Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2009, Article ID 437824, 18 pages
doi:10.1155/2009/437824

Research Article

Securing OFDM over Wireless Time-Varying Channels Using Subcarrier Overloading with Joint Signal Constellations

Gill R. Tsouri[1] and Dov Wulich (EURASIP Member)[2]

[1] *Department of Electrical Engineering, Rochester Institute of Technology, Rochester, NY 14623, USA*
[2] *Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer-sheva 84105, Israel*

Correspondence should be addressed to Gill R. Tsouri, grteee@rit.edu

Received 29 November 2008; Revised 29 May 2009; Accepted 30 July 2009

Recommended by Merouane Debbah

A method of overloading subcarriers by multiple transmitters to secure OFDM in wireless time-varying channels is proposed and analyzed. The method is based on reverse piloting, superposition modulation, and joint decoding. It makes use of channel randomness, reciprocity, and fast decorrelation in space to secure OFDM with low overheads on encryption, decryption, and key distribution. These properties make it a good alternative to traditional software-based information security algorithms in systems where the costs associated with such algorithms are an implementation obstacle. A necessary and sufficient condition for achieving information theoretic security in accordance with channel and system parameters is derived. Security by complexity is assessed for cases where the condition for information theoretic security is not satisfied. In addition, practical means for implementing the method are derived including generating robust joint constellations, decoding data with low complexity, and mitigating the effects of imperfections due to mobility, power control errors, and synchronization errors.

1. Introduction

Orthogonal Frequency Division Multiplexing (OFDM) is a leading choice for many current and future air interfaces. When using OFDM over a wireless channel the broadcast nature of the channel exposes transmission to eavesdropping. Securing communication links from eavesdropping is commonly done by implementing enciphering and deciphering algorithms in software, and is usually detached from the physical layer of communication. Prominent methods rely on public keys cryptography such as RSA [1], or symmetric cryptography with a common secret, such as the US National *Data Encryption Standard* (DES) [2]. There are some encryption methods which rely on the physical layer of communication for their implementation, such as spread spectrum *Frequency Hopping* (FH) and *Direct Sequence* (DS) [3]. In FH and DS a key has to be generated and distributed securely between the communicating parties. The key is used to set the FH hopping pattern or DS spreading sequence. Prominent key distribution methods rely on the Diffie-Hellman algorithm [4]. Encryption, decryption, and key distribution impose overheads on data throughput, energy consumption, memory space, and computation power. These overheads are a crucial implementation issue for low complexity systems with strict constraints on system resources [5], such as sensor and mobile networks [6–8].

Secrecy capacity analysis of random, noisy, and fading channels showed that in theory, a communication link can be perfectly secured from eavesdropping for certain limited information rates [9–11]. Recent work provided specific analysis of the secrecy capacity of wireless fading channels [12–17]. Past work suggested practical methods for using randomness in the wireless channel to alleviate the need for key distribution. In [18–20], reciprocal channel estimation of a slow fading wireless time varying channel was used as a common secret to generate and distribute encryption keys to be used by traditional encryption algorithms. In [21] a differential frequency modulation technique coupled with reverse piloting was used in a multitone channel to achieve secure transmission for point-to-point systems. In [22] a practical approach is depicted for key agreement in wireless channels based on multilevel and *Low Density Parity Check*

(LDPC) codes. In [18–22] the wireless channel was assumed to be a reciprocal slow flat fading channel, which decorrelates rapidly in space. The assumptions of reciprocity and space decorrelation were well established in previous work [21] and are adopted in this work as well.

It is common practice in wireless communications to have the transmitter use asynchronous bursts of transmission to access the channel. The burst starts with a prior known pilot signal followed by modulated data symbols. The pilot is used by the receiver to estimate the channel. The receiver then uses the channel estimate to compensate for channel attenuation and phase prior to decoding. Decoding of the received data symbols is done based on the a prior known signal constellation of the transmitter. Since the wireless channel changes with time, a pilot signal has to be sent every channel coherence time. An eavesdropper can use the pilot signal to estimate the channel from the transmitter to itself and decode the information in exactly the same manner as the intended receiver. This means that sending a pilot signal from the transmitter to the receiver compromises security.

In [23] the asynchronous burst transmission approach was replaced with synchronous transmission to achieve security. A reverse piloting protocol was proposed to secure transmission bursts in a narrow-band single carrier point-to-point system over slow flat fading channels. Synchronous transmission allows for the pilot signal to be sent from the receiver instead of the transmitter. The transmitter can estimate the channel from the receiver to itself using the receiver's pilot signal and deduce the channel from itself to the receiver based on channel reciprocity. The transmitter can then send a burst of channel-compensated data symbols over the same frequency as the pilot, and the receiver would receive a readily decodable channel-compensated signal. The receiver can use decision feedback to compensate for small changes in the channel, so that its channel estimate remains accurate until the original channel is fully decorrelated in time. After the channel decorrelates in time the receiver can send a new pilot signal. Since no pilot signal is sent from the transmitter, the eavesdropper would be deprived of estimating the channel from the transmitter to itself prior to receiving the data symbols, and would be forced to estimate the channel using blind estimation. Even for a noiseless channel, no decoding of the data would be possible until blind estimation is completed because the eavesdropper will not be able to map the received symbols to decoded bits. In this work, the reverse piloting protocol presented in [23] is elaborated to support a plurality of transmitters in a superposition modulation setting with joint decoding at the receiver. It is shown that the elaborated protocol can be practically used to obtain information theoretic security and security by complexity with low implementation complexity, no memory requirements and no overhead on throughput and energy.

In contradistinction to previous work in literature, the focus of this work is on facilitating channel overloading of multiple transmitters over subcarriers in an OFDM system. The purpose is to increase security strength and decoding gain for transmitters in an OFDM system with limited emission power, memory space, and online computation power. Although we focus our attention on OFDM, our analysis and results hold for securing narrowband single carrier transmission as well. The novelty of this work is in suggesting the use of reverse piloting for implementing superposition modulation with joint decoding to achieve information security. The main contributions are in two categories: analysis of security strength of the proposed method and practical implementation of the proposed method. The analysis of security strength results in a quantitative condition for achieving information theoretic security, given a prior known channel and system parameters and assessment of security by complexity when the condition is not satisfied. Practical implementation considerations include generating robust signal constellations, low complexity *Maximum Likelihood* (ML) decoding, network-optimization, evaluation of the effects of mobility, power control errors and synchronization errors, and formulating simple piloting rules for mitigating their effect.

The rest of the paper is organized as follows. In Section 2 the method is presented using a multiple access protocol. In Section 3 the mathematical model used for analysis is defined. In Section 4 security strength is analyzed. In Section 5 practical implementation is considered. Section 6 depicts an illustrative scenario of Rayleigh fading and three transmitters, and Section 7 concludes the work.

