저지연 보안 통신 시스템을 위한 전송 기법 설계

오민택, 박정훈*, 최진석
한국과학기술원 전기 및 전자공학부, *연세대학교 전기전자공학부
ohmin@kaist.ac.kr, jhpark@yonsei.ac.kr, jinseok@kaist.ac.kr

Transmission Design for Low-latency Secure Communication Systems

Mintaek Oh, Jeonghun Park*, and Jinseok Choi
School of Electrical Engineering, KAIST
*School of Electrical and Electronic Engineering, Yonsei University

요 약

본 논문에서는 저지연 보안 통신 시스템을 위해 유한 블록 길이(FBL) 체제 하에서 다수의 사용자와 도청자를 포함한 다운링크 통신에 대한 공동 최적화 문제를 해결한다. 해당 시나리오의 주요 목표는 비밀율의 합을 최대화하고 최대 오류 확률 및 정보 유출율을 최소화하는 것이다. 이를 위해, 보안 프리코딩 설계와 최대 오류 확률 및 정보 유출율 최소화를 위한 두 단계로 문제를 분해하는 번갈아 최적화하는 접근 방식을 채택한다.

Ⅰ. 서론

초신뢰성 저지연 통신(URLLC)은 5G 및 6G 통신에서 주요 사용 시나리오 중 하나로, 짧은 데이터 패킷 전송의 이점을 활용하기 위해 유한 블록 길이(FBL) 기반 통신이 적합하다 [1]. 그러나 FBL 체제에서는 해석 오류 확률과 블록 길이에 의해 결정되는 백오프 요소에 의해 통신이 제한되는 문제가 존재한다. URLLC 와 더불어 통신의 보안 문제는 차세대 통신에서 중요한 이슈로 부상하고 있다. 이전 연구에서는 다중 사용자와 단일 도청자를 포함하는 무선 네트워크에서 보안 프리코딩 솔루션에 대해 연구되었다. 특히 다중 안테나를 사용하는 다중 도청자를 포함하는 시스템에서 비밀율을 최대화하는 보안 전송 전략이 제안되어왔다. 또한, 무한한 코딩 길이를 갖는 일반적인 통신 시스템을 넘어 저지연 통신을 위해 고려된 FBL 기반 통신 시스템에서도 최대 코딩율에 대한 분석 및 최적화 기법들이 활발하게 연구되어왔다 [2].

본 논문에서는 FBL 기반 다운링크 저지연 보안 통신 시스템을 고려하며, 다중 안테나를 갖춘 엑세스 포인트(AP)가 다중 사용자에게 서비스를 제공하는 동안 여러 도청자가 사용자 메시지를 도청하려고 시도한다고 가정한다. 해당 네트워크의 물리 계층 보안 이슈를 해결하기 위해 보안 전송률(secrecy rate)을 주요 성능 지표로 채택하고, 이를 최대화하는 방법과 동시에 URLLC 을 만족하는 공동 최적화 기법에 대해 알아본다.

Ⅱ. 본론

본 논문에서는 N개의 안테나인 AP 와 K명의 단일 안테나 유저, M명의 단일 안테나 도청자가 존재하는 유한한 코딩 길이($L<\infty$)를 갖는 다운링크 시스템을 고려한다. 이 시스템에서 프리코딩을 포함한 전송 신호는 $\mathbf{x}=\mathbf{Fs}$이며, 여기서 $\mathbf{F}=[\mathbf{f}_1,\mathbf{f}_2,\dots,\mathbf{f}_K]\in\mathbb{C}^{N\times K}$는 프리코딩 행렬, $\mathbf{s}\sim\mathcal{CN}(\mathbf{0}_{N\times 1},P\boldsymbol{I}_N)$는 유저 심볼 벡터이며, P는 최대 전송 전력이다. 이를 토대로 k번째 유저와 k번째 유저를 도청하는 m번째 도청자의 SINR 은 다음과 같다:

$$\gamma_k=\frac{|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_k|^2}{\sum_{i=1,i\neq k}^{K}|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_i|^2+\sigma^2/P},\ \gamma_{m,k}^{\mathrm{e}}=\frac{|\mathbf{g}_m^{\mathrm{H}}\mathbf{f}_k|^2}{\sum_{i=1,i\neq k}^{K}|\mathbf{g}_m^{\mathrm{H}}\mathbf{f}_i|^2+\sigma^2/P}.$$

이를 기반으로 k번째 유저를 도청하는 m번째 도청자의 전송률은 다음과 같다:

$$R_k=\log_2(1+\gamma_k),\ R_{m,k}^{\mathrm{e}}=\log_2\left(1+\gamma_{m,k}^{\mathrm{e}}\right)$$

