Physical Layer Security of AF Relay Systems With Jamming.

Kwadwo Boateng Ofori-Amanfo and Kyoung-Jae Lee
Department of Electronics and Control Engineering,
Hanbat National University, Daejeon 34158, South Korea
Emails: gigaofori11@gmail.com, kyoungjae@hanbat.ac.kr

***Abstract* - This paper studies the secrecy capacity for a wireless cooperative network with perfect channel state information at the relays, and receiver. A similar assumption is also made for the instance where there exist a direct link between the transmitter and receiver. Physical Layer security techniques are employed in wireless networks to mitigate against the activity of eavesdroppers. It offers a viable alternative to computationally intensive encryption. In this paper the design of a protocol utilizing jamming (*via jamming nodes*) for better security and relaying (*via relay nodes*) for the amplify-and-forward (AF) operation, is investigated. A a signal-to-noise variant of secrecy known as secrecy gap is explored because of its use of lesser computational power - preferable for practical systems. Thus we maximize this signal-to-noise approach instead of the conventional secrecy capacity maximization method. With this, an iterative algorithm using geometric programming (GP) and semi-definite programming (SDP) is presented with appreciable benefits. The results show here highlight the benefits of using fractional components of the powers of the relays to offer better secrecy capacity.**

***Index Terms*—Secrecy, eavesdropper, relay networks, semi-definite programming, power control, capacity**

I. Introduction

IT is well accepted that the performance in wireless networks is affected by promiscuious nodes. In trying to mitigate the influence of such nodes in wireless networks, physical layer security has offered a very viable path. By utilizing the nature of the wireless medium, eavesdropping nodes are cut off whiles genuine ones are able to successfully communicate. Thus secrecy capacity - the maximum attainable rate of secrecy, offers standard for measuring how secure the wireless network is. One other technique in wireless communciation is the use of cooperative networks. In cooperative networks, assisting nodes are available to relay the transmitted signal to the destination or to offer some other predermined vital functionality such as jamming[1], for the efficient transmission of the signal of interest. In the former case, several strategies are popular - for example, amplify-and-forward (AF), and decode-and-forward (DF) [2].

This paper distinguishes itself from existing ones in several ways. These distinguishing features include the following:

- It provides a model which offers secrecy capacity analysis for a cooperative network in cases where a direct link exists.
- Second, intends at exploiting the functionality of a hybrid multi-phase transmission scheme that uses both AF and cooperative jamming (CJ) to get the information signal securely from the source to the destination. The new technique therefore is an amplify and forward cooperative jamming protocol (AFCJ).
- It uses the approach of secrecy gap to offer a computational less intensive algorithm for practical scenarios.

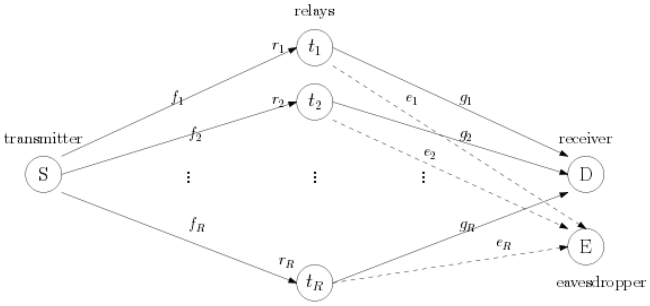

Fig. 1. The network model

II. Network Model and Problem Statement

We consider a wireless network made up of a pair of communicating nodes. One node serves as the source and the other as the destination. It also assumed that there is the presence of a passive eavesdropping node. Therefore, there is the need to ensure secure communication. There are also *m* relay nodes available, to forward the received signal using the AF protocol. It is assumed that all nodes bear omnidirectional antenna while operating in half-duplex mode. This is depicted in Fig. 1

A two step AF protocol is used where the transmitter with power P_0 sends $\alpha_0\sqrt{P_0}x$ where x is the information symbol. Communication takes place in two phases. These phases are given by the equations below:
Phase I: Using (1a) from [3] The source transmits the signal to the relay. The received signal and SNR at the the i-th relay for $i = 1 \dots m$ is therefore computed as:

$$y_{R_i} = \sqrt{P_s} f_i x + n_{R_i} \tag{1}$$

$$y_R = \sqrt{P_s}\mathbf{f}x + \mathbf{n}_{R_i} \tag{2}$$

$$\gamma_{R_i} = \frac{Ps|h_i|^2}{\sigma_n^2} \tag{3}$$

Phase II: Using (4a) from [4]
Relay i sends amplified signal to the destination. Thus the signal received by the destination and eavsdropper respectively are captured as:

$$y_D = \sqrt{P_R} g^T w u^T y_R + n_D \tag{4}$$
$$y_E = \sqrt{P_R} h^T w u^T y_R + n_E \tag{5}$$

where:

- $\alpha_i \dots \alpha_k$: power allocation factor
- P_0 : source power
- $f_i : for \quad i = 1 \dots \quad m$ source to relay channel coefficient
- $g_0 : for \quad i = 1 \dots \quad m$ relay to receiver channel coefficient

The equations together with are used to obtain the secrecy capacity equation 7 below.

