IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Enhanced Relay Selection Strategy and Adaptive Filter Use in Cooperative Networks

Asna Nazar

M.Tech scholar, Department of ECE, MZCE, Kadammanitta, Pathanamthitta, Kerala

Abstract: Cooperative transmission in a decode-and-forward (DF) two-hop network where multiple cooperative nodes coexist with a potential eavesdropper can be secured with enhanced relay selection strategy and interference can be reduced by the use of an adaptive filter at the receiver. Under the practical assumption that only the channel distribution information (CDI) of the eavesdropper is known, also we propose an Artificial jamming and beamforming, where a "best" cooperative node is chosen among a collection of N possible cooperative nodes based on the transmission rate and SNR to forward the confidential signal and the others send jamming signals to confuse the eavesdroppers. Since the optimization problems are non-convex, we use a sequential parametric convex approximation (SPCA) algorithm to locate the Karush Kuhn-Tucker (KKT) solutions; we generalize the analysis with multiple eavesdroppers, and find the asymptotic analytical results of the achievable ESR. Simulation results confirm our analytical results. We also obtain the simulation of capacity and BER with respect to SNR to show the effectiveness of the system.

Keywords: Adaptive filters, beam forming, decode and forward, ergodic secrecy rate, extreme order statistics, outdated CSIs, Sequential parametric convex approximation.

I. INTRODUCTION

Secure communication is when two entities are communicating and do not want the third party to listen in. for that they need to communicate in a way not susceptible to eavesdropping or interception. A cooperative communication can be said secure if it is susceptible to eavesdropping. Coorpeartion happens when a direct communication between source and destination is improved due to the help provided by a neighbouring node. The roles of the cooperative nodes for securing the legitimate transmissions can be divided into two categories: the relay nodes and the jammers. When the cooperative nodes act as relay nodes, they employ the amplify-and-forward (AF) or decode-and forward (DF) protocol to forward the confidential information

In Hybrid Opportunistic Relaying and Jamming with Power Allocation for Secure Cooperative Networks with only CDI of the eavesdropper, a relay scheme is derived, where a best cooperative node is chosen to forward the desired signal and the other nodes send jamming signals to confuse the potential eavesdroppers, then investigating the ergodic secrecy rate maximization (ESRM) problem .when more eavesdroppers are there the system can't provide much security.

We propose a secrecy scheme which can provide more security than hybrid opportunistic relaying and jamming with power allocation, here introducing an adaptive filter at the receiver section for reducing the interference also the selection of the relay based on the transmission rate and SNR can enhance the system security. Since it combines both jamming and beamforming it has low BER. Our contributions can be summarized by assuming that the perfect CSIs of the legitimate nodes are available and there is a single eavesdropper, we jointly design the relay selection scheme and the power allocation between the confidential signal and the jamming signals for ESRM.

The power allocation is obtained by using SPCA (sequential and parametric convex approximation algorithm). Simulation results shows that compared with the exhaustive search, the proposed power allocation strategy can achieve almost optimal performance.

With the optimized power allocations, we derive a closed form expression of the achievable ESR, which reduces the complexity of the system analysis and design. Our proposed system has significant difference from the existing system. It adds an adaptive filter and beamforming process to increase the security. Also relay selection strategy is modified.

II. EXISTING SYSTEM

Hybrid opportunistic relaying and jamming with power allocation system DF network is made up of a source node S, N trusted cooperative nodes R , k ∈ N, N = {1, . . . ,N}, a legitimate destination node D and a passive eavesdropper. All nodes in the network are equipped with a single antenna and operate in the half-duplex DF mode.

All channels are assumed to be quasi-static flat fading and there is no direct communication link between S and D. The eavesdropper can wiretap the confidential information in the two cooperative phases: from S to R and from R to D.

