Eavesdropping on the IS–95 Downlink: Reduced Complexity Optimum and Suboptimum Multiuser Detectors

D.R. Brown and C.R. Johnson, Jr.
Cornell University
Ithaca, NY 14853

H.V. Poor
Princeton University
Princeton, NJ 08544

Abstract— **We consider multiuser detection techniques for an eavesdropping receiver in an IS–95 cellular communication system observing interfering downlink transmissions from a cluster of B base stations. The receiver desires to accurately estimate the symbols transmitted from these base stations to their active local users. For a system with K total asynchronous users and an observation of $2L+1$ bits, the optimum detector is reviewed and shown to have complexity on the order of $2^{K(2L+1)}$. Taking advantage of the structure of the IS–95 downlink, we develop a reduced complexity *optimum* detector with exponentially lower complexity. In typical scenarios with two or three base stations, the reduced complexity optimum detector is significantly less complex than the brute-force optimum detector. We also consider a suboptimum, low complexity IS–95 downlink eavesdropping detector with connections to reduced complexity optimum detection as well as group detection and parallel interference cancellation. We demonstrate via simulation that the performance of this receiver can be near-optimum while offering very low computational complexity.**

I. Introduction

The IS–95 [1] downlink eavesdropping problem has at least two unique challenges not often considered in the multiuser detection literature:

- The non-cyclostationary nature of the cochannel interference in the IS–95 downlink precludes the use of linear multiuser detectors that use subspace tracking or require matrix inversions (e.g. decorrelating and MMSE) since the interference subspace changes at each symbol interval.
- The IS–95 downlink eavesdropper observes the downlink transmissions from *multiple* base stations hence it is possible that the total number of active users K could be greater than the spreading gain.
- IS–95 downlink power control (or allocation) may lead to widely disparate user amplitudes observed at the eavesdropper. This implies that there may be scenarios where the cochannel interference creates near-far problems [2] with conventional matched filter detection.

These challenges lead us to consider the application of nonlinear multiuser detection techniques for IS–95 downlink eavesdropping in this paper.

This paper is organized as follows. In Section II we develop a concise model with mild simplifying assumptions for the IS–95 downlink that includes the effects of the time and phase asynchronous, nonorthogonal, and noncyclostationary transmissions of the B base station communication system. In Section III we use this model to examine the optimum (joint maximum likelihood) detector in the IS–95 downlink eavesdropping context. Although the optimum detector is often too complex for implementation in realistic systems, its role is still important in order to determine the relative performance of suboptimum multiuser detectors. In Section IV we examine the structure of the IS–95 downlink model to develop a reduced complexity optimum detector that has exponentially less complexity than the brute-force optimum detector. In Section V we examine the properties of this reduced complexity optimum detector in order to develop a suboptimum Group Parallel Interference Cancellation (GPIC) detector with computational complexity similar to conventional matched filter detection. In Section VI we examine the performance of the GPIC detector relative to the conventional matched filter and optimum detectors via simulation and show that the GPIC detector exhibits near-optimum performance in the cases we examined.

II. IS–95 Downlink System Model

Consider the simplified IS–95 downlink system model depicted in Figure 1 where B cellular base stations each transmit digital information to a group of K_b local users[1]. The system thus has a total of $K = \sum_{b=1}^{B} K_b$ users. In general, a receiver in the cell system observes each base station's transmission through an individual propagation channel (including multipath, delay, and attenuation) summed and corrupted by additive channel noise. The components of Figure 1 are described below:

- Channelizer: Orthogonalizes the transmissions of the users within the base station's cell by assigning a unique Walsh-64 code to each user.
- Power Control: Sets the gain on each user's transmission to provide an acceptable transmission quality to that user while minimizing the generated cochannel interference.
- Modulator: Multiplies the aggregate base station transmission by a complex pseudonoise (PN) code for base sta-

Supported in part by NSF grants MIP-9509011, ECS-9528363, ECS-9811297 and Applied Signal Technology.