III. Mathematical Derivations

Considering all the phases presented in sectionII, the final secrecy capacity can be formulated as:

$$C_S = \frac{1}{2}\left\{\log_2\left(1+\gamma_D\right) - \log_2\left(1+\gamma_E\right)\right\} \tag{6}$$

$$C_S = \frac{1}{2}\log\left[\frac{1+\frac{\alpha_0 P_0(\sum_{i=1}^{R}\frac{\alpha_i |f_i g_i|\sqrt{P_i}}{\sqrt{1+\alpha_0^2|f_i|^2 P_0}})^2}{1+\sum_{i=1}^{R}\frac{\alpha_i^2|g_i|^2 P_i}{1+\alpha_0^2|f_i|^2 P_0}}}{1+\frac{\alpha_0 P_0(\sum_{i=1}^{R}\frac{\alpha_i |f_i e_i e^{j\theta_i}|\sqrt{P_i}}{\sqrt{1+\alpha_0^2|f_i e^{j\psi_i}|^2 P_0}})^2}{1+\sum_{i=1}^{R}\frac{\alpha_i^2|e_i e^{j\gamma_i}|^2 P_i}{1+\alpha_0^2|f_i e^{j\psi_i}|^2 P_0}}}\right] \tag{7}$$

where:

- $\alpha_0 \dots \alpha_k$: power allocation factor
- $e_0 : for \quad i = 1 \dots \quad n$ relay to eavesdropper channel coefficient
- $\theta_i : -(arg f_0 + arg g_i)$

Equation 7 is used to generated the plots in Fig. 2.

IV. Simulation Results

In simulating, all channels are assumed to undergo Rayleigh fading. Each simulation is executed for 10^5 Monte-Carlo iterations. We get a comparison of the plot using the maximum power allocation factors possible of 1 (□ symbol) with that of an exhaustive search method to maximize secrecy rate (+ symbol). The secrecy capacity is plotted against the various SNR values as show in Fig 1. It is observed that the exhaustive search performs similarly to the full allocation scheme at low SNRs whiles outperforming it at high SNR values.

V. Conclusion

The result shows that the exhaustive search algorithm out performs the case where there is full power allocation at the relay for AF retransmission. This means that an optimization algorithm is necessitated. However the secrecy capacity equation offers a highly non convex problem during optimization. Therefore a process know as a single condensation GP method

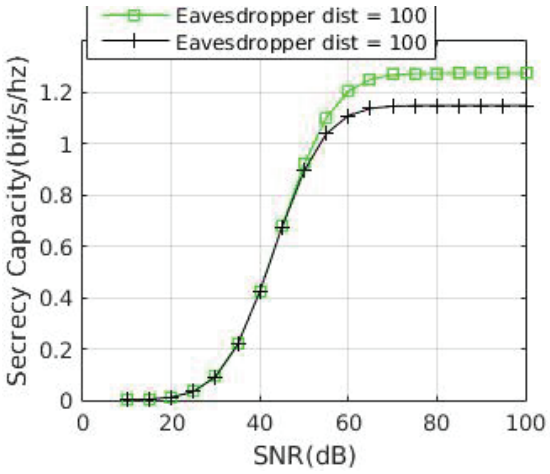

Fig. 2. Secrecy capacity vs SNR for network with two relays

can be applied during the optimization phase to provide an optimized algorithm. This iterative algorithm that relies on SDP and GP is therefore sought for in further simulations work. It results in a suboptimal method, which is developed particularly for practical scenarios - with the aim of reducing computational complexity.

References

[1] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE transactions on signal processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[2] J. Huang and A. L. Swindlehurst, "Secure communications via cooperative jamming in two-hop relay systems," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. IEEE, 2010, pp. 1–5.

[3] Y. Jing and H. Jafarkhani, "Network beamforming using relays with perfect channel information," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2499–2517, 2009.

[4] N. Kolokotronis and M. Athanasakos, "Improving physical layer security in df relay networks via two-stage cooperative jamming," in *2016 24th European Signal Processing Conference (EUSIPCO)*. IEEE, 2016, pp. 1173–1177.