Subspace-Based Active User Identification for a Collision-Free Slotted Ad Hoc Network

Darryl Dexu Lin, *Student Member, IEEE,* and Teng Joon Lim, *Senior Member, IEEE*

***Abstract*—We propose a novel spreading code scheme, transmitter–receiver-based code, for wireless ad hoc networks. The design facilitates collision resolution using multiuser detection at each node, and is more bandwidth efficient than creating orthogonal channels in time or frequency. A subspace-based receiver structure is introduced, which identifies users of interest, or "active" users, with minimal prior information on the spreading code ensemble. A subspace-based blind multiuser detector can then be implemented to suppress multiaccess interference. The performance of the proposed active user identifier is studied by investigating its false alarm rate P_f and miss rate P_m. Tradeoffs between P_f and P_m are discussed, and a graphical method to determine the threshold value d_{th} of the decision statistic used in discriminating between active and inactive channels is introduced.**

***Index Terms*—Ad hoc networks, code-division multiple access (CDMA), collision resolution, multiuser detection, subspace identification.**

I. Introduction

In packet-oriented, random-access ad hoc networks, packet collision is an important problem to address. Conventionally, when a collision occurs, the collided packets are discarded and later retransmitted. However, retransmissions have the potential to create further collisions, and thus, severely penalize the throughput performance, even at relatively light traffic loads. Effective collision resolution is, therefore, an important system design issue.

Current collision-resolution research in random-access, slotted wireless systems [1] involves techniques at the protocol level, modulation level [2], and signal processing level [1], [3], [4]. Protocol-level collision resolution concentrates on avoiding collisions before they take place, and in scheduling retransmissions after a collision is detected. However, this implies that only one packet can access the channel in a time slot and results in low maximum throughput. Signal-processing-level collision resolution usually requires a large amount of overhead, such as embedding known symbols in the transmitted data packets. It also tends to be very computationally expensive when applied to an uncoordinated system. Modulation-level collision resolution, on the other hand, is much more versatile and attractive. It enables multipacket reception in a well-designed system, as we will demonstrate in this paper.

Modulation-level collision resolution is achieved with the help of channelization. Channelization is traditionally achieved by transmitting signals in orthogonal channels. The most common channelization techniques include frequency-division multiple access (FDMA), time-division multiple access (TDMA), and code-division multiple access (CDMA). Given a central controller, such as a cellular base station assigning orthogonal channels to individual users, packet collision will not arise. However, applying the same concept to a fully connected wireless network with M nodes requires $O(M^2)$ orthogonal channels, one for each possible transmitter–receiver pair, in order to totally solve the packet-collision problem via channelization. This translates into a bandwidth expansion factor of $O(M^2)$, whether using TDMA, FDMA, or CDMA, and represents a great waste of bandwidth, because when the network carries bursty traffic, only a small percentage of these channels are occupied at any given time.

However, with a carefully tailored spreading code design, such as the one to be presented in Section II, CDMA allows us to have a small bandwidth expansion factor $N \ll M^2$ which is designed for the average network traffic, instead of the maximum number of possible connections. In the proposed design, the value of N must not be smaller than M, but can otherwise be chosen as spectrally efficient as desired under some quality of service (QoS) constraints, such as the probability of missing a transmitted packet P_m or the probability of flagging an inactive channel as active P_f.

The coupling of this spectrally efficient CDMA modulation scheme and random access comes with a price, however, as packets are no longer transmitted using orthogonal channels. Fortunately, multiuser detection enables the reliable separation of nonorthogonal signal streams. In particular, certain multiuser detection schemes [5], [6] are "blind," in the sense that they do not require knowledge of the interfering code channels at the receiver. Once the desired spreading code is known, in our case, through active user identification, multiaccess interference (MAI) can be suppressed using a blind multiuser detector. This setup consisting of a subspace-based active user identifier, followed by a subspace-based blind multiuser detector, is what we propose in our "collision-free" CDMA ad hoc network design. Unlike the protocol-level collision resolution method, it allows for multipacket reception; unlike previous signal-processing-level techniques, it is not fully blind and is therefore less complex to implement. In fact, because both of the main modules in the receiver are based on subspace identification, a

Paper approved by X. Wang, the Editor for Equalization of the IEEE Communications Society. Manuscript received February 28, 2003; revised August 27, 2003. This work was supported in part by a grant from Bell Canada University Laboratories and in part by an Ontario Graduate Scholarship. This paper was presented in part at the IEEE International Symposium on Information Theory, Yokohama, Japan, July 2003.

The authors are with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: linde@comm.utoronto.ca; limtj@comm.utoronto.ca).

Digital Object Identifier 10.1109/TCOMM.2004.826415

lot of necessary information is common, and this reduces complexity.

The rest of the paper is organized as follows. Section II introduces a new spreading code scheme. Section III explains the signal model used in this paper. Section IV addresses the issue of active user identification by applying a multiple signal classification (MUSIC)-based technique. Section V presents the performance analysis of this active user-identification technique. Section VI includes simulations that compare our theoretical analysis with experimental data. Finally, Section VII contains the conclusions.

II. Spreading Code Scheme

In this section, we will introduce a spreading scheme for ad hoc networks that is both immune to packet collisions and creates less MAI than competing schemes. The proposed scheme is based on the following packet radio spread-spectrum techniques [2].

1) **Transmitter-Based Code:** A unique spreading code is allocated to each terminal. Each transmitter transmits data using its own code. If the system is synchronous and these codes are orthogonal to each other, there will be no collision.
2) **Receiver-Based Code:** A unique spreading code is allocated to each terminal. The transmitter transmits data using the destination's code. The receiver does not need any addressing information in the received data packet, because the knowledge of its own spreading code is sufficient to decode messages directed to it.

The practical issues with the above schemes are as follows. For the transmitter-based code, a heavy decoding burden is placed on the receiver, because at the beginning of each packet, it needs to retrieve the destination address information in the header of all concurrently transmitted packets to determine if it is one of the intended receivers. For the receiver-based code, unresolvable collisions would occur if two users transmit packets to the same user in the same packet slot.

In light of these concerns, we propose a novel spreading code scheme, transmitter–receiver-based code (TRBC), for wireless ad hoc networks. As its name implies, TRBC is based on the identities of both the originating and destination nodes.

TRBC: Each node in the network is assigned two unique binary spreading codes $\mathbf{w}_m$ and $\mathbf{p}_m$ $(m = 1, \dots, M)$ of processing gain N. Suppose node i needs to transmit a packet to node j, the spreading code used by node i is

$$\mathbf{s}_{i,j} = \mathbf{w}_i \circ \mathbf{p}_j \tag{1}$$

where $\circ$ denotes the Hadamard (or Schur) product of two matrices, i.e., $\mathbf{s}_{i,j}$ is the element-wise product of vectors $\mathbf{w}_i$ and $\mathbf{p}_j$.

Notice that the transmitter-based code and receiver-based code are two special cases of the proposed TRBC code scheme. By setting $\mathbf{p}_m$ or $\mathbf{w}_m$ to an all-one vector, the TRBC code reduces to the transmitter-based or receiver-based code, respectively. The optimal code-design scheme for $\mathbf{w}_m$ and $\mathbf{p}_m$ is an open question, which will not be discussed in this paper. For simplicity, we will choose $\mathbf{w}_m$ to be a set of orthogonal codes, a subset of a group of Walsh codes of length N, for instance. In addition, we will make $\mathbf{p}_m$ a set of pseudonoise (PN) codes of length N. Specifically, $\mathbf{w}_m$ is used as the source identifier, and $\mathbf{p}_m$ as the destination identifier. The advantage of such a choice is twofold. First, $\mathbf{w}_m$ makes the packets transmitted to any given receiver from two or more nodes orthogonal to each other, which renders the joint detection of these packets much simpler. Second, $\mathbf{p}_m$ causes all the spreading codes to appear "random" to each other, which reduces the chance of strong interference between highly correlated spreading codes.

