논문 21-46-05-07 The Journal of Korean Institute of Communications and Information Sciences '21-05 Vol.46 No.05
https://doi.org/10.7840/kics.2021.46.5.814

물리 계층 스푸핑을 위한 다중 스푸퍼 기반 협력 빔포밍

양 희 철◆°, 한 승 엽*, 이 정 우**

Coordinated Beamforming with Multiple Spoofers for Physical Layer Spoofing

Heecheol Yang◆°, Sungyeob Han*, Jungwoo Lee**

요 약

본 논문에서는 다수의 스푸퍼(spoofer)가 악의적 송수신단 사이의 무선 통신을 방해하는 물리 계층 스푸핑(spoofing) 환경을 고려한다. 다수의 스푸퍼를 활용해 달성가능한 스푸핑 용량을 최대로 하는 협력 빔포밍 기법을 제안한다. 제안하는 기법이 동일한 스푸핑 전력 하에서 기존 기법보다 더 높은 스푸핑 용량을 가지는 것을 보인다.

Key Words : Physical layer spoofing, Beamforming, Spoofer

ABSTRACT

In this letter, we consider a physical layer spoofing scenario, where the multiple spoofers aim to spoof a wireless communication link between malicious transmitter and receiver. We propose a coordinated beamforming scheme between multiple spoofers to maximize the achievable spoofing rate. We show that our proposed scheme achieves the higher spoofing rate than the existing scheme with the same spoofing power.

Ⅰ. Introduction

As the usage of infrastructure-free wireless communications has been increasing, a new kind of wireless attacks from these devices is becoming an important issue for public security. To prevent the wireless attacks from the malicious devices, authorized or public devices can intervene proactively in wireless communications to do eavesdropping and jamming on malicious links. In particular, there has been a significant research on the physical layer security issue[1].

Recently, the authors in [2] have proposed proactive eavesdropping techniques which sends legitimate jamming signals to the malicious users for the purpose of interrupting malicious users. However, the malicious users can change the way of performing wireless attacks to conceal their signals if they notice the presence of jamming signals. To overcome this limitation, a new technique for preserving physical layer security has been proposed, which is referred to as spoofing[3-6]. By spoofing, we can replace the transmitted information over malicious links to the target information. The authors in [3] have suggested symbol-level spoofing strategies to minimize the error rate of spoofing symbols. In addition, the fundamental limits of spoofing have been derived in [4]. Furthermore, physical layer spoofing has been extended to various wireless communication environments under adversarial attack[5] or spoofing attack[6].

Our focus in this paper is to extend the physical-layer spoofing scenario proposed in [3], [4] to the multi-spoofer environments. We propose a new coordinated beamforming strategy for multiple spoofers. The main idea of the proposed scheme is to design spoofing signals based on the information obtained through backbone links between the spoofers, and to iteratively update the coefficients of

※ 본 연구는 한국연구재단 연구과제(2020R1G1A1003759) 지원 및 충남대학교 학술연구비로 수행되었습니다.
◆° First and Corresponding Author : Chungnam National University, Division of Computer Convergence, hcyang@cnu.ac.kr, 조교수, 종신회원
* Seoul National University, Department of Electrical and Computer Engineering, syhan@cml.snu.ac.kr, 박사과정
** Seoul National University, Department of Electrical and Computer Engineering, junglee@snu.ac.kr, 교수, 종신회원
논문번호 : 202102-035-A-LU, Received February 8, 2021; Revised February 24, 2021; Accepted March 4, 2021

the spoofing signals to maximize the achievable spoofing rate. We reveal that the proposed scheme can achieve the higher spoofing rate compared to the simple extension of the existing spoofing scheme for a single spoofer[4] and the benchmark schemes.

Ⅱ. System Model

Consider a multi-spoofer spoofing channel, where a set of malicious transmitter A and receiver B communicate and K legitimate spoofers $\{S_i\}_{i=1}^{K}$ aim to change the message from A to B. The channel coefficient from A to B is defined as h and the spoofing channel coefficient from S_i to B is defined as g_i for all $i \in [K]$. We assume that A transmits the desired message s, but the legitimate spoofers aim to change the decoded message to the target message x at B. We also assume that the legitimate spoofers are aware of the desired message s, the target message x, and the channel coefficients from A to B, and their incoming and outgoing links with A and B, by obtaining these information through backbone links from the legitimate center which controls the legitimate spoofers with information on A and B. Without spoofing, the received signal at B is given by $y = h\sqrt{P}s + n$, where P denotes the constant transmit power at A and n denotes the Gaussian noise at B with zero mean and unit variance. The legitimate spoofer S_i sends its spoofing signal $z_i = \alpha_i s + \beta_i x$ to B, where α_i and β_i are the complex coefficients for the spoofing signal. The received signal at B is represented as

$$\begin{aligned} y &= h\sqrt{P}s + \sum_{i=1}^{K} g_i z_i + n \\ &= \left(h\sqrt{P} + \sum_{i=1}^{K} g_i \alpha_i\right) s + \sum_{i=1}^{K} g_i \beta_i x + n \end{aligned} \tag{1}$$