To secure the data transmission, the opportunistic DF relaying is adopted to forward the desired signal, where one cooperative node, say R k , is selected as the relay node based on the CSIs of the legitimate links S → R → D before the data transmission (the selection criterion will be detailed in the following sections). The other N - 1 nodes act as the jammers to send jamming signals for covering the confidential information transmission during two cooperative stages.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

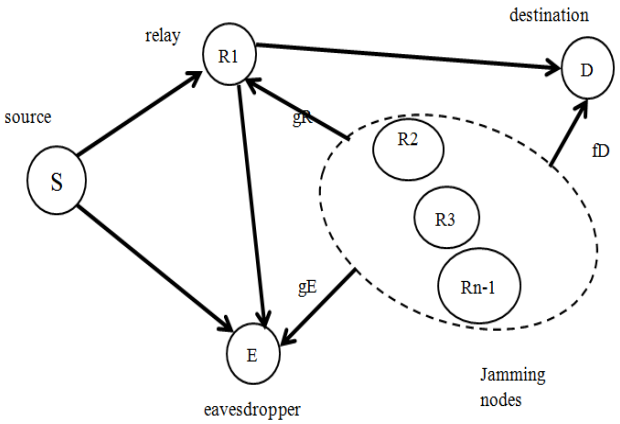

Fig.1 system model

We make the following key assumptions:
1) The opportunistic relay selection and jamming signal design are assumed to be made at S, which collects all the available instantaneous CSI[2] and feeds them back to the cooperative nodes. This assumption has been widely for both optimal beamforming design and jamming design.
2) We only assume the CDI of the eavesdropper to be available. Specially, we assume that multiple relay nodes form a DF cooperative cluster. Then for a distant eavesdropper, the channels from the relay nodes to the eavesdropper can be assumed to be complex circularly symmetric independent and identically distributed (i.i.d.) Gaussian distributed.
3) We assume that the whole network is to operate under a total power budget. For SNR balancing, half of the available total transmission power is consumed by the relays. For these reasons, the total energy consumption constraint has been widely adopted for both performance analysis and optimal design.

During Phase I, S broadcasts its data and the optimal relay node chosen in advance R_{K^*} listens. Concurrently, the jammers transmit jamming signals in a collaborative manner. During phase II R_{K^*} decodes the message and forwards its decoded outcomes to D using the same codewords as the source. Note that in both phases, jammers need to emit jamming signals collaboratively to confuse the eavesdroppers. The CJ precoding matrix WJ and UJ may be known to the eavesdropper but the jamming signal vectors should be secured from the eavesdropper. They can be generated by the seed of the random noise generator which is shared among the relays in a secure fashion

JOINT RELAY SELECTION AND POWER ALLOCATION OPTIMIZATION FOR ESRM

Since the relay uses the same code words as the source to forward the decoded signals and the instantaneous eavesdropper's CSI is absent, our goal is to design the relay selection and power allocation jointly for maximizing R. Mathematically, the joint optimization problem can be formulated as

$$\max_{\varphi 1,\varphi 2,r_{k^*}} R_s \text{ , s.t. } 0 < \varphi 1 < 1, \;\; 0 < \varphi 2 < 1$$

Employing the order statistics, we build a tractable result for approximatingR_s,, which would facilitate the power allocation optimization. Conditioned on the power allocation strategy $\phi 1$, $\phi 2$, the optimal relay selection criterion is to maximize RS by selectingK^*. Since the eavesdropper's instantaneous CSI absent and the channel coefficients of the eavesdropper are assumed to be i.i.d

$$K^* = \arg\max_{k \in N} \min(\varphi 1 P|h_{SRk\,2}|^2, \varphi 2 P|h_{RkD\,2}|^2)$$