To demonstrate the first advantage of TRBC mentioned above, we rewrite (1) as $\mathbf{s}_{i,j} = \mathbf{P}_j \mathbf{w}_i$, where $\mathbf{P}_j = \mathrm{diag}(\mathbf{p}_j)$ (i.e., $\mathbf{P}_j$ is a square diagonal matrix formed by elements of vector $\mathbf{p}_j$). So we have, for $j \neq k$

$$\begin{aligned} \mathbf{s}_{i,j}^T \mathbf{s}_{k,j} &= \mathbf{w}_i^T \mathbf{P}_j \mathbf{P}_j \mathbf{w}_k \\ &= \mathbf{w}_i^T \mathbf{w}_k \\ &= 0. \end{aligned} \tag{2}$$

This implies there is no interference between desired packets at any receiver. In the extreme case, if all packets are destined for one receiver, a cellular-type network topology, for example, that receiver sees an MAI-free channel and can use a simple matched-filter bank to detect different packets. All other receivers see only noise. On the other hand, if some packets are destined for a receiver and others are not, that receiver sees an MAI channel. This motivates the use of a multiuser detector to recover the packets of interest among unknown interferers. The orthogonality between the desired packets allows us to use a group multiuser detector with reduced complexity [6], in which the "intracell" interference is zero.

The spreading gain N in a CDMA ad hoc network is closely tied to the average network traffic, as N is roughly the upper bound of the multiuser receiver decoding capability. We will see in Section V that the value of N also influences the total number of concurrent packets that the active-user identifier can accommodate. These issues imply that a larger N results in a better system performance, both in terms of number of allowable users and error rate. But on the other hand, the bandwidth occupied by the system increases as N increases. Therefore, a suitable N should be as small as possible to conserve bandwidth, while at the same time, large enough to ensure that typical network traffic (indicated by number of packets per packet slot) is within the capability of the multiuser receiver and the active-user identifier.

III. System Model

Consider a synchronous direct-sequence (DS)-CDMA wireless ad hoc network with M users. Each user is free to enter or leave the channel in a random fashion with data transmitted in packets. The system is slotted and the nodes are only allowed to initialize transmission at the beginning of each time slot. We now look at one packet interval over an additive white Gaussian noise (AWGN) channel. The number of packets that are transmitted simultaneously is assumed to be K. The received baseband signal is thus

$$r(t) = \sum_{k=1}^{K} A_k \sum_{i=0}^{L-1} b_k(i) s_k(t - iT) + n(t) \tag{3}$$

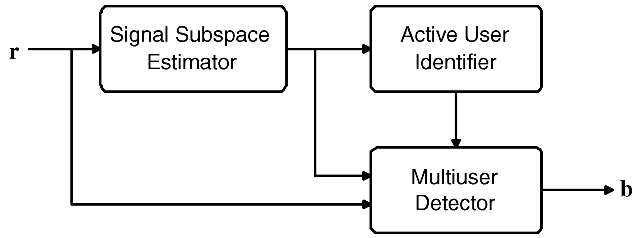

Fig. 1. Proposed receiver structure.

where L is the packet size in symbols ignoring the packet header, T is the symbol duration, $s_k(t)$ is the spreading waveform of the kth packet, A_k is the amplitude of the kth packet, and $b_k(i)$ is the ith symbol transmitted in the kth packet. We assume $n(t)$ to be white Gaussian noise with zero mean and power spectral density $\mathcal{N}_o/2$. It should be noted that k does not correspond to the identity of any node in the network. It is simply a convenient label to differentiate between the K concurrent packets. A more proper set of labels which corresponds to the identities of the transmitters and receivers is shown in (1).

The spreading waveform $s_k(t)$ can be expressed as

$$s_k(t) = \sum_{n=1}^{N} s_k(n)p(t-(n-1)T_c) \tag{4}$$

where $p(t)$ denotes a unit rectangular pulse with chip duration $T_c = T/N$ and $s_k(n)$ is the nth chip of the kth spreading sequence.

By sampling the received signal at chip rate, (3) can be rewritten in the well-known vector form

$$\mathbf{r} = \mathbf{SAb} + \mathbf{n} \tag{5}$$

where $\mathbf{S} = [\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_K]$ is the spreading code matrix consisting of the spreading sequences of the K active packets in the current slot. Also, we have $\mathbf{A} = \mathrm{diag}(A_1, \ldots, A_k)$ and $\mathbf{b} = [b_1, b_2, \ldots, b_K]^T$, which represent the amplitude and transmitted information bits of these packets, respectively. Given that the system is synchronous, we will drop the symbol index i from our notation hereafter.

IV. Subspace-Based Active-User Identification

A. Receiver Structure

As shown in Fig. 1, our proposed multiuser receiver is a combination of two functional modules, namely, the active-user identifier and the multiuser detector. The active-user identifier is designed to identify the spreading codes modulating the packets that the multiuser detector needs to detect. A very important feature of this structure is that the two modules are both subspace based, and hence, are capable of sharing a single subspace estimation unit, leading to some saving of computation resources. Although the optimal joint design of the receiver is an interesting problem, for the purpose of this paper, we will only concentrate on the design and analysis of the active-user identifier.

B. Signal Subspace Estimation

The proposed active-user-identification algorithm is subspace based, and thus requires eigenvalue decomposition (EVD) of the autocovariance matrix of the received vectors. The autocovariance matrix is given by

$$\mathbf{R} = E\{\mathbf{r}\mathbf{r}^T\} = \mathbf{S}\mathbf{A}^2\mathbf{S}^T + \sigma^2\mathbf{I} \tag{6}$$

and is approximated by $\hat{\mathbf{R}} = (J-1)^{-1}\sum_i \mathbf{r}(i)\mathbf{r}^T(i)$ in practice. Since $\mathbf{R}$ is positive definite, we are able to perform EVD as follows:

$$\mathbf{R} = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^T = [\,\mathbf{U}_s \quad \mathbf{U}_n\,]\begin{bmatrix}\boldsymbol{\Lambda}_s & \mathbf{0}\\ \mathbf{0} & \boldsymbol{\Lambda}_n\end{bmatrix}\begin{bmatrix}\mathbf{U}_s^T\\ \mathbf{U}_n^T\end{bmatrix} \tag{7}$$

where $\mathbf{U}_s \in \mathbb{R}^{N\times K}$ contains the signal subspace eigenvectors, and $\mathbf{U}_n \in \mathbb{R}^{N\times(N-K)}$ contains the noise subspace eigenvectors. The diagonal matrix $\boldsymbol{\Lambda}_s$ contains the signal eigenvalues, denoted by $\{\rho_i\}_{i=1}^K$, where K is the rank of the signal subspace. Similarly, the diagonal matrix $\boldsymbol{\Lambda}_n$ contains the noise eigenvalues, denoted by $\{\rho_i\}_{i=K+1}^N$. Without loss of generality, we assume that the eigenvalues are sorted in nonincreasing order $\rho_1 \ge \rho_2 \ge \cdots \ge \rho_K \ge \rho_{K+1} = \rho_{K+2} = \cdots = \rho_N = \sigma^2$.

The separation of the autocovariance matrix into signal and noise components requires knowledge of the rank K of the signal subspace, which is also equal to the number of packets that are concurrently transmitted or, alternatively, the cardinality of $\mathcal{A}$ (the set of all active users). Various rank-estimation techniques have been reported in the literature [7], [8]. In this paper, we shall assume the rank of the signal subspace is always perfectly estimated.

C. Active-User Identification

Wu and Chen [9] suggested a MUSIC-based method for identifying the active users, provided that we know the pool of all possible spreading codes that may be used in transmission. In other words, if we denote the set of all possible spreading codes as $\mathcal{S}$, the identifier is able to find the set of all active users, designated by $\mathcal{A}$.

The scenario in this paper is slightly different. First of all, the set of relevant spreading codes is different for each receiver. We will denote the set of relevant spreading codes for receiver j to be $\mathcal{S}_j$, which has the following properties:

$$\begin{aligned}\mathcal{S} &= \mathcal{S}_1 \cup \mathcal{S}_2 \cup \cdots \cup \mathcal{S}_M\\ \mathcal{S}_a \cap \mathcal{S}_b &= \emptyset \quad (1 \le a, b \le M; a \ne b)\end{aligned} \tag{8}$$

where M is the total number of nodes in the network.

