Physical Communication 25 (2017) 201–213

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Secure wireless multicasting with linear equalization

D.K. Sarker *, M.Z.I. Sarkar, M.S. Anower

Department of Electrical and Electronic Engineering, Rajshahi University of Engineering and Technology, Rajshahi-6204, Bangladesh

ARTICLE INFO

Article history:
Received 15 June 2016
Accepted 24 July 2017
Available online 4 August 2017

Keywords:
Cooperative spatial multiplexing
Security
Secure outage probability
Zero-forcing equalization

ABSTRACT

A confidential communication scenario is considered in which a base station (BS) transmits a common stream of information to a group of users in the presence of multiple eavesdroppers via multiple relays. Multiple relays are used to provide cooperative spatial multiplexing that significantly increases the spectral efficiency with the help of linear equalization at the users. In order to analyze the performance of proposed model showing the effect of fading and multiplexing gain, we derive the closed-form analytical expressions for the ergodic secrecy multicast capacity and the secure outage probability with and without equalization. Then, we study the effect of fading and shadowing, and the number of users, eavesdroppers and relays on the ergodic secrecy multicast capacity and the secure outage probability assuming channel state information at the receiver. The secure outage performances of the proposed model with zero-forcing (ZF) case are also compared without the case of ZF. In addition, we show the effect of the number of user and eavesdropper antennas and the distances from relays to users and eavesdroppers on the secure outage probability, and a comparison is shown between the composite and Rayleigh fading environments. Finally, the analytical expressions are verified via Monte Carlo simulation.

1. Introduction

In wireless communication networks, the issues of security and privacy have attracted a lot of interest due to the mobility of users and network components, and wireless channels offer a shared medium favorable to eavesdropping. Moreover, the expansion of wireless networks, inevitably renders security into a challenging quality of service constraint that must be accounted for the design of wireless networks. On the other hand, the effects of fading and shadowing can be exploited significantly to increase the spectral efficiency [1]. The confirmation of reliable communications often require highly reliable connections to all users, which are more difficult to achieve in wireless networks. Multicasting is an appropriate approach to achieve this. Since the traditional multicasting does not provide a secure framework for authentication, integrity and privacy for multicast sessions, so the security is a crucial aspect in multicasting, the lack of which is currently preventing the large-scale deployment of group-oriented applications. In addition, security policies in multicasting provide a secure framework for protecting the secrecy and integrity of the data sent as well as the privacy and authentication of the members of multicast group.

Recently, a cooperative multicast network in the presence of single eavesdropper was studied in [2], where the authors showed that their proposed scheme outperforms the direct multicast in terms of secure outage probability. An artificial-noise alignment scheme for multicasting was proposed in [3], where the noise symbols could mask the information symbols at the eavesdroppers but the legitimate receivers decode the information symbols with high probability. In [4], power minimization and secrecy rate maximization problems were investigated with iterative algorithms. A cooperative multiple-input-multiple-output (MIMO) network with ZF receiver and amplify-and-forward (AF) relaying was proposed in [5], to investigate the symbol error probability. In [6], the symbol error probability was analyzed for a relay network with multiplexing scheme having the base-stations equipped with multiple antennas.

In [7], bit error rate (BER) of the detector was analyzed for multicast wireless network in which a source equipped with single antenna communicates with a destination having single antenna via a multi-antenna decode-and-forward (DF) relay. A two-hop multi-relay decode-and-forward cooperative communication system with single source and single destination was proposed in [8], where selection relaying method was used to mitigate the problem of error propagation due to incorrect decoding of symbols at the relays. In order to exploit the characteristics of scalable video effectively over wireless networks, two cooperative multicast schemes namely, OppCM and CodedCM were proposed in [9], where average outage probabilities of the two schemes were compared to that of direct multicast scheme. The outage probability and ergodic sum rate performance for multiple cooperative relay network was studied in [10] considering Rician fading channel. Two relaying

* Corresponding author.
E-mail address: dks_ms@yahoo.com (D.K. Sarker).

http://dx.doi.org/10.1016/j.phycom.2017.07.007
1874-4907/

modes referred to as reactive and proactive were used in [11] to investigate the outage probability and error probability for a multiple cooperative relay network.

