AMPLIFY-AND-FORWARD BASED COOPERATION FOR SECURE WIRELESS COMMUNICATIONS

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

A physical layer approach to security for wireless networks is considered. In single-antenna wireless systems, such approaches are hampered by channel conditions in the presence of one or more eavesdroppers. Cooperation has the potential to overcome this problem and improve the security of of wireless communications. In this paper, an amplify-and-forward based cooperative protocol is proposed. Assuming availability of global channel state information, system design that maximizes the secrecy capacity is considered. Since the optimal solution to this problem is intractable, suboptimal closed-form solutions are proposed that optimize bounds on secrecy capacity for the case of a single eavesdropper, or that introduce additional constraints, such as nulling of signals at all eavesdroppers, for the case of multiple eavesdroppers.

Index Terms— physical layer based wireless security, cooperation, amplify-and-forward, secrecy capacity

1. INTRODUCTION

Secure communication in wireless networks is typically achieved using cryptographic algorithms that are implemented at higher network layers. Recently, there has been considerable interest in techniques that involve the physical (PHY) layer in achieving wireless security. In his pioneering work [1], Wyner introduced the wiretap channel and established the possibility of creating almost perfectly secure communication links without relying on secret keys by using the physical properties of the channel. In particular, he 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 those messages from his observations. The maximal rate at which information from the source can be transmitted secretly to its intended destination is referred to as the *secrecy capacity*.

However, traditional PHY-based security approaches based on single antenna systems are at the mercy of channel conditions: if the channel between source and destination is worse than the channel between source and eavesdropper, the secrecy capacity is typically zero [1]-[3]. Some recent works [4]-[8] have proposed to overcome this limitation by taking advantage of multiple antenna systems at the transmitter and/or receiver. However, due to cost and size limitations of wireless transceivers, it may not be practical to deploy multiple antennas at a single network node. For such scenarios, node cooperation is an effective way to enable single-antenna nodes to enjoy the benefits of multiple-antenna systems. For example, in [9], it was shown that a relay can be used to send jamming signals to confuse an eavesdropper and thereby increase the range of channel conditions under which secure communications can take place. In our own recent work [10], we proposed a PHY-based security protocol based on decode-and-forward (DF) based cooperation. According to [10], the source first broadcasts its message using low power to its neighboring relays. Each relay node decodes the signal that it received, and then transmits a weighted version of the decoded signal to the destination. The weights were optimized to maximize secrecy capacity or minimize transmit power.

In this paper, we propose an amplify-and-forward (AF) based cooperative protocol for PHY-based wireless security. As compared to the DF-based protocol in [10], the AF-based protocol requires lower complexity at the cost of somewhat degraded performance. As in [10], we assume here that relays and the source node are located in the same cluster, while the destination and eavesdropper(s) are at faraway locations from the cluster. The protocol operates as follows. In Stage 1, the source node broadcasts its message locally to other relay nodes within the cluster. In Stage 2, for the AF-based protocol each relay node forwards a weighted version of the noisy signal that it received in Stage 1. At the same time, the source node also transmits a weighted version of the noiseless message signal. We consider the optimization problem of designing node weights to maximize the secrecy capacity subject to a transmit power constraint. Global channel state information (CSI) is assumed to be available for weight design. In the proposed AF-based protocol, the contribution of noise at relays plays an important role in secrecy capacity,

This work was supported in part by the National Science Foundation under Grants CNS-06-25637 and CCF-07-28208.

and greatly affects weight design. More specifically, both signal power and noise level are related to node weights, which makes weight design more complicated as compared with the DF-based protocol in [10]. As a result, the optimal weights for the AF-based protocol are in general intractable even for the simple case of one eavesdropper. For the case of one eavesdropper, we derive bounds on the secrecy capacity, and design the node weights to achieve these bounds. For the case of multiple eavesdroppers, we obtain a suboptimal closed-form solution, by introducing an additional constraint, i.e., nulling of signals at all eavesdroppers in Stage 2.