Second, receiver j is not interested in decoding all the active users $(\mathcal{A})$, since some of the packets being transmitted may be communications between two other users k and l, and is picked up only because receiver j is within range of the transmitted signal. The set of active users of interest to receiver j is denoted as $\mathcal{A}_j$, which has the following properties:

$$\begin{aligned}\mathcal{A} &= \mathcal{A}_1 \cup \mathcal{A}_2 \cup \cdots \cup \mathcal{A}_M\\ \mathcal{A}_a \cap \mathcal{A}_b &= \emptyset \quad (1 \le a, b \le M; a \ne b) \qquad (9)\\ \mathcal{A}_j &= \mathcal{A} \cap \mathcal{S}_j \quad (j = 1, \ldots, M). \qquad (10)\end{aligned}$$

The task of the active-user identifier of receiver j, therefore, is to find $\mathcal{A}_j$, i.e., to identify the spreading codes among all active users (denoted by $\mathcal{A}$) that are in $\mathcal{S}_j$. The data-detection

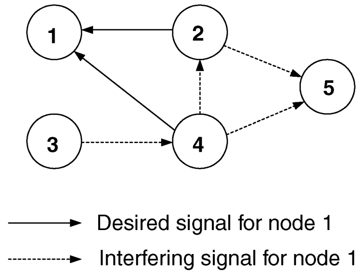

Fig. 2. Five-node network example.

stage that follows will then decode information modulated by the spreading codes in $\mathcal{A}_j$. These spreading codes also act as identity labels for the senders of the information, due to the TRBC code format.

In the simple five-node network example shown in Fig. 2, $\mathcal{A} = \{\mathbf{s}_{2,1}, \mathbf{s}_{2,5}, \mathbf{s}_{3,4}, \mathbf{s}_{4,1}, \mathbf{s}_{4,2}, \mathbf{s}_{4,5}\}$ and $\mathcal{S}_1 = \{\mathbf{s}_{2,1}, \mathbf{s}_{3,1}, \mathbf{s}_{4,1}, \mathbf{s}_{5,1}\}$. Therefore, $\mathcal{A}_1 = \mathcal{A} \cap \mathcal{S}_1 = \{\mathbf{s}_{2,1}, \mathbf{s}_{4,1}\}$. The task of the user identifier in receiver 1 is to detect that users 2 and 4 are transmitting to it.

For receiver j, the MUSIC-based identification method works by projecting all the spreading codes in $\mathcal{S}_j$ onto the estimated signal subspace (which is the space spanned by all spreading codes in $\mathcal{A}$ and is represented by $\mathbf{U}_s$). This approach is supported by the observation $\mathrm{Span}(\mathbf{S}_A) = \mathrm{Span}(\mathbf{U}_s)$, where $\mathbf{S}_A$ is a spreading code matrix formed by all spreading codes in $\mathcal{A}$.

By definition, the set $\mathcal{S}_j$ contains spreading codes $\{\mathbf{s}_{i,j}\}_{i=1;i\neq j}^{M}$, where i represents the sender of the packet and j represents the intended receiver of the packet. Using the MUSIC-based projection method, we obtain a set of identifier outputs for the candidate spreading codes of receiver j

$$d_{i,j} = \|\mathbf{U}_s^T \mathbf{s}_{i,j}\|^2 = \mathbf{s}_{i,j}^T \mathbf{U}_s \mathbf{U}_s^T \mathbf{s}_{i,j}, \quad i = 1, \ldots, M; \quad i \neq j. \tag{11}$$

Ignoring subspace estimation errors, for an active sender i who is transmitting a packet to receiver j, $d_{i,j}$ would have a value of one because $\mathbf{s}_{i,j} \in \mathrm{Span}(\mathbf{U}_s)$. Conversely, for an inactive user, i.e., $\mathbf{s}_{i,j} \notin \mathcal{A}$ but $\mathbf{s}_{i,j} \in \mathcal{S}_j$, the identifier output does not, in general, take on discrete values. Instead, it will be a continuous random variable distributed in (0,1). In this ideal situation, the active and inactive users can be easily separated depending on whether the identifier output is one. However, in practice, due to unavoidable subspace estimation errors, $d_{i,j}$ for an active $\mathbf{s}_{i,j}$ is also a continuous random variable distributed in (0,1). Thus, we need to separate active users from inactive users based on the set of values $\{d_{i,j}\}_{i=1,i\neq j}^{M}$ by setting a threshold value $0 < d_{\mathrm{th}} < 1$ so that $\mathcal{A}_j$ is estimated as

$$\hat{\mathcal{A}}_j = \{\mathbf{s}_{i,j} \in \mathcal{S}_j \mid d_{i,j} \geq d_{\mathrm{th}}\}. \tag{12}$$

The setting of this threshold value is crucial to the performance of the identifier and is strongly dependent upon the distribution of $d_{i,j}$ for both active and inactive users. Wu and Chen [9] studied the effect of finite window size on discrete identifier outputs. A special case of Gold codes is considered, where $d_{i,j}$ only takes on one possible value for inactive users. However, the Gold code set has a very limited population (maximum of N different spreading sequences for a spreading gain of N), which makes it unsuitable to be used in an ad hoc network where a large spreading code population (M^2) is needed. This motivates us to consider a more general case where the codes are randomly selected, and have unit norm. For a random spreading code set of reasonably large size, the distribution of the spreading vectors in N-dimensional space is well approximated by a uniform continuous distribution over the surface of an N-dimensional sphere. (This *continuous approximation* was originally used for the analysis of lattice codes [10].) We use this observation to study the distribution of identifier outputs for both inactive users (hereafter denoted as d_{in} for convenience) and active users (denoted as d_{ac}).

It should be noted that TRBC can be analyzed using the random spreading assumption, because it uses pseudorandom scrambling sequences, and whether a spreading vector is active is a random event. This claim is supported by simulations in Section VI.

V. Performance Analysis of Active-User Identification

A. Mathematical Model

From this section to Section V-D, we investigate the distribution function of d_{in}. The statistics of d_{in} (inactive users), together with the statistics of d_{ac} (active users), determine the best value for the threshold d_{th}, given the constraints on false alarm rate and miss rate.

The eigenmatrix $\mathbf{U}$ of $\mathbf{R}$ spans the N-dimensional vector space, and since $\mathbf{s}_{i,j}$ is unit norm, the vector $\mathbf{x} = \mathbf{U}^T \mathbf{s}_{i,j}$ also has unit norm. The first K components of $\mathbf{x}$, denoted x_k, $k = 1, \ldots, K$, comprise the projection of $\mathbf{s}_{i,j}$ onto the signal subspace. More importantly, our decision statistic $d_{i,j} = \sum_{k=1}^{K} |x_k|^2$. When $\mathbf{s}_{i,j}$ is active, obviously $d_{i,j} = d_{\mathrm{ac}} = 1$, in the absence of subspace estimation errors.

When $\mathbf{s}_{i,j}$ is inactive, $d_{i,j}$ is denoted d_{in} and is a random variable, because now $\mathbf{s}_{i,j}$ has no fixed relationship with $\mathbf{U}_s$. It is clear that the distribution of d_{in} depends on the distribution of $\mathbf{x}$. Since all unitary matrices, such as $\mathbf{U}$, represent rotations, $\mathbf{x}$ is simply the rotation of a random vector that is uniformly distributed on the surface of a unit sphere to another point on that sphere, and must itself be uniformly distributed on the unit N-dimensional sphere.

Hence, the distribution of d_{in} is equivalent to that of

$$\hat{y}_K = \sum_{k=1}^{K} |x_k|^2 \tag{13}$$

given that $\mathbf{x}$ is uniformly distributed on the surface of a unit sphere. To find the distribution of $\hat{y}_K$, we introduce the following lemma.

Lemma 1: The probability density function (pdf) of

$$\hat{y}_K = \sum_{k=1}^{K} x_k^2 \tag{14}$$

when $\mathbf{x} = [x_1, \ldots, x_N]^T$ is uniformly distributed on the surface of an N-dimensional unit sphere, is equivalent to the pdf of

$$y_K = \frac{\sum_{k=1}^{K} x_k^2}{\sum_{k=1}^{N} x_k^2} \tag{15}$$

when $\mathbf{x}$ is uniformly distributed inside the volume of an N-dimensional unit sphere. (Such an $\mathbf{x}$ is called a spherically uniform random vector [11].)