2. Proposed Method

In the proposed method the frequency and phase of subcarriers from multiple transmitters are matched and synchronized at the receiver. All transmitters transmit together and their start of transmission is coordinated by the receiver to have their signals reach the receiver simultaneously. All transmitters use the same subcarrier frequencies. The receiver is equipped with a single *Matched Filter* (MF) matched to each subcarrier. Each transmitter is assigned (offline) a set of arbitrary *Base Band* (BB) symbols to represent its information bits. Since the transmit-channel-receive path is linear, the receiver's MF output is a sum of the BB symbols of all the transmitters, and represents the transmitted bits of all the transmitters at once. This is in fact superposition modulation of multiple transmitters on a single subcarrier which is repeated individually for multiple subcarriers. The BB symbol sets are computed offline to have all their possible summations create a signal constellation with highest resistance to noise. The receiver decodes the information bits of all the transmitters at once from a single received symbol as if originating from a single transmitter. Since the received signal constellation is jointly formed by all the transmitters BB symbols, the proposed method is herein termed *Joint Constellation Multiple Access* (JCMA). A multiple access reverse piloting protocol over a single subcarrier is given in what follows to implement the method.

(1) The receiver obtains knowledge on signal propagation time from each transmitter to itself through some standard association procedure.

(2) The receiver assigns *index* and *delay* parameter to each transmitter.

(3) Each transmitter uses its *index* to access a preloaded table for retrieving a BB symbol set.

(4) The receiver sends a pilot signal and starts sensing for an incoming signal.

(5) Each transmitter individually estimates the reciprocal channel's phase and amplitude using the pilot signal from the receiver.

(6) Each transmitter awaits its *delay* and sends a burst of information symbols compensated for channel phase and amplitude.

(7) The receiver receives a burst of joint information symbols, which belong to its predefined joint signal set.

(8) The receiver decodes all transmitters at once.

(9) The receiver uses decision feedback to compensate for slow channel decorrelation in time.

(10) Steps 4–9 are repeated after a channel decorrelation period has passed.

A preliminary simpler version of the proposed protocol in this work was disclosed in [24], with the purpose of enhancing decoding but no information security considerations.

JCMA is superposition modulation with joint decoding. It should be distinguished from the well-known *Superposition Modulation with Successive Decoding* (SM-SD) [25]. In SM-SD the transmitters transmit at the same time and frequency and a joint signal is formed at the receiver. Each transmitter's symbol is treated as noise to the other transmitters. The receiver decodes the information of each transmitter individually in a successive manner. First, the transmitter with the highest received signal energy is decoded. The decoded bits are used as feedback to remove the transmitter's signal from the received joint signal. The next transmitter with the highest received signal energy is decoded and so on. In SM-SD the transmitters send pilot signals to facilitate channel estimation at the receiver. As explained before, this compromises security. In JCMA pilots are sent only by the receiver. It follows that knowledge of the channel is obtained only by the transmitters.

JCMA should also be distinguished from multiuser detection [26] and rather recent advances in cooperative transmit diversity [27]. In multiuser detection the structure of the interfering signals from multiple transmitters is used to reduce their effect. The achievable coding gains are considerable, but the use of multiple MFs is required and the computational complexity grows exponentially with the number of transmitters. In addition, no security is gained. In cooperative transmit diversity, the transmitter sends its own information while relaying the information of another transmitter to the receiver. The method offers some performance gains, but the limited power of the relaying transmitter has to be distributed between the data streams of the participating nodes and no security is gained.

Beside SM-SD and multiuser detection, literature presents other approaches to channel overloading of transmitters over the same frequency band. For example, the work in [28–30] uses symbol-synchronous superposition modulation to create a joint rectangular lattice at the receiver to support multiple transmitters using trellis codes. There are also numerous works dealing with the adder-channel for performing joint coding from multiple transmitters through superimposed signals. In general, codebooks of individual transmitters are optimized under some criterion over the joint signal at the receiver—usually the focus is on coding gain. More relevant to the focus of this work is the work in [31, 32], where the joint minimal Euclidean distance was used as the optimizing criterion of a symbol-synchronous superimposed signal. A comprehensive review of other channel overloading techniques is provided in [39].

The work in [25, 27–32] addresses the issue of designing joint signal constellations to satisfy various optimization criteria according to the problem explored. We are unaware of previous work (including [25, 27–32]) using secure, low complexity, joint symbol by symbol decoding as the optimization criteria.

As would be apparent in the following sections, the suggested method offers a low complexity solution for securing OFDM over the time-varying wireless channel. The receiver uses a single MF and performs decoding of multiple transmitters with the same complexity as decoding a single transmitter. The transmitters' complexity is the same as that of a point-to-point scenario without security features. No memory space, computation power, or transmitted energy is required in order to secure transmission. For comparison, consider the analysis of energy consumption due to implementing security algorithms performed in [5]. In [5], it was shown that a typical sensor-node using asymmetric key establishment coupled with symmetric encryption per transmission session losses 20%–80% of its battery life due to encryption, depending on the session length. See [5] for energy consumption of RSA, DES, and DH in specific systems. Other analysis provided in [8] considered the *Central Processing Unit* (CPU), memory and transmission overheads required for implementing standard security algorithms implemented in specific off-the-shelf nodes. The analysis in [8] concluded that DES is too resource demanding to be used in a sensor network and that a minimum of 128 KB RAM and ability to tolerate a considerable delay in data delivery are required to implement security algorithms of lesser strength. See [8] for CPU processing and memory and transmission overheads of encryption algorithms DES, TEA, RC6, RC5, and SkipJack in specific systems.

3. Mathematical Model

In JCMA a joint constellation is constructed over each subcarrier separately. It follows that most of the analysis can be done using a model for a single subcarrier. In what follows, a single subcarrier is considered. The expansion of the analysis to an entire OFDM symbol is done when evaluating security of the entire OFDM transmission.

The BB model of the multiple access scheme for a single subcarrier is depicted in Figure 1, x_i; $i = 1, 2, \ldots, N$ represent the transmitted complex BB symbols. Subcarriers in OFDM experience flat fading. It follows that the channel

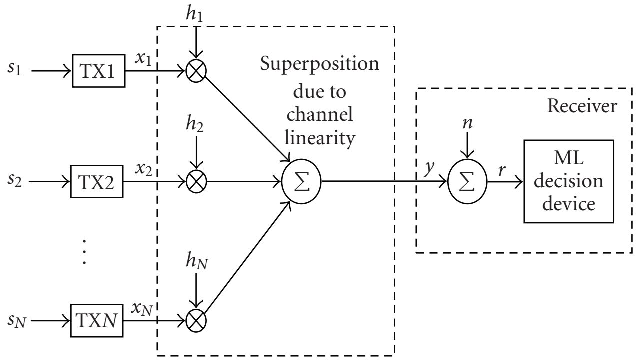

Figure 1: Baseband model of JCMA.

over a single subcarrier is flat and is described by a single complex number h_i. The transmitted symbols are summed via channel superposition and the MF output, without noise, is given by y. Also, n is the BB additive white complex Gaussian noise. The received signal r is fed to an ML decision device, which decodes all the transmitted bits at once, as if originating from a single transmitter (the so-called "super-user" in [25]).