In [2–4], although the issues of security of multicast networks were addressed but no works had been done considering the distances of relays from the destination and eavesdropper to locate the strategic position of the relays for achieving better and secure system performance. On the other hand, in [5,6,8–11], authors studied cooperative relay networks but they did not consider the security issues. Moreover, the impact of spatial diversity provided by multiple relays with linear equalization on the secrecy multicast capacity of cooperative networks is not investigated yet. So far to authors' knowledge, for the first time, this paper addresses the problems of security of multicast networks with cooperative spatial multiplexing in the presence of multiple eavesdroppers, taking the location of source, destinations and eavesdroppers into account. Here, we analyze the security of multicast cellular network with cooperative spatial multiplexing in the presence of multiple eavesdroppers. The impact of spatial multiplexing provided by multiple relays is investigated with and without linear equalization.

At first, we derive the closed-form expressions for the ergodic secrecy multicast capacity with and without ZF equalization using the Gauss–Hermite quadrature integration formula. Secondly, we derive the closed-form expressions for the secure outage probability with and without ZF equalization. For both the cases composite log-normal shadowing and Rayleigh fading channel is considered. Thirdly, we investigate the effect of fading and shadowing on the ergodic secrecy multicast capacity and the secure outage probability. Finally, we investigate the effect of distances of the users and eavesdroppers from the relays on the secure outage probability.

The rest of this paper is structured as follows. Section 2 outlines the system model and formulation of the problem. Sections 3 and 4 describe the formulation of the analytical expressions for the ergodic secrecy multicast capacity and the secure outage probability for multicasting, respectively. In Section 5, numerical results are presented. Finally, this paper is concluded in Section 6.

Notation: Throughout this paper, scalars are represented by lowercase letters, whereas, vectors and matrices are denoted by bold lower case letters and bold upper case letters, respectively. $\mathbf{I}_n$ represents the $n \times n$ identity matrix. A complex Gaussian distribution with mean μ and variance σ^2 is denoted by $\mathcal{C}\tilde{\mathcal{N}}(\mu, \sigma^2)$. The superscript $(\cdot)^\dagger$ stands for the complex conjugate transpose and $\mathbb{E}[\cdot]$ is the expectation operator. Ei$(\cdot)$ and $P_r(\cdot)$ denote the exponential integral function and the probability, respectively.

2. System model and problem formulation

We consider a confidential multicasting scenario through cellular network as shown in Fig. 1 in which a BS transmits a common stream of information to a group of M users via K relays in the presence of N eavesdroppers. Each relay and BS are equipped with single antenna while each user and eavesdropper are equipped with n_U and n_E antennas, respectively. We assume that communication occurs only through the relays and there are no direct paths between the relays and the users as well as eavesdroppers. This scenario arises when the users are situated at a long distance away from the source, so that, the transmitted signals need to be reconstructed or amplified by a cooperative device. Here the cooperative multiplexing system provided by the relays plays a role to deploy linear equalization, i.e., ZF at the receivers and thus form a virtual MIMO antenna array at the relay terminals. All the channels are assumed to be composite i.e. Rayleigh fading with log-normal shadowing. In the first-hop, the BS transmits s symbol to the relays. Therefore, received signal at the kth relay is given by

$$x_k = g_k s + \hbar_k, \tag{1}$$

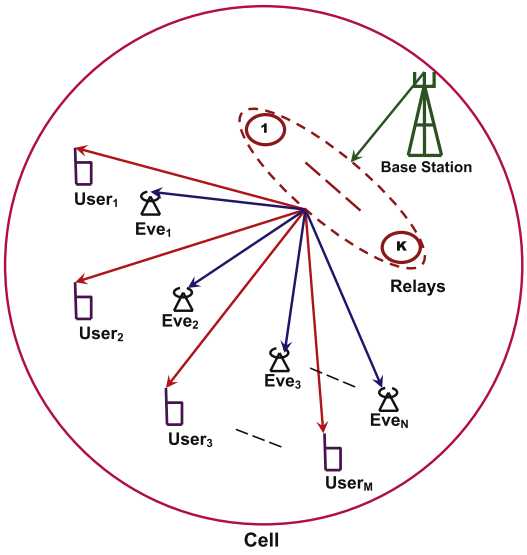

Fig. 1. Secure wireless multicasting through a cellular system with K relays and M users in the presence of N eavesdroppers.

where g_k denotes the channel coefficient between BS to kth relay and $\hbar_k \sim \tilde{\mathcal{N}}\left(0, \varepsilon^2\right)$ denotes the background noise of kth relay with zero mean and variance ε^2.