Proof: See Appendix A. ■

For spherically uniform $\mathbf{x}$, the joint pdf of the components of $\mathbf{x}$ is

$$f_{X_1,X_2,\ldots,X_N}(x_1,x_2,\ldots,x_N)=\frac{1}{\mathrm{V_N}},\quad \sum_{i=1}^{N}x_k^2\le 1 \tag{16}$$

where $\mathrm{V_N}$ is the volume of an N-dimensional unit sphere.

The rationale behind such a transformation is the ease of evaluation of a volume integral as compared to a surface integral. The cumulative distribution function (cdf) of y_K can be easily formulated as

$$F_{Y_K}(u)=\int_{\left(\sum_{k=1}^{K}x_k^2/\sum_{k=1}^{N}x_k^2\right)\le u} f_{X_1,X_2,\ldots,X_N} \times(x_1,x_2,\ldots,x_N)dx_1dx_2\cdots dx_N. \tag{17}$$

The evaluation of this integral in Cartesian coordinates is quite cumbersome, thus we shall use polar coordinates.

B. Polar Coordinates in n-Dimensional Space

Polar coordinates (ρ,θ_1) in two-dimensional space are connected with Cartesian coordinates (x_1,x_2) via the relations

$$x_1=\rho\cos\theta_1 \tag{18}$$

$$x_2=\rho\sin\theta_1. \tag{19}$$

The transformation from Cartesian coordinates to polar coordinates can be generalized for n-dimensional space with the following transition formulas [12]–[15]:

$$\begin{aligned}x_1&=\rho\cos\theta_1\\ x_k&=\rho\left[\prod_{i=1}^{k-1}\sin\theta_i\right]\cos\theta_k,\quad k=2,3,\ldots,n-1\\ &\vdots\\ x_n&=\rho\prod_{i=1}^{n-1}\sin\theta_i\end{aligned} \tag{20}$$

$0\le\rho\le R$, $0\le\theta_i<\pi$ $(i=1,\ldots,n-2)$, $0\le\theta_{n-1}<2\pi$. With some straightforward manipulations [12], [13], we obtain the volume element as

$$dx_1\cdots dx_n=\rho^{n-1}\sin^{n-2}\theta_1\sin^{n-3}\theta_2\cdots \sin^2\theta_{n-3}\sin\theta_{n-2}d\theta_1\cdots d\theta_{n-1}d\rho. \tag{21}$$

We denote the interior of an n-dimensional sphere of radius R as $S_n(R)$. The volume of an n-dimensional sphere of radius R can be evaluated as[1]

$$\mathrm{V_n}(R)=\int\cdots\int_{S_n(R)}dx_1\cdots dx_n \tag{22}$$

$$=\int_0^R\int_0^{2\pi}\int_0^{\pi}\cdots\int_0^{\pi}r^{n-1}\sin^{n-2}\theta_1\cdots\sin\theta_{n-2}d\theta_1\cdots d\theta_{n-1}d\rho \tag{23}$$

$$=n^{-1}2^{n-1}R^n\pi a_1a_2\cdots a_{n-2} \tag{24}$$

where $a_i=\int_0^{\pi/2}\sin^i x dx$. a_i can be calculated as in [14] by introducing the following notation:

$$0!!=1,\quad 1!!=1,\quad i!!=i\cdot(i-2)!!\text{ for } i>1. \tag{25}$$

[1]If V_n is used without an argument, it is understood that $R=1$.

Hence

$$a_i=\begin{cases}\frac{(i-1)!!}{i!!}, & \text{if } i \text{ is odd}\\ \frac{(i-1)!!}{i!!}\cdot\frac{\pi}{2}, & \text{if } i \text{ is even.}\end{cases} \tag{26}$$

Consequently

$$\mathrm{V_N}(R)=\frac{2^{\lfloor n+1/2\rfloor}\cdot\pi^{\lfloor n/2\rfloor}}{n!!}R^n. \tag{27}$$

C. d_{in} pdf Approximation for Small K

To derive the pdf for d_{in}, or equivalently y_K, we make use of an inherent connection between Cartesian coordinates and polar coordinates. The angles in polar coordinates can be determined via [12]

$$\cos^2\theta_i=\frac{x_i^2}{\sum_{k=i}^{N}x_k^2},\quad \sin^2\theta_i=\frac{\sum_{k=i+1}^{N}x_k^2}{\sum_{k=i}^{N}x_k^2}. \tag{28}$$

Subsequently, we have

$$\prod_{k=1}^{i}\sin^2\theta_k=\frac{\sum_{k=i+1}^{N}x_k^2}{\sum_{k=1}^{N}x_k^2}. \tag{29}$$

We are, therefore, able to rewrite (17) in polar coordinates using (16), (21), and (29) as

$$\begin{aligned}F_{Y_K}(u)&=\int_{\left(\sum_{k=1}^{K}x_k^2\right)/\left(\sum_{k=1}^{N}x_k^2\right)\le u}f_{X_1,X_2,\ldots,X_N}\times(x_1,x_2,\ldots,x_N)dx_1\cdots dx_N\\ &=\int_{\left(\sum_{k=N-K+1}^{N}x_k^2\right)/\left(\sum_{k=1}^{N}x_k^2\right)\le u}f_{X_1,X_2,\ldots,X_N}\times(x_1,x_2,\ldots,x_N)dx_1\cdots dx_N\\ &=\frac{1}{\mathrm{V_N}}\int_{\prod_{k=1}^{N-K}\sin^2\theta_k\le u}\rho^{N-1}\sin^{N-2}\theta_1\cdots\sin\theta_{N-2}d\theta_1\cdots d\theta_{N-1}d\rho.\end{aligned} \tag{30}$$

Equation (30) is the integral representation of the cdf we intend to derive in polar coordinates. In general, this integral does not have a closed-form solution, but for $K=1$, we can use (28) to simplify the region of integration substantially. Now the cdf becomes

$$\begin{aligned}F_{Y_1}(u)&=\frac{1}{\mathrm{V_N}}\int_{\cos^2\theta_1\le u}\rho^{N-1}\sin^{N-2}\theta_1\cdots\sin\theta_{N-2}d\theta_1\cdots d\theta_{N-1}d\rho\\ &=\frac{1}{\mathrm{V_N}}\int_0^R\int_0^{2\pi}\int_0^{\pi}\cdots\int_{\arccos(\sqrt{u})}^{\pi-\arccos(\sqrt{u})}\times\rho^{N-1}\sin^{N-2}\theta_1\cdots\sin\theta_{N-2}d\theta_1\cdots d\theta_{N-1}d\rho\\ &=\frac{N^{-1}2^{N-1}R^N\pi a_1a_2\cdots b_{N-2}}{\mathrm{V_N}}\\ &=\frac{N^{-1}2^{N-1}R^N\pi a_1a_2\cdots b_{N-2}}{N^{-1}2^{N-1}R^N\pi a_1a_2\cdots a_{N-2}}\\ &=\frac{b_{N-2}}{a_{N-2}}\end{aligned} \tag{31}$$

where $b_i = \int_{\arccos(\sqrt{u})}^{\pi/2} \sin^i x dx$. We already calculated a_i in (26) and will do the same for b_i

$$\begin{aligned} b_i &= \int_{\arccos(\sqrt{u})}^{\pi/2} \sin^i x dx \\ &= \left[-\frac{\sin^{i-1} x \cos x}{i} \right]_{\arccos(\sqrt{u})}^{\pi/2} \\ &\quad + \frac{i-1}{i} \int \arccos(u)^{\pi/2} \sin^{i-2} x dx \\ &= \frac{(\sqrt{1-u})^{i-1}\sqrt{u}}{i} + \frac{i-1}{i}\frac{(\sqrt{1-u})^{i-3}\sqrt{u}}{i-2} \\ &\quad + \frac{i-1}{i}\frac{i-3}{i-2}\frac{(\sqrt{1-u})^{i-5}\sqrt{u}}{i-4} + \cdots. \end{aligned} \tag{32}$$

After simplifying the finite series, we obtain a general representation of b_i as shown in (33) at the bottom of the page.

Note that we have relaxed the definition of the notation !! in (25) to allow $-1!! = 1$ so as to make the expression more compact. The cdf can thus be expressed as shown in (34) at the bottom of the page.