Let us define

$$h_i = \alpha_i \exp(j\beta_i); \qquad x_i = \frac{\exp(-j\beta_i)}{\alpha_i} s_i, \tag{1}$$

where s_i is an information-carrying symbol with unit energy which belongs to a predefined set S_i. It is assumed that $1/\alpha_i$ is small enough to allow the transmitter to adjust its power within its power constraint. If this is not the case, communication would be severed, as would also happen in a standard point to point scenario.

For now, it is assumed that β_i, α_i are known without error at the ith transmitter-perfect *Channel State Information* (CSI), and that h_i remains constant during the decorrelation time. In later sections, derivations to the model are defined to analyze the effects of imperfect CSI and mobility on system performance.

From (1) and Figure 1 it follows that

$$r = y + n = \sum_{i=1}^{N} s_i + n. \tag{2}$$

The joint signal constellation at the receiver is made up of all the permutations in $s_i, i = 1, 2, \ldots, N$ which generate y.

Note that S_i; $i = 1, \ldots, N$ are sets of complex numbers, where $S_i = \{s_1^i, s_2^i, \ldots, s_{2^M}^i\}$. In addition, M is the number of bits per symbol per transmitter, and y is a set of complex numbers made of all possible summations of N numbers, where each number belongs to a different set S_i. Moreover, $y = \{y_1, y_2, \ldots, y_{2^{MN}}\}$, $y_i = \sum_{j=1}^{N} l_i^j; l_i^j \in S_j$ where $\{l_i^1, l_i^2, \ldots, l_i^N\} \neq \{l_k^1, l_k^2, \ldots, l_k^N\}$ for all $i \neq k$.

The symbol sets are determined offline. For additive Gaussian noise, the minimum Euclidian distance in the joint constellation represented by y should be maximal while constraining the average instantaneous energy over the transmitter symbols to be less than P (peak power constraint on transmitted power). Finding the best BB symbol sets is explicitly formulated as follows.

Given the definition:

$$d_{\min} \overset{\text{def}}{=} \min_{i \neq j} \left\{ \left| y_i - y_j \right| \right\}, \tag{3}$$

find S_i; $i = 1, \ldots, N$ which yield $\max\{d_{\min}\}$, while satisfying the constraint:

$$\frac{1}{2^M} \sum_{j=1}^{2^M} \left| S_j^i \right|^2 \leq P; \quad i = 1, \ldots, N. \tag{4}$$

For additive Gaussian noise, ML detection translates to finding the joint constellation symbol g in y which has the smallest Euclidean distance from the received symbol q, so

$$g = \arg \left\{ \min_{y_i} (|q - y_i|) \right\}. \tag{5}$$

4. Security Analysis

To facilitate analysis, we assume that the eavesdropper uses a single MF for decoding the data. At first glance, this seems to be an unreasonable limitation on the eavesdropper resources. The justification for this constraint would be given as part of the discussion in this section.

In JCMA, the joint constellation at the receiver's MF output is the result of a coherent sum of the transmitter BB symbols and is unique to the location of the transmitters and receiver in space. This is achieved due to the individual compensation of delay, phase, and attenuation of each transmitter. The receiver's joint constellation would always be the same and the bit mapping from the transmitters to the joint symbols would be known a prior to the receiver. Since an eavesdropper would naturally occupy a different location in space, the transmitters BB symbols would create a different joint constellation than that of the receiver. This is practically always true even when the eavesdropper is close to the receiver because the wireless channel decorrelates fast in space. A distance of a few carrier wavelengths apart (a few centimeters for frequencies of the order of GHz) decorrelates the channel almost completely [33]. It follows that the eavesdropper would have no a prior knowledge of the bit mapping from transmitters to joint symbols. This is the basis for achieving information theoretic security.

The joint constellation is constructed optimally at the receiver's location in space. It follows that the joint constellation at the eavesdropper location would have suboptimal structure and would change after every reverse pilot sent due to different channel compensation performed at the transmitters. In addition, the signals from the transmitters would not reach the eavesdropper simultaneously. It follows that even after discovering the bit mapping from transmitters to joint symbols, the eavesdropper would have to decode the information based on a deteriorated joint signal constellation and the decoding complexity would be higher than that of the receiver. This is the basis for security by complexity.

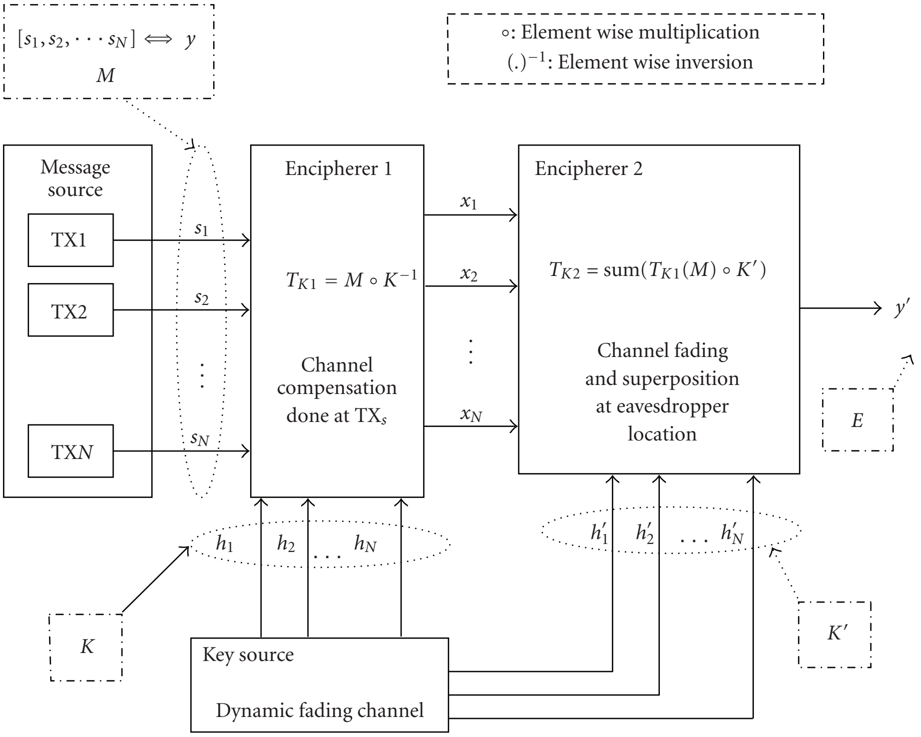
$[s_1, s_2, \cdots s_N] \Longleftrightarrow y$
M
$\circ$: Element wise multiplication
$(.)^{-1}$: Element wise inversion
Message source
TX1
TX2
TXN
s_1
s_2
s_N
Encipherer 1
$T_{K1} = M \circ K^{-1}$
Channel compensation done at TX$_s$
x_1
x_2
x_N
Encipherer 2
$T_{K2} = \mathrm{sum}(T_{K1}(M) \circ K')$
Channel fading and superposition at eavesdropper location
y'
E
h_1 h_2 ... h_N
h'_1 h'_2 ... h'_N
K
K'
Key source
Dynamic fading channel

Figure 2: JCMA as a Shannon secrecy model.