[1] We simplify this development by ignoring the voice activity, soft handoff, and antenna sectorization features of IS–95 in this paper.

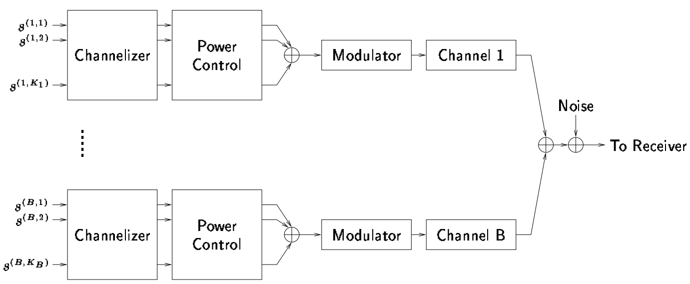

Fig. 1. IS–95 Downlink System Model

tion discrimination and performs baseband filtering and RF conversion. The PN-code has elements from $\{1+j, 1-j, -1+j, -1-j\}$ and has a period of 2^{15} chips. Each base station uses the same PN-code but is distinguished by a unique, fixed phase shift. Baseband filtering is specified by a FIR model in the IS–95 standard.

- Channel Noise: Modeled as an additive, white, complex Gaussian random process $w(t)$ where $E(w(t)) = 0$ and $E(\mathrm{Re}(w(t))^2) = E(\mathrm{Im}(w(t))^2) = 1/2$. The real and imaginary parts are uncorrelated and also assumed to be independent of all user transmissions.

Before we develop the IS–95 downlink mathematical model, we wish to establish the following notation. The superscript form $x^{(b,k)}$ will only be used with scalar quantities and denotes a variable corresponding to the b^{th} base station's k^{th} user. The superscript $\mathbf{x}^{[b]}$ will only be used with vector quantities or diagonal matrices and denotes a variable corresponding to all users from the b^{th} base station at all symbol indices. The notation $\mathbf{x}_\ell^{[b]}$ will also only be used with vector quantities or diagonal matrices and denotes a variable corresponding to all users from the b^{th} base station at the ℓ^{th} symbol index. The superscripts $\mathbf{x}^\top$, $\mathbf{x}^*$ and $\mathbf{x}^H$ denote transpose, complex conjugate, and complex conjugate transpose, respectively. Subscripts will consistently denote the symbol index and may be used with scalar and vector variables.

Assuming the propagation channels are approximately single-path, the $(b,k)^{th}$ user's amplitude and phase adjusted signature waveform at symbol index ℓ may be represented as $e^{j\phi_b} a_\ell^{(b,k)} c_\ell^{(b,k)}(t-\tau_b)$ where ϕ_b is the phase of the transmission from the b^{th} base station, $a_\ell^{(b,k)}$ is the user's positive real amplitude, and $c_\ell^{(b,k)}(t-\tau_b)$ is the normalized[2] signature waveform that includes the effects of the combined channelization code and PN-code as well as the baseband pulse shaping and transmission/propagation delay. The baseband signal observed at the receiver may then be written as

$$r(t) = \sum_{b=1}^{B} e^{j\phi_b} \sum_{\ell=-L}^{L} \sum_{k=1}^{K_b} s_\ell^{(b,k)} a_\ell^{(b,k)} c_\ell^{(b,k)}(t-\ell T-\tau_b) + \sigma w(t)$$

[2]By normalized we mean that $\int |c_\ell^{(b,k)}(t)|^2\, dt = 1$.

where $s_\ell^{(b,k)}$ is the $(b,k)^{th}$ user's binary symbol transmitted at symbol index ℓ. Note that in general $c_\ell^{(b,k)}(t) \neq c_m^{(b,k)}(t)$ for $\ell \neq m$ since the PN-code changes at each symbol interval.