Differentiating $F_{Y_1}(u)$, we have the pdf of y_1 as shown in (35) at the bottom of the page.

The above equation provides the theoretical exact pdf for the case of one active user. Interestingly, it so happens that the one active user case cannot adopt this approach, because d_{in} is a discrete random variable, rather than a continuous one. It is only when K is larger that d_{in} becomes essentially a continuous random variable. In fact, for the case of $K = 1$, the analysis could have been a lot simpler as d_{in} only takes on discrete values $0, (2/N)^2, \ldots, (N-4/N)^2, (N-2/N)^2$ for even N, and $(1/N)^2, (3/N)^2 \ldots, (N-4/N)^2, (N-2/N)^2$ for odd N.

However, the exact pdf (35) of y_1 provides a foundation for approximating the pdf of y_K for larger values of K. For large N and relatively small K, the pdf of y_K can be approximated as

$$f_{Y_K}(u) \approx \begin{cases} \overbrace{f_{Y_1}(u) * f_{Y_1}(u) * \cdots * f_{Y_1}(u)}^{K}, & (0 \le u \le 1) \\ 0, & (u < 0 \text{ or } u > 1). \end{cases} \tag{36}$$

This approximation is valid for large N and small K because the random variables $x_1^2/\sum_{k=1}^N x_k^2, x_2^2/\sum_{k=1}^N x_k^2, \ldots, x_K^2/\sum_{k=1}^N x_k^2$ are only loosely correlated in such cases, and thus can be approximated as independent random variables. In brief, y_K can be approximated as the K-fold convolution of the pdf of y_1, $f_{Y_1}(y_1)$.

D. d_{in} *pdf Approximation for Large* N

For large N, there is an alternative way to approximate the pdf of d_{in}, which is obtained by observing the following property about (15).

Lemma 2: In the limit as $N \to \infty$, when $\mathbf{x} = [x_1, x_2, \ldots, x_N]^T$ is spherically uniform within the unit sphere, $x_1, x_2, \ldots, x_N$ are independent and identically distributed (i.i.d.) random variables with Gaussian density

$$f_X(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-x^2/2\sigma^2} \tag{37}$$

where $\sigma^2 = 1/(N+2)$.

Proof: See Appendix B. ■

This proof was presented in [11] and is provided here for completeness. A different proof is independently shown in [10] by a conditional-entropy argument.

Based on *Lemma 2*, we are able to derive a closed-form pdf expression for y_K given the following properties [16, pp. 101-102], [17].

$$b_i = \begin{cases} \frac{(i-1)!!}{i!!} \sum_{m=1}^{(i+1/2)} \frac{(i-2m)!!}{(i-2m+1)!!} (1-u)^{(i-2m+1/2)} u^{1/2}, & i \text{ odd} \\ \frac{(i-1)!!}{i!!} \sum_{m=1}^{i/2} \frac{(i-2m)!!}{(i-2m+1)!!} (1-u)^{(i-2m+1/2)} u^{1/2} + \frac{(i-1)!!}{i!!} \left(\frac{\pi}{2} - \arccos(\sqrt{u}) \right), & i \text{ even} \end{cases} \tag{33}$$

$$F_{Y_1}(u) = \frac{b_{N-2}}{a_{N-2}} = \begin{cases} \sum_{m=1}^{(N-1/2)} \frac{(N-2m-2)!!}{(N-2m-1)!!} (1-u)^{(N-2m-1/2)} u^{1/2}, & N \text{ odd} \\ \frac{2}{\pi} \sum_{m=1}^{(N/2-1)} \frac{(N-2m-2)!!}{(N-2m-1)!!} (1-u)^{(N-2m-1/2)} u^{1/2} + 1 - \frac{2}{\pi} \arccos(\sqrt{u}), & N \text{ even} \end{cases} \tag{34}$$

$$f_{Y_1}(u) = \begin{cases} \sum_{m=1}^{(N-1/2)} \frac{(N-2m-2)!!}{(N-2m-1)!!} \frac{1-u(N-2m)}{2} (1-u)^{(N-2m-3/2)} u^{-1/2}, & N \text{ odd} \\ \frac{2}{\pi} \sum_{m=1}^{(N/2)-1} \frac{(N-2m-2)!!}{(N-2m-1)!!} \frac{1-u(N-2m)}{\pi} (1-u)^{(N-2m-3/2)} u^{-1/2} + \frac{1}{\pi}(1-u)^{-1/2} u^{-1/2}, & N \text{ even} \end{cases} \tag{35}$$

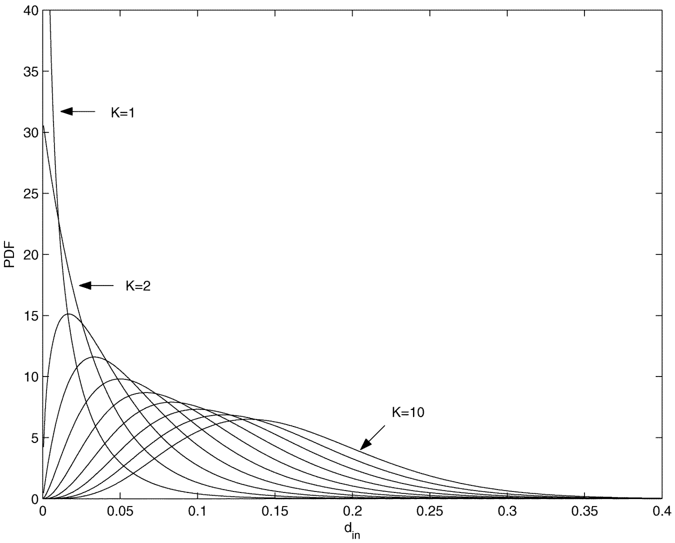

Fig. 3. Beta approximation for the pdf of d_{in} ($N = 64, K = 1$–10).

- If $X_1, X_2, \ldots, X_N$ are i.i.d. Gaussian random variables with zero mean, then $(X_1/\sigma)^2$, $(X_2/\sigma)^2, \ldots, (X_N/\sigma)^2$ are χ^2 random variables with one degree of freedom. And $\sum_{i=1}^{n}(X_i/\sigma)^2$ is a χ^2 random variable with n degrees of freedom.
- A χ^2 random variable with n degrees of freedom is a special case of a Gamma random variable

$$f_X(x) = \frac{\lambda(\lambda x)^{\alpha-1}e^{-\lambda x}}{\Gamma(\alpha)} \quad (x > 0 \text{ and } \alpha > 0, \lambda > 0) \quad (38)$$

with $\alpha = n/2$ and $\lambda = 1/2$.
- If X_1 and X_2 are independent random variables with Gamma distribution having parameters (α_1, λ) and (α_2, λ), then $Y = X_1/(X_1 + X_2)$ has a Beta distribution with parameters (α_1, α_2), and the pdf is

$$f_Y(y) = \frac{\Gamma(\alpha_1 + \alpha_2)}{\Gamma(\alpha_1)\Gamma(\alpha_2)} y^{\alpha_1 - 1}(1 - y)^{\alpha_2 - 1}. \quad (39)$$

With the above properties, we have that $(W_K/\sigma^2) = \sum_{k=1}^{K}(X_k/\sigma)^2$ is a Gamma random variable with parameters $(K/2, 1/2)$, and $(W_{N-K}/\sigma^2) = \sum_{k=K+1}^{N}(X_k/\sigma)^2$ is a Gamma random variable with parameters $((N-K)/2, 1/2)$. According to (39), $y_K = (\sum_{k=1}^{K} x_k^2 / \sum_{k=1}^{N} x_k^2) = W_K/(W_K + W_{N-K})$ has a Beta distribution with parameters $(K/2, (N-K)/2)$, therefore

$$f_{Y_K}(y) = \frac{\Gamma(\frac{N}{2})}{\Gamma(\frac{K}{2})\Gamma(\frac{N-K}{2})} y^{(K/2)-1}(1-y)^{(N-K)/2-1}. \quad (40)$$

The cdf is an incomplete Beta function

$$F_{Y_K}(y) = \frac{\Gamma(\frac{N}{2})}{\Gamma(\frac{K}{2})\Gamma(\frac{N-K}{2})} \int_0^y t^{(K/2)-1}(1-t)^{(N-K)/2-1} dt. \quad (41)$$

A family of curves of $f_{Y_K}(y)$ in (40) is plotted in Fig. 3 for $N = 64$ and $K = 1$–10.