For decoding data successfully the eavesdropper must first perform blind channel estimation to map its received joint constellation symbols to information bits. Finding the bit mapping is an act of deciphering, where the received joint symbols are the cipher-text, the channel coefficients are the encryption key and the information bits are the encrypted message. After deciphering, the eavesdropper must decode the data from a deteriorated signal.

4.1. Information Theoretic Security. We start by describing the JCMA BB model as a Shannon secrecy model. Figure 2 depicts the secrecy model for an eavesdropper. The pilot from the receiver invokes key generation and distribution from the wireless medium to the transmitters. This key is the channel estimates at the transmitters. Each part of the key is known exclusively at each transmitter. In accordance with the Shannon secrecy model and its notation in [34], the message M as defined in [34] corresponds to the vector of transmitted symbols across the transmitters. This joint message is encrypted by the transmitters—each transmitter transforms its symbol by scaling and rotating it with the key. So K in [34] corresponds to the vector of channel estimates at the transmitters. For the receiver's location in space, the channel itself performs a deciphering operation by rotating and scaling the encrypted message back to the original y. For the eavesdropper location in space the channel performs another enciphering operation with another key K', being the channels from the transmitters to the eavesdropper location. The eavesdropper constellation point y' corresponds to the cryptogram E in [34]. The eavesdropper has to decipher M from E using all possible prior knowledge, such as the offline-determined transmitters BB symbol sets, the channel statistics, and the prior probabilities of the messages M.

A new key is generated every time a reverse pilot signal is sent by the receiver. Due to the time varying nature of the fading channel, a key uncorrelated with previous keys is invoked after the channel decorrelates in time. This is why the receiver is required to track the channel during the decorrelation period. Note that encryption and decryption are done automatically by the channel, so no overheads are required for these operations.

The unicity distance was defined in [34] as the amount of intercepted cryptograms by the eavesdropper beyond which the eavesdropper can deduce the key. Equivalently, the cryptogram is undecipherable when the message length is less than the unicity distance [34]. So, to achieve information theoretic security the message should be enciphered by a new key before the eavesdropper gathers enough cryptograms for deciphering. To secure an entire OFDM transmission burst, the number of joint symbols within the channel decorrelation period must be less than the unicity distance.

In the point-to-point narrow-band scenario ($N = 1$) described in [23] a single channel took part in encrypting a single message. It was shown that the channel acts as a shift cipher for cases where the phase of the complex *Random Variable* (RV) representing the channel is uniformly distributed. Uniform distribution of phase is a common assumption for describing wireless time-varying channels. For the multipoint to point scenario we assume that the phase of each channel is uniformly distributed over the range $[0, 2\pi)$. We derive the unicity distance for JCMA based on this single assumption. For clarity of presentation we consider the case where a single bit is transmitted by each transmitter ($M = 1$). The derivation scales easily for general M.

The received joint constellation at the eavesdropper is given by (see Figure 2)

$$y' = \sum_{i=1}^{N}\left(s_i \frac{h_i'}{h_i}\right). \tag{6}$$

Using amplitude-phase representation a single transmitter symbol set is given by

$$S_i = \left\{\left|s_1^i\right| \exp\left(j\theta_1^i\right), \left|s_2^i\right| \exp\left(j\theta_2^i\right)\right\}. \tag{7}$$

The structure of any signal constellation must be constrained to achieve an output signal with zero mean, so that no power is wasted. This means that the two signals in the constellation are antipodal:

$$\left|s_1^i\right| = \left|s_2^i\right| \equiv |s_i|; \qquad \theta_1^i = \theta_2^i + \pi. \tag{8}$$

Using $s_i = |s_i| \exp(j\theta_s)$, $h_i = |h_i| \exp(j\theta_i)$, $h_i' = |h_i'| \exp(j\theta_i')$, (7) and (8) in (6) give

$$y' = \sum_{i=1}^{N}(\delta_i \exp(j(\varphi_i))) \equiv \sum_{i=1}^{N}\widetilde{s}_i, \tag{9}$$

where $\varphi_i = \theta_s + \theta_i' - \theta_i$ and $\delta_i = |s_i||h_i'|/|h_i|$.

We find that $\widetilde{s}_i$ originating from a single transmitter arrives at the eavesdropper with the same amplitude δ_i for either of the two possible bit values. The phase of $\widetilde{s}_i$ is the sum of three RVs. Two of the RVs (θ_i,θ_i') are uniformly and independently distributed over the range $[0, 2\pi)$ and the third (θ_s) assumes one of two possible values θ_1^i, θ_2^i corresponding to the two possible bit values.

Since the phase is uniformly distributed and cyclic over $[0, 2\pi)$, taking its colinear values (multiplying the RV with -1) results in the same distribution. It follows that the *Probability Density Function* (PDF) of $\theta_i' - \theta_i$ is equal to the PDF of $\theta_i' + \theta_i$ which is the result of convolution of two uniform PDFs:

$$\begin{aligned} f_{\theta_i'-\theta_i}(z) &= \left[\frac{1}{2\pi}\Pi\left(\frac{z-\pi}{2\pi}\right)\right] * \left[\frac{1}{2\pi}\Pi\left(\frac{z-\pi}{2\pi}\right)\right], \\ &= \begin{cases} \dfrac{(z-\pi)}{(4\pi^2)}, & \pi \le z < 3\pi, \\ \dfrac{1}{(2\pi)} - \dfrac{(z-3\pi)}{(4\pi^2)}, & 3\pi \le z < 5\pi, \\ 0, & \text{otherwise}. \end{cases} \end{aligned} \tag{10}$$

Due to the cyclic property of the phase (modulo 2π), (10) is equivalent to

$$\begin{aligned} &f_{\theta_i'-\theta_i}(z) \\ &\quad = \begin{cases} \left(\dfrac{1}{(4\pi)} + z\right) + \left(\dfrac{1}{(4\pi)} + z\right), & 0 \le z < \pi, \\ \left(\dfrac{1}{(2\pi)} - (z-\pi)\right) + (z-\pi), & \pi \le z < 2\pi, \end{cases} \\ &\quad = \begin{cases} \dfrac{1}{(2\pi)}, & 0 \le z < 2\pi, \\ 0, & \text{otherwise}. \end{cases} \end{aligned} \tag{11}$$

It follows that $\theta_i' - \theta_i$ is uniformly distributed over the range $[0, 2\pi)$. Adding θ_s to $\theta_i' - \theta_i$ results in a cyclic shift of phase values over the range $[0, 2\pi)$ but does not change the PDF regardless the value of θ_s. It follows that φ_i is always uniformly distributed over the range $[0, 2\pi)$. This means that the mappings from the two possible transmitter bit values to a received symbol $\widetilde{s}_i$ at the eavesdropper are equally probable.

