COOPERATIVE JAMMING FOR WIRELESS PHYSICAL LAYER SECURITY

Lun Dong†, *Zhu Han*‡, *Athina P. Petropulu*† *and H. Vincent Poor**

†Electrical & Computer Engineering Department, Drexel University
‡Electrical & Computer Engineering Department, University of Houston
*School of Engineering and Applied Science, Princeton University

ABSTRACT

Cooperative jamming is an approach that has been recently proposed for improving physical layer based security for wireless networks in the presence of an eavesdropper. While the source transmits its message to its destination, a relay node transmits a jamming signal to create interference at the eavesdropper. In this paper, a scenario in which the relay is equipped with *multiple* antennas is considered. A novel system design is proposed for determining the antenna weights and transmit power of source and relay, so that the system secrecy rate is maximized subject to a total transmit power constraint, or, the transmit power is minimized subject to a secrecy rate constraint. Since the optimal solutions to these problems are difficult to obtain, suboptimal closed-form solutions are proposed that introduce an additional constraint, i.e., the complete nulling of jamming signal at the destination.

Index Terms— physical layer security, secrecy rate, cooperation, cooperative jamming

1. INTRODUCTION

Security is an important issue in wireless networks due to the open wireless medium. Security against an eavesdropper is typically achieved via cryptographic algorithms that are implemented at higher network layers [1]. Physical (PHY) layer based security, a line of work that has attracted considerable recent attention in this context, exploits the physical characteristics of the wireless channel to transmit messages securely (see [2] for a review of recent developments in this area). The idea was pioneered by Wyner, who introduced the wiretap channel and established the possibility of creating perfectly secure communication links without relying on private (secret) keys [3]. Wyner showed that when an eavesdropper's channel is a degraded version of the main channel, the source and destination can exchange perfectly secure messages at a non-zero rate, while the eavesdropper can learn almost nothing about the messages from its observations. The maximal rate of perfectly secret transmission from the source to its intended destination is named the *secrecy rate*. However, the feasibility of traditional PHY layer security approaches based on single antenna systems is hampered by channel conditions: absent feedback, if the channel between source and destination is worse than the channel between source and eavesdropper, the secrecy rate is typically zero.

Some recent work has been proposed to overcome this limitation by taking advantage of user cooperation [4]-[9]. For conventional wireless networks without secrecy constraints (i.e., without eavesdropper), the most common strategy for user cooperation is *cooperative relaying*, e.g., the well-known decode-and-forward and amplify-and-forward schemes. Cooperative relaying with secrecy constraints was discussed in [4]-[6]. Cooperative jamming is another approach to implement user cooperation for wireless networks with secrecy constraints [7]-[9]. In cooperative jamming, a relay transmits a jamming signal at the same time when the source transmits the message signal, with the purpose of jamming the eavesdropper. Existing works on cooperative jamming have focused primarily on the case of one single-antenna relay, and on the analysis of secrecy rate and the capacity-achieving strategy.

In this paper, we consider a different system model and different design objectives for implementing cooperative jamming. We consider a scenario in which a source communicates with a destination in the presence of one eavesdropper. The communication is aided by a relay that is equipped with *multiple* antennas that provide more degrees of freedom for the relay channel. Our goal is to assign weights to the antenna elements in an optimum fashion, and also allocate the power of source and relay in an optimum fashion. The weight and power design problem is formulated as the following optimization problem: (1) maximize achievable secrecy rate subject to a total transmit power constraint; or (2) minimize the total transmit power subject to a secrecy rate constraint. We assume that global channel state information (CSI) is available for system design. As the optimum design is in general difficult, we consider a suboptimal weight design, i.e., to completely null out the jamming signal at the destination. From the simulation results, cooperative jamming could significantly improve the system performance especially when the eavesdropper is close to the relay.

This research was supported by the National Science Foundation under Grants CNS-06-25637, CCF-07-28208, CNS-0831371 and CNS-0910461.

2. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a wireless network model consisting of one source, one trusted relay[1], one destination, and one eavesdropper. The source, destination and eavesdropper are each equipped with a single omni-directional antenna each, while the relay has $N > 1$ omni-directional antennas[2]. All channels are assumed to undergo flat fading. We denote by h_{SD} the source-destination channel, by h_{SE} the source-eavesdropper channel, by $\mathbf{h}_{SR}$ the source-relay channel ($N \times 1$ column vector), by $\mathbf{h}_{RD}$ the relay-destination channel ($N \times 1$ column vector), and by $\mathbf{h}_{RE}$ the relay-eavesdropper channel ($N \times 1$ column vector). A narrowband message signal s is to be transmitted from the source to the destination. The power of the message signal s is normalized to unity, i.e, $\mathbb{E}\{|s|^2\} = 1$. The total power budget for transmitting the message signal to its destination is P. Thermal noise at any node is assumed to be zero-mean white complex Gaussian with variance σ^2.

2.1. Cooperative jamming

In cooperative jamming, while the source transmits, the relay transmit a jamming signal that is independent of the source message. The goal is to interfere with the eavesdropper's received signal. More specifically, the source transmits the message signal $\sqrt{P_s}s$, where P_s is the transmit power of the source; at the same time, the relay transmits a weighted version of a common jamming signal z, i.e., $\mathbf{w}z$, where $\mathbf{w}$ is the weight vector applied on the N antennas. The transmit power budget for transmitting the jamming signal is thus $P_j = P - P_s$.

The received signal at the destination equals

$$y_d = \sqrt{P_s} h_{SD} s + \mathbf{w}^\dagger \mathbf{h}_{RD} z + n_d \,, \tag{1}$$

where n_d represents white complex Gaussian noise at the destination and $(\cdot)^\dagger$ represents the Hermitian transpose. The received signal at the eavesdropper equals

$$y_e = \sqrt{P_s} h_{SE} s + \mathbf{w}^\dagger \mathbf{h}_{RE} z + n_e \,, \tag{2}$$

where n_e represents white complex Gaussian noise at the eavesdropper.

2.2. Problem formulation

In the presence of an eavesdropper, *secrecy rate* is the figure of merit to represent the maximal *secrecy information* rate one can transmit from a source to its destination. Recall that the secrecy rate is $R_s = \max\{0, R_d - R_e\}$ where R_d is the rate from the source to the destination and R_e is the rate from the source to the eavesdropper [3]. We consider the practical case in which the system can be designed so that the secrecy rate is positive. In that case, the secrecy rate can be simplified to $R_s = R_d - R_e$. From (1) and (2), the secrecy rate is given by

$$\begin{aligned} R_s \;=\; & \log_2\left(1 + \frac{P_s|h_{SD}|^2}{|\mathbf{w}^\dagger \mathbf{h}_{RD}|^2 + \sigma^2}\right) \\ & - \log_2\left(1 + \frac{P_s|h_{SE}|^2}{|\mathbf{w}^\dagger \mathbf{h}_{RE}|^2 + \sigma^2}\right) \,. \end{aligned} \tag{3}$$

In the subsequent section we determine the relay weights $\mathbf{w}$ and the power P_s based on the objectives: (i) maximize secrecy rate subject to a transmit power constraint P_0, or, (ii) minimize the transmit power subject to a secrecy rate constraint R_s^0. We assume that global CSI is available for system design (a common assumption in the PHY security literature), even the eavesdropper's channel are known. Information on the eavesdropper's channel can be obtained in cases where the eavesdropper is active in the network and their transmissions can be monitored. This is applicable particularly in networks combining multicast and unicast transmissions, in which terminals play dual roles as legitimate receivers for some signals and eavesdroppers for others.

3. SYSTEM DESIGN

In this section we address system design that maximizes the secrecy rate subject to a total transmit power constraint P_0 or minimize the total transmit power subject to a secrecy rate constraint R_s^0. There are two aspects in system design: one is to determine the optimal transmit power allocated to the source and to relay; another is to design the optimal relay weights. In the following, we first fix P_s to obtain the weights for secrecy rate maximization or power minimization, and then find the optimal value of P_s.

3.1. Secrecy rate maximization

From (3), it can be seen that the secrecy rate is a product of two correlated generalized eigenvector problems and is in general difficult to handle. To simplify the analysis, in the following we consider a suboptimal design. We add one more constraint to completely null out the jamming signal at the destination, i.e., $\mathbf{w}^\dagger \mathbf{h}_{RD} = 0$. Then, the problem of secrecy rate maximization can be formulated as

$$\begin{aligned} & \arg\max_{\mathbf{w}} \; |\mathbf{w}^\dagger \mathbf{h}_{RE}|^2 \\ & \text{s.t.} \left\{ \begin{array}{l} \mathbf{w}^\dagger \mathbf{h}_{RD} = 0 \\ \|\mathbf{w}\|^2 \le P_j \end{array} \right. \end{aligned} \tag{4}$$

where $\|\cdot\|$ denotes the vector 2-norm. It is easy to show that the inequality constraint (i.e., $\|\mathbf{w}\|^2 \le P_j$) in (4) is equivalent to the equality constraint $\|\mathbf{w}\|^2 = P_j$ by contradiction.