We define an equivalent matrix expression for $r(t)$ as follows. Define the $K(2L+1)$-vector of transmitted symbols as

$$\begin{aligned} \mathbf{s} &= [\mathbf{s}^{\top[1]}, \ldots, \mathbf{s}^{\top[B]}]^\top \text{ where} \\ \mathbf{s}^{[b]} &= [\mathbf{s}_{-L}^{\top[b]}, \ldots, \mathbf{s}_L^{\top[b]}]^\top \text{ and} \\ \mathbf{s}_\ell^{[b]} &= [s_\ell^{(b,1)}, \ldots, s_\ell^{(b,K_b)}]^\top. \end{aligned}$$

Similarly, define the $K(2L+1)$-vector of signature waveforms as

$$\begin{aligned} \mathbf{c}(t) &= [\mathbf{c}^{\top[1]}(t), \ldots, \mathbf{c}^{\top[B]}(t)]^\top \text{ where} \\ \mathbf{c}^{[b]}(t) &= [\mathbf{c}_{-L}^{\top[b]}(t), \ldots, \mathbf{c}_L^{\top[b]}(t)]^\top \text{ and} \\ \mathbf{c}_\ell^{[b]}(t) &= [c_\ell^{(b,1)}(t-\ell T-\tau_b), \ldots, c_\ell^{(b,K_b)}(t-\ell T-\tau_b)]^\top. \end{aligned}$$

Denote $\mathbf{a}$ as the $K(2L+1)$-vector of amplitudes defined in the same manner and let $\mathbf{A} = \mathrm{diag}(\mathbf{a})$ represent the $K(2L+1) \times K(2L+1)$ diagonal amplitude matrix. Finally, let $\mathbf{\Phi}$ be a diagonal matrix of transmission phases with order corresponding to $\mathbf{A}$. Then we can write the continuous time observation compactly as

$$r(t) = \mathbf{c}^\top(t)\mathbf{\Phi}\mathbf{A}\mathbf{s} + \sigma w(t).$$

III. Optimum Detector

In this section we review optimum (joint maximum likelihood) detection in the context of our IS–95 downlink system model. In a single-cell scenario where a receiver observes the transmission of K synchronous, orthogonal signals in the presence of independent AWGN, it is easy to show that the optimum detector is equivalent to the conventional single user matched filter detector. However, when additional cells are considered, the receiver now observes nonorthogonal cochannel interference from the other cells and the optimum detector is more complicated.

The optimum detector requires that the eavesdropper must have perfect knowledge of all transmission phases and delays (ϕ_b and τ_b respectively) as well as the users' signature waveforms ($c_\ell^{(b,k)}(t)$) and amplitudes ($a_\ell^{(b,k)}$). These assumptions are not unreasonable in the IS–95 downlink since the IS–95 standard requires each base station to transmit a pilot channel for straightforward estimation of ϕ_b and τ_b with arbitrary accuracy. The pilot channel also provides the receiver with the phase of the periodic PN-code hence it is straightforward to determine which users are active in each cell and construct the set of $c_\ell^{(b,k)}(t)$ for these users. Finally, although amplitude estimation is not as straightforward as estimation of the other parameters, we will assume the amplitude estimates are perfect in the following analytical development.

Let $\mathcal{I}$ represent a compact interval containing the support of $r(t)$ and let $\mathcal{U}$ represent the set of cardinality $2^{K(2L+1)}$ containing all admissible binary symbol vectors. Then the decision rule for jointly optimum estimates [2] is given by

$$\hat{\mathbf{s}} = \arg\max_{\mathbf{u}\in\mathcal{U}} \exp\left(-\frac{1}{\sigma^2}\int_{\mathcal{I}} |r(t) - \mathbf{c}^\top(t)\mathbf{\Phi}\mathbf{A}\mathbf{u}|^2 dt\right).$$