Since the channel decorrelates fast across space, the received individual symbols from the different transmitters at the eavesdropper $\widetilde{s}_i, i = 1, \ldots, N$ are uncorrelated, each received symbol from a transmitter has two equally probable bit mappings. The result is 2^N equally probable bit mappings for the joint signal constellation at the eavesdropper. It follows that JCMA is analogous to a substitution cipher with 2^N equally probable keys.

The unicity distance of a substitution cipher is given by [34]

$$U_d = \frac{H(K)}{1-\eta}, \tag{12}$$

where $H(K)$ is the entropy of the key. Also, η is the efficiency of the information source defined as $\eta \overset{\text{def}}{=} 1 - D$, where D is the redundancy of the information source [34]. In our case, $H(K) = H(2^N) = N$ and the JCMA unicity distance is given by

$$U_d = \frac{N}{1-\eta}. \tag{13}$$

The model in Figure 2 depicts a single subcarrier. Neighboring subcarriers in OFDM experience similar channel response due to channel correlation across bandwidth. This means that neighboring subcarriers can be used by the eavesdropper to discover their similar channel response (encryption key). It is common to assume that the channel decorrelates in frequency every coherence bandwidth (B_c). To be on the safe side, it is assumed that all subcarriers within B_c experience exactly the same channel. This is a strict assumption, since subcarriers which are less than B_c apart are not fully correlated.

Secrecy is required for the entire data transmission burst. This means that the unicity distance must be larger than the number of received joint symbols during the channel decorrelation period (L_c) times the number of subcarriers within the channel coherence bandwidth (N_c). It follows from (13) that for

$$N_c L_c \leq \frac{N}{1-\eta}, \tag{14}$$

information theoretic security is achieved for the entire data burst.

Note that L_c and N_c are given by

$$\begin{aligned} N_c &= B_c T_s, \\ L_c &= \frac{T_d}{T_s}, \end{aligned} \tag{15}$$

where T_s is the transmitted symbol time.

The channel temporal decorrelation time (T_d), is governed by the Doppler spread (B_d) and is defined as

$$T_d \overset{\text{def}}{=} \frac{\alpha}{B_d}, \tag{16}$$

where α is set to achieve sufficient channel decorrelation in time. However, B_d is determined by the relative movement of the transmitter with respect to the receiver described by the Doppler shift, and by the movement of reflectors in their path. Moreover, B_d increases with mobility and carrier frequency. In the context of encryption strength a short channel decorrelation time (higher mobility) is preferred. This results in a higher key generating rate. In this sense, the worse-case scenario is a stationary transmitter and receiver, for which B_d has the smallest possible value.

Using (15), (16) in (14) results in

$$B_d \geq \frac{(1-\eta)\alpha B_c}{N}. \tag{17}$$

If the system and channel parameters satisfy (17) the data transmission burst is secured from eavesdropping.

If (17) is difficult to satisfy due to small B_d, security can be obtained by shortening the number of data symbols in the transmission burst so that it equals the unicity distance. This results in an equality in (14) regardless of the channel decorrelation period. This approach would result in throughput reduction as the transmitters must wait in idle mode for the channel to decorrelate. Throughput loss can be avoided by having multiple JCMA groups accessing the channel in a TDMA fashion, so that one group uses the channel while the others wait for it to decorrelate. Alternatively, the protocol can be applied to only some of the subcarriers preferably spaced apart as much as possible across the bandwidth.

We now justify constraining the use of a single MF at the eavesdropper. An MF is the optimal demodulator for achieving a maximal SNR from the received signal [35]. Using multiple MFs connected to a signal antenna makes no sense because the joint constellation is constructed over a single complex dimension for any number of transmitters. It follows that the optimal choice for the eavesdropper is to use a single MF with soft decoding. If the eavesdropper would try to use multiple antennas for finding the bit mapping faster (for decreasing the unicity distance), the result would be multiple equivalent deciphering problems and the eavesdropper would gain nothing as far as deciphering time is concerned.

4.2. Security by Complexity.

In the previous section, information theoretic security of the entire data transmission burst was found. Deciphering amounted to discovering the bit mapping from the transmitters to each joint symbol. Knowledge of the mapping is obtained by the eavesdropper after the unicity distance has passed only if the eavesdropper uses the best possible algorithm to decipher the data. After deciphering is accomplished, the eavesdropper still has to decode the data. When information theoretic security is not achievable, security boils down to making decoding much more difficult for the eavesdropper compared to the intended receiver. We identify four such security-by-complexity features of JCMA.

(1) The eavesdropper would have difficulty to know the expected joint symbol constellation at its MF output, since it has no knowledge of the channel compensation done at each transmitter, no immediate knowledge of the CSI from the nodes to itself, and it receives noisy samples.

(2) The signals from the group nodes would not reach the eavesdropper simultaneously, resulting in an overlap of past and present symbols.

(3) The eavesdropper joint constellation would change every decorrelation period. This is due to the changing of channel compensation at the transmitters. This makes it impossible to design a constant and computationally efficient decoding algorithm, meaning that the eavesdropper would have to perform an exhaustive search for ML detection of every received symbol. At the same time, the receiver decoding algorithm would be constant because each channel instance is compensated for.

(4) The joint constellation formed at the eavesdropper MF output is not optimal for decoding, since it was made to be optimal at a different and unique location in space—that of the receiver.

Due to Factor 1, the eavesdropper must first decide on its joint signal constellation. This precedes deciphering (mapping bits to joint symbols) and could prove to be a difficult task, since the joint samples are noisy and the joint constellation changes with every new pilot from the receiver.

The deterioration of the signal at the eavesdropper due to Factor 2 is substantial when the eavesdropper is far from the receiver and is difficult to evaluate as it depends greatly on the multipath propagation of the transmitted signal. Factor 2 could be compromised when the eavesdropper is close enough to the receiver.

Due to Factor 3, the asymptotic decoding complexity of the eavesdropper is $O(2^N)$, corresponding to an exhaustive search over all possible constellation points. It would be shown in Section 5 that the asymptotic decoding complexity of the receiver is $O(N)$. The difference in complexity can become substantial for small N as well. For example, for $N = 5$ the receiver would be required to perform five simple calculations per symbol, while the eavesdropper would have to calculate and compare 32 Euclidean distances. Although the decoding complexity of the eavesdropper is expected to be high, it is prudent to assume that the eavesdropper might have unlimited computational power, which would allow it to perform ML detection using exhaustive search, so Factor 3 could be compromised.

