 원소는 평균이 0이고 분산이 N_0인 복소 가우시안 분포를 따른다고 가정하였다. 본 논문에서 공인 송신기와 수신기 간 채널 $\mathbf{h}_i(\in\mathbb{C}^M)$는 통계적으로 $\mathcal{CN}(\mathbf{0},\mathbf{I}_M)$ 분포를 따르는 레일리 페이딩(Rayleigh fading) 채널 환경을 가정하였으며, $\mathbf{a}(\in\mathbb{C}^M)$는 재머와 수신기 사이의 LoS 채널을 나타낸다. 균일 선형 배열안테나(uniform linear array: ULA) 수신기를 가정할 때 $m(\in\{1,\cdots,M\})$째 원소 a_m은 다음과 같이 정의된다.

$$a_m=e^{-j\frac{2\pi}{\lambda}d(m-1)\cos\theta},$$

여기서 d는 안테나 간 이격거리를 나타내고, λ는 파장을 의미하며, θ는 재머가 송신한 SLJ 신호의 입사각을 의미한다. 수신기는 에너지 탐지를 통해 SLJ 신호가 존재하는 심볼을 추정하며, SLJ 신호가 존재하는 심볼에 대해 공인 송신기와 수신기 간 채널 성분을 제거함으로써 재머와 수신기 간 LoS 채널 $\mathbf{a}$를 추정하기 위한 방향탐지를 수행할 수 있다.

이후, 수신기는 추정한 재머의 LoS 채널을 이용하여 다음과 같이 SLJ 신호가 존재하는 심볼에 대해 간섭 제거(zero-forcing: ZF) 빔포밍을 수행하고 SLJ 신호가 없는 심볼에 대해선 주어진 공인 송신기 간 무선 채널의 이득을 극대화하도록 최대 비율 결합(maximum ratio combining: MRC) 빔포밍을 수행한다.

$$\tilde{y}_i=\begin{cases}\mathbf{b}^i_{\mathrm{MRC}}\mathbf{y}_i=\|\mathbf{h}_i\|x_i+\tilde{w}_i, & \text{w.p. } \alpha,\\ g_i\mathbf{b}^i_{\mathrm{ZF}}\mathbf{y}_i=g_ix_i+\tilde{w}_i, & \text{w.p. } 1-\alpha,\end{cases}$$

여기서 $\mathbf{b}^i_{\mathrm{MRC}}(\in\mathbb{C}^{1\times M})=\mathbf{h}_i^{\mathrm{H}}/\|\mathbf{h}_i\|$이며, $\mathbf{b}^i_{\mathrm{ZF}}(\in\mathbb{C}^{1\times M})$은 공인 송신기와 재머의 채널을 결합한 $\mathbf{H}_i(\in\mathbb{C}^{M\times 2})=[\mathbf{h}_i\ \mathbf{a}]$의 유사-역행렬의 첫 번째 행을 나타낸다. 이때, $g_i=\sqrt{1/\left[(\mathbf{H}_i^{\mathrm{H}}\mathbf{H}_i)^{-1}\right]_{1,1}}$는 동일 신호 대 잡음비(signal-to-noise ratio: SNR)를 가지면서 유효 잡음 $\tilde{w}_i$의 분산을 σ_n^2으로 표현하기 위한 정규화 요소(regularization factor)를 나타낸다 [5].

Ⅲ. 제안하는 적응형 수신 빔포밍 기술의 BER 성능 분석

본 논문에서는 직교 위상 편이 변조(quadrature phase shift keying: QPSK)와 채널 부호 기법으로 RC와 CC를 고려할 때의 제안하는 적응형 수신 빔포밍 기법의 BER 성능을 수학적으로 분석한다. 이때, QPSK 심볼은 첫 번째 비트와 두 번째 비트가 각각 복소부와 실수부에 대응되며 비트 0과 1은 각각 복소평면에서의 양수와 음수에 대응되도록 설정하였다 [3]. 또한, 본 논문에서는 일반적인 채널 환경에서의 BER 성능을 분석하기 위해 주파수-선택(frequency-selective) 페이딩 환경을 가정하였으며 SLJ 신호 탐지 및 채널 추정 오차는 없다고 가정하였다.

