

Multiuser Detection for Eavesdropping in Cellular CDMA

Andrew McKellips and Sergio Verdú
Department of Electrical Engineering
Princeton University, Princeton, NJ 08544 *

Abstract

Multiuser detection techniques are considered for use by an eavesdropper in a cellular CDMA communication system with power-control. Eavesdropper susceptibility to the near-far problem is demonstrated, and the induced distribution of received power from an active user with uniformly random location within the cell is determined. Various detection schemes are compared for a log-distance path loss model with and without shadowing.

1. Introduction

Power control is implemented in cellular communication systems to insure that active users are received with approximately equal power at the base station. The purpose of such control is to mitigate multiple access interference (MAI) in the reverse channel by preventing the domination of any user's signal by that of any other user at the base station detector, effectively realizing a fair distribution of MAI among all users. The potential for a significant discrepancy in received user power is commonly referred to as the near-far problem, and can result in significant performance degradation.

Although power control mitigates the received power distribution from active users at the base station, it does so with disregard to the induced power distribution throughout the rest of the cell. Consequently, an eavesdropper located somewhere other than the base station may not benefit from power control; in fact, the range of potential received powers at an off-center eavesdropper can actually *increase* as a result of base station power control. The eavesdropper is therefore susceptible to near-far effects, as depicted in Figure 1. In this paper, we study eavesdropper performance in

a cellular CDMA environment, demonstrating the potential for a significant performance improvement using multiuser detection techniques. In Section 2, we compute the received power distribution throughout a communication cell with ideal power control. We then compare several eavesdropper detection strategies in Section 3, and consider the effect of shadowing in Section 4. Our conclusions are presented in Section 5.

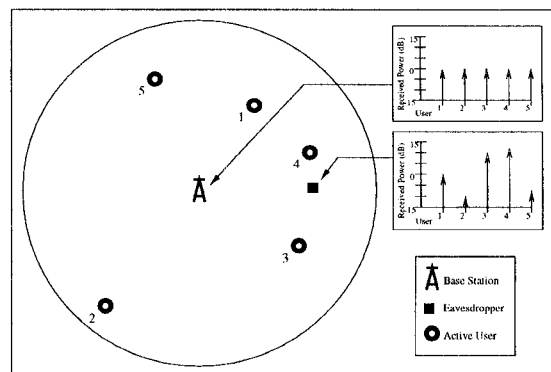


Figure 1. Near-Far Effect for an Eavesdropper in a Power-Controlled Cell

2. Received Power Distribution

Consider a communication cell of radius A , with a single centrally-located base station, K active users, and an eavesdropper located a distance $a \leq A$ from the base station. The locations of the users within the cell are modelled as uniformly random and independent. Path loss is assumed to satisfy a log-distance model of the form

$$p_R = p_T/d^{2\alpha} \quad (1)$$

where p_T represents the user's transmit power, p_R the received power, d the propagation distance, and α the path loss exponent, typically ranging from 1 (rural) to 2 (urban). The additional effect of log-normal shadowing will be considered in Section 4.

*This work was supported in part by the U.S. Army Research Office under Grant DAAH04-96-1-0379.

For an active user located in the far-field region of the base station and eavesdropper antennas at a distance u from the base station ($0 < u \leq A$) and on a line θ radians from the line between eavesdropper and base station (Figure 2), the received power at the eavesdropper is given by

$$p = (u^2 / (u^2 + a^2 - 2ua \cos \theta))^\alpha \quad (2)$$

where the reference level at the base station is taken to be 0 dB. Figure 2 depicts a representative set of contours corresponding to equal received power at the eavesdropper. The cumulative distribution function (CDF) of the random variable P representing received power from a user distributed uniformly within the cell is given by