Notation: Bold uppercase letters denote matrices and bold lowercase letters denote column vectors; transpose and conjugate transpose are represented by $(\cdot)^T$ and $(\cdot)^\dagger$ respectively; $\mathrm{diag}\{\mathbf{a}\}$ denotes a diagonal matrix with the elements of vector $\mathbf{a}$ along its diagonal; $\mathbf{I}_M$ is the identity matrix of size $M \times M$; $\mathbf{0}_{M\times N}$ denotes an all-zero matrix of size $M \times N$; $\mathcal{CN}(\mu, \sigma^2)$ denotes circularly symmetric, complex Gaussian distribution with mean μ and variance σ^2; $\mathbb{E}\{\cdot\}$ denotes expectation.

2. SYSTEM MODEL AND AF-BASED COOPERATIVE PROTOCOL

2.1. System Model

We consider a wireless network model consisting of one source node (node index: 0), $N-1$ ($N > 1$) trusted relay nodes (node indices $1, 2, \ldots, N-1$), a destination node, and J ($J \geq 1$) eavesdroppers. We assume that source and relays are located within the same cluster, while destination and eavesdropper(s) are at faraway locations outside the cluster. Each node is equipped with a single omni-directional antenna and operates in half-duplex mode.

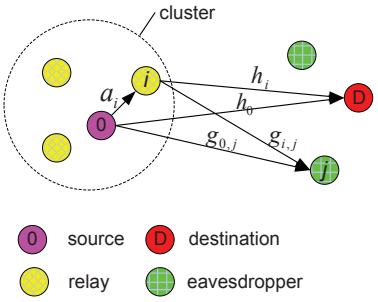

Fig. 1. Illustration of notation and system model.

A narrowband message signal s_0 is to be transmitted from the source to the destination. The power of the message signal s_0 is normalized to one, i.e, $\mathbb{E}\{|s_0|^2\} = 1$. All channels are assumed to undergo flat fading. We denote by a_i the baseband complex channel gain between the source and the ith cluster node, by h_i the channel gain between the ith cluster node and the destination, and by $g_{i,j}$ the channel gain between the ith cluster node and the jth eavesdropper. Thermal noise at any node is assumed to be zero-mean white complex Gaussian, i.e., $\mathcal{CN}(0, \sigma^2)$. This configuration is illustrated in Fig. 1.

2.2. AF-based Cooperative Protocol

In this subsection, we describe the AF-based cooperative transmission protocol based on our system model.

Stage 1: The source broadcasts its message signal s_0 locally to its trusted relays within the cluster. The received signal at the ith relay node x_i equals

$$x_i = \sqrt{P_1} a_i s_0 + n_i \tag{1}$$

where P_1 is the transmit power at the source and $n_i \sim \mathcal{CN}(0, \sigma^2)$ is white complex Gaussian noise at the ith relay.

As only local communication is needed here, Stage 1 usually requires a small amount of transmit power (i.e., small P_1) only. In this paper, for simplicity we assume that P_1 is known a priori.

Stage 2: Both the source node and all the $N-1$ trusted relays participate in this stage. For the source node, it transmits a weighted signal of the noiseless signal s_0, i.e., $w_0 s_0$; for the ith relay, it transmits a weighted version of the received noisy signal in Stage 1, i.e., $w_i x_i$, where x_i is given by (1) and w_i represents the weight the weight of the ith cluster node.

Let us define the vectors $\mathbf{a} = [\sqrt{P_1}h_0, \sqrt{P_1}a_1 h_1, \ldots, \sqrt{P_1}a_{N-1}h_{N-1}]^\dagger$ and $\mathbf{b}_j = [\sqrt{P_1}g_{0,j}, \sqrt{P_1}a_1 g_{1,j}, \ldots, \sqrt{P_1}a_{N-1}g_{N-1,j}]^\dagger$ and the $N \times N$ matrices $\mathbf{R}_\mathrm{a} = \mathbf{a}\mathbf{a}^\dagger$, $\mathbf{R}_\mathrm{b}^j = \mathbf{b}_j\mathbf{b}_j^\dagger$, $\mathbf{U} = \mathrm{diag}\{0, |h_1|^2, \ldots, |h_{N-1}|^2\}$, and $\mathbf{V}_j = \mathrm{diag}\{0, |g_{1,j}|^2, \ldots, |g_{N-1,j}|^2\}$.