E. d_{ac} *pdf Approximation*

The approximate distribution of d_{ac} as a function of the window size J (number of symbols used to evaluate the covariance matrix $\mathbf{R}$) was first derived in [9] as a modified noncentral chi-square random variable with K degrees of freedom

$$f_{Z_K}(z) = \frac{\frac{J}{2} z^{(K-2)/4} \exp\left(-\frac{K(z+1)}{2}\right) I_{K/2-1}(\sqrt{z})}{1 - Q_{K/2}(\sqrt{J}, \sqrt{J})} \quad (42)$$

where $0 < z < 1$, and $I_\alpha(x)$ is the αth-order modified Bessel function of the first kind. $Q_m(a, b)$ is the mth-order generalized Marcum's Q-function. Unfortunately, this approximation is relatively crude and does not take into account the signal subspace estimation error due to finite signal-to-noise ratio (SNR). Indeed, the distribution of d_{ac} is a joint function of N, K, J, SNR, and the channel model. The large number of parameters makes it nontrivial to rigorously derive an accurate approximation for d_{ac}.

To preserve the generality of analysis in this paper, we chose not to adopt this analytical approximation due to the limitations of the model it assumes. In other words, a general analytical expression $f_{Z_K}(z)$ for the distribution of d_{ac} remains an important open issue, which is for now best addressed on a case-by-case basis. In the rest of the paper, we will use Monte Carlo simulations to approximate the distribution of d_{ac}.

F. *Identifier Error Rate*

The identifier error rate is governed by the value of d_{th}, which is, in turn, determined by the distribution of d_{ac} (active users) and d_{in} (inactive users). There are two types of identifier errors, encapsulated in the following performance measures.

$\mathbf{P_f}$ Probability of false alarm. A false alarm occurs when an inactive user is mistakenly categorized as an active user by the active-user identifier.

$\mathbf{P_m}$ Probability of miss. A miss occurs when an active user is mistakenly overlooked by the active-user identifier.

A practical design problem would be to choose the value for d_{th}, given the required P_f, P_m, and network traffic K. These constraints cannot be satisfied independently, as the variation in d_{th} and K changes P_f and P_m simultaneously. Section VI will demonstrate a graphical approach to determine d_{th} given the maximum allowable P_m and P_f.

Relating to the cdf approximations introduced in previous sections, the probability of generating a false alarm for a particular inactive user and the probability of generating a miss for a particular active user with a network traffic of K packets are, respectively

$$P_f = P(d_{\text{in}} \geq d_{\text{th}}) = 1 - F_{Y_K}(d_{\text{th}}) \quad (43)$$

$$P_m = P(d_{\text{ac}} \leq d_{\text{th}}) = F_{Z_K}(d_{\text{th}}) \quad (44)$$

where $f_{Y_K}(z)$ and $f_{Z_K}(z)$ are the cdfs of d_{in} and d_{ac}, respectively.

VI. Simulation Examples

A. *Distributions of* d_{in} *and* d_{ac}

As Fig. 4 illustrates, we present a set of experimental and analytical pdfs for d_{in} and d_{ac}. First, we generate the experimental pdfs of d_{in} and d_{ac} using statistics of the identifier output over 100 000 independent trials. In each trial, a set of $M(M-1)$ TRBC codes are generated by setting $\mathbf{w}_m$ to be a set of orthog-

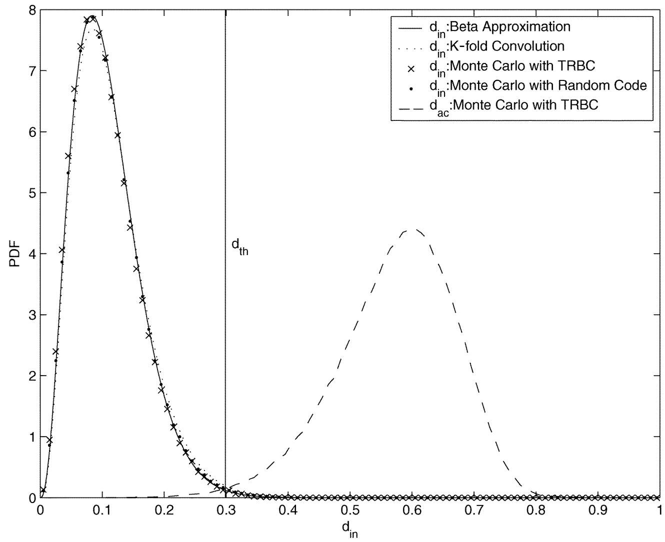

Fig. 4. pdf of $d_{\rm in}$ ($N = 64, K = 7$, SNR $= 15$ dB).

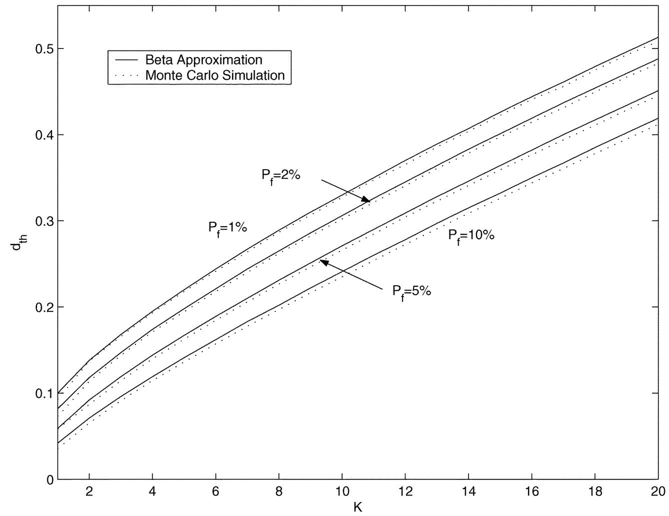

Fig. 5. $d_{\rm th}$ as a function of K for $P_f = 1\%, P_f = 2\%, P_f = 5\%$, and $P_f = 10\%$.

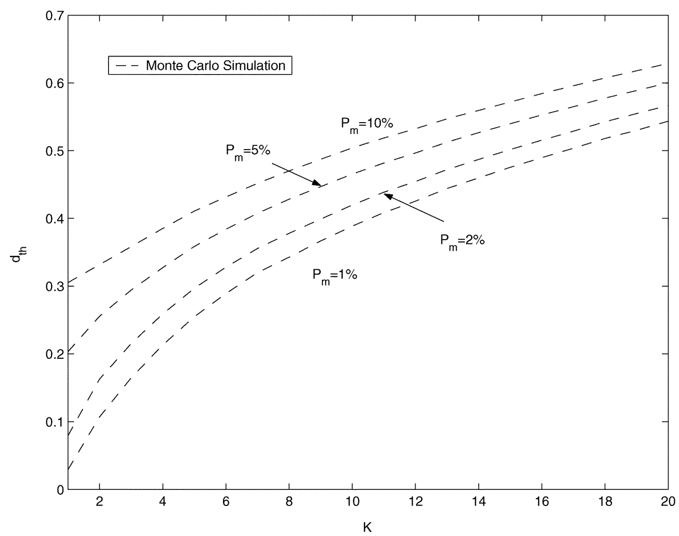

Fig. 6. $d_{\rm th}$ as a function of K for $P_m = 1\%, P_m = 2\%, P_m = 5\%$, and $P_m = 10\%$.

onal codes, and $\mathbf{p}_m$ a set of random codes of length N. K of these spreading codes are randomly chosen and placed in $\mathcal{A}$ (the set of active users) with equal power. One of the receivers is randomly chosen, and its inactive spreading codes are projected onto the estimated signal subspace to generate the experimental pdf of $d_{\rm in}$. Another spreading code randomly chosen from the set $\mathcal{A}$ is projected on the estimated signal subspace to generate the experimental pdf of $d_{\rm ac}$.