여기서, $\mathbf{h}_k\in\mathbb{C}^N$, $\mathbf{g}_m\in\mathbb{C}^N$는 각각 k번째 유저와 m번째 도청자의 채널 벡터이며, σ^2와 σ_{e}^2는 유저와 도청자 신호에서의 잡음 분산이다. 이를 기반으로 k번째 유저에 대한 FBL 최대 보안 전송률은 다음과 같이 정의한다:

$$R_k^{\mathrm{sec}}=R_k-\sqrt{\frac{V_k}{L}}Q^{-1}(\epsilon_k)-\max_{m\in\mathcal{M}}\left\{R_{m,k}^{e}+\sqrt{\frac{V_{m,k}^{\mathrm{e}}}{L}}Q^{-1}(\delta_{m,k})\right\}.$$

위의 수식에서 FBL 체제에서 선천적으로 생기는 백오프 요소 안에 얽혀져 있는 $V_k, V_{m,k}^{\mathrm{e}}$는 채널 분산이며, ϵ_k는 디코딩 에러 확률이며, $\delta_{m,k}$는 정보 유출율이다. 따라서, 기존 통신율과 달리 FBL 을 가정함으로써 백오프 요소 안에 있는 값들도 추가적으로 고려되어야 한다.

알고리즘 1: Proposed Alternating Algorithm

1. **initialize**: $\bar{\mathbf{f}}^{(0)}, \epsilon_k^{(0)}, \delta_{m,k}^{(0)}, \forall k \in \mathcal{K}, \forall m \in \mathcal{M}$, and $t = 1$.
2. **while** *increment of* $\sum_{k=1}^{K} R_k^{\text{sec}} > \varepsilon$ & $t \le t_{\max}$ **do**
3. $\quad \bar{\mathbf{f}}^{(t)} = \text{GPIP}\left(\epsilon_1, \dots, \epsilon_K, \delta_{1,1}, \dots, \delta_{M,K}\right)$.
4. $\quad$ Compute $\tau^\star$ and $\xi^\star$ for $\bar{\mathbf{f}}^{(t)}$.
5. $\quad t \leftarrow t + 1$.
6. **return** $\bar{\mathbf{f}}^\star = \left[\mathbf{f}_1^{T(t)}, \dots, \mathbf{f}_K^{T(t)}\right]^T, \boldsymbol{\epsilon}^\star = \left[\epsilon_1^{(t)}, \dots, \epsilon_K^{(t)}\right]^T, \boldsymbol{\delta}^\star = \left[\delta_{1,1}^{(t)}, \dots, \delta_{M,K}^{(t)}\right]^T$.

이제 총 최대 보안 전송률 및 에러 확률과 정보 유출량에 대한 최적화 문제를 에러 확률과 정보 유출율의 최대 제약조건 $\hat{\epsilon}_k, \hat{\delta}_{m,k}$ 값을 고려하여 다음과 같이 정의한다:

$$\underset{\mathbf{f}_1, \mathbf{f}_2, \dots \mathbf{f}_K}{\text{maximize}} \ \sum_{k=1}^{K} R_k^{\text{sec}}\left(\mathbf{f}_k, \epsilon_k, \delta_{m,k}; L\right)$$

$$\underset{\epsilon_1, \epsilon_2, \dots, \epsilon_K}{\text{minimize}} \ \max\{\epsilon_1, \epsilon_2, \dots, \epsilon_K\}$$

$$\underset{\delta_{1,1}, \delta_{1,2}, \dots, \delta_{M,K}}{\text{minimize}} \ \max\{\delta_{1,1}, \delta_{1,2}, \dots, \delta_{M,K}\}$$

$$\text{s.t.} \sum_{k=1}^{K} \|\mathbf{f}_k\|^2 \le 1, \epsilon_k \le \hat{\epsilon}_k, \delta_{m,k} \le \hat{\delta}_{m,k} \forall m \in \mathcal{M}, \forall k \in \mathcal{K}$$

위에서 정의된 최적화 문제는 다목적 최적화이며 non-convex 하다. 이는 두 단계로 문제를 분해한 뒤 번갈아 최적화하는 방법을 사용한다.

Phase I. 최적의 보안 프리코더 설계

정의된 최적화 문제에서 프리코더를 제외한 나머지 변수들을 고정한 뒤, GPIP [3] 형태로 나타낼 수 있다:

$$\underset{\mathbf{f}_1, \mathbf{f}_2, \dots \mathbf{f}_K}{\text{maximize}} \ \sum_{k=1}^{K} \log_2 \left(\frac{\bar{\mathbf{f}}^{\mathrm{H}} \mathbf{A}_k \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathrm{H}} \mathbf{B}_k \bar{\mathbf{f}}}\right)^{\omega_k} - \ln\left\{\sum_{m=1}^{M} \beta \left(\frac{\bar{\mathbf{f}}^{\mathrm{H}} \mathbf{C}_{m,k} \bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathrm{H}} \mathbf{D}_{m,k} \bar{\mathbf{f}}}\right)^{\omega_{m,k}^{\mathrm{e}}}\right\}^{\frac{1}{\alpha}}$$

위의 수식의 자세한 값들은 [3]에 정리되어 있다. GPIP 를 따르면 non-convex 한 목적함수의 가장 좋은 국부 최적해를 찾을 수 있다.