$$F_P(p) = \begin{cases} 0, & 0 \leq p < \frac{1}{M} \\ \frac{p^{1/\alpha} \gamma^2}{(1-p^{1/\alpha})^2}, & \frac{1}{M} \leq p \leq \max \left\{ \frac{1}{M}, \frac{1}{(1+\gamma)^{2\alpha}} \right\} \\ \frac{1}{2} + \frac{1}{\pi} \sin^{-1} \left(\frac{p^{1/\alpha} (1+\gamma^2) - 1}{2p^{1/\alpha} \gamma} \right) + \frac{p^{1/\alpha} \gamma^2}{(1-p^{1/\alpha})^2} \\ \quad \times \left(\frac{1}{2} - \frac{1}{\pi} \sin^{-1} \left(\frac{p^{1/\alpha} (p^{1/\alpha} + 1) \gamma^2 - (1-p^{1/\alpha})^2}{2p^{3/2\alpha} \gamma^2} \right) \right) \\ \quad + \frac{\sqrt{2p^{1/\alpha} (1+\gamma^2) - p^{2/\alpha} (1-\gamma^2)^2 - 1}}{2\pi(p^{1/\alpha} - 1)}, & \max \left\{ \frac{1}{M}, \frac{1}{(1+\gamma)^{2\alpha}} \right\} < p < 1 \\ \frac{1}{2} + \frac{1}{\pi} \sin^{-1} \left(\frac{\gamma}{2} \right) + \frac{\gamma}{4\pi} \sqrt{4 - \gamma^2}, & p = 1 \\ \frac{1}{2} + \frac{1}{\pi} \sin^{-1} \left(\frac{p^{1/\alpha} (1+\gamma^2) - 1}{2p^{1/\alpha} \gamma} \right) - \frac{p^{1/\alpha} \gamma^2}{(1-p^{1/\alpha})^2} \\ \quad \times \left(\frac{1}{2} - \frac{1}{\pi} \sin^{-1} \left(\frac{p^{1/\alpha} (p^{1/\alpha} + 1) \gamma^2 - (1-p^{1/\alpha})^2}{2p^{3/2\alpha} \gamma^2} \right) \right) \\ \quad + \frac{\sqrt{2p^{1/\alpha} (1+\gamma^2) - p^{2/\alpha} (1-\gamma^2)^2 - 1}}{2\pi(p^{1/\alpha} - 1)}, & 1 < p < \min \left\{ M, \frac{1}{(1-\gamma)^{2\alpha}} \right\} \\ 1 - \frac{p^{1/\alpha} \gamma^2}{(1-p^{1/\alpha})^2}, & \min \left\{ M, \frac{1}{(1-\gamma)^{2\alpha}} \right\} \leq p \leq M \\ 1, & p > M \end{cases} \quad (3)$$

where $\gamma = a/A$ and the range of $\sin^{-1}(\cdot)$ is taken to be $[-\pi/2, \pi/2]$. The restriction of potential received power to the interval $[1/M, M]$ represents the inconsistency of the path loss model (1) for small transmitter-receiver separation d . Of note is the dependency of the received power distribution on the location of the eavesdropper and the radius of the cell through a single parameter $0 \leq \gamma \leq 1$ representing ‘‘off-centered-ness’’ of the eavesdropper.

3. Two-User CDMA System Analysis

Consider a synchronous CDMA system with two active users, where users 1 and 2 are assigned the signature waveforms $s_1(t)$ and $s_2(t)$ respectively. The waveforms are assumed to be time-limited to the interval $[0, T]$ where T is the inverse of the bit transmission

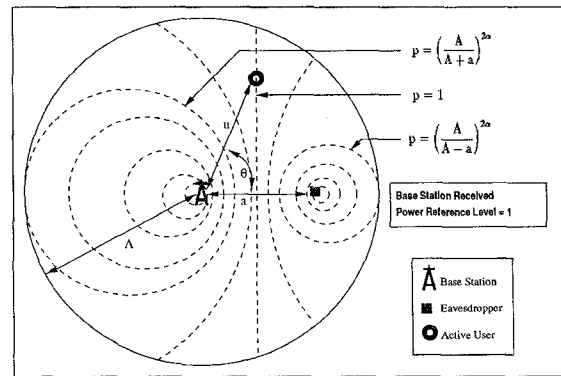


Figure 2. Equal Received Power Contours for an Eavesdropper

rate, and are assumed to exhibit normalized signal energy. User 1 transmits the signal