The Lagrangian of (4) is

$$L(\mathbf{w}^\dagger, \lambda, \eta) = (2\mathbf{h}_{RE}^\dagger \mathbf{w})\mathbf{h}_{RE} + \lambda \mathbf{h}_{RD} + 2\eta \mathbf{w} \tag{5}$$

[1] We still adopt the name "relay", though it is not used for relaying here.

[2] This can also be understood as multiple relays with one antenna each.

where λ and η are Lagrange multipliers. As $\mathbf{h}_{RE}^{\dagger}\mathbf{w}$ is a scalar, by setting the Lagrangian to zero, we can see that $\mathbf{w}$ is a linear combination of $\mathbf{h}_{RD}$ and $\mathbf{h}_{RE}$, represented as

$$\mathbf{w} = a\mathbf{h}_{RD} + b\mathbf{h}_{RE} \; . \tag{6}$$

Substituting $\mathbf{w}$ into the two equality constraints in (4), we can solve a and b. Notice that the values of a and b are not unique: it is straightforward to see that, if $\mathbf{w}^*$ is the solution of (4), after rotating an arbitrary phase, $e^{j\theta}\mathbf{w}^*$ is still the solution of (4). A possible selection is $a = -\sqrt{P_j}\mu\mathbf{h}_{RD}^{\dagger}\mathbf{h}_{RE}$ and $b = \sqrt{P_j}\mu\|\mathbf{h}_{RD}\|^2$ where

$$\mu = \left[\|\mathbf{h}_{RD}\|^4\|\mathbf{h}_{RE}\|^2 - \|\mathbf{h}_{RD}\|^2|\mathbf{h}_{RD}^{\dagger}\mathbf{h}_{RE}|^2\right]^{-1/2} \; . \tag{7}$$

Next, we find the optimal value of P_s. Noticing that the above designed weight vector $\mathbf{w}$ is proportional to $\sqrt{P_s}$, let us denote $\mathbf{w}$ by $\mathbf{w} = \sqrt{P_s}\mathbf{v}$ where

$$\mathbf{v} = (-\mu\mathbf{h}_{RD}^{\dagger}\mathbf{h}_{RE})\mathbf{h}_{RD} + (\mu\|\mathbf{h}_{RD}\|^2)\mathbf{h}_{RE} \; . \tag{8}$$

Substituting it into the expression of R_s, the secrecy rate can be expressed as a function of P_s:

$$R_s(P_s) = \log_2\left(\frac{e_0 + e_1P_s + e_2P_s^2}{f_0 + f_1P_s}\right) \tag{9}$$

where e_i and f_i are coefficients independent of P_s and given by

$$\begin{aligned}
e_0 &= \sigma^2(\sigma^2 + P_0|\mathbf{v}^{\dagger}\mathbf{h}_{RE}|^2) \; , && (10)\\
e_1 &= (|h_{SD}|^2P_0 - \sigma^2)|\mathbf{v}^{\dagger}\mathbf{h}_{RE}|^2 + |h_{SD}|^2\sigma^2 \; , && (11)\\
e_2 &= -|h_{SD}|^2|\mathbf{v}^{\dagger}\mathbf{h}_{RE}|^2 \; , && (12)\\
f_0 &= \sigma^2(\sigma^2 + P_0|\mathbf{v}^{\dagger}\mathbf{h}_{RE}|^2) \; , && (13)\\
f_1 &= \sigma^2(|h_{SE}|^2 - |\mathbf{v}^{\dagger}\mathbf{h}_{RE}|^2) \; . && (14)
\end{aligned}$$

Taking the derivative of $2^{R_s(P_s)}$ and setting to zero, the optimal value of P_s is the solution of the quadratic equation

$$e_2f_1(P_s)^2 + 2e_2f_0P_s + (e_1f_0 - e_0f_1) = 0 \; . \tag{15}$$

In case no solution exists within $(0, P_0]$, it holds that $P_s = P_0$ (i.e., the case of direct transmission without jamming).