*A. RC*를 적용할 때의 적응형 수신 빔포밍 기법의 *BER* 성능 분석

본 논문에서는 일반성을 잃지 않고, QPSK 심볼의 대칭성을 이용하여 공인 송신기가 00 비트를 전송할 때 첫 번째 비트의 오류 확률을 유도한다. 따라서, 부호화율 $R_C=1/n$을 갖는 n-RC를 가정할 때, $k(\in\{1,\cdots,n\})$째 반복 수신 빔포밍 신호 $\tilde{y}_k$는 다음과 같다.

$$\tilde{y}_k=\begin{cases}\|\mathbf{h}_k\|x+\tilde{w}_k, & \text{w.p. } \alpha,\\ g_kx+\tilde{w}_k, & \text{w.p. } 1-\alpha,\end{cases}$$

여기서 x는 $\sqrt{E/2}+j\sqrt{E/2}$를 나타낸다. 채널 이득 벡터로써 $\boldsymbol{\gamma}(\in\mathbb{C}^{1\times n})=[\gamma_1,\cdots,\gamma_n]$, $\gamma_k\in\{\|\mathbf{h}\|_k,g_k\}$로 정의하면, 위 식은 n 반복에 대한 수신 신호 벡터 $\tilde{\mathbf{y}}(\in\mathbb{C}^{1\times n})=\boldsymbol{\gamma}x+\tilde{\mathbf{w}}$로 표현할 수 있으며 채널 이득 벡터 $\boldsymbol{\gamma}$가 주어질 때의 조건부 오류 확률은 다음과 같다.

$$\Pr(\epsilon|\boldsymbol{\gamma})=\mathrm{Q}\left(\sqrt{\frac{\mathrm{E}\|\boldsymbol{\gamma}\|^2}{\mathrm{N}_0}}\right),$$

여기서 $\|\boldsymbol{\gamma}\|^2$은 n-반복 신호 중 SLJ 신호가 존재하는 반복 신호의 개수가 K일 때 자유도 $2(nM-K)$의 카이제곱(chi-squared) 분포를 따른다고 알려져 있으며 SLJ 신호의 수 K가 주어질 때 조건부 오류 확률은 다음과 같이 유도될 수 있다 [5].

$$\Pr(\epsilon|K)=\frac{1}{2}\left[1-\sum_{k=0}^{nM-K-1}\binom{2k}{k}\sqrt{\frac{E_b/N_0}{E_b/N_0+n}}\left(\frac{n}{4E_b/N_o+4n}\right)^k\right],$$

여기서 $E_b(=nE/2)$는 비트당 에너지를 나타낸다. 따라서, n-RC를 적용할 때의 제안하는 적응형 수신 빔포밍 기법의 BER 성능은 전체 확률 정리와 이항 정리에 따라 다음과 같이 유도될 수 있다.

$$\Pr(\epsilon)=\sum_{K=0}^{n}\Pr(\epsilon|K)\Pr(K)$$
$$=\sum_{K=0}^{n}\binom{n}{K}\frac{\alpha^K(1-\alpha)^{n-K}}{2}\left[1-\sum_{k=0}^{nM-K-1}\binom{2k}{k}\sqrt{\frac{E_b/N_0}{E_b/N_0+n}}\left(\frac{n}{4E_b/N_o+4n}\right)^k\right].$$

*B. CC*를 적용할 때의 적응형 수신 빔포밍 기법의 *BER* 성능 분석

CC를 고려하면서 Viterbi 복호기를 사용할 때 수학적으로 분석할 수 있는 BER 표현 중 하나로 상한(upper bound)인 $\Pr(\epsilon)<\sum_{d=d_{free}}^{\infty}A_d\Pr(d)$으로 BER 성능을 분석할 수 있다. 여기서 가중치 A_d와 d_{free}는 CC 부호기에 따라 결정되는 파라미터이다 [3]. $\Pr(d)$는 일반성을 잃지 않고 모든 원소가 0으로만 이루어진 부호가 해밍 가중치(Hamming weight)가 d인 부호로 오류가 발생할 pairwise error probability (PEP)를 나타내며 QPSK의 비트 매핑과 주파수-선택 페이딩 환경을 고려함에 따라 $\Pr(d)$는 d-RC를 적용한 BER 성능과 동일하다고 알려져 있다 [5]. 따라서, 부호율 R_c에 대한 CC를 적용할 때의 제안하는 적응형 수신 빔포밍 기법의 BER 성능 상한은 다음과 같이 유도된다.