$$u_1(t) = A_1 b_1 s_1(t)$$

and user 2 the signal

$$u_2(t) = A_2 b_2 s_2(t)$$

where the information-bearing bits b_1 and b_2 are independent and identically distributed, taking on the values $+1$ and -1 equiprobably, and the transmitted amplitudes A_1 and A_2 are chosen to realize ideal power control at the base station. Our goal is to analyze eavesdropper performance as it depends on eavesdropper off-centered-ness γ and signal cross-correlation ρ where

$$\rho = \int_0^T s_1(t) s_2(t) dt.$$

The eavesdropper is faced with determining b_1 given the reception

$$y(t) = \sqrt{p_1} b_1 s_1(t) + \sqrt{p_2} b_2 s_2(t) + n(t) \quad (4)$$

where $n(t)$ is white Gaussian background noise with variance σ^2 and p_1 and p_2 are received powers at the eavesdropper, given by (2). When both users are independently and uniformly distributed within the cell, p_1 and p_2 will independently take the distribution (3).

With conventional matched-filter detection, the eavesdropper decides

$$\hat{b}_1(\text{conv}) = \text{sgn} \left(\int_0^T y(t) s_1(t) dt \right)$$

where $\text{sgn}(x)$ takes the value 1 if $x \geq 0$ and -1 if $x < 0$. The probability of detection error is then given by

$$P_e(\text{conv}) = \frac{1}{2} \left\{ Q \left(\frac{\sqrt{p_1} - \rho \sqrt{p_2}}{\sigma} \right) + Q \left(\frac{\sqrt{p_1} + \rho \sqrt{p_2}}{\sigma} \right) \right\}$$

from which it is clear that performance will be satisfactory as long as the background noise power remains small and $\rho^2 p_2 \ll p_1$. In light the fact that an off-centered eavesdropper is susceptible to the near-far problem (characterized by $p_2 \gg p_1$), the conventional detector may not provide dependable results.

Hence, it is of interest to an eavesdropper to consider using multiuser detection techniques designed to mitigate MAI and provide near-far resistance. Given knowledge of the signature waveforms and received powers of all K active users, optimum detection amounts to performing a maximum likelihood decision over all possible 2^K potential transmitted bit combinations. In the two-user case, jointly optimum detection of user 1 is achieved by computing (*e.g.* [1])

$$y_1 = \int_0^T y(t) s_1(t) dt$$

as in the conventional detector, and in addition

$$y_2 = \int_0^T y(t) s_2(t) dt,$$

leading to the decision

$$\hat{b}_1(\text{opt}) = \begin{cases} \text{sgn}(y_1), & \min\{\sqrt{p_1}|y_1|, \sqrt{p_2}|y_2|\} \\ & \geq |\rho|\sqrt{p_1 p_2} \\ \text{sgn}(y_1 - \text{sgn}(\rho)y_2), & \text{otherwise.} \end{cases}$$

A drawback to optimum detection is the exponential growth in complexity with an increasing number of active users. An alternative strategy with linear complexity is the decorrelating detector, which also requires knowledge of the signature waveforms of all users, but not the received powers. The decorrelating detector eliminates all MAI, but at the expense of increased background noise power, and in the two-user case amounts to deciding

$$\hat{b}_1(\text{dec}) = \text{sgn}(y_1 - \rho y_2).$$

Another alternative is the Minimum Mean Square Error (MMSE) linear multiuser detector, which minimizes the sum of MAI power and background noise power. Although the MMSE detector requires knowledge of the signature waveforms and received powers of all users, in addition to the background noise power, it lends itself to a blind adaptive implementation [2]. In the two-user system, the MMSE decision is given by

$$\hat{b}_1(\text{MMSE}) = \text{sgn} \left(\left(1 + \frac{\sigma^2}{p_2} \right) y_1 - \rho y_2 \right).$$

