논문 21-46-09-08 The Journal of Korean Institute of Communications and Information Sciences '21-09 Vol.46 No.09
https://doi.org/10.7840/kics.2021.46.9.1407

시분할 다중 접속 네트워크에서의 은닉 통신 기법

문 지 환•

Covert Communications in Time Division Multiple Access Networks

Jihwan Moon•

요 약

본 논문에서는 시분할 다중 접속 네트워크에서의 은닉 통신 기법을 기술한다. 하나의 송신 노드와 여러 개의 일반 수신 노드, 그리고 한 개의 은닉 수신 노드가 존재하는 네트워크에서 송신 노드가 일반 수신 노드의 통신 링크를 활용하여 동시에 은닉 수신 노드에게 정보를 전달하는 시스템을 고려한다. 통신의 존재가 노출되지 않도록 일반 수신자와 은닉 수신 노드를 위한 전력 분배 방법을 제시하며 실험 결과를 통해 일정 수준의 탐지 오류 확률을 유지하며 달성할 수 있는 은닉 통신 속도를 확인한다.

Key Words : Wireless communications, Physical layer security, Time division multiple access, covert communications, covert channel

ABSTRACT

In this paper, we investigate covert communications in time division multiple access (TDMA) networks. The considered system consists of one transmitter, a number of ordinary receivers, and one convert receiver. The transmitter exploits the communications link for the ordinary receiver to simultaneously support a covert transmission for the covert receiver. We propose a power allocation method to ensure the covertness, and the simulation result verifies its impact on the covert rate performance while maintaining a certain detection error probability at the ordinary receivers.

Ⅰ. 서 론

급격하게 발전하고 있는 무선 통신[1]을 위한 정보 보안 기술이 학계 및 산업계로부터 큰 관심을 받고 있다. 특히 물리 계층에서의 보안 기술은 크게 세 가지 방향으로 개발됐다. 하나는 주변 도청자가 정상적으로 디코딩할 수 없도록 만드는 보안 통신 기술[2], 또 다른 방향은 주변에 범죄를 일으킬 것으로 의심되는 사용자끼리 어떤 정보를 주고받는지 감시하는 무선 감시 시스템이다[3].

마지막으로는 주위로 통신 존재 자체를 노출하지 않는 은닉 통신 기법이 있다[4]. 비직교 다중 접속 네트워크, 지능형 반사 표면, 밀리미터파, 무인이동체 등의 다양한 환경에서 활발한 연구가 진행되고 있다[5]. 하지만 아직 시분할 다중 접속 네트워크에서의 은닉 통신 속도 최대화를 고려한 연구는 불충분한 상태이다.

본 논문은 시분할 다중 접속 네트워크에서의 은닉 통신 기법을 다룬다. 하나의 송신 노드와 여러 개의 일반 수신 노드, 그리고 한 개의 은닉 수신 노드가 존재하는 네트워크에서 송신 노드가 일반 수신 노드의 통신 링크를 활용하여 동시에 은닉 수신 노드에 정보를 전달하는 시스템을 고려한다. 따라서 본 연구에서는 기존 계층적 변조[6]의 전송 용량 최대화 목적과는 다르게 통신의 존재가 노출되지 않도록 일반 수신자와 은닉 수신 노드를 위한 전력 분배 방법을 제시한다. 실험 결과를 통해 일정 수준의 탐지 오류 확률을 유지하며 달성할 수 있는 은닉 통신 속도를 확인한다.

Ⅱ. 본 론

2.1 시스템 모델

그림 1은 본 논문에서 고려하는 시스템 모델을 도시한다. 모든 노드는 하나의 안테나를 가지고 있으며 하나의 송신 노드 S가 K개의 일반 수신 노드 U_1, ..., U_K에게 하향 링크로 정보를 전송한다. 시분할 다중 접속 방식을 사용하며 동시에 은닉 수신 노드 C에게 높은 보안이 요구되는 정보를 전달한다. 따라서 송신 노드는 일반 수신 노드의 정보와 은닉 수신 노드의 정

※이 논문은 조선대학교 학술연구비의 지원을 받아 연구되었음(2020)

• First Author : (ORCID:0000-0002-9812-7768)Department of Information and Communication Engineering, Chosun University, Gwangju 61452, South Korea, anschino@chosun.ac.kr, 조교수, 정회원

논문번호 : 202107-179-A-LU, Received July 24, 2021; Revised July 29, 2021; Accepted August 3, 2021

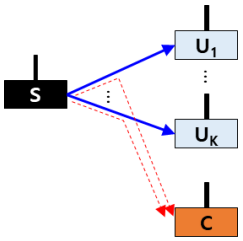

그림 1. 시스템 모델
Fig. 1. System model

보에 할당되는 전력을 조절하여 일반 수신 노드가 은닉 통신 링크 존재를 인지하기 힘들게 만든다.

