

단방향 릴레이 은닉 통신 환경에서 정보 최신성 향상을 위한 재밍 전략

심승민¹, 김진웅², 이제민¹

¹성균관대학교 전자전기컴퓨터공학과, ²대구경북과학기술원 전기전자컴퓨터공학과

ssm4591@g.skku.edu, yoy876@dgist.ac.kr, jemin.lee@skku.edu

Jamming Strategy for Improving Data Freshness in One-Way Relay Covert Communications

Seungmin Sim¹, Jinwoong Kim², Jemin Lee¹

¹Department of Electrical and Computer Engineering, Sungkyunkwan Univ.,

²Department of Electrical Engineering and Computer Science, DGIST.

요약

본 논문은 단방향 릴레이 은닉 통신 환경에서 높은 정보의 최신성과 은밀성을 달성하기 위하여 릴레이 재밍 전략을 제안하고, 이를 age of information (AoI)와 detection error probability (DEP)를 이용하여 분석하였다. 은닉 조건을 만족하는 평균 AoI 최소화 문제를 통해 최적의 릴레이 재밍 비율을 제시하고, 시뮬레이션 결과를 통하여 이를 검증하였다.

I. 서론

최근 무선 환경에서 보안의 중요성이 커지면서 릴레이 시스템을 비롯하여 여러 환경의 은닉 통신 연구가 활발하게 진행되고 있다 [1]. 또한 실시간 군사 전략 시스템 (e.g., 미사일 요격)의 경우, 무선 통신의 은밀성 뿐만 아니라 정보의 최신성도 중요하므로 두가지를 모두 고려해야 한다[2]. 이에 본 논문에서는 단방향 릴레이 은닉 환경에서 릴레이 재밍 전략을 제안하였고, 릴레이 재밍 전력과 데이터 전력 간의 최적 비율을 유도함으로써 은닉 통신의 조건을 만족하며 최대의 정보의 최신성을 달성하였다.

II. 본론

2.1 시스템 모델

본 논문에서는 decode-and-forward (DF)-relay 환경을 고려하며 Source(S) 그리고 Destination (D), Relay (R), Warden (W)이 존재한다. S와 D 사이의 거리가 멀어 통신은 R을 통해서만 전송되며 W라는 감시자에 의해 S와 R 사이의 통신이 감시된다. 각 노드는 한 개의 안테나를 가지며, R은 데이터 수신과 재밍 신호 전송을 위해 안테나 하나를 더 가진다. S와 D의 통신은 2단계로 구성된다. 1 단계에서 S는 전력 P_A 를 사용하여 사전 전송 확률 p 에 따라 R로 신호를 전송하며 R은 전력 ρP_{sum} 로 재밍 신호를 전송하여 W를 방해한다. P_{sum} 은 R의 데이터 전력과 재밍 전력의 합이며 ρ 는 재밍 전력의 비율이다. 2 단계에서 R은 수신된 신호를 전력 $(1-\rho)P_{sum}$ 을 사용하여 D로 전송한다. R이 S의 신호를 수신 시 자신의 재밍 신호에 대해 완벽한 self-interference cancellation을 거친다고 가정한다. 통신 채널은 block Rayleigh fading을 따르며, 각 노드 사이의 채널은 h_x , 채널 이득의 평균값은 λ_x 로 $x \in \{SR, RD, SW, RW\}$ 로 정의된다. 따라서 R과 D의 수신된 신호는 다음과 같다.

$$y_R[i] = \sqrt{P_S} h_{SR} x_S[i] + n_R[i] \quad (1)$$

$$y_D[i] = \sqrt{(1-\rho)P_{sum}} h_{RD} x_R[i] + n_D[i] \quad (2)$$

여기서 $i = 1, 2, \dots, n$ 으로 channel use의 index이다. $x_S[i]$ 와 $x_R[i]$ 는 각각 S와 R로부터 전송된 신호로 $\mathbb{E}[x_S[i]x_S^*[i]] = 1$, $\mathbb{E}[x_R[i]x_R^*[i]] = 1$ 을 만족한다. 또한 $n_R[i]$, $n_D[i]$ 는 R과 D의 additive white gaussian noise (AWGN)이며 분산은 σ_R^2 와 σ_D^2 이다. 이때 DF 환경에서 R과 D의 decoding error probability는 다음과 같이 정의된다 [1].

$$o_R = Q\left(\frac{C_R - R_R}{\sqrt{\frac{1}{n}(1-2^{-2C_R})\log_2 e}}\right) \quad (3)$$

$$o_D = Q\left(\frac{C_D - R_D}{\sqrt{\frac{1}{n}(1-2^{-2C_D})\log_2 e}}\right) \quad (4)$$