ITERATIVE OPTIMIZATION ALGORITHM

It can be solved by a two-dimensional search, it is very computational expensive, and the optimality depends heavily on the search interval. In the following, we are using a SPCA method to handle it. The general SPCA optimizes a sequence of approximating convex programs to locate the KKT solution of a non-convex program. In each iteration, each non-convex constraint is replaced by an appropriate inner convex constraint. Under appropriate conditions on the inner convex approximation, a monotone convergence to a KKT point is established and the rigorous proof can be found in. Generally, SPCA has a fast convergence speed. Introducing the slack variables t1, t2, t3, t4, the problem can be transferred to

$$\max_{t1\geq 0,t2\geq 0,t3\geq 0,t4\geq 0,z1,z2} t1 + \log_2(1+t2) - t3$$

This non-convex problem can be transformed into a sequence of convex approximation. Which is called algorithm1. Then the secrecy rate achieved by D now can be computed by

$$R_d^0 = E[\log_2(1 + r_d^0)]$$

Finally we are investigating the secrecy performance of the strategy in the presence of multiple eavesdroppers. Based on the assumption that M non-colluding eavesdroppers coexist with N cooperative nodes.

III.PROPOSED SYSTEM

In the proposed system we enhancing the hybrid opportunistic relaying and jamming with power allocation by introducing an adaptive filter at the receiver side with a modification in the relay selection strategy and beamforming. The best relay is chosen based on the transmission rate and SNR. Adaptive filter provides interference reduction henceforth increase transmission rate & reduction in BER is obtained.

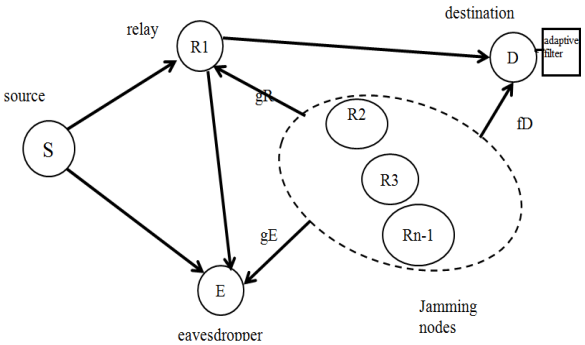

Fig. 2 proposed system mode.

DOI 10.17148/IJARCCE.2016.51102

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

IV. PERFORMANCE EVALUATION

By using MATLAB performance characteristic of the proposed system under various conditions are obtained. Firstly the performance of the cooperative node with a single eavesdropper is considered.