$$\Pr(\epsilon)<\sum_{d=d_{free}}^{\infty}A_d\sum_{K=0}^{d}\binom{d}{K}\frac{\alpha^K(1-\alpha)^{d-K}}{2}$$
$$\times\left[1-\sum_{k=0}^{dM-K-1}\binom{2k}{k}\sqrt{\frac{E_b/N_0}{E_b/N_0+1/R_c}}\left(\frac{1}{4R_cE_b/N_o+4}\right)^k\right].$$

Ⅳ. 모의실험 결과 및 결론

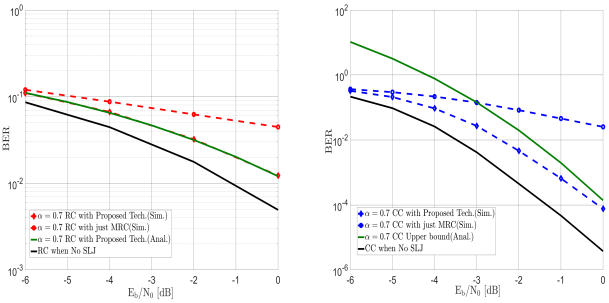

그림 2 적응형 수신 빔포밍 기술의 BER 성능

그림 2는 SLJ 신호가 재밍 확률에 따라 수신 받은 패킷 내 존재할 때 제안하는 적응형 수신 빔포밍 기법의 항재밍 성능을 BER 측면에서 도시한 결과이다. 본 모의실험에서 $M=4$, $\theta=30^\circ$이고, 중심 주파수는 3.5GHz로 설정하였다. 또한, 본 실험에선 재머의 동기 오차를 고려하지 않아 $\phi=0$ 및 $\beta=3$인 이상적인 재밍 환경을 고려하였다. RC와 CC 모두 1/2의 부호율을 갖는 인코더를 고려하였으며, CC는 8진수로 (133, 171)의 생성 다항식을 가지며 $d_{free}=10$인 인코더를 사용하였다 [6]. 본 논문에서 제안하는 기법의 항재밍 성능은 SLJ 신호가 있음에도 수신기가 공인 사용자와의 채널 이득을 극대화할 수 있는 MRC 빔포밍만을 수행할 때의 결과와 비교하였다. 그림 2를 통해 본 논문에서 제안하는 항재밍용 적응형 수신 빔포밍 기법이 SLJ 신호를 효과적으로 완화하는 것을 확인할 수 있으며, 또한 본 논문에서 분석한 수학적 BER 표현이 실제 모의실험 결과를 잘 나타내는 것을 검증하였다.

ACKNOWLEDGMENT

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(2021-0-00486, ABC-MIMO: 증강 빔 라우팅 기반 차세대 다중 입출력 통신 시스템) 및 한국연구재단의 지원(No. NRF-2022R1I1A3073740)을 받아 수행된 연구임.

참 고 문 헌

[1] S. V. Balkus, *et. al*, "A survey of collaborative machine learning using 5G vehicular communications," *IEEE Commun. Surveys Tut.*, vol. 24, no. 2, pp. 1280-1303, 2nd Quart. 2022.

[2] Z. Kaleem, M. Ali, I. Ahmad, W. Khalid, A. Alkhayyat, and A. Jamalipour, "Artificial intelligence-driven real-time automatic modulation classification scheme for next-generation cellular networks," *IEEE Access*, vol. 9, pp. 155584-155597, Nov. 2021.

[3] H. S. Jang and B. C. Jung, "Performance analysis of reactive symbol-level jamming techniques," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12432-12437, Dec 2018.

[4] Y. S. Jang, J. T. Park, and I. S. Kim, "BER expression of QAM for symbol-level jamming," *IEEE Trans. Wireless Commun.*, vol. 21, no. 2, pp. 1037-1048, Feb. 2022.

[5] Y. -S. Lee, K. -H. Lee, H. S. Jang, G. Jo, and B. C. Jung, "Performance analysis of resource hopping-based grant-free multiple access for massive IoT networks," *IEEE Wireless Commun. Lett.*, vol. 11, no. 12, pp. 2685-2689, Dec. 2022.

[6] J. Conan, "The weight spectra of some shor low-rate convolutional codes," *IEEE Trans. Commun.*, COM-32, no. 9, pp. 1050-1053, Sep. 1984.