Second, we want to show that the statistics of $d_{\rm in}$ as a result of the TRBC spreading code scheme can be closely approximated by the "random" spreading code assumption. We generate the experimental pdf of $d_{\rm in}$ using statistics of the identifier output over 100 000 independent trials. In each trial, K randomly generated spreading codes are placed in $\mathcal{A}$. One other spreading code is randomly generated (which does not belong to $\mathcal{A}$) and is tested as the inactive user. We see that the experimental pdf of $d_{\rm in}$ generated here using the random spreading code assumption is almost exactly the same as the one generated using the TRBC scheme. The similar observation goes for $d_{\rm ac}$, although the pdf of $d_{\rm ac}$ generated using random spreading code assumption is not plotted here. The almost identical $d_{\rm in}$'s resulting from two different spreading code schemes demonstrate the validity of our effort in deriving the analytical pdf of $d_{\rm in}$ using the random spreading code assumption.

Lastly, we compare the Monte Carlo simulations of $d_{\rm in}$ with the analytical predictions. In particular, we plot the approximation by Beta distribution in (40) and the K-fold convolution in (36). We see that the analytical pdfs for $d_{\rm in}$ are very good matches for the experimental results. The closeness of the Beta distribution shows that it is not necessary for N to be excessively large for this approximation to be accurate. The fact that the K-fold convolution pdf also fits the experimental result well shows the assumption that $x_1^2/\sum_{k=1}^N x_k^2, x_2^2/\sum_{k=1}^N x_k^2, \ldots, x_K^2/\sum_{k=1}^N x_k^2$ are weakly correlated is a correct one.

As depicted in Fig. 4, we also see how important it is to set an appropriate value for $d_{\rm th}$, so as to minimize the probability of miss and false alarm. Obviously, the region for the best threshold is around $d_{\rm th} = 0.3$, which is almost impossible to predict without the prior knowledge of the pdfs of $d_{\rm in}$ and $d_{\rm ac}$.

B. Miss Rate and False Alarm Rate

From the simulation in Fig. 5, we show the variation of $d_{\rm th}$ as a function of K for false alarm rate $P_f = 1\%, 2\%, 5\%$, and 10%. The curves obtained from both experimental and analytical results are consistently close to each other. The analytical values are calculated based on (43). We make use of experimental pdfs of $d_{\rm in}$ generated from Monte Carlo simulations using TRBC spreading codes described in Section V to arrive at the experimental values for $d_{\rm th}$.

Fig. 6 illustrates the change of $d_{\rm th}$ as a function of K (J and SNR are fixed) for miss rate $P_m = 1\%$, 2%, 5% and 10%. As pointed out in Section V-E, we do not have a good analytical prediction of the simulation result, so we only plot the experimental curves calculated based on Monte Carlo simulations using TRBC spreading codes.

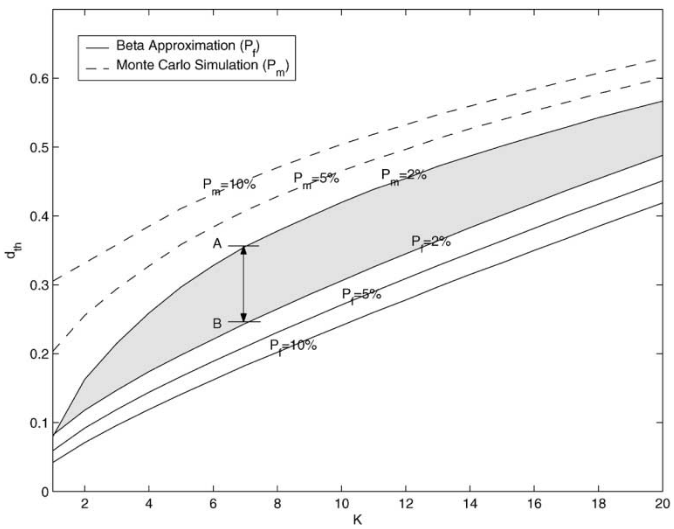

Fig. 7. Permissible range of $d_{\rm th}$ as a function of K for $P_m = 2\%, P_f = 2\%$.

Finally, we will summarize the tradeoffs between the false alarm rate P_f and miss rate P_m by introducing a graphical approach to select a range of values for $d_{\rm th}$ for given N, J, SNR, and maximum P_f, P_m. For the case of $N = 64$, $J = 200$, SNR $= 15$ dB, and $P_f = 2\%$, $P_m = 2\%$, the shaded region in Fig. 7 is where $d_{\rm th}$ can be chosen to satisfy the constraint set by P_f and P_m. In particular, the range A–B is where $d_{\rm th}$ can be chosen for $K = 7$. The result agrees with our observation from Fig. 4 that the best value for $d_{\rm th}$ is in the vicinity of 0.3. Obviously, if we have a family of such curves, we may easily locate $d_{\rm th}$ where the tradeoff between P_f and P_m is optimized.

VII. Conclusions

In this paper, we studied the problem of improving the throughput of a random-access wireless ad hoc network through multiuser detection at the physical layer. We developed a novel spreading code scheme (TRBC) for DS-CDMA networks which embeds the address information of both the transmitter and receiver in the spreading codes, so that the receiver may identify the packets addressed to it without actually decoding the packet.

Furthermore, a subspace-based active-user identification technique was discussed, followed by the corresponding performance analysis. The subspace-based approach introduces almost no additional complexity to the receiver if the receiver is designed to use a subspace-based multiuser detector [5], for in this case, the eigenvalue and eigenvector information is readily available. A group-blind multiuser detector [6] can be used when multiple packets are concurrently transmitted to the receiver. The fact that the spreading codes of these packets are orthogonal to each other, as a result of our TRBC code-design scheme in (1), makes the implementation of such a detector particularly simple. In addition, an adaptive version of joint active-user identification and multiuser detection can be easily derived based on the adaptive subspace multiuser detection algorithm presented in [5], [18], and [19].

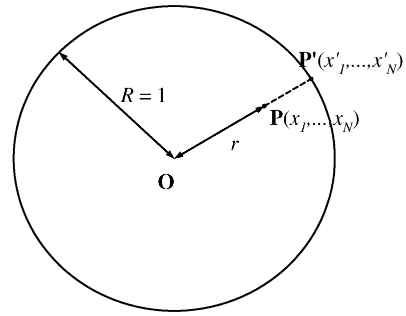

Fig. 8. Projection of uniformly distributed points inside the unit sphere to the surface of the sphere.

Appendix A

Proof of Lemma 1

A spherically uniform random vector $\mathbf{x}$ has a pdf in polar coordinate as

$$f(\rho, \theta_1, \ldots, \theta_{N-1}) = Q(\rho, N) \tag{45}$$

where $0 < \rho < 1$. The independence of the pdf with respect to $\theta_1, \ldots, \theta_{N-1}$ is due to the fact that a spherically uniform random vector has uniformly distributed angles to the Cartesian axes, but a nonuniform distribution along the radius. For any random point $\mathbf{P}(x_1, x_2, \ldots, x_N)$ uniformly distributed inside the N-dimensional unit sphere, there is a projection along the direction of $\overrightarrow{\mathbf{OP}}$ onto the surface of the sphere at $\mathbf{P}'(x_1', x_2', \ldots, x_N')$, where $\mathbf{O}$ is the center of the sphere (see Fig. 8). Denoting $r \doteq |\overrightarrow{\mathbf{OP}}| = \sqrt{x_1^2 + x_2^2 + \cdots + x_N^2}$, the coordinates of point $\mathbf{P}'$ may also be written as $\mathbf{P}'(x_1/r, x_2/r, \ldots, x_N/r)$.

The projected point $\mathbf{P}'$ has a distribution $f'(\theta_1, \ldots, \theta_{N-1})$ on the surface of the sphere, evaluated as follows:

$$\begin{aligned} f'(\theta_1, \ldots, \theta_{N-1}) &= \int_0^1 f(\rho, \theta_1, \ldots, \theta_{N-1}) d\rho & (46)\\ &= \int_0^1 Q(\rho, N) d\rho & (47)\\ &= g(N). & (48)\end{aligned}$$

Since this pdf is a constant given N, $\mathbf{P}'$ is uniformly distributed on the surface of the sphere. We are interested in finding the distribution of

$$Y = {x_1'}^2 + {x_2'}^2 + \cdots + {x_K'}^2. \tag{49}$$

But equivalently

$$\begin{aligned} Y &= \frac{x_1^2}{r^2} + \frac{x_2^2}{r^2} + \cdots + \frac{x_K^2}{r^2} & (50)\\ &= \frac{x_1^2 + x_2^2 + \cdots + x_K^2}{x_1^2 + x_2^2 + \cdots + x_N^2}. & (51)\end{aligned}$$

Therefore, the distribution of $Y = {x_1'}^2 + {x_2'}^2 + \cdots + {x_K'}^2$ subject to (s.t.) $(x_1', x_2', \ldots, x_N')$ uniformly distributed on the surface of the unit sphere is equivalent to the distribution of $Y = (x_1^2 + x_2^2 + \cdots + x_K^2)/(x_1^2 + x_2^2 + \cdots + x_N^2)$ s.t. $(x_1, x_2, \ldots, x_N)$ uniformly distributed inside the unit sphere.