여기서 $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{u^2}{2}\right) du$ 는 Q-function, $C_R = \log_2(1 + \frac{P_S |h_{SR}|^2}{\sigma_R^2})$ 와 $C_D = \log_2(1 + \frac{(1-\rho)P_{sum} |h_{RD}|^2}{\sigma_D^2})$ 는 Shannon 채널용량, R_R , R_D 는 S와 R, R과 D의 통신속도이다. 이를 통해 D의 successful decoding probability는 다음과 같다.

$$q = (1 - o_R)(1 - o_D) \quad (5)$$

2.2 Average age of information (AoI)

본 논문에서는 D가 수신하는 데이터 정보의 최신성을 분석하기 위해 [3]에서 제안된 AoI를 사용하며 D의 평균 AoI는 다음과 같이 표현된다 [4].

$$\bar{\Delta} = \frac{\mathbb{E}[Q_k]}{\mathbb{E}[U_k]} = \frac{\mathbb{E}[U_k^2]}{2\mathbb{E}[U_k]} + \frac{3}{2} = \frac{1}{pq} + 1 \quad (6)$$

여기서 Q_k 는 D의 $k-1$ 과 k 번째 전송 성공 사이의 시간에 대한 AoI 면적의 적분 값을 의미하며 U_k 는 $k-1$ 과 k 번째 전송 성공 사이의 시간 간격을 의미한다.

2.3 최적의 재밍 전력 비율

시스템 내의 W가 수신한 신호는 다음과 같다.

$$y_W[i] = \begin{cases} \sqrt{\rho P_{sum}} \hat{h}_{RW} x_J[i] + n_W[i], & H_0 \\ \sqrt{P_S} \hat{h}_{SW} x_S[i] + \sqrt{\rho P_{sum}} \hat{h}_{RW} x_J[i] + n_W[i], & H_1 \end{cases} \quad (7)$$

여기서 $x_J[i]$ 는 R의 재밍 신호로 $\mathbb{E}[x_J[i]x_J^*[i]] = 1$ 을 만족한다. $n_W[i]$ 는 W의 AWGN이며 분산 σ_W^2 을 가진다. H_0 와 H_1 은 S가 신호를 전송하지 않은 경우와 전송한 경우이다. W의 감지 성능은 detection error probability로 정의되며 다음과 같다.

$$p_{WE} = (1-p)p_{FA} + pp_{MD} \quad (8)$$

여기서 p 는 사전 전송 확률, $p_{FA} = \Pr(D_1|H_0)$ 은 false alarm probability, $p_{MD} = \Pr(D_0|H_1)$ 은 miss detection probability을 의미한다. 그리고 D_0 와 D_1 은 W의 H_0 , H_1 에 대한 의사결정이다. W의 의사결정은 한 time slot 내에 수신한 전력에 대해 detection threshold τ 와 비교하여 내려지며 다음과 같다.

$$P_W \geq_{D_0}^{D_1} \tau \quad (9)$$

P_W 는 수신 전력으로 다음과 같이 정의된다.

$$P_W = \begin{cases} \rho P_{sum} |h_{RW}|^2 + \sigma_W^2, & H_0 \\ P_S |h_{SW}|^2 + \rho P_{sum} |h_{RW}|^2 + \sigma_W^2, & H_1 \end{cases} \quad (10)$$

수식 (8)로부터 최적 detection threshold τ^* 를 구할 수 있으며, 이를 이용한 최적 detection error probability p_{WE}^* 는 다음과 같다 [4].

$$p_{WE}^* = \begin{cases} (1-p)\theta_0, & |h_{SW}|^2 \geq \mu \\ p, & |h_{SW}|^2 < \mu \end{cases} \quad (11)$$

여기서 $\theta_0 = \exp(-\frac{\lambda_{RW}|h_{SW}|^2 P_S}{\rho P_{sum}})$, $\mu = \frac{\rho P_{sum}}{\lambda_{RW} P_S} \ln(\frac{1-p}{p})$ 이다.

이때 S와 D은 W와 관련된 정확한 채널이득에 대해서 알 수 없으므로 expected detection error probability를 사용하며, 이는 $p \geq \frac{1}{2}$ 일 때 다음과 같이 표현된다 [4].

$$\bar{p}_{WE}^* = (1-p)\theta_1 \quad (12)$$

여기서 $\theta_1 = \frac{\lambda_{SW} \rho P_{sum}}{\lambda_{SW} \rho P_{sum} + \lambda_{RW} P_S}$ 를 의미한다.