Due to Factor 4, the eavesdropper has to perform decoding using a suboptimal joint symbol constellation and is expected to suffer a considerable penalty on *Bit Error Rate* (BER) compared to the receiver. The exact decoding loss depends on the number of transmitters, and the characteristics of the channel which prevents a general analysis. Evaluation of decoding loss for three transmitters over a Rayleigh channel is given in Section 6.

The eavesdropper could use soft decoding and reception using multiple antennas to achieve decoding gains. However, at least some of the gains can be matched by the receiver. The illustrative scenario provided in Section 6 demonstrates that the required gain to match the receiver's hard-decoding BER is 20 dB for three transmitters in Rayleigh fading.

5. Practical Implementation

JCMA is based on superposition modulation with joint decoding. Superposition modulation schemes require accurate symbol synchronization and power control, and are adversely affected by mobility. These limitations are commonly deemed prohibitive in practical applications. Although superposition modulation is assumed in many theoretical works, practical means of implementation are usually not addressed, see [28–32], for examples.

To implement JCMA, robust joint signal constellations and the transmitters' symbols sets that construct them must be found offline. The joint constellations must not result in performance loss. Efficient low complexity joint decoding must be formulated as well. The expected increased sensitivity to synchronization and power control errors must be mitigated without increasing implementation complexity. These issues are addressed in what follows.

5.1. Joint Signal Constellations

5.1.1. Decoding Gain for Power Limited Transmitters. The overall signal energy collected by the receiver's MF in JCMA grows with the number of transmitters. However, this does not necessarily mean that performance would be enhanced. The BER of ML detection in Gaussian noise is governed by the Euclidean distance between points in the constellation [35]. A key requirement for enhancing performance with JCMA is that the increased energy per joint symbol translates to an increase in the minimal Euclidean distance. In what follows, a probabilistic approach is taken to prove that this is indeed the case.

From (2),

$$y_N = \sum_{n=1}^{N} s_n, \tag{18}$$

where the index N is introduced to denote that y was created by N transmitters.

Assuming equal probability for each transmitted symbol per transmitter,

$$\Pr\left(s_n = s_l^n\right) = 2^{-M}, \quad l = 1, 2, \ldots, 2^M. \tag{19}$$

Let μ_n and σ_n^2 denote the mean value and the variance of the RV s_n, respectively. It is assumed that the transmitters transmit independent data and, therefore, $\{s_n\}_{n=1}^N$ are mutually independent. For N sufficiently large, y_N is a complex normal RV with mean $\mu_N = \sum_{n=1}^N \mu_n$ and variance

$$\sigma_N^2 = \sum_{n=1}^{N} \sigma_n^2. \tag{20}$$

The following RV is defined

$$\Delta_N \overset{\text{def}}{=} y_N^{(1)} - y_N^{(2)}, \tag{21}$$

where $y_N^{(1)}$ and $y_N^{(2)}$ are two received constellation points. Since the probability for receiving one joint constellation point is independent of the probability for receiving any other constellation point, $y_N^{(1)}$ and $y_N^{(2)}$ are independent RVs. Also, $y_N^{(1)}$ and $y_N^{(2)}$ are characterized by complex normal distributions with mean μ_N and variance σ_N^2. Another RV is defined as

$$\rho_N \overset{\text{def}}{=} |\Delta_N|^2, \tag{22}$$

where ρ_N has a chi-squared distribution with two degrees of freedom and its PDF is given by [36]

$$f_{\rho_N}(x) = \frac{\exp\left(-x/2\sigma_N^2\right)}{2\sigma_N^2}, \tag{23}$$

where ρ_N is the squared Euclidean distance between two randomly chosen points from the joint constellation. It follows that for Gaussian noise, ρ_N governs system performance as it is directly related to BER.

To proceed, let us define a d_N^2 such that

$$\Pr\left(\rho_N > d_N^2\right) = 1 - \delta, \tag{24}$$

where δ is a small positive number. However, (24) means that the probability that the Euclidian distance between two arbitrarily chosen points from the joint constellation would be greater than d_N is very close to 1.

Let us find d_N^2 that satisfies (24). From (23),

$$\Pr\left(\rho_N > d_N^2\right) = \int_{d_N^2}^{\infty} f_{\rho_N}(x)dx = \exp\left(-\frac{d_N^2}{2\sigma_N^2}\right). \tag{25}$$

Introducing (24) to (25) yields

$$d_N^2 = -2\sigma_N^2 \ln(1-\delta) = \sigma_N^2 \ln\left[(1-\delta)^{-2}\right]. \tag{26}$$

From (20), it follows that $\sigma_{N+1}^2 > \sigma_N^2$, therefore, from (26),

$$d_{N+1}^2 > d_N^2. \tag{27}$$

The minimum distance increases (in a probability sense) as N increases. In other words, the increased energy reaching the receiver is translated to increased distance between joint constellation points at the receiver.

Now consider a *Time Division Multiple Access* (TDMA) system with power limited transmitters and the same data rate as a JCMA system. To maintain the same data rate as that of the JCMA system, the constellation of each transmitter would have to become more crowded as N increases. Because the overall constellation power remains constant, the minimal distance of the received constellation would decrease and performance would deteriorate.

5.1.2. Suboptimal Symbol Search. To find the optimal joint constellation, one must solve (3), (4) analytically. The goal is to find BB symbol sets which maximize the minimal Euclidean distance in the resulting joint symbol constellation. This is an optimization problem with quadratic constraint. While a closed form solution may be found under limiting assumptions, this approach is avoided and suboptimal search methods are used instead. This alternative approach is justified because optimization is done only once for a set of transmitters and is performed offline, so there is no need for a fast real-time solution.

For simplicity of presentation it is assumed that each transmitter has two symbols in its symbol set, which means that each transmitter has a single information bit represented in the joint constellation (or chip when forward error correction is employed). To make sure no transmission power is wasted, each BB symbol set is made to be a rotated and scaled version of *Binary Phase Shift Keying* (BPSK). This insures that the mean value of each BB symbol set and the mean value of the joint constellation are zero. The derivations that follow are easily applicable to more than one bit (chip) per symbol.

A random search approach can be used, for which symbol sets are found using a Monte Carlo simulation. A random set of BB symbols for each transmitter is randomly generated and is normalized to meet the power constraint in (4). The resulting joint constellation is derived and its minimal Euclidean distance as defined in (3) is evaluated. This process is repeated in numerous trials and the collection of BB sets which result in the best joint constellation is chosen. It is possible to add constraints on the BB symbol sets sizes to comply with *Quality of Service* (QoS) demands. In addition, the peak power constraints may vary across transmitters to address unequal channel fading attenuations which could represent near-far scenarios common in multiple access scenarios. Preliminary results for such optimization scenarios were presented in [37]. The solutions found with the random symbol search are asymptotically optimal as the number of search trials approaches infinity.