Manipulation of the term inside the exponent yields the familiar expression for optimum decisions

$$\hat{\mathbf{s}} = \arg\max_{\mathbf{u}\in\mathcal{U}} \underbrace{2\mathrm{Re}(\mathbf{u}^\top\mathbf{A}\mathbf{\Phi}^H\mathbf{y}) - \mathbf{u}^\top\mathbf{A}\mathbf{\Phi}^H\mathbf{R}\mathbf{\Phi}\mathbf{A}\mathbf{u}}_{\Omega(\mathbf{u})}$$

where $\mathbf{y} = \int_{\mathcal{I}} \mathbf{c}^*(t)r(t)\,dt$ represents the $K(2L+1)$-vector of matched filter outputs and $\mathbf{R} = \int_{\mathcal{I}} \mathbf{c}^*(t)\mathbf{c}^\top(t)\,dt$ represents the matrix of signature cross correlations. The brute-force solution to this problem requires the evaluation of $2^{K(2L+1)}$ different hypotheses to find the maximum. Several authors have noted that $\mathbf{R}$ exhibits a banded structure and have used this fact to achieve complexity reduction using Viterbi-style dynamic programming algorithms [2]. Although a good idea in practice, we will not consider Viterbi-style dynamic programming algorithms in this paper in order to clarify the development of the IS–95 structure based complexity reduction. The reduced complexity optimum detector developed in the next section does not prevent the use of Viterbi-style dynamic programming algorithms and both ideas can be combined to achieve even greater complexity reduction.

IV. Reduced Complexity Optimum Detector

In this section we exploit the structure of the IS–95 downlink in order to propose an *optimum* detector requiring significantly less complexity than the brute-force approach. The intuitive idea behind the reduced complexity optimum detector is to use the fact that the K_b synchronous user transmissions from base station b are mutually orthogonal at every symbol index. This will allow us to "decouple" the decisions of one base station's users to achieve the desired complexity reduction while retaining optimality.

The cross correlation matrix $\mathbf{R}$ has dimensions $K(2L+1) \times K(2L+1)$ and exhibits the structure

$$\mathbf{R} = \begin{bmatrix} \mathbf{R}^{[1,1]} & \dots & \mathbf{R}^{[1,B]} \\ \vdots & \ddots & \vdots \\ \mathbf{R}^{[B,1]} & \dots & \mathbf{R}^{[B,B]} \end{bmatrix}$$

where the superscript $\mathbf{X}^{[b,b']}$ denotes a matrix quantity of dimension $K_b(2L+1) \times K_{b'}(2L+1)$ constructed from the outer product of vectors corresponding to the users of base stations b and b'. The submatrices $\mathbf{R}^{[b,b']}$ have the structure

$$\mathbf{R}^{(b,b')} = \begin{bmatrix} \mathbf{R}^{[b,b']}_{-L,-L} & \dots & \mathbf{R}^{[b,b']}_{-L,L} \\ \vdots & \ddots & \vdots \\ \mathbf{R}^{[b,b']}_{L,-L} & \dots & \mathbf{R}^{[b,b']}_{L,L} \end{bmatrix}$$

where

$$\mathbf{R}^{[b,b']}_{\ell,\ell'} = \int_{\mathcal{I}} \mathbf{c}^{*[b]}_{\ell}(t)\mathbf{c}^{\top[b']}_{\ell'}(t)\,dt = \mathbf{R}^{H[b',b]}_{\ell',\ell}.$$

The IS–95 downlink cross correlation matrix exhibits two special properties that lead to the reduced complexity optimum detector:

- The group-orthonormality of the signature sequences transmitted by each base station implies that $\mathbf{R}^{[b,b]}_{\ell,\ell} = \mathbf{I}$.
- Our single-path channel assumption and the fact that the IS–95 pulse shaping filters do not create significant intersymbol interference imply that $\mathbf{R}^{[b,b]}_{\ell,\ell'} = \mathbf{0}$ for $\ell \neq \ell'$.