The constant transmit power at each of the legitimate spoofers is Q, i.e., $|\alpha_i|^2 + |\beta_i|^2 \le Q$ for all $i \in [K]$. We assume that the malicious receiver B uses the decoding method of treating interference as noise (TIN) approach. If the spoofing is successful, the achievable spoofing rate is expressed as

$$r(\alpha, \beta) = \log_2\left(1 + \frac{\left|\sum_{i=1}^{K} g_i \beta_i\right|^2}{\left|h\sqrt{P} + \sum_{i=1}^{K} g_i \alpha_i\right|^2 + 1}\right) \tag{2}$$

where $\alpha = \{\alpha_1, ..., \alpha_K\}$ and $\beta = \{\beta_1, ..., \beta_K\}$. The spoofing strategy for K legitimate spoofers is to determine α and β in order to maximize the achievable spoofing rate.

Ⅲ. Coordinated Beamforming

In this section, we propose a coordinated beamforming scheme to maximize the spoofing rate with multiple spoofers. At each of the legitimate spoofers, the spoofing signal is formulated for the desired message s to be destructively combined at B. On the other hand, the target message x should be constructively combined at B to maximize the achievable spoofing rate. Thus, the complex coefficients for the spoofing signal is given by

$$\alpha_i = -\frac{h g_i^*}{|h||g_i|}\tilde{\alpha}_i,\ \beta_i = \frac{g_i^*}{|g_i|}\sqrt{Q - \tilde{\alpha}_i^2} \tag{3}$$

for all $i \in [K]$, where $\tilde{\alpha}_i \ge 0$ denotes the magnitude of α_i. After this phase coordination of spoofing signals, the received signal at B is illustrated in Fig. 1. In this case, the achievable spoofing rate is reformulated as

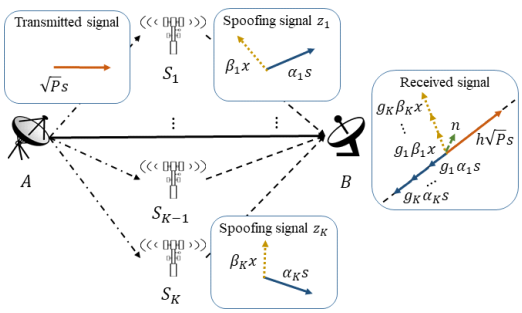

Fig. 1. Received signal at B

$$r(\tilde{\alpha}) = \log_2\left(1 + \frac{\left(\sum_{i=1}^{K}|g_i|\sqrt{Q-\tilde{\alpha}_i^2}\right)^2}{\left(|h|\sqrt{P}-\sum_{i=1}^{K}|g_i|\tilde{\alpha}_i\right)^2+1}\right) \quad (4)$$

where $\tilde{\alpha}=\{\tilde{\alpha}_1,...,\tilde{\alpha}_K\}$. Consequently, the achievable spoofing rate maximization problem is formulated as follows.

$$(P1): \max_{0\le\tilde{\alpha}_i\le Q} \frac{\left(\sum_{i=1}^{K}|g_i|\sqrt{Q-\tilde{\alpha}_i^2}\right)^2}{\left(|h|\sqrt{P}-\sum_{i=1}^{K}|g_i|\tilde{\alpha}_i\right)^2+1}$$
$$s.t.\left(\sum_{i=1}^{K}|g_i|\sqrt{Q-\tilde{\alpha}_i^2}\right)^2 \ge \left(|h|\sqrt{P}-\sum_{i=1}^{K}|g_i|\tilde{\alpha}_i\right)^2+\delta$$

To maximize the spoofing rate, we need to find the magnitude of $\tilde{\alpha}_i$ for all $i\in[K]$ by solving the maximization problem (P1). Since the problem (P1) is not a convex form, we propose an iterative algorithm to determine $\tilde{\alpha}_i$ at each of the spoofers to get the near-optimal solution. In our algorithm, we iteratively maximize the objective function in (P1) with respect to $\tilde{\alpha}_k$ for any $k\in[K]$. The objective function $f(\tilde{\alpha}_k)$ is given by

$$f(\tilde{\alpha}_k) = \frac{\left(|g_k|\sqrt{Q-\tilde{\alpha}_k^2}+\sum_{i\ne k}|g_i|\sqrt{Q-\tilde{\alpha}_i^2}\right)^2}{\left(|h|\sqrt{P}-|g_k|\tilde{\alpha}_k-\sum_{i\ne k}|g_i|\tilde{\alpha}_i\right)^2+1} \quad (5)$$