수식 (6)과 (12)를 바탕으로 은닉 조건을 만족하며 D의 평균 AoI를 최소화하기 위한 문제는 다음과 같다.

$$\begin{aligned} \min_{\rho} \quad & \bar{\Delta} \\ \text{s.t.} \quad & \bar{p}_{WE}^* \geq 1 - \epsilon \\ & 0 < \rho < 1 \end{aligned} \quad (13)$$

우리는 수식 (12)로부터 ρ 가 증가할수록, 즉 재밍에 할당된 전력이 커질수록 \bar{p}_{WE}^* 이 증가함을 알 수 있다. 또한 ρ 가 증가하면 R의 데이터 전력이 감소하여 평균 AoI가 증가하므로, 은닉 조건을 만족하는 최소의 ρ 값이 평균 AoI를 최소화하는 최적의 ρ 가 된다. 따라서 최적의 ρ 값은 다음과 같다.

$$\rho^* = \frac{(1-\epsilon)\lambda_{RW} P_S}{\lambda_{SW} P_{sum}(\epsilon - p)} \quad (14)$$

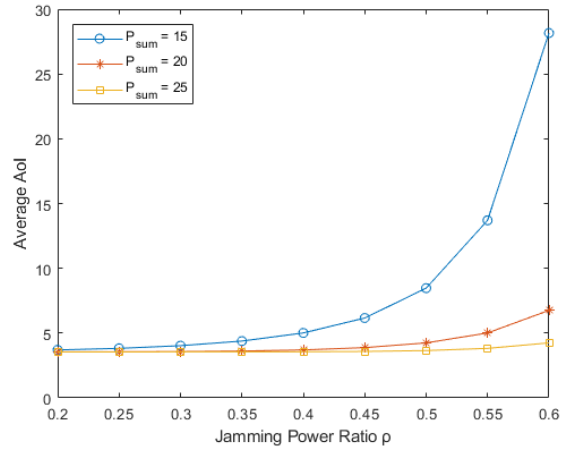


그림 1 Relay 재밍 전력 비율에 따른 평균 AoI

III. 실험 결과

본 논문에서 제안한 시스템의 성능을 파악하기 위하여 시뮬레이션에서 사용된 파라미터 값들은 $R_R = R_D = 0.5$,

$n = 100$, $\frac{P_S |h_{SR}|^2}{\sigma_R^2} = \frac{|h_{RD}|^2}{\sigma_D^2} = 0.05$, $P_S = 10\text{mW}$ 이다.

그림 1은 R의 총 전력 대비 재밍 전력 비율 ρ 에 따른 평균 AoI를 나타낸다. 재밍 전력 비율이 상승할수록 평균 AoI가 증가함을 확인할 수 있다. 이는 재밍 전력 비율이 증가할수록 R의 데이터 전력이 낮아지기 때문이다. 또한 P_{sum} 이 증가할수록 R의 재밍 전력 비율이 높아져도 상대적으로 낮은 AoI를 보이는 것을 확인할 수 있다. 이는 높은 P_{sum} 을 가진 R의 데이터 전력이 은닉 통신 환경에서 D의 successful decoding probability를 만족할 확률이 높기 때문이다.

IV. 결론

본 논문에서는 단방향 릴레이 은닉 환경에서 릴레이의 재밍 전력과 데이터 전력 간의 최적의 비율 조절을 통해 정보의 최신성을 보장하기 위하여 평균 AoI를 최소화하는 문제를 공식화하였다. 이를 통하여 은닉 조건을 만족하는 최소의 재밍 전력 비율이 평균 AoI를 최적화하는 최적의 비율이 된다는 것을 보였다.

ACKNOWLEDGMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2020R1A2C2C008878).

참고 문헌

- [1] X. Yu, S. Yan, J. Hu, P. Haskell-Dowland, Y. Han and D. W. K. Ng, "On Relaying Strategies in Multi-Hop Covert Wireless Communications," 2022 IEEE International Conference on Communications, Seoul, Korea, Republic of, 2022, pp. 666-672.
- [2] W. Yang, X. Lu, S. Yan, F. Shu and Z. Li, "Age of Information for Short-Packet Covert Communication," IEEE Wireless Communications Letters, vol. 10, no. 9, pp. 1890-1894, 2021.
- [3] S. Kaul, R. Yates and M. Gruteser, "Real-time status: How often should one update?," 2012 Proceedings IEEE INFOCOM, Orlando, FL, USA, 2012, pp. 2731-2735.
- [4] Y. Wang, S. Yan, W. Yang and Y. Cai, "Covert Communications With Constrained Age of Information," in IEEE Wireless Communications Letters, vol. 10, no. 2, pp. 368-372, 2021.