The combination of these two properties implies that $\mathbf{R}^{[b,b]} = \mathbf{I}$ for $b = 1, \dots, B$. Let $\mathbf{X} = \mathbf{A}\mathbf{\Phi}^H\mathbf{R}\mathbf{\Phi}\mathbf{A}$ and note that since $\mathbf{R}$ is a Hermitian matrix then $\mathbf{X}$ is also Hermitian. Moreover, since $\mathbf{\Phi}$ and $\mathbf{A}$ are diagonal, $\mathbf{X}$ shares the same IS–95 structure properties as $\mathbf{R}$ except that $\mathbf{X}^{[b,b]} = (\mathbf{A}^{[b,b]})^2$. It turns out that this difference will not matter in the maximization of $\Omega(\mathbf{u})$. Using our previously developed notation, we can write

$$\Omega(\mathbf{u}) \quad = \quad 2\mathrm{Re}(\mathbf{u}^\top\mathbf{A}\mathbf{\Phi}^H\mathbf{y}) - \mathbf{u}^\top\mathbf{X}\mathbf{u}. \tag{1}$$

The quadratic term may be rewritten as

$$\mathbf{u}^\top\mathbf{X}\mathbf{u} = \sum_{b=1}^{B}\sum_{b'=-1}^{B} \mathbf{u}^{\top[b]}\mathbf{X}^{[b,b']}\mathbf{u}^{[b']}.$$

The binary nature of $\mathbf{u}$ and the fact that $\mathbf{X}^{[b,b]}$ is diagonal implies that $\mathbf{u}^{\top[b]}\mathbf{X}^{[b,b]}\mathbf{u}^{[b]} = \kappa_b$ where κ_b is a real positive constant that does not depend on $\mathbf{u}$. Denoting $\kappa = \sum_{b=1}^{B}\kappa_b$ then

$$\mathbf{u}^\top\mathbf{X}\mathbf{u} = \kappa + \sum_{b=1}^{B}\sum_{b'\neq b} \mathbf{u}^{\top[b]}\mathbf{X}^{[b,b']}\mathbf{u}^{[b']}.$$

We isolate the symbols from the first[3] base station to write

$$\mathbf{u}^\top\mathbf{X}\mathbf{u} = \kappa + \sum_{b=2}^{B}\mathbf{u}^{\top[b]}\mathbf{X}^{[b,1]}\mathbf{u}^{[1]} + \sum_{b=2}^{B}\mathbf{u}^{\top[1]}\mathbf{X}^{[1,b]}\mathbf{u}^{[b]} + \underbrace{\sum_{b=2}^{B}\sum_{\substack{b'\neq b\\ b'\neq 1}} \mathbf{u}^{\top[b]}\mathbf{X}^{[b,b']}\mathbf{u}^{[b']}}_{G(\bar{\mathbf{u}})}$$

[3] In order to achieve the maximum complexity reduction we assume WLOG that $K_1 = \max_b K_b$.

where $\bar{\mathbf{u}}$ denotes the vector of symbols corresponding to all base stations except $b = 1$. Since $\mathbf{X}$ is a Hermitian matrix then $\mathbf{X}^{H[b,1]} = \mathbf{X}^{[1,b]}$ and we can write

$$\mathbf{u}^\top \mathbf{X}\mathbf{u} = \kappa + \sum_{b=2}^{B} 2\mathrm{Re}\left(\mathbf{u}^{\top[1]}\mathbf{X}^{[1,b]}\mathbf{u}^{[b]}\right) + G(\bar{\mathbf{u}}). \qquad (2)$$