In the second-hop, all the relays simultaneously transmit their received signal to the ith $(i = 1, \ldots, M)$ user over the same physical channel and N eavesdroppers try to extract information from the relays. Let $\mathbf{y}_{u_i}$ and $\mathbf{y}_{e_j}, (j = 1, \ldots, N)$ respectively denote the received signals at the ith user and jth eavesdropper. Then we have

$$\begin{aligned}\mathbf{y}_{u_i} &= \sum_{k=1}^{K} \mathbf{h}_{i,k} x_k + \mathbf{w}_i = \sum_{k=1}^{K} \mathbf{h}_{i,k} \left(g_k s + \hbar_k\right) + \mathbf{w}_i \\ &= \sum_{k=1}^{K} \mathbf{h}_{i,k} g_k s + \sum_{k=1}^{K} \mathbf{h}_{i,k} \hbar_k + \mathbf{w}_i = \mathbf{H}_i \mathbf{s} + \mathbf{z}_i, \end{aligned} \tag{2}$$

$$\begin{aligned}\mathbf{y}_{e_j} &= \sum_{k=1}^{K} \mathbf{u}_{j,k} x_k + \mathbf{v}_j = \sum_{k=1}^{K} \mathbf{u}_{j,k} \left(g_k s + \hbar_k\right) + \mathbf{v}_j \\ &= \sum_{k=1}^{K} \mathbf{u}_{j,k} g_k s + \sum_{k=1}^{K} \mathbf{u}_{j,k} \hbar_k + \mathbf{v}_j = \mathbf{D}_j \mathbf{s} + \mathbf{q}_j, \end{aligned} \tag{3}$$

where $\mathbf{H}_i = \left[\mathbf{h}_{1,k} g_1 \ \mathbf{h}_{2,k} g_2 \ \ldots \ \mathbf{h}_{n_U,k} g_K\right] \in \mathbb{C}^{n_U \times K}$ and $\mathbf{D}_j = \left[\mathbf{u}_{1,k} g_1 \ \mathbf{u}_{2,k} g_2 \ \ldots \ \mathbf{u}_{n_E,k} g_K\right] \in \mathbb{C}^{n_E \times K}$ denote the channel coefficients from relays to ith user and jth eavesdropper, respectively. $\mathbf{s} \in \mathbb{C}^{K \times 1}$ denotes the transmit signal vector of K relays. $\mathbf{z}_i = \sum_{k=1}^{K} \mathbf{h}_{i,k} \hbar_k + \mathbf{w}_i$ and $\mathbf{q}_j = \sum_{k=1}^{K} \mathbf{u}_{j,k} \hbar_k + \mathbf{v}_j$, where $\mathbf{w}_i \sim \mathcal{C}\tilde{\mathcal{N}}\left(0, \varepsilon_u^2 \mathbf{I}_{n_U}\right)$ and $\mathbf{v}_j \sim \mathcal{C}\tilde{\mathcal{N}}\left(0, \varepsilon_e^2 \mathbf{I}_{n_E}\right)$ denote the additive white Gaussian noise imposed on the receivers of ith user and jth eavesdropper, respectively. All the elements of $\mathbf{H}_i$ and $\mathbf{D}_j$ are complex random variables which are independent and not identically distributed due to the separation of relays. The channel mean power from the kth relay to ith user and jth eavesdropper are denoted by $\alpha_{i,k}$ and $\Omega_{j,k}$, respectively. In order to focus the role of ZF equalization in enhancing the performance of the proposed model, we separately describe the formulation of the probability density functions (PDFs) of received signal-to-noise ratios (SNRs) at the receivers of users and eavesdroppers with and without ZF-filtering as follows.