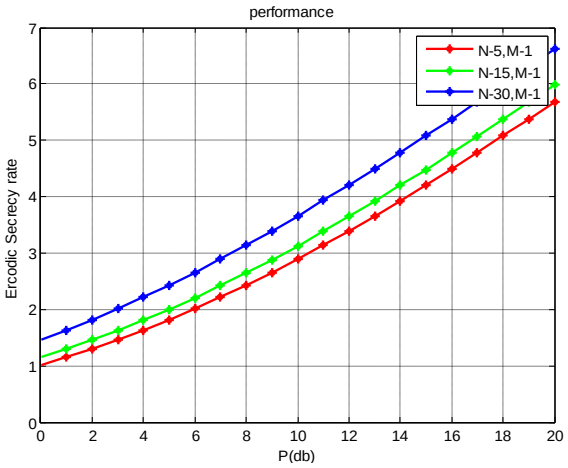

Fig. 3 validation of the theoretical result with lsr=.6,lrd=.5.lse=.2,lre=.2

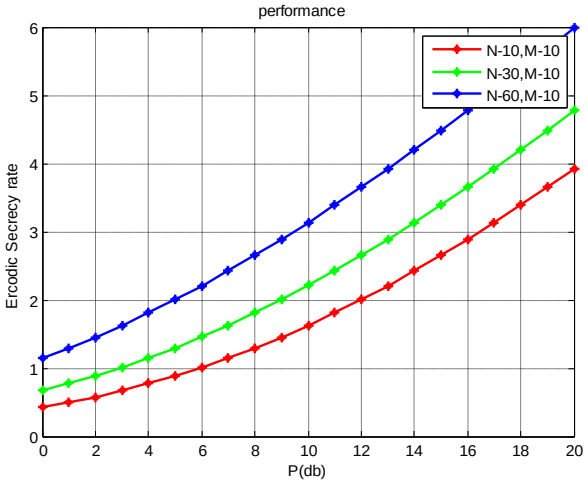

Fig. 4 validation of theoretical result with γ=1,φ=.4

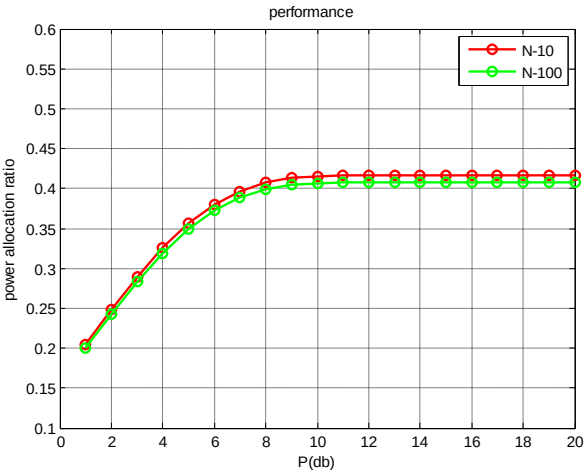

Fig. 5 power allocation ratio versus P(dBm) with lsr=1,lrd=1, γ=1 for different cooperative nodes

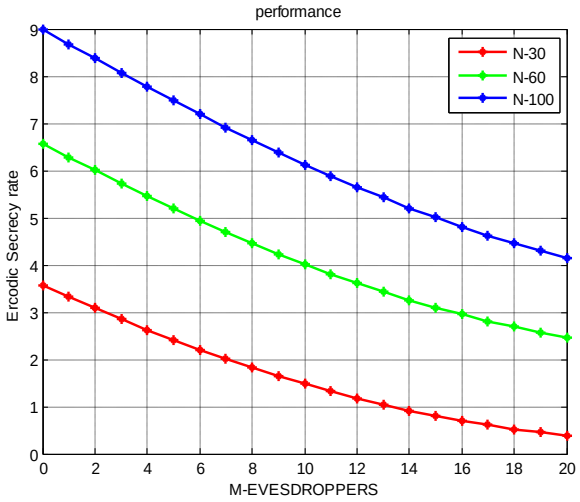

Fig.6 comparison between the no. of non-colluding eavesdroppers M in the network with different No.of relays N

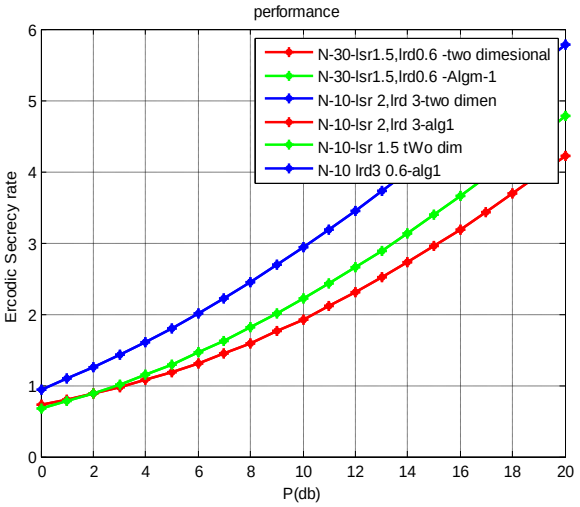

Fig. 7 performance comparison between algorithm 1 and two-dimensional search with lse=.2,lre=.2

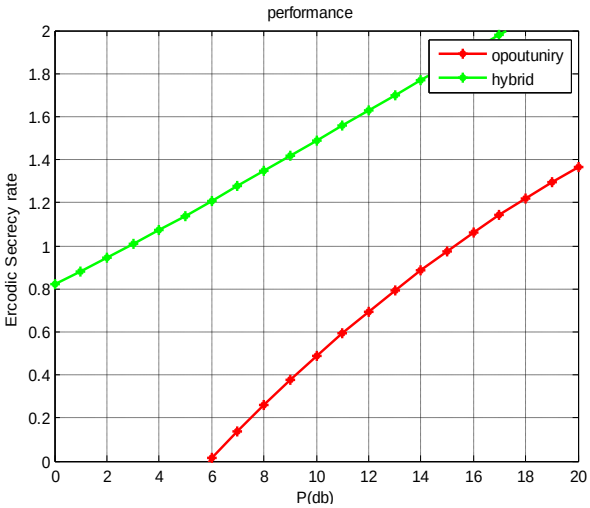

Fig. 8 performance comparison between opportunistic relaying and jamming with hybrid opportunistic relaying and jamming