Finally, we combine equations (1) and (2) to write

$$\begin{aligned}\Omega(\mathbf{u}) =& \mathbf{u}^{\top[1]} \underbrace{2\mathrm{Re}\left(\mathbf{A}^{[1]}\mathbf{\Phi}^{H[1]}\mathbf{y}^{[1]} - \sum_{b=2}^{B}\mathbf{X}^{[1,b]}\mathbf{u}^{[b]}\right)}_{F(\bar{\mathbf{u}})} \\ &+ 2\mathrm{Re}(\bar{\mathbf{u}}^\top \bar{\mathbf{A}}\bar{\mathbf{\Phi}}^H \bar{\mathbf{y}}) - G(\bar{\mathbf{u}}) - \kappa.\end{aligned} \qquad (3)$$

Equation (3) leads to the reduced complexity optimum detector algorithm outlined as follows:

1. Construct a set of $2^{(K-K_1)(2L+1)}$ hypotheses for all admissible values of $\bar{\mathbf{u}}$. Perform the following calculations for each hypothesis:
 (a) Under the current hypothesis $\bar{\mathbf{u}}$, (3) is maximized when $\mathbf{u}^{[1]} = \mathrm{sgn}(F(\bar{\mathbf{u}}))$. Let $\mathbf{u} = [\mathbf{u}^{\top[1]}\ \bar{\mathbf{u}}^\top]^\top$.
 (b) Calculate $\Omega(\mathbf{u})$ and store the result.
2. The jointly optimum symbol estimates are then equal to the hypothesis $\mathbf{u}$ that maximizes Ω.

The reduced complexity optimum detector requires the evaluation of $2^{(K-K_1)(2L+1)}$ hypotheses in order to maximize $\Omega(\mathbf{u})$ whereas the brute-force optimum detector requires the evaluation of $2^{K(2L+1)}$ hypotheses. For an eavesdropper in a cell system with two or three base stations, this complexity reduction can be significant.

This prior analysis can also be easily applied to the synchronous CDMA case where sequence detection is not necessary and the brute-force optimum detector requires the evaluation of Ω for 2^K hypotheses. In this case, the reduced complexity optimum detector requires the evaluation of Ω for 2^{K-K_1} hypotheses.

V. Group Parallel Interference Cancellation Detector

Although the IS–95 downlink has a structure which lends itself to reduced complexity optimum detection, it is often the case that the reduced complexity optimum detector is too computationally expensive to implement in real time even with Viterbi-style dynamic programming algorithms. In this section we pose a suboptimum detector that is remarkably similar to the reduced complexity optimum detector in its analytical development but also has connections to Parallel Interference Cancellation (PIC) (originally called multistage detectors in [3] and [4]) and group detection [5]. This detector also uses the IS–95 downlink structure by taking advantage of the orthogonality between user transmissions from the same base station.

Two observations regarding (3) will be useful in the development of the Group Parallel Interference Cancellation (GPIC) detector:

- Suppose the receiver has perfect knowledge of the symbols transmitted from base stations $2, \ldots, B$ such that $\bar{\mathbf{u}} = \bar{\mathbf{s}}$. Then $\hat{\mathbf{s}}^{[1]} = \mathbf{u}^{[1]} = \mathrm{sgn}(F(\bar{\mathbf{u}}))$ is the optimum estimate for the symbols from base station 1. The orthogonality of these users results in single user error probability and the complexity of this receiver is very low.
- Suppose the receiver was given the joint maximum likelihood (JML) estimate for $\bar{\mathbf{s}}$ denoted by $\bar{\mathbf{u}}$. In this case, $\hat{\mathbf{s}}^{[1]} = \mathbf{u}^{[1]} = \mathrm{sgn}(F(\bar{\mathbf{u}}))$ is the JML estimate for the symbols from base station 1. This receiver also has very low complexity.

Unfortunately, realistic receivers do not have access to the actual symbols $\bar{\mathbf{s}}$ or their JML estimates but we are compelled to ask the following question: What if the receiver used some low-complexity estimate $\bar{\mathbf{u}}$ of $\bar{\mathbf{s}}$ and we let $\hat{\mathbf{s}}^{[1]} = \mathbf{u}^{[1]} = \mathrm{sgn}(F(\bar{\mathbf{u}}))$? In the following we consider the lowest complexity estimate of $\bar{\mathbf{s}}$: conventional matched filter estimates where $\bar{\mathbf{u}} = \mathrm{sgn}(\mathrm{Re}(\bar{\mathbf{\Phi}}^H \bar{\mathbf{y}}))$.