The received signal at the destination equals

$$y_d = \mathbf{w}^\dagger \mathbf{a} s_0 + \sum_{i=1}^{N-1} w_i h_i n_i + n_d \tag{2}$$

where n_d represents white complex Gaussian noise at the destination. To maximize the signal-to-noise ratio (SNR), the destination combines the two received signals in both stages using maximal ratio combining (MRC). Then, the capacity at the destination is

$$C_d = \frac{1}{2}\log_2\left(\alpha + \frac{\mathbf{w}^\dagger \mathbf{R}_\mathrm{a} \mathbf{w}}{(\mathbf{w}^\dagger \mathbf{U} \mathbf{w} + 1)\sigma^2}\right) \tag{3}$$

where $\alpha \triangleq 1 + P_1|h_0|^2/\sigma^2$, and the scalar factor $1/2$ is due to the fact that two time units are required in the two-stage cooperative protocol. Note that $P_1|h_0|^2/\sigma^2$ is the received SNR in Stage 1 at the destination.

The received signal at the jth eavesdropper equals

$$y_e^j = \mathbf{w}^\dagger \mathbf{b}_j s_0 + \sum_{i=1}^{N-1} w_i g_{i,j} n_i + n_e^j \tag{4}$$

where n_e^j represents white complex Gaussian noise at the jth eavesdropper. The jth eavesdropper combines the two received signals in both stages using MRC. The capacity at the jth eavesdropper is then

$$C_e^j = \frac{1}{2}\log_2\left(\beta + \frac{\mathbf{w}^\dagger \mathbf{R}_{\rm b}^j \mathbf{w}}{(\mathbf{w}^\dagger \mathbf{V}_j \mathbf{w} + 1)\sigma^2}\right) \quad (5)$$

where $\beta \triangleq 1 + P_1|g_{0,j}|^2/\sigma^2$. Note that $P_1|g_{0,j}|^2/\sigma^2$ is the received SNR in Stage 1 at the jth eavesdropper.

3. SYSTEM DESIGN

Our objective is to determine the node weights that maximize secrecy capacity subject to a transmit power constraint. For convenience, the weight design is discussed based on the equality power constraint, and it can be shown that the equality and inequality constraints are equivalent for optimization problems in this paper. The secrecy capacity for J eavesdroppers is defined as [3]

$$C_s = \max\{0, C_d - \max(C_e^1, \ldots, C_e^J)\}\,. \quad (6)$$

The global CSI is assumed to be available for weight design (the same assumption as in most of PHY-based security literature).

3.1. One Eavesdropper

For the simple scenario of one eavesdropper, the index of the eavesdropper is dropped for notional convenience. We focus on the case of practical importance in which there exists a set of weights so that the secrecy capacity is non-zero. Thus, from (3) and (5), the secrecy capacity in (6) can be written as

$$C_s = \frac{1}{2}\log_2\left(\alpha + \frac{\mathbf{w}^\dagger \mathbf{R}_{\rm a} \mathbf{w}}{(\mathbf{w}^\dagger \mathbf{U} \mathbf{w} + 1)\sigma^2}\right) - \frac{1}{2}\log_2\left(\beta + \frac{\mathbf{w}^\dagger \mathbf{R}_{\rm b} \mathbf{w}}{(\mathbf{w}^\dagger \mathbf{V} \mathbf{w} + 1)\sigma^2}\right)\,. \quad (7)$$

It is easy to show that the transmit power of Stage 2 is $\mathbf{w}^\dagger \mathbf{T} \mathbf{w}$ where $\mathbf{T} = \mathrm{diag}\{[1, P_1|a_1|^2 + \sigma^2, \ldots, P_1|a_{N-1}|^2 + \sigma^2]\}$.