In order to compare eavesdropper detection strategies, we apply the performance criteria of asymptotic

multiuser efficiency (AME) and bit error rate (BER). The AME quantifies the SNR attenuation required in an equivalent single-user system (without interferers) in order to match error performance with the given multiuser system in the low background noise region. The following expressions quantify the two-user AMEs of the conventional, optimal, decorrelating and linear MMSE detectors respectively for a given received power ratio $r^2 = p_2/p_1$ and a given cross-correlation ρ [1]:

$$\eta(\text{conv}; r, \rho) = \max^2 \{0, 1 - |\rho|r\} \quad (5)$$

$$\eta(\text{opt}; r, \rho) = \min \{1, 1 + r^2 - 2|\rho|r\} \quad (6)$$

$$\eta(\text{dec}; r, \rho) = 1 - \rho^2$$

$$\eta(\text{MMSE}; r, \rho) = 1 - \rho^2.$$

The induced distribution F_R of received power ratio $R = P_2/P_1$ for two independently and uniformly distributed users exhibits log-normal characteristics when calculated for a linear cell geometry. Simulations demonstrate that accurate performance results are obtained by applying a log-normal approximation for a standard circular geometry as well, especially for off-centered-ness values $\gamma \geq 0.1$. We apply the log-normal approximation to received power ratio with mean 0 dB and standard deviation σ_R given (in dB) through (3) by

$$\sigma_R^2 = 2E[(10 \log_{10} P)^2] - 2E[10 \log_{10} P]^2. \quad (7)$$

The expected AMEs of the conventional and optimal detectors for two uniformly distributed users with cross-correlation ρ are then given by

$$E[\eta(\text{conv}; R, \rho)] = \frac{20/\log(10)}{\sqrt{2\pi\sigma_R^2}} \int_0^{1/|\rho|} \frac{(1 - |\rho|\tau)^2}{\tau} \exp \left\{ -\frac{(20 \log_{10} \tau)^2}{2\sigma_R^2} \right\} d\tau \quad (8)$$

$$E[\eta(\text{opt}; R, \rho)] = \frac{20/\log(10)}{\sqrt{2\pi\sigma_R^2}} \int_0^{2|\rho|} \frac{1 + \tau^2 - 2|\rho|\tau}{\tau} \exp \left\{ -\frac{(20 \log_{10} \tau)^2}{2\sigma_R^2} \right\} d\tau + Q \left(\frac{20 \log_{10}(2|\rho|)}{\sigma_R} \right) \quad (9)$$

where $\log(\cdot)$ denotes the natural logarithm.

Figure 3 depicts expected eavesdropper performance using various detection strategies for two uniformly and independently located users with signal cross-correlation $\rho = 0.2$ as a function of eavesdropper off-centered-ness; the path loss exponent is taken to be $\alpha = 1$. The curves are computed using the log-normal

approximation to received power ratio via (8) and (9); simulation results are shown for comparison. Note that the multiuser detection techniques substantially outperform the conventional detector. In order to evalu-

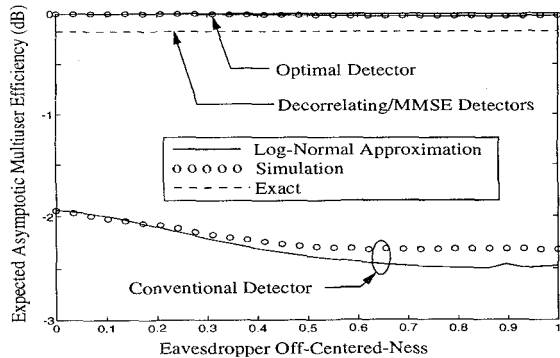


Figure 3. Asymptotic Multiuser Efficiency for Various Detection Strategies (Two Uniformly-Distributed Users with Cross-correlation $\rho = 0.2$)

ate eavesdropper performance for non-negligible noise power levels, Figure 4 depicts BER curves for the two-user system described above at a SNR level of 10 dB, as obtained through simulation of the users' locations using exact BER expressions. System SNR is taken to be the ratio of signal power from a single active user to background noise power for an eavesdropper situated at the base station. It is clear that BER performance is improved significantly in all cases through the use of multiuser detection. It is also apparent that for the chosen parameters, the loss in performance incurred through use of the lower-complexity decorrelating and linear MMSE detectors is very small in comparison to optimal detection.