이때 단위 시간 k 동안 일반 수신 노드 U_k와 은닉 수신 노드 C에 수신되는 신호는 각각

$$y_{U_k} = h_{SU_k}(\sqrt{P_S\alpha_k}x_{U_k} + \sqrt{P_S\beta_k}x_C[k]) + z_{U_k} \quad (1)$$

$$y_C = h_{SC}(\sqrt{P_S\alpha_k}x_{U_k} + \sqrt{P_S\beta_k}x_C[k]) + z_C[k] \quad (2)$$

로 표현된다. h_{XY}는 노드 X-Y 사이 Rayleigh 무선 채널, P_X는 노드 X에서의 송신 전력, $\alpha_k, \beta_k \in [0,1]$는 각각 일반 수신 노드 U_k와 은닉 수신 노드 C의 정보에 할당되는 전력 비율, $x_X \sim CN(0,1)$는 노드 X의 정보, $z_{U_k} \sim CN(0,\sigma_{U_k}^2)$와 $z_C[k] \sim CN(0,\sigma_C^2)$는 각각 일반 수신 노드 U_k와 은닉 수신 노드 C에서의 잡음, $\sigma_{U_k}^2$와 σ_C^2는 각각 잡음 z_{U_k}와 $z_C[k]$의 세기를 뜻한다.

수식 (1)과 (2)를 바탕으로 단위 시간 k 동안 일반 수신 노드 U_k가 자신의 정보 x_{U_k}를 정보 이론적으로 오류 없이 복구할 수 있는 최대 전송 속도는

$$\overline{R}_{U_k,U_k}(\alpha_k,\beta_k) = \log_2\left(1 + \frac{|h_{SU_k}|^2 P_S\alpha_k}{|h_{SU_k}|^2 P_S\beta_k + \sigma_{U_k}^2}\right) \quad (3)$$

이다. 한편 단위 시간 k 동안 은닉 수신 노드 C는 자신에게 전달된 정보인 $x_C[k]$를 효과적으로 복구하기 위해 일반 수신 노드의 정보 x_{U_k}를 제거해야 한다. 즉, 은닉 수신 노드 C의 실질적 수신 정보는

$$\tilde{y}_C = h_{SC}\sqrt{P_S\beta_k}x_C[k] + z_C[k] \quad (4)$$

이다. 그리고 위와 같이 은닉 수신 노드 C가 x_{U_k}와 $x_C[k]$를 동시에 정보 이론적으로 오류 없이 복구할 수 있는 최대 전송 속도는 각각 다음과 같다.

$$\overline{R}_{U_k,C}(\alpha_k,\beta_k) = \log_2\left(1 + \frac{|h_{SC}|^2 P_S\alpha_k}{|h_{SC}|^2 P_S\beta_k + \sigma_C^2}\right) \quad (5)$$

$$\overline{R}_{C,C}(\alpha_k,\beta_k) = \log_2\left(1 + \frac{|h_{SC}|^2 P_S\beta_k}{\sigma_{U_k}^2}\right) \quad (6)$$

2.2 잡음 불확실성

본 논문에서는 [4]와 같이 잡음 불확실성을 고려한다. 구체적으로는 $\sigma_{U_k}^2$의 dB 단위 수치인 $\sigma_{U_k,dB}^2$가

$$\sigma_{U_k,dB}^2 \sim U(\overline{\sigma}_{U_k,dB}^2 - \zeta_{dB}, \overline{\sigma}_{U_k,dB}^2 + \zeta_{dB}) \quad (7)$$