3.2. Transmit power minimization

We again consider to completely null out the jamming signal at the destination. For a fixed P_s, the problem of secrecy rate maximization can be formulated as

$$\arg\min_{\mathbf{w}} \; \|\mathbf{w}\|^2 \tag{16}$$
$$\text{s.t.} \begin{cases} \mathbf{w}^{\dagger}\mathbf{h}_{RD} = 0 \\ |\mathbf{w}^{\dagger}\mathbf{h}_{RE}|^2 \geq \rho \end{cases}$$

where $\rho = \frac{P_s|h_{RE}|^2}{2^{-R_s^0}(1+P_s|h_{RD}|^2/\sigma^2)-1} - \sigma^2$. By using the Lagrange multiplier method (similarly as in Section 3.1), it can be shown that $\mathbf{w}$ is a linear combination of $\mathbf{h}_{RD}$ and $\mathbf{h}_{RE}$, represented as $\mathbf{w} = a\mathbf{h}_{RD} + b\mathbf{h}_{RE}$. A possible selection is $a = -\mu\mathbf{h}_{RD}^{\dagger}\mathbf{h}_{RE}$ and $b = \mu||\mathbf{h}_{RD}||^2$ where

$$\mu = \sqrt{\frac{\rho}{\|\mathbf{h}_{RD}\|^2\|\mathbf{h}_{RE}\|^2 - |\mathbf{h}_{RD}^{\dagger}\mathbf{h}_{RE}|^2}} \; . \tag{17}$$

Let us denote $\mathbf{w} = \sqrt{\rho}\mathbf{v}$ where

$$\mathbf{v} = \frac{-\mathbf{h}_{RD}^{\dagger}\mathbf{h}_{RE}\mathbf{h}_{RD} + \|\mathbf{h}_{RD}\|^2\mathbf{h}_{RE}}{\|\mathbf{h}_{RD}\|^2\|\mathbf{h}_{RE}\|^2 - |\mathbf{h}_{RD}^{\dagger}\mathbf{h}_{RE}|^2} \; . \tag{18}$$

Then, the total transmit power can be represented as

$$P_s + \|\mathbf{w}\|^2 = \frac{e_0 + e_1P_s + e_2P_s^2}{f_0 + f_1P_s} \tag{19}$$

where

$$\begin{aligned}
e_0 &= -(2^{-R_s^0} - 1)\sigma^2\|\mathbf{v}\|^2 \; , && (20)\\
e_1 &= 2^{-R_s^0} - 1 + (|h_{SE}|^2 - 2^{-R_s^0}|h_{SD}|^2)\|\mathbf{v}\|^2 \; , && (21)\\
e_2 &= 2^{-R_s^0}|h_{SD}|^2/\sigma^2 \; , && (22)\\
f_0 &= 2^{-R_s^0} - 1 \; , && (23)\\
f_1 &= 2^{-R_s^0}|h_{SD}|^2/\sigma^2 \; . && (24)
\end{aligned}$$

Then, the optimal value of P_s is obtained by solving the quadratic equation which is of the same form as (15).

4. SIMULATIONS

For convenience, we consider a simple one-dimension system model, as illustrated in Fig. 1, in which the source, relay, destination and eavesdropper are placed along a line. To highlight the effects of distances, channels are modeled by a simple line-of-sight channel model including the path loss (path loss exponent is 3.5) and a random phase (uniformly distributed). The source-destination distance is fixed at 50 m, and the source-relay distance is fixed at 25 m (i.e., the relay is located at the middle point of source and destination). The noise power σ^2 is -100 dBm.

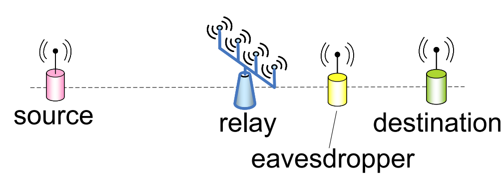

Fig. 1. Simulation model.