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

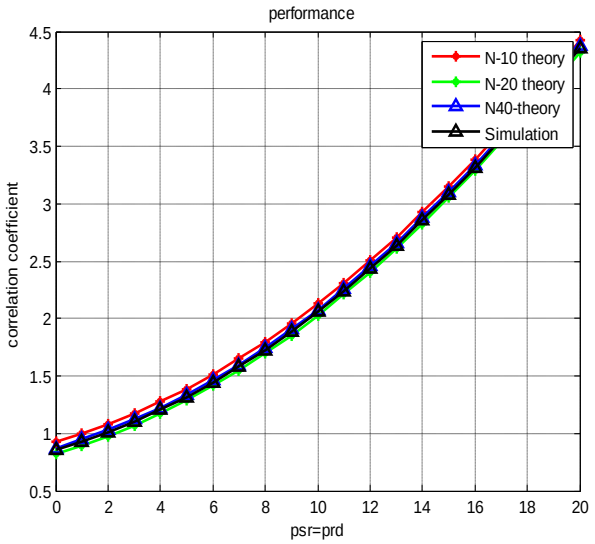

Fig. 9 validation of the theoretical result of the correlation coefficient

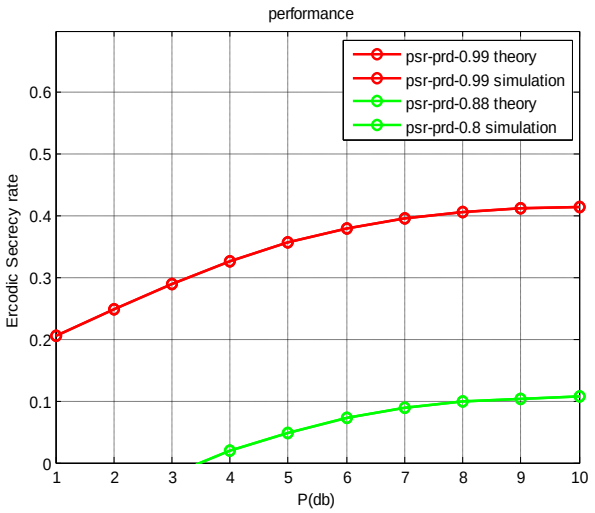

Fig .10 Ergodic secracy rate versus P

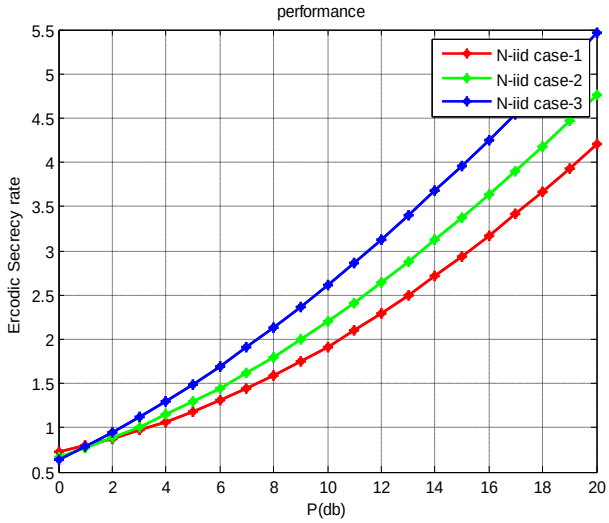

Fig.11 Ergodic secrecy rate for different cases of the eavesdropper channel distribution