APPENDIX B

Proof of Lemma 2

Given that $\mathbf{x}$ is spherically uniform inside an N-dimensional unit sphere, the probability density of $\mathbf{x}$, $f_{\mathbf{X}}(\mathbf{x})$, is $1/\mathrm{V}_N$, where V_N is the volume of an N-dimensional unit sphere. The marginal density of one component of $\mathbf{x}$, say $f_{X_1}(x_1)$, is $f_{\mathbf{X}}(\mathbf{x})$ integrated over the region $\sum_{k=2}^{N} x_k^2 \leq 1 - x_1^2$. The region of integration is itself an $(N-1)$-dimensional sphere of radius $\sqrt{1-x_1^2}$, and the integral is the volume of this sphere. So we have

$$f_{X_1}(x_1) = \frac{\mathrm{V}_{N-1}(\sqrt{1-x_1^2})}{\mathrm{V}_N} = \frac{\mathrm{V}_{N-1}}{\mathrm{V}_N}(1-x_1^2)^{(N-1)/2} \quad (52)$$

where $\mathrm{V}_{N-1}(R)$ denotes the volumn of an $(N-1)$-dimensional sphere with radius R, and the second equality comes from (27). Since the marginal pdf must integrate to unity, we have

$$\frac{\mathrm{V}_N}{\mathrm{V}_{N-1}} = \int_{-1}^{1} (1-\rho^2)^{(N-1)/2} d\rho. \quad (53)$$

The variance of x_1 can also be evaluated as

$$\begin{aligned} E\left\{x_1^2\right\} &= \frac{\mathrm{V}_{N-1}}{\mathrm{V}_N} \int_{-1}^{1} \rho^2 (1-\rho^2)^{(N-1)/2} d\rho \\ &= \frac{\int_{-1}^{1} \rho^2 (1-\rho^2)^{(N-1)/2} d\rho}{\int_{-1}^{1} (1-\rho^2)^{(N-1)/2} d\rho} \\ &= \frac{1}{(N+2)}. \end{aligned} \quad (54)$$

To show that x_1 asymptotically approaches a Gaussian random variable, we let $z_1 = x_1/(\sqrt{N+2})$. So z_1 is a unit variance random variable with pdf

$$f_{Z_1}(z_1) = C \cdot \left(1 - \left(\frac{z_1}{\sqrt{N+2}}\right)^2\right)^{(N-1)/2}. \quad (55)$$

As $N \to \infty$, both $(N+2)$ and $(N-1)$ can be replaced by N, and

$$f_{Z_1}(z_1) \to C \cdot \left(1 - \frac{{z_1}^2}{N}\right)^{N/2} \to C \cdot e^{-z_1^2/2}. \quad (56)$$

Therefore, x_1 is a Gaussian random variable with variance $1/(N+2)$ for $N \to \infty$. Simple argument can be used to show that $x_1, x_2, \ldots, x_N$ are asymptotically i.i.d.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for constructive comments that helped improve this paper to its present form.

REFERENCES

[1] M. K. Tsatsanis and R. Zhang, "Network-assisted diversity for random-access wireless networks," *IEEE Trans. Signal Processing*, vol. 48, pp. 702–711, Mar. 2000.
[2] E. Sousa and J. Silvester, "Spreading code protocols for distributed spread-spectrum packet radio networks," *IEEE Trans. Commun.*, vol. 36, pp. 272–281, Mar. 1988.
[3] R. Zhang, N. D. Sidiropoulos, and M. K. Tsatsanis, "Collision resolution in packet radio networks using rotational invariance techniques," *IEEE Trans. Commun.*, vol. 50, pp. 146–155, Jan. 2002.
[4] G. B. Giannakis, Y. Hua, P. Stoica, and L. Tong, *Signal Processing Advances in Wireless & Mobile Communications*. Englewood Cliffs, NJ: Prentice-Hall, 2000, ch. 8, pp. 315–354.
[5] X. Wang and H. V. Poor, "Blind multiuser detection: A subspace approach," *IEEE Trans. Inform. Theory*, vol. 44, pp. 677–690, Mar. 1998.
[6] X. Wang and A. H. Madsen, "Group-blind multiuser detection for uplink CDMA," *IEEE J. Select. Areas Commun.*, vol. 17, pp. 1971–1984, Nov. 1999.
[7] M. Wax and T. Kailath, "Detection of signals by information theoretic criteria," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-33, pp. 179–182, Apr. 1985.
[8] P. Chen, M. C. Wicks, and R. S. Adve, "Development of a statistical procedure for detecting the number of signals in a radar measurement," *IEE Proc. Radar, Sonar Navig.*, vol. 148, no. 4, pp. 219–226, Aug. 2001.
[9] W. Wu and K. Chen, "Identification of active users in synchronous CDMA multiuser detection," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 1723–1735, Dec. 1998.
[10] G. D. Forney and L.-F. Wei, "Multidimensional constellations—Part I: Introduction, figures of merit, and generalized cross constellations," *IEEE J. Select. Areas Commun.*, vol. 7, pp. 877–892, Aug. 1989.
[11] E. A. Lee and D. G. Messerschmitt, *Digital Communication*. Norwell, MA: Kluwer, 1994, ch. 14, pp. 664–667.
[12] W. Neutsch, *Coordinates*. New York: Walter de Gruyter, 1996, ch. 26, pp. 991–994.
[13] R. S. Borden, *A Course in Advanced Calculus*. Amsterdam, The Netherlands: North Holland, 1983, ch. 9, pp. 278–279.
[14] R. Sikorski, *Advanced Calculus*. Warszawa, Poland: Polish Scientific, 1969, ch. 9, pp. 314–318.
[15] A. H. Stroud, *Approximate Calculation of Multiple Integrals*. Englewood Cliffs, NJ: Prentice-Hall, 1971, ch. 2, pp. 32–40.
[16] A. Leon-Garcia, *Probability and Random Processes for Electrical Engineering*. Reading, MA: Addison-Wesley, 1994.
[17] M. Woodroofe, *Probability With Applications*. New York: McGraw-Hill, 1975, ch. 7, pp. 186–187.
[18] B. Yang, "An extension of the PASTd algorithm to both rank and subspace tracking," *IEEE Signal Processing Lett.*, vol. 2, pp. 179–182, Sept. 1995.
[19] ——, "Projection approximation subspace tracking," *IEEE Trans. Signal Processing*, vol. 44, pp. 95–107, Jan. 1995.

Darryl Dexu Lin (S'01) received the B.A.Sc. degree in engineering science and M.A.Sc. degree in electrical engineering in 2001 and 2003, respectively, from the University of Toronto, Toronto, ON, Canada, where he is currently working toward the Ph.D. degree in the Department of Electrical and Computer Engineering.

His research interests include multipacket reception in ad hoc networks and signal processing for MIMO OFDM systems.

Teng Joon Lim (S'92–M'95–SM'02) obtained the B.Eng. degree with first class honors from the National University of Singapore, Singapore, in 1992, and the Ph.D. degree from Cambridge University, Cambridge, U.K., in 1996.

From September 1995 to November 2000, he was a Member of Technical Staff at the Centre for Wireless Communications, Singapore, where he was the leader of the Digital Communications research group. Since December 2000, he has been an Assistant Professor at the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada. He has published extensively in the areas of adaptive filtering, multiuser detection, and wireless communications. His current research interests include multiuser space-time systems, ad hoc networks, iterative decoding and analysis of fading channels. He served as the Technical Program Chair of ICCS 2000.