와 같이 평균값 $\overline{\sigma}_{U_k,dB}^2$를 기준으로 최대 변동치가 ζ_{dB}인 균일 분포 $U(\bullet)$를 따른다고 가정한다. 이때 $\sigma_{U_k,dB}^2$의 확률밀도함수와 누적분포함수는 각각

$$f_{\sigma_{U_k,dB}^2}(\nu_{dB}) = \frac{1}{2\zeta_{dB}} \quad (8)$$

$$F_{\sigma_{U_k,dB}^2}(\nu_{dB}) = \frac{1}{2\zeta_{dB}}(\nu_{dB} - (\overline{\sigma}_{U_k,dB}^2 - \zeta_{dB})) \quad (9)$$

이며 $\nu_{dB} \in [\overline{\sigma}_{U_k,dB}^2 - \zeta_{dB}, \overline{\sigma}_{U_k,dB}^2 + \zeta_{dB}]$이다. 나아가 $\sigma_{U_k,dB}^2 = 10\log_{10}\sigma_{U_k}^2$임을 통해 $\sigma_{U_k}^2$의 확률밀도함수와 누적분포함수를

$$f_{\sigma_{U_k}^2}(\nu) = \frac{1}{2\ln\zeta}\frac{1}{\nu} \quad (10)$$

$$F_{\sigma_{U_k}^2}(\nu) = \frac{1}{2\ln\zeta}\left(\ln\nu - \ln\left(\frac{1}{\zeta}\overline{\sigma}_{U_k}^2\right)\right) \quad (11)$$

로 나타낼 수 있고 $\nu \in \left[\overline{\sigma}_{U_k}^2/\zeta, \zeta\overline{\sigma}_{U_k}^2\right]$이다.

2.3 탐지 오류 확률

단위 시간 k 동안 은닉 통신이 없는 경우의 귀무가설 H_0, 존재하는 경우의 대립가설 H_1은

$$\begin{aligned} H_0 &: y_{U_k} = h_{SU_k}\sqrt{P_S}x_{U_k} + z_{U_k} \\ H_1 &: y_{U_k} = h_{SU_k}(\sqrt{P_S}x_{U_k} + \sqrt{P_S\beta_k}x_C[k]) + z_{U_k} \end{aligned} \quad (12)$$

로 표현 가능하다. 일반 수신 노드 U_k는 수신 신호의 전력 세기 T를 이용하여 은닉 통신의 존재 여부를 판단하며 자신의 정보 x_{U_k}를 제거한 후 잔여 신호 전력 세기 T를 각각의 상황에 대해 구하면

$$\begin{aligned} H_0 &: T = E\left[\left|z_{U_k}\right|^2\right] = \sigma_{U_k}^2 \\ H_1 &: T = E\left[\left|h_{SU_k}\sqrt{P_S}\left(\left(\sqrt{\alpha_k}-1\right)x_{U_k}+\sqrt{\beta_k}\,x_C[k]\right)+z_{U_k}\right|^2\right] \\ &= \left|h_{SU_k}\right|^2 P_S\left(\sqrt{\alpha_k}-1\right)^2 + \left|h_{SU_k}\right|^2 P_S\beta_k + \sigma_{U_k}^2 \end{aligned} \tag{13}$$

이다. 따라서 사전에 고정된 실수 λ에 대해 $T \le \lambda$이면 H_0, $T > \lambda$이면 H_1로 판단할 시 탐지 오류 확률은 오경보 확률과 검출 실패 확률 두 개의 합으로 나타나게 되고 이는 다음과 같다.

$$\Pr\{error\} = \Pr\{T > \lambda \mid H_0\} + \Pr\{T \le \lambda \mid H_1\} \tag{14}$$

2.4 총 은닉 통신 속도 최대화

위를 바탕으로 총 은닉 속도 최대화 문제는

$$\begin{aligned} \max_{\{\alpha_k\},\{\beta_k\},\{R_{U_k}\}} \quad & \sum_{k=1}^{K} \overline{R}_{C,C}[k](\alpha_k,\beta_k), \\ s.t. \quad & \sum_{k=1}^{K} R_{U_k} \ge R_{SUR,\min} \\ & R_{U_k} \le \overline{R}_{U_k,U_k}(\alpha_k,\beta_k) \mid_{\sigma_{U_k}^2 = \zeta\overline{\sigma}_{U_k}^2}, k = 1,\ldots,K, \\ & R_{U_k} \le \overline{R}_{U_k,C}(\alpha_k,\beta_k), k = 1,\ldots,K, \\ & \overline{\Pr}\{error \mid \alpha_k\} \ge \epsilon, k = 1,\ldots,K, \\ & \alpha_k + \beta_k = 1, k = 1,\ldots,K, \\ & 0 \end{aligned}$$

로 정립되며 $\overline{\Pr}\{error \mid \alpha_k\}$는 일반 수신 노드 U_k에서의 최소 탐지 오류 확률, R_{U_k}는 일반 수신 노드 U_k의 통신 속도이다. 위 문제는 비볼록 문제이기에 일반적으로 풀기 쉽지 않아 전수 조사가 필요하다. 따라서 본 논문은 저복잡도 알고리즘을 제시한다.