4. Shadowing

The log-distance path loss model we have adopted to this point can be augmented to incorporate the effects of shadowing, which models unpredictable signal attenuation due to varying terrain and obstructions within the cell. Typically, shadowing is modelled by a log-normal random variable [3] with standard deviation σ_S derived from system measurements. The log-distance model (1) is thus augmented to the new path loss expression

$$p_R = X p_T / d^{2\alpha} \quad (10)$$

where X is a log-normal random variable representing shadowing effects, $10 \log_{10} X \sim \mathcal{N}(0, \sigma_S^2)$. We assume

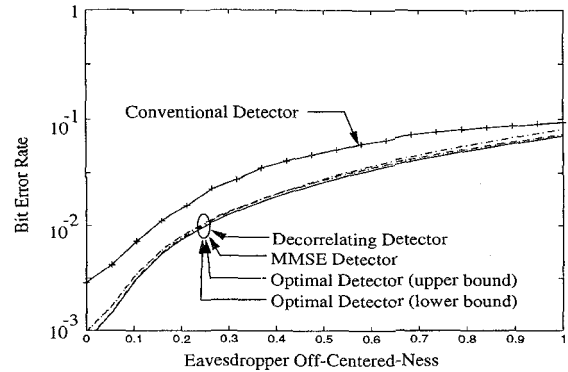


Figure 4. Bit Error Rate for Various Detection Strategies, SNR=10 dB (Two Uniformly-Distributed Users with Cross-correlation $\rho = 0.2$)

that the base station and eavesdropper experience independent shadowing from different users and from each other, which is reasonable for non-negligible eavesdropper off-centered-ness and inter-user separation.

If the base station compensates for shadowing through the use of feedback power control, an achievable goal given the typically slow behavior of shadowing dynamics in comparison with transmission bit rates, received power p^S is given by

$$p^S = p X^e / X^{bs} \quad (11)$$

where p is received power for log-distance path loss, given by (2), and X^e and X^{bs} represent shadowing experienced by the base station and eavesdropper respectively.

Recalling the two-user analysis of the previous section, where the ratio of received powers P_2/P_1 at an eavesdropper for two uniformly and independently located active users under a log-distance path loss model was found to be well-approximated by a log-normal random variable, we note that the ratio (in dB) of received powers P_2^S/P_1^S in the added presence of shadowing effects can be rewritten according to (11) as

$$\begin{aligned} & 10 \log_{10}(P_2^S/P_1^S) \\ &= 10 \log_{10} X_2^e - 10 \log_{10} X_1^e - 10 \log_{10} X_2^{bs} \\ & \quad + 10 \log_{10} X_1^{bs} + 10 \log_{10}(P_2/P_1) \end{aligned}$$

where the terms in the summation are mutually independent zero-mean normal random variables, with X_1^e , X_2^e , X_1^{bs} and X_2^{bs} exhibiting variance σ_S^2 , and the log-distance power ratio $10 \log_{10}(P_2/P_1)$ exhibiting variance σ_R^2 according to (7). Hence, given the log-normal approximation for received power ratio under the log-distance path loss model, the received power ratio with

shadowing is also log-normal with zero mean and standard deviation $4\sigma_S^2 + \sigma_R^2$ dB. It is interesting to note that power control actually amplifies the deleterious effect of shadowing at the eavesdropper; coupled with the previous observation that power control contributes to the near-far problem for the eavesdropper by introducing a larger potential range of received powers, we conclude that employed power control is a significant hindrance to the eavesdropper.