The position of the eavesdropper is varied so that the source-eavesdropper distance varies from 10 m to 90 m. Fig. 2 shows the secrecy rate versus the source-eavesdropper distance for a transmit power constraint $P_0 \leq -40$ dBm. For direct transmission without the relay's help, the secrecy rate is positive only if the source-eavesdropper distance is larger than the source-destination distance. Also, the secrecy rate of direct transmission increases with the increase of source-eavesdropper distance, as the rate at the eavesdropper R_j decreases. For cooperative jamming, the closer the eavesdropper is located to the relay, the higher the secrecy rate is. This is because when relay and eavesdropper are close, even a small amount of power allocated to the relay can create enough interference at the eavesdropper, and a large amount of power can be used for the source to transmit the message signal. When the eavesdropper moves away from the relay and closer to the source, the secrecy rate decreases, since more jamming power is needed for creating larger interference and less power is available for the source to transmit message signal. When the eavesdropper moves away from both the relay and source, it is interesting to see that the secrecy rate at first decreases, then increases, and eventually becomes equal to the secrecy rate of direct transmission. This is because when the eavesdropper is very far from the relay and the source, we should spend most of the power on transmitting the message signal. In that situation it is not worth spending a large amount of power on the jamming signal, since the received power of the message signal at the eavesdropper is always small (regardless of jamming) due to the large path loss. Also, as expected, increasing the number of antennas of the relay N can always improve the secrecy rate.

Fig. 3 shows the total transmit power versus the source-eavesdropper distance for a secrecy rate constraint $R_s^0 \geq 1$ b/s/Hz. For the curve corresponding to direct transmission, we only show the feasible region in which the required secrecy rate can be satisfied. The curves for cooperative jamming exhibits similar characteristics to Fig. 2, therefore a detailed discussion is omitted.

5. CONCLUSIONS

In this paper, we have addressed practical system design problems for the cooperative jamming protocol for secure wireless communications in the presence of a relay with multiple antennas. For cooperative jamming, while the the source transmits its message signal, the relay transmits a jamming signal to create interference at the eavesdropper. The multiple antennas at the relay can provide degrees of freedom for the relay channel and thus eliminate the effects of jamming signals at the destination. The objectives of our system design are the secrecy rate maximization subject to a total power constraint and the transmit power minimization subject to a secrecy rate constraint. Simulation results show that cooperative jamming could significantly improve the system performance especially when the eavesdropper is close to the relay. Future work includes the investigations of performance degradation and system design in the presence of imperfect channel estimates.

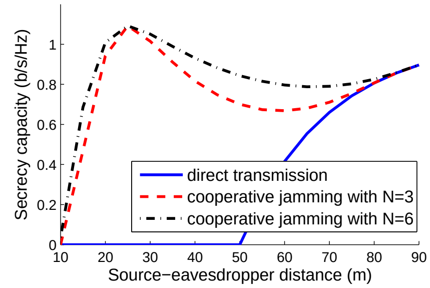

Fig. 2. Secrecy rate versus source-eavesdropper distance.

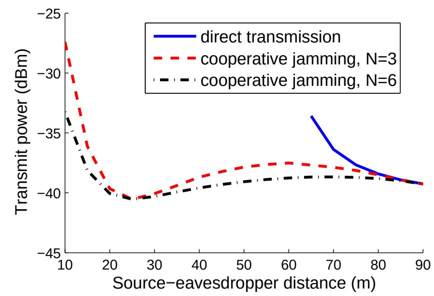

Fig. 3. Transmit power versus source-eavesdropper distance.

6. REFERENCES

[1] N. Sklavos and X. Zhang (Ed.), *Wireless Security and Cryptography: Specifications and Implementations*. CRC Press, Boca Raton, FL, 2007.

[2] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Now Publishers: Dordrecht, The Netherlands, 2009.

[3] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[4] L. Dong, Z. Han, A. Petropulu and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annual Allerton Conf. Commun., Control, and Computing*, Monticello, IL, Sept. 2008.

[5] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. IEEE Int'l Conf. Acoust. Speech Signal Proc.*, Taipei, Taiwan, Apr. 2009.

[6] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, " Secrecy capacity of a class of orthogonal relay eavesdropper channels," *Eurasip Journal on Wireless Communications and Networking*, submitted in Dec. 2008. [Online]. Available: http://arxiv.org/abs/0812.2275

[7] R. Negi and S. Goelm, "Secret communication using artificial noise," in *Proc. IEEE Vehicular Tech. Conf*, vol. 3, Dallas TX, pp. 1906-1910, Sept. 2005.

[8] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, Jun. 2008.

[9] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005 - 4019, Sept. 2008.