The optimization problem of maximizing the secrecy capacity C_s for a fixed transmit power P_2 (in Stage 2) can be readily formulated as

$$\arg\max_{\mathbf{w}} \ \frac{\mathbf{w}^\dagger \widetilde{\mathbf{V}} \mathbf{w}}{\mathbf{w}^\dagger \widetilde{\mathbf{U}} \mathbf{w}} \cdot \frac{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{\rm a} \mathbf{w}}{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{\rm b} \mathbf{w}} \quad \text{s.t. } \mathbf{w}^\dagger \mathbf{T} \mathbf{w} = P_2 \quad (8)$$

where $\widetilde{\mathbf{U}} = \mathbf{U} + (1/P_2)\mathbf{T}$, $\widetilde{\mathbf{V}} = \mathbf{V} + (1/P_2)\mathbf{T}$, $\widetilde{\mathbf{R}}_{\rm a} = \mathbf{R}_{\rm a} + \alpha\sigma^2\widetilde{\mathbf{U}}$ and $\widetilde{\mathbf{R}}_{\rm b} = \mathbf{R}_{\rm b} + \beta\sigma^2\widetilde{\mathbf{V}}$. Note that $\widetilde{\mathbf{U}}$ and $\widetilde{\mathbf{V}}$ are diagonal. The objective function in (8) is a product of two correlated Rayleigh quotient problems, and is thus in general intractable. To simplify the analysis, in the following we will derive the suboptimal weights that maximize the upper and lower bounds of the objective function in (8).

Note that the maximum and minimum of the Rayleigh quotient $\frac{\mathbf{w}^\dagger \widetilde{\mathbf{V}} \mathbf{w}}{\mathbf{w}^\dagger \widetilde{\mathbf{U}} \mathbf{w}}$ correspond to the maximal eigenvalue $\lambda_{\max}$ and the minimal eigenvalue $\lambda_{\min}$ of the matrix $\widetilde{\mathbf{U}}^{-1}\widetilde{\mathbf{V}}$, respectively [11]. As the matrix $\widetilde{\mathbf{U}}^{-1}\widetilde{\mathbf{V}}$ is diagonal, we can readily show that

$$\lambda_{\max} = \max\left\{1, \max_i\left(\frac{P_1|a_i|^2 + P_2|h_i|^2 + \sigma^2}{P_1|a_i|^2 + P_2|g_i|^2 + \sigma^2}\right)\right\} \quad (9)$$

and

$$\lambda_{\min} = \min\left\{1, \min_i\left(\frac{P_1|a_i|^2 + P_2|h_i|^2 + \sigma^2}{P_1|a_i|^2 + P_2|g_i|^2 + \sigma^2}\right)\right\}\,. \quad (10)$$

Then, the objective function in (8) is lower and upper bounded as

$$\lambda_{\min}\frac{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{\rm a} \mathbf{w}}{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{\rm b} \mathbf{w}} \le \frac{\mathbf{w}^\dagger \widetilde{\mathbf{V}} \mathbf{w}}{\mathbf{w}^\dagger \widetilde{\mathbf{U}} \mathbf{w}} \cdot \frac{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{\rm a} \mathbf{w}}{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{\rm b} \mathbf{w}} \le \lambda_{\max}\frac{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{\rm a} \mathbf{w}}{\mathbf{w}^\dagger \widetilde{\mathbf{R}}_{\rm b} \mathbf{w}}\,. \quad (11)$$

Finally, the weight vector that maximizes the lower or upper bound in (11) is $\mu_1 \mathbf{q}_1^{\rm unit}$ where $\mathbf{q}_1^{\rm unit}$ is the unit-norm eigenvector of the matrix $\widetilde{\mathbf{R}}_{\rm b}^{-1}\widetilde{\mathbf{R}_{\rm a}}$ corresponding to its largest eigenvalue, and μ_1 is a scalar chosen to satisfy the power constraint, i.e., $\mu_1 = \sqrt{\frac{P_2}{(\mathbf{q}_1^{\rm unit})^\dagger \mathbf{T} \mathbf{q}_1^{\rm unit}}}$.