Extending this idea to all base stations we can write the following expression for the GPIC detector from (3),

$$\hat{\mathbf{s}}^{[b]}_{\mathsf{GPIC}} = \mathrm{sgn}\left[\mathrm{Re}\left(\mathbf{\Phi}^{H[b]}\left(\mathbf{y}^{[b]} - \sum_{b' \neq b}\mathbf{R}^{[b,b']}\mathbf{\Phi}^{[b']}\mathbf{A}^{[b']}\mathbf{u}^{[b']}\right)\right)\right]$$

where $\mathbf{u}^{[b']} = \mathrm{sgn}(\mathrm{Re}(\bar{\mathbf{\Phi}}^{H[b']}\mathbf{y}^{[b']}))$, any positive real terms that do not affect the sign operation have been factored out, and $\mathbf{X}$ has been replaced by its constituents. It is evident from this expression that the GPIC receiver is actually performing group parallel interference cancellation by subtracting the estimated cochannel interference $b' \neq b$ from the matched filter inputs corresponding to the users in cell b. Some algebraic manipulation yields a simple expression for the GPIC receiver

$$\hat{\mathbf{s}}_{\mathsf{GPIC}} = \mathrm{sgn}\left[\mathrm{Re}\left(\mathbf{\Phi}^H\mathbf{y} + \left(\mathbf{I} - \mathbf{\Phi}^H\mathbf{R}\mathbf{\Phi}\right)\mathbf{A}\mathbf{u}\right)\right].$$

We note that although it is certainly possible to perform GPIC detection in batch where all $K(2L+1)$ symbols are first estimated with the conventional matched filter detector and stored prior to calculation of the GPIC symbol estimates, it is also possible to implement the GPIC receiver with detection delay proportional to K. This feature is in contrast to the previously considered optimum detectors where detection cannot occur until all of $r(t)$ is observed.

VI. Simulation Results

In this section we compare the performance of the GPIC detector to the optimum detector and conventional matched filter detector via simulation. The simulation parameters were $B = 2$ base stations, $K_1 = 2$ and $K_2 = 2$

users in each cell, and 5 bits in each user's transmission ($L = 2$). The received phases ϕ_b and propagation delays τ_b were assumed to be random and uniformly distributed on the intervals $[0, 2\pi)$ and $[0, T)$ respectively. Phases and delays were assumed to be time invariant over the 5-bit transmissions.

The user amplitudes are generated using a log-distance path loss model where the ratio of received power to transmitted power is given by $1/d^{2\alpha}$ where d is the distance between the transmitter and receiver and 2α is the path loss exponent. To simplify matters, we also assume that each base station is centrally located within a unit radius circular cell and the user locations are uniformly distributed within the cell. We also assume that perfect power control is maintained between the base station and each user in its cell such that each user receives their transmission (after path losses) at the same power. Under these assumptions it can be shown that the pdf of the eavesdropper received power relative to power received by the mobile is given by

$$f_\Psi(x) = \begin{cases} \alpha^{-1}\kappa_e^2 x^{(1-\alpha)/\alpha} & x \in [0, \kappa_e^{-2\alpha}], \\ 0 & \text{otherwise} \end{cases}$$

where κ_e is the eavesdropper's distance from the base station in units of cell radii. Note that the received power distribution for the uplink was derived in [6] using similar assumptions. The amplitudes were assumed time invariant over the 5-bit transmissions.