Figure 5 depicts the AMEs of various eavesdropper detection strategies for a two-user power-controlled system subject to log-normal shadowing with standard deviation 10 dB. Comparing with Figure 3, which was computed without consideration to shadowing effects, it is apparent that performance sensitivity to eavesdropper off-centered-ness is reduced by the effect of shadowing, an expected product of the location-independent contribution to received power variance represented by shadowing. In addition, the performance loss incurred by use of conventional detection is increased in the presence of shadowing. Figure 6 depicts BER performance curves for the same system with a background SNR level of 10 dB. The effect of shadowing in comparison to Figure 4 is seen to flatten the performance curves, representative of a decreased sensitivity of eavesdropper performance to location, a result of the dominant effect of shadowing on received power variance.

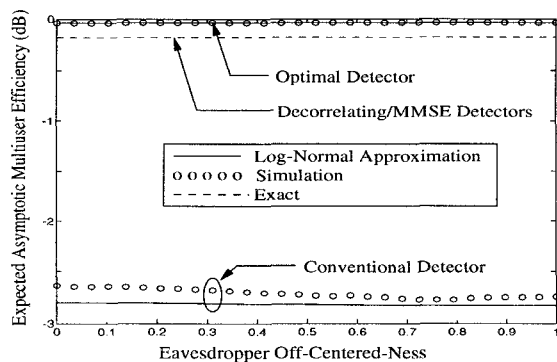


Figure 5. Asymptotic Multiuser Efficiency for Various Detection Strategies in Log-Normal Shadowing with Standard Deviation 10 dB (Two Uniformly-Distributed Users with Cross-correlation $\rho = 0.2$)

5. Conclusions

The off-center eavesdropper was shown to be susceptible to the near-far problem when operating in the reverse channel of a cellular CDMA system with power control. The distribution of received power from an

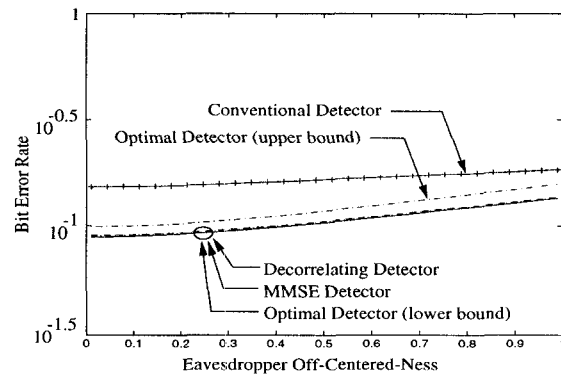


Figure 6. Bit Error Rate for Various Detection Strategies in Log-Normal Shadowing with Standard Deviation=10 dB (Two Uniformly-Distributed Users with Cross-correlation $\rho = 0.2$, SNR=10 dB)

active user with uniformly random location was determined for a log-distance path loss model, with dependency on eavesdropper location represented by a single "off-centered-ness" parameter.

In order to improve performance in light of the demonstrated near-far problem, several multiuser detection strategies exhibiting various levels of computational complexity were considered for use by an eavesdropper in a cellular CDMA system. A performance comparison was performed using a log-normal approximation to the distribution of received power ratio under the AME criterion, with results supported by simulation. A BER comparison was also performed via simulation of the users' locations using exact BER expressions. These comparisons demonstrated the potential for significant eavesdropper performance improvement through the use of multiuser detection techniques.

Finally, log-normal shadowing effects were incorporated into the eavesdropper performance analysis. A performance comparison for a two-user system subject to both log-distance path loss and shadowing also demonstrated a significant performance improvement using multiuser detection.

References

- [1] S.Verdú: *Multiuser detection*. Cambridge University Press, New York, 1998.
- [2] M. Honig, U.Madhow, S.Verdú: *Blind multiuser detection*. "IEEE Trans. Inform. Theory", Vol. IT-41, No. 4, July 1995, p. 944-960.
- [3] T.S.Rappaport: *Wireless communication: principles and practice*. Prentice Hall PTR, 1996.