Remark: The above suboptimal solution works well in the case of $\lambda_{\max} \approx \lambda_{\min}$. The possible scenarios include: (i) the channel fading amplitudes between the eavesdropper and cluster nodes are approximately the same as those between the destination and cluster nodes, i.e., $|h_i|^2 \approx |g_i|^2$; (ii) the signal power at the relay is much greater than the signal power at the destination, i.e., $P_1|a_i|^2 \gg P_2|h_i|^2$ and $P_1|a_i|^2 \gg P_2|g_i|^2$. In these cases, the bounds in (11) are tight, and the above solution that maximizes the bounds of the secrecy capacity is near-optimal. Also, for these cases, the equality power constraint in (8) is equivalent to the inequality power constraint $\mathbf{w}^\dagger \mathbf{T} \mathbf{w} \le P_2$ [7],[8]. For other cases, the above suboptimal solution may not perform well and the solution in the next subsection could be used instead.

3.2. Multiple Eavesdroppers

For a scenario involving multiple eavesdroppers, we consider completely nulling out the Stage 2 signals at all eavesdroppers. Let us define the $J \times N$ matrix $\mathbf{B} \triangleq [\mathbf{b}_1, \ldots, \mathbf{b}_J]^\dagger$. To null the signals at all eavesdroppers, we need

$$\mathbf{B}\mathbf{w} = \mathbf{0}_{J\times 1}\,. \quad (12)$$

The problem of maximizing the secrecy capacity under a fixed transmit power can be formulated as

$$\arg\max_{\mathbf{w}} \ \frac{\mathbf{w}^\dagger \mathbf{R}_{\rm a} \mathbf{w}}{\mathbf{w}^\dagger \mathbf{U} \mathbf{w} + 1} \quad \text{s.t. } \mathbf{B}\mathbf{w} = \mathbf{0}_{J\times 1} \text{ and } \mathbf{w}^\dagger \mathbf{T} \mathbf{w} = P_2 \quad (13)$$

Let us define the matrix $\mathbf{F}$ containing all of the right singular vectors corresponding to zero singular values of $\mathbf{B}$. To satisfy the first constraint in (13), $\mathbf{w}$ should be a linear combination of the basis of the null space of $\mathbf{B}$, i.e., $\mathbf{w} = \mathbf{F}\mathbf{v}$, where $\mathbf{v}$ is a column vector. Then, the optimization problem in (13) is equivalent to

$$\arg\max_{\mathbf{v}} \frac{\mathbf{v}^\dagger \mathbf{F}^\dagger \mathbf{R}_a \mathbf{F}\mathbf{v}}{\mathbf{v}^\dagger \mathbf{F}^\dagger \mathbf{U}\mathbf{F}\mathbf{v}+1} \quad \text{s.t. } \mathbf{v}^\dagger \mathbf{F}^\dagger \mathbf{T}\mathbf{F}\mathbf{v} = P_2 \tag{14}$$