먼저 R_{U_k}를 조건식 2와 3의 상한값 중 작은 값으로 고정한 뒤 조건식 1에 대입하여 조건식 1, 2, 3을 모두 만족시킬 수 있으며 α_k에 대해 단조 증가한다. 한편 목적 함수는 α_k에 대해 단조 감소하기 때문에 다음의 알고리즘을 제안한다.

또한 $R_{SUR,\min}$을 만족하는 $\{\alpha_k\}$가 존재하면 은닉 통신이 가능함을 (3)과 (5)을 통해 증명할 수 있다.

초기화: $\alpha_k \leftarrow 1, \forall k, \ \Delta\alpha \ll 1$
반복:
각 U_k에 대한 $\overline{R}_{C,C}[k](\alpha_k,\beta_k)$ 미분값 계산.
값이 가장 큰 노드 U_l에 대해 $\alpha_l \leftarrow \alpha_l - \Delta\alpha$.
조건식 1, 2, 3이 만족하지 않게 되면 종료.

Ⅲ. 실험 결과 및 결론

$K=2$이고 송신 노드로부터 일반 수신 노드와 은닉 수신 노드까지의 거리는 0에서 1000 m 사이에서 무작위로 선택됐다. 그 외 $\overline{\sigma}_{U_k,dB}^2$=-100 dBm, ζ_{dB}=50 dB, σ_C^2=-160 dBm, ϵ=0.7, $R_{SUR,\min}$=5 bps/Hz, 거리에 따른 신호 감쇠 계수는 3.5로 설정했다. 무작위로 α_k를 선택한 "Random alphas"이나 α_k를 0.5로 고정한 "Fixed alphas" 대비 전수 조사된 α_k "Optimal alpha"와 제안한 알고리즘 "Low complexity"가 더 높은 성능을 보였다. 또한 $R_{SUR,\min}$이 적당한 범위일 때 총 은닉 속도는 감소하고 일반 노드 통신 속도는 증가하지만 특정값을 넘어서면 두 통신 모두 불가능함을 확인할 수 있다.

본 논문의 신호 중첩 외 다른 효과적인 은닉 통신 방법은 향후 연구 주제로서 충분한 가치가 있을 것이다.

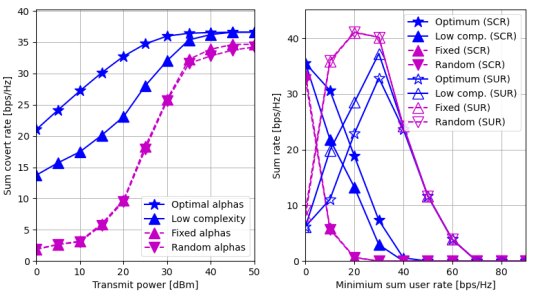

그림 2. 총 은닉 통신 속도
Fig. 2. Sum covert rate

References

[1] Y. Jeon, S.-H. Park, C. Song, J. Moon, S. Maeng, and I. Lee, "Fronthaul designs with self-interference mitigation for full-duplex cloud radio access networks," *2017 Winter Conf. KICS*, Jan. 2017.

[2] A. D. Wyner, "The wire-tap channel," *Bell*

Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80-83, Feb. 2016.

[4] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Wireless Commun. Lett.*, vol. 21, no. 4, pp. 941-944, Apr. 2017.

[5] J. Zhang, M. Li, S. Yan, C. Liu, X. Chen, M.-J. Zhao, and P. Whiting, "Joint beam training and data transmission design for covert millimeter-wave communication," *IEEE Trans. Info. Forens. and Secur.*, Jan. 2021.

[6] H. Jiang and P. A. Wilford, "A hierarchical modulation for upgrading digital broadcast systems," in *IEEE Trans. Broadcasting*, vol. 51, no. 2, pp. 223-229, Jun. 2005.