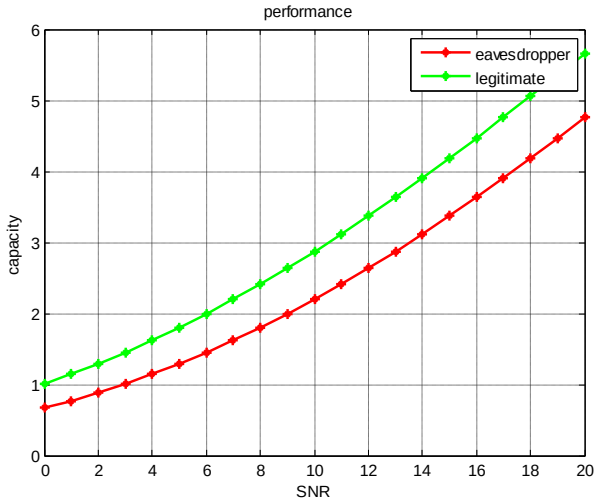

Fig .12 capacity versus SNR for eavesdropper and legitimate

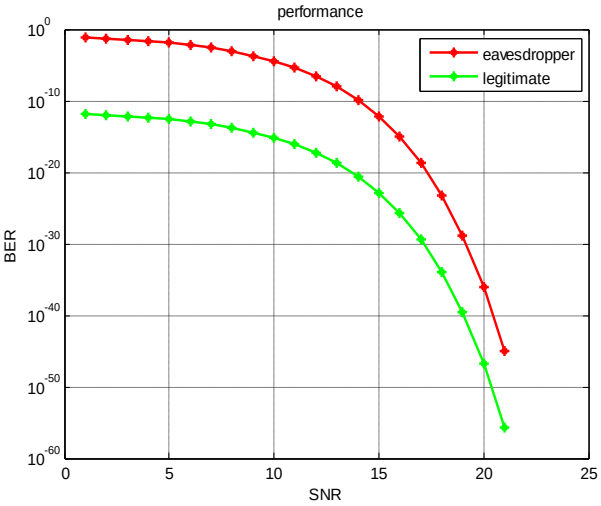

Fig.13 BER versus SNR for eavesdropper and legitimate

V. CONCLUSION

We obtained various graphs plotting the characteristics of hybrid opportunistic relaying and jamming with power allocation. The selection strategy of the relay is compared with the concept of choosing the relay based on the transmission rate and SNR. Also we implemented an adaptive filter in the existing system. Based on this we plotted graph showing the capacity and BER of the proposed system with respect to SNR. The proposed system can provide better security than the existing system; It has lower BER and interference.

ACKNOWLEDGMENT

I sincerely thank to all those who helped me in completing this task.

REFERENCES

[1] "Hybrid Opportunistic Relaying and Jamming with Power Allocation for Secure Cooperative Networks" Chao Wang, Hui-Ming Wang, Member, IEEE, Xiang-Gen Xia, Fellow, IEEE 2014

[2] "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia. IEEE Trans. Information Forensics and Security, vol.8, no.12, pp. 2007-2020, Dec. 2013.

[3] "Destination assisted cooperative jamming for wireless physical layer security," IEEE Trans. Information Forensics and Security, Y. Liu, J. Li, and A. Petropulu vol.8, no. 4, pp. 682-694, Apr. 2013.

[4] "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, IEEE Commun. Lett, vol. 17, no. 5, pp. 864-867, May 2013

[5] "The diversity potential of relay selection with practical channel estimation," IEEE Trans. Wireless Commun., D. S. Michalopoulos, N. D. Chatzidiamantis, R. Schober, and G. K. Karagiannidis. vol. 12, no. 2, pp. 481-493, Feb. 2013.

BIOGRAPHY

Asna Nazar received the B.Tech degrees in Electronics and Communication Engineering from M.G University, Kerala at Mount Zion College of Engineering and Technology in 2014. And now she is pursuing her M.Tech degree in Communication Engineering under the same university in Mount Zion College of Engineering.

DOI 10.17148/IJARCCE.2016.51102