Phase II. 에러 확률 및 정보 유출량 최소화

이번 단계에서는 GPIP 를 통해 얻어진 프리코더를 고정한 뒤, 가중-합 접근법과 모든 도청자의 합을 고려한 다중 최적화 문제를 다음과 같이 나타낼 수 있다:

$$\underset{\substack{\epsilon_1, \epsilon_2, \dots, \epsilon_K \\ \delta_{1,1}, \delta_{1,2}, \dots, \delta_{M,K}}}{\text{minimize}} \ \frac{w}{R_\infty} \sum_{k=1}^{K} \left[\sqrt{\frac{V_k}{L}} Q^{-1}(\epsilon_k) + \sum_{m=1}^{M} \sqrt{\frac{V_{m,k}^{\mathrm{e}}}{L}} Q^{-1}(\delta_{m,k})\right] + (1-w)\left(\frac{\tau}{\hat{\epsilon}_{\max}} + \frac{\xi}{\hat{\delta}_{\max}}\right)$$

$$\text{s.t.} \ 0 \le \epsilon_k \le \hat{\epsilon}_k, \epsilon_k \le \tau, 0 \le \tau \le \hat{\epsilon}_{\max},$$

$$0 \le \delta_{m,k} \le \hat{\delta}_{m,k}, \delta_{m,k} \le \xi, 0 \le \xi \le \hat{\delta}_{\max}, \forall m \in \mathcal{M}, \forall k \in \mathcal{K}$$

위의 문제에서 $\hat{\epsilon}_{\max}$와 $\hat{\delta}_{\max}$는 목표 에러 확률과 정보 유출율 중 가장 큰 값을 취한 것이다. 또한 τ, ξ 는 모든 $\epsilon_k, \delta_{m,k}$중 가장 큰 값을 나타낸다.

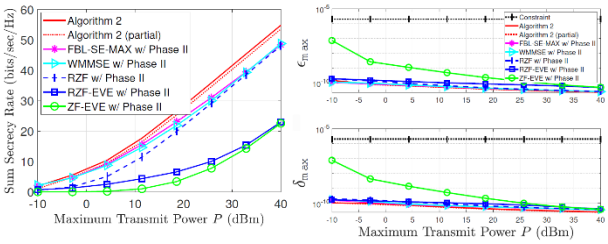

그림 1. 전송 전력 대 목표 처리량

이제 해당 문제는 convex하기 때문에, KKT 조건을 이용하여 closed-form 솔루션을 [3]을 따라 다음과 같이 얻을 수 있다:

$$\tau^\star = Q\left(\sqrt{2\ln\left(\frac{\sqrt{L}(1-w)R_\infty}{\hat{\epsilon}_{\max} w \sqrt{2\pi} \sum_{k=1}^{K} \sqrt{V_k}}\right)}\right),$$

$$\xi^\star = Q\left(\sqrt{2\ln\left(\frac{\sqrt{L}(1-w)R_\infty}{\hat{\delta}_{\max} w \sqrt{2\pi} \sum_{m=j(k)}^{K} \sum_{k=1}^{K} \sqrt{V_{m,k}^{\mathrm{e}}}}\right)}\right).$$

그림 1 에서 전송 전력이 증가함에 따라 제안된 알고리즘들과 기존 기법들 간에 최대 보안 전송률의 합 성능 차이가 증가하는 것을 확인할 수 있다. 또한 최대 보안 전송률의 합을 유지하며, 또다른 목표 처리량인 에러 확률과 정보 유출율을 최소화하는 것을 확인할 수 있다.

Ⅲ. 결론

본 논문에서는 유한한 블록길이를 갖는 FBL 체제 안에서 다수 유저들과 도청자들이 공존하는 네트워크에서의 보안 프리코딩 설계와 동시에 에러 확률 및 정보 유출율을 최소화하는 공동 최적화 문제를 해결하였다. 제안된 알고리즘은 모든 전송 파워 구간에서 목표 처리량에 대한 뛰어난 성능을 보였으며, 이를 통해 URLLC 를 지원할 수 있는 기법임을 입증하였다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단(No. 2021R1C1C1004438)의 지원과, 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터 사업(IITP-2023-RS-2023-00259991)의 지원을 받아 수행된 연구임.

참 고 문 헌

[1] G. Durisi, et al. "Toward massive, ultrareliable, and low-latency wireless communication with short packets." Proc. of the IEEE 104, no. 9 (2016).

[2] W. Yang, et al. "Wiretap channels: Nonasymptotic fundamental limits." IEEE Trans. on Info. Theory 65, no. 7 (2019).

[3] M. Oh, et al. "Joint Optimization for Secure and Reliable Communications in Finite Blocklength Regime." IEEE Trans. on Wireless Commun. (2023).