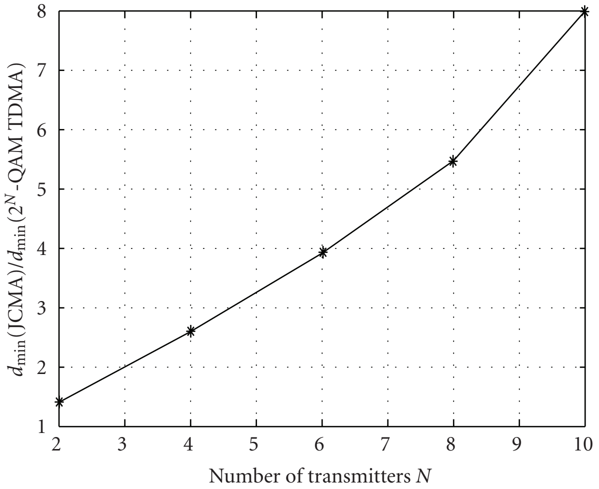

Figure 3: Performance gain buildup using random symbol search.

A parametric symbol search approach can be used as well. The phase and amplitude of each BB constellation point is quantized with some resolution. The resulting joint constellation is tested for each sample of phase and amplitude. The granularity of the parametric search increases with the quantization resolution, and the result is asymptotically optimal for infinitely small granularity.

To explore the proposed approach the joint constellation for N transmitters was optimized using a random symbol search. For comparison, a TDMA system using a 2^N-QAM constellation is used, which results in the same overall bit rate. Figure 3 displays the gain in $d_{\min}$ for the received constellations. It is clearly seen that JCMA results in better constellations for all tested N. This result shows that the performance gain buildup proven before is achievable using the random symbol search approach and that JCMA is energy efficient. An example of a joint constellation obtained via random symbol search is given in Section 6.

5.2. Maximum Likelihood Detection. The received joint signal sample at the MF output is to be decoded based on the expected joint constellation using ML detection. ML detection in the presence of Gaussian noise boils down to finding the constellation point which is closest to the received sample (minimal Euclidean distance). Performing ML detection using exhaustive search over all possible constellation points has algorithmic complexity of $O(2^N)$. This complexity grows exponentially with the number of transmitters. For systems with constrained resources, exhaustive search might be impractical to implement even for small values of N. For example, $N = 3$ requires calculating and comparing eight Euclidean distances for every received symbol. This complexity problem exists for any single transmitter user constellation with 2^N constellation points. Traditionally, in point-to-point systems the decoding complexity is reduced by using suboptimal constellations such as rectangular QAM. Suboptimal constellations are designed to exhibit structural symmetries which are used for efficient decoding of the received samples [38].

The JCMA constellation exhibits structural symmetries as well. Using a simple manipulation on the expression for the received joint symbol gives

$$y_N = s_i + \sum_{\substack{n=1\\ n\neq i}}^{N-1} s_n; \quad i = 1,\dots,N. \tag{28}$$

Symmetry lines can be drawn between the BB symbols of s_i shifted to $\sum_{\substack{n=1\\ n\neq i}}^{N-1} s_n$. If the symmetry lines are drawn for all $i = 1,\dots,N$ symbol sets, the receiver's observation space is divided to decision regions with a constellation point at the center of each region. The ML decoding problem in Gaussian noise reduces to finding the decision region in which the received sample is located.

Assuming the angles of the symmetry lines with the *real* axis value in the complex plane are given by $\phi_i; i = 1,\dots,N$, the following guidelines for finding a computationally efficient ML decoding algorithm are defined.

(1) Rotate the received joint symbol sample r by an angle of φ_1: $q = r\ \exp(-j\phi_1)$.

(2) If $q_R = \mathrm{Re}(q)$ is to the right of the symmetry line intersection with the *real* axis, set $L_i = 1$, else set $L_i = 0$.

(3) Repeat steps 1,2 for all i.

(4) Use $L_i; i = 1,\dots,N$ to access a predefined *Look Up Table* (LUT) containing the bit loading of the constellation point in the decision region of the received sample.

The algorithmic complexity of the suggested efficient ML decoding is $O(N)$. This is also the complexity of traditional 2^N-QAM ML decoding of a single transmitter with equal rate to a JCMA system with N transmitters and 1 bit per symbol per transmitter.

5.3. Effects of Imperfect Power Control, Synchronization Errors and Mobility. JCMA requires synchronization between the transmitters at the symbol level. This is a higher synchronization demand than that of TDMA, for example. Methods with equivalent synchronization demands as those of JCMA are symbol-synchronous *Code Division Multiple Access* (CDMA) [26, 41], SM-SD [25], and the methods defined in [28–32]. In addition, JCMA demands a higher accuracy in power control. In this section, the effects of synchronization errors, power control errors, and mobility on JCMA are discussed. For coherency of presentation, the rigorous analysis leading to this discussion is given in Appendix A.

Lack of perfect synchronization is manifested by errors in the channel phase estimates, and inaccurate power control is manifested by errors in the channel amplitude estimate. It follows that both are accurately modeled by an additive complex RV representing an error in the channel estimate (CSI errors). The effects of CSI errors (phase and amplitude) on system performance are analyzed in a comparative manner to TDMA. Since the transmitters are required to be simple in design, we assume that each transmitter obtains its CSI by estimating the channel coefficient using some linear estimator, such as a linear *Minimum Mean Square Error* (MMSE) estimator.

In Appendix A the required energy of the JCMA receiver sent pilot signal is found with respect to that of a TDMA system, so that the JCMA system performance loss would be the same as the TDMA system performance loss. This analysis results in a quantitative estimate of the effects of synchronization and power control errors, and the required pilot energy to support the synchronization demands of JCMA. In Appendix A it is shown that in order to achieve the same synchronization/power control error in JCMA as that of TDMA while maintaining the decoding gain, the pilot energy used for channel estimation must have N times more energy. This increase in energy can be achieved by using longer pilots resulting in decreased throughput or by increasing pilot signal power. Alternatively, the performance gain can be waived by reducing the transmitters' power emission resulting in no need for increasing pilot energy.

In JCMA a pilot is sent every channel decorrelation time. In Appendix A the rate of pilot transmission for JCMA is calculated to achieve the same channel decorrelation as for TDMA. This analysis results in a quantitative estimate of the effects of mobility of transmitters and the required system resources to support such mobility (throughput loss due to pilot signal transmission). It is also shown that the JCMA system effectively shortens the channel decorrelation time. This results in a need for more frequent pilot transmission which causes throughput reduction. As far as security is concerned, the shortening of decorrelation time is a benefit. This is because faster variation in the channel allows for a higher cryptographic key generating rate. If the coding gain is waived by reducing power emission, the decorrelation time is the same for JCMA and TDMA and no overhead on throughout is incurred.

Following the analysis in Appendix A we define the following piloting rule: if the transmitters in a JCMA setting use all their available power, decoding gain and faster key generating rate are obtained at the expense of higher energy consumption. To support these benefits without degrading decoding the receiver's pilot energy must be increased times the number of transmitters. Alternatively, the decoding gain and fast channel decorrelation can be waived by reducing the transmitters' power emission. This would result in same energy consumption as that of a single transmitter and there would be no need to increase pilot energy.