which is also a Rayleigh quotient problem. The solution of (14) is then $\mathbf{v} = \sqrt{P_2}\mathbf{q}_2^{\text{unit}}$ where $\mathbf{q}_2^{\text{unit}}$ is the unit-norm eigenvector of matrix $\mathbf{F}^\dagger[\mathbf{U} + (1/P_2)\mathbf{T}]^{-1}\mathbf{F}\mathbf{F}^\dagger\mathbf{R}_a\mathbf{F}$ corresponding to the largest eigenvalue. Finally, the solution of (13) is $\mathbf{w} = \mu_2 \mathbf{F}\mathbf{q}_2^{\text{unit}}$ where $\mu_2 = \sqrt{\frac{P_2}{(\mathbf{q}_2^{\text{unit}})^\dagger \mathbf{F}^\dagger \mathbf{T}\mathbf{F}\mathbf{q}_2^{\text{unit}}}}$. It is easy to see that the secrecy capacity is an increasing function of P_2, so the equality power constraint in (13) is equivalent to the inequality power constraint $\mathbf{w}^\dagger\mathbf{T}\mathbf{w} \leq P_2$.

3.3. Numerical Results

In this subsection, we use simulations to demonstrate the performance of the proposed weights and also provide comparison to direct transmission and DF-based cooperation. The noise power σ^2 is -60 dBm. The cluster nodes are uniformly located in a disk with radius $R = 5$ m. The distance between source and destination is fixed at $10R$. The distances between the source and eavesdroppers are uniformly distributed within $[10R, 30R]$. Rayleigh fading with path loss is assumed, with path loss exponent equal to 3.5. In Stage 1, the average received SNR at the relays is 25 dB. A Monte-Carlo experiment consisting of 1000 independent trials is performed to obtain the average results.

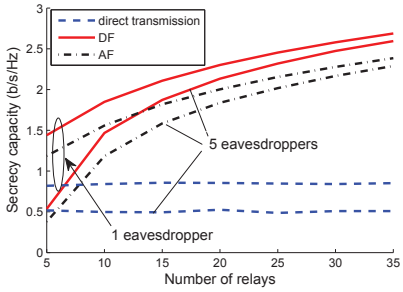

Fig. 2. Secrecy capacity versus number of relays.

Fig. 2 shows the secrecy capacity versus the number of relay nodes $N-1$ for a fixed power ($P_2 = 0$ dBm). The secrecy capacity with DF-based cooperation is computed based on the algorithms in [10]. For a single eavesdropper, the secrecy capacity with AF-based cooperation is obtained based on the greater between the capacity of obtained via the weights of Section 3.1 and the capacity obtained via the weights of Section 3.2. For multiple eavesdroppers, the secrecy capacity with AF-based cooperation is computed based on the weights of Section 3.2. As expected, the secrecy capacity of direct transmission without cooperation is independent of the number of relays. As observed, the secrecy capacity for cooperation decreases as the number of eavesdroppers increases, and increases as the number of relays increases. As compared to DF, there is a performance penalty for AF-based cooperation due to the noise at relays.

4. CONCLUSIONS AND FUTURE WORK

In this paper, we have considered an amplify-and-forward based cooperative protocol to improve the performance of secure wireless communications in the presence of one or multiple eavesdroppers. For the case of one eavesdropper, we have proposed a system design that maximizes the upper and lower bounds of secrecy capacity. For the case of multiple eavesdroppers, we have proposed a suboptimal design by adding an additional constraint, i.e., the complete nulling of signals at all eavesdroppers. In future work, we will investigate the performance degradation in the presence of imperfect channel estimates, and study the system design based on channel statistics or partial channel state information.

5. REFERENCES

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

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451 - 456, Jul. 1978.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339 - 348, May 1978.

[4] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no.12, pp. 3235 -3249, Dec 2003.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: the MISOME wiretap channel," submitted in Aug. 2007 (available at http://arxiv.org/abs/0708.4219).

[6] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels." in *Proc IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, pp. 2152 - 2155, Sept. 2005.

[7] Z. Li, W. Trappe and R. Yates, "Secret communication via multi-antenna transmission,' in' *Proc. 41st Conference on Information Sciences and Systems*, Baltimore, MD, Mar 2007.

[8] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007.

[9] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, to appear.

[10] 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.

[11] G. Golub and C. V. Loan, *Matrix Computations, 3rd ed.* The Johns Hopkins Univ. Press, Baltimore, MD, 1996.