Figure 2 shows the bit error rates of the conventional matched filter, optimum, and GPIC detectors averaged over the users in the first cell. The results were averaged over 5000 Monte Carlo runs where each run generated new realizations of the random delays, phases, amplitudes, PN-codes, transmitted symbols, and channel noise. The single user error probability (averaged over the random amplitude realizations) was 10^{-3}. In this simulation, the eavesdropper was located at the edge of first cell such that $\kappa_{e_1} = 1$ but the eavesdropper's distance from the second base station was varied over the range $\kappa_{e_2} \in [0.5, 2]$.

As expected, the conventional matched filter detector performs poorly in the presence of high power interference (i.e., when κ_{e_2} is small). The GPIC detector does not suffer from this problem and actually exhibits performance indistinguishable from the optimum detector in this example. This simulation suggests that the GPIC detector may offer near-optimum performance over a wide range of cochannel interference powers with little added complexity over the conventional matched filter detector. The GPIC detector also appears to offer significant advantages over the conventional matched filter detector when the eavesdropper is centrally located between the base stations ($\kappa_{e_2} = 1$) implying that GPIC might also offer improved performance for IS–95 mobile receivers located at a point equidistant between two base stations.

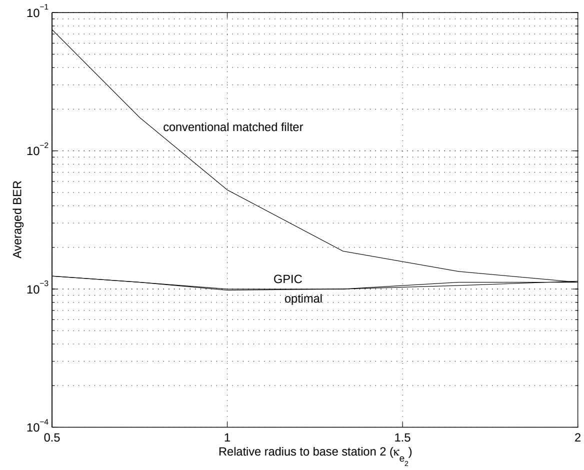

Fig. 2. Averaged bit error rates for users in cell 1. The eavesdropper is positioned at $\kappa_{e_1} = 1$ and several values of κ_{e_2}.

VII. Conclusions

In this paper we considered the application of two nonlinear multiuser detection techniques for IS–95 downlink eavesdropping. We used the group-orthogonal structure of the IS–95 downlink to develop a reduced complexity optimum detector with exponentially lower complexity than the brute-force optimum detector. Examination of the properties of the reduced complexity optimum detector led us to develop the suboptimum GPIC detector. The GPIC detector has very low complexity and does not require any form of subspace tracking, matrix inversions, or exhaustive searches for global maxima. Simulations suggest that the GPIC detector offers the greatest performance improvements in severe cochannel interference environments but may also offer near-optimum performance for IS–95 downlink eavesdropping over a wide range of cochannel interference powers.

References

[1] Telecommunications Industry Association, *Mobile Station – Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular Systems IS–95A*. Washington, DC: TIA/EIA, 1995.

[2] S. Verdú, *Multiuser Detection*. Melbourne, Austrialia: Cambridge University Press, 1998.

[3] M. Varanasi and B. Aazhang, "Multistage detection in asynchronous code-division multiple-access communications," *IEEE Transactions on Communications*, vol. 38, pp. 509–19, April 1990.

[4] M. Varanasi and B. Aazhang, "Near-optimum detection in synchronous code-division multiple-access systems," *IEEE Transactions on Communications*, vol. 39, pp. 725–36, May 1991.

[5] M. Varanasi, "Group detection for synchronous gaussian code-division multiple-access channels," *IEEE Transactions on Information Theory*, vol. 41, pp. 1083–96, July 1995.

[6] A. McKellips and S. Verdú, "Eavesdropping syndicates in cellular communications," in *1998 IEEE 48th Vehicular Technology Conference*, vol. 1, (Ottowa, Canada), pp. 318–22, May 18-21 1998.