The possible value for maximizing $f(\tilde{\alpha}_k)$ is the local maximum point where $f'(\tilde{\alpha}_k)=0$. By deriving the first-order derivate of $f(\tilde{\alpha}_k)$, we find that $f(\tilde{\alpha}_k)$ has one maximum point at $f'(\tilde{\alpha}_k)=0$. We define $\tilde{\alpha}_{opt}$ as the optimal value which satisfies $f'(\tilde{\alpha}_{opt})=0$. We also find that $f(\tilde{\alpha}_k)$ is monotonically increasing when $\tilde{\alpha}_k<\tilde{\alpha}_{opt}$ and monotonically decreasing when $\tilde{\alpha}_k>\tilde{\alpha}_{opt}$ since $f(\tilde{\alpha}_k)$ has a single point which satisfies $f'(\tilde{\alpha}_k)=0$. Due to the power constraint, the optimal value to maximize $f(\tilde{\alpha}_k)$ is given by

$$\tilde{\alpha}_k=\begin{cases}\tilde{\alpha}_{opt}, & 0\le\tilde{\alpha}_{opt}\le Q,\\ \arg\max_{\tilde{\alpha}_k=0,\sqrt{Q}} f(\tilde{\alpha}_k), & otherwise.\end{cases} \quad (6)$$

By using this update policy, we iteratively update $\tilde{\alpha}_k$ until there is no change during iteration. We finally design the spoofing signals as

$$z_k = \alpha_k s+\beta_k x = -\frac{hg_k^*}{|h||g_k|}\tilde{\alpha}_k s+\frac{g_k^*}{|g_k|}\sqrt{Q-\tilde{\alpha}_k^2}\,x \quad (7)$$

Ⅳ. Numerical Results

We dedicate this section to analyze the achievable spoofing rate. We compare the achievable spoofing rate of our scheme with the modified scheme for single-spoofer scenario and the benchmark schemes of [4].

- Perfect cancellation: The spoofers try to perfectly cancel the desired message s at B.
- Naive spoofing: The spoofers try to spoof the transmitted messages by sending the target message with their all transmit energy.
- Uncoordinated spoofing: Each spoofer sends its spoofing signal without knowledge about other spoofers' transmit strategies as in a single-spoofer scenario, which was proposed in [4].

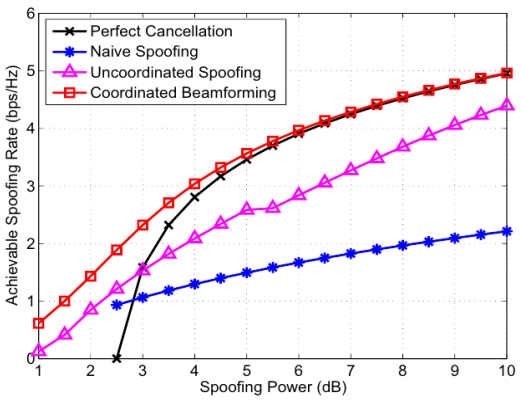

Fig. 2. Achievable spoofing rate

Fig. 2 shows the achievable spoofing rates of two-spoofer scenario versus the spoofing power Q when the transmit power P is 10dB and $R=2$ bps/Hz. We assume that the average channel gains from the transmitter and the spoofers to the receiver are equal. We can see that the proposed scheme shows better performance than the existing scheme and the benchmark schemes on the achievable spoofing rate.

References

[1] M. A. Abbas and J. -P. Hong, “Survey on physical layer security in downlink networks,” *J. ICCE*, vol. 15, no. 1, pp. 14-20, Mar. 2017.

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

[3] J. Xu, L. Duan, and R. Zhang, “Transmit optimization for symbol-level spoofing,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 41-55, Oct. 2017.

[4] J. Xu, L. Duan, and R. Zhang, “Fundamental rate limits of physical layer spoofing,” *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 154-157, Apr. 2017.

[5] O. A. Topal, M. O. Demir, G. Dartmann, A. Schmeink, G. Ascheid, A. E. Pusane, and G. K. Kurt, “Physical layer spoofing against eavesdropping attacks,” in *Proc. 8th Mediterranean Conf. Embedded Computing*, Budva, Montenegro, Jun. 2019.

[6] X. Wang, N. Li, M. Li, and X. Tao, “A physical layer spoofing attack in spatial modulation,” in *Proc. IEEE Globecom Workshops*, Waikoloa, HI, Dec. 2019.