5.4. Network Management. JCMA is expected to operate in a multiple access scenario. Multiple access scenarios require network management protocols to resolve near-far problems, facilitate QoS requirements, and optimize the overall data throughput.

In the classical CDMA near-far scenario, a dominant transmitter deprives other transmitters from service by masking their transmitted signal at the receiver. The solution is to use power-control by the receiver to reduce the power of the dominant transmitter so that other transmitters can be detected as well. In JCMA each transmitter adjusts its power emission according to channel fading and the symbol set it is assigned by the receiver. The receiver can solve near-far scenarios by assigning symbol sets which should be received with low power to transmitters with higher attenuating channels. Transmitters with lower attenuating channels can be assigned a symbol set with higher power in the joint constellation.

Another possible solution is to match transmitters into JCMA groups according to the channel they experience over different subcarriers. This is an extension of *OFDM-Access* (OFDMA). In OFDMA subcarriers are allocated to different transmitters according to the quality of their channel over the frequency selective bandwidth. The basic idea is to allocate parts of the bandwidth to each transmitter in an efficient way so that the overall network throughput is increased. In JCMA transmitters should be grouped to facilitate the construction of the joint signal constellation at the receiver with minimal power-loss due to power reduction at the dominant transmitters.

In addition, it is possible to perform offline optimization of symbol sets to resolve specific near-far scenarios. The resulting symbol sets would be kept at the transmitters' symbol sets tables and used when the receiver dims it appropriate. This possibility does not exist in a classical CDMA system.

Offline optimization of symbol sets can be defined with different sizes of the transmitters' symbols sets. A transmitter with a larger symbol set size would be represented at the joint constellation with more bits and so its throughout would be higher than that of the other transmitters.

6. Illustrative Scenario—Rayleigh Fading

Performance in Rayleigh fading channels is evaluated in what follows. First, the channel conditions for achieving information theoretic security are depicted for various N in accordance with the condition in (17). Following analysis of information theoretic security, a JCMA setting of three transmitters is depicted, including generating the joint constellation and an algorithm for efficient ML decoding. The effects of security factors 1, 3, and 4 described before are evaluated and demonstrated as well. A scenario with three transmitters was also used in the preliminary analysis given in [40].

6.1. Information Theoretic Security. Recall that α in (17) has to be set according to the temporal decorrelation behavior of the channel. The normalized temporal autocorrelation function for a Rayleigh fading channel is given by [33]

$$R(\tau) = J_0(2\pi B_d \tau), \tag{29}$$

where $J_0(\cdot)$ is the zero-order Bessel function of the first kind and τ is the time difference. $J_0(2.4) \approx 0$ for the shortest elapsed time. This is equivalent to setting $\tau = 2.4/2\pi B_d$ in (29), so it makes sense to set $\alpha = T_d B_d(2.4/2\pi) = 0.382$.

Using $\alpha = 0.382$ in (17) results in

$$B_d \geq \frac{(1-\eta)0.382 B_c}{N}. \tag{30}$$

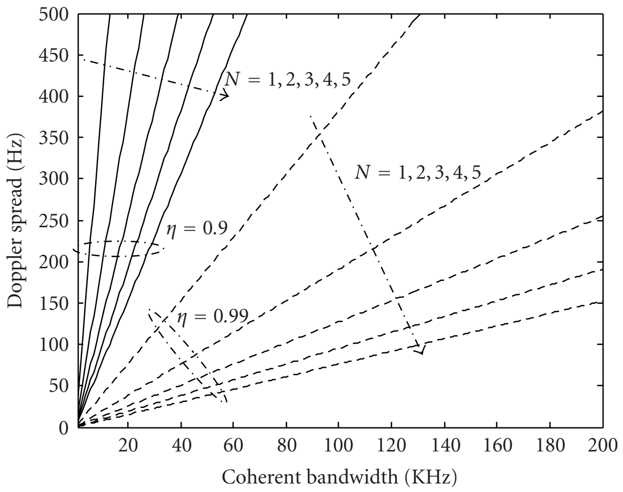

FIGURE 4: Minimal Doppler spread for security, Rayleigh fading; $N = 1, 2, 3, 4, 5$.

Figure 4 depicts the minimum B_d required for achieving information theoretic security for the entire channel decorrelation period as a function of B_c for $N = 1, 2, 3, 4, 5$ and $\eta = 0.9, 0.99$. The arrows directions indicate increasing values of N. It is evident that increasing N lowers the required B_d dramatically for a given B_c. The decrease is moderated as N increases. For $\eta = 0.9$, the required B_d is very high, making it difficult to use the method for securing the entire decorrelation period. However, for $\eta = 0.99$, the required B_d is reasonably low for practical channels. For example, consider the IEEE 802.16*e* standard (a.k.a. mobile WiMax) [42]. In [42] the delay spread is assumed to be $10\,\mu$s, which means that $B_c = 100$ kHz. For this value of B_c, the Rayleigh fading channel achieves security for $N = 1, 2, 3, 4, 5$ when $B_d \geq 382$ Hz, 191 Hz, 127 Hz, 96 Hz, 76 Hz, respectively. Assuming a carrier frequency of $f_c = 3.5$ GHz, these values of B_d correspond to relative velocities between transmitter and receiver of $v \geq 60, 30, 20, 15, 12$ [km/h], respectively. These velocities are expected for many mobile scenarios.

6.2. Security by Complexity—Three Transmitters. In this illustrative Rayleigh fading scenario, subcarriers are overloaded by 3 transmitters in a JCMA setting. The symbol sets $S_n, n = 1, 2, 3$ were found using a random symbol search with $\max\{d_{\min}\}$ defined in (3) being the optimizing criterion and (4) being the optimization constraint. The following symbol sets were found offline and assigned arbitrarily to the transmitters:

$$\begin{aligned} S_1 &= \{0.7124\exp(-j2.5558); 0.7124\exp(j0.5858)\}, \\ S_2 &= \{0.9965\exp(j1.3720); 0.9965\exp(-j1.7696)\}, \\ S_3 &= \{0.9890\exp(-j0.2016); 0.9890\exp(j2.9400)\}. \end{aligned} \tag{31}$$

The received joint constellation at the intended receiver along with the corresponding bit mapping is depicted in

Table 1: LUT for ML detection of the three transmitters scenario.

	$q_I < -0.775$	$-0.775 \leq q_I < 0.775$	$0.775 \leq q_I$
$q_R < -1.545$	If $(u_I < 0.555)$ 010 else 011	011	If $(u_R < -0.555)$ 011 else 001
$-1.545 \leq q_R < 0$	010	111	001
$0 \leq q_R < 1.545$	110	000	101
$1.545 \leq q_R$	If $(u_R < 0.555)$ 110 else 100	100	If $(u_I < -0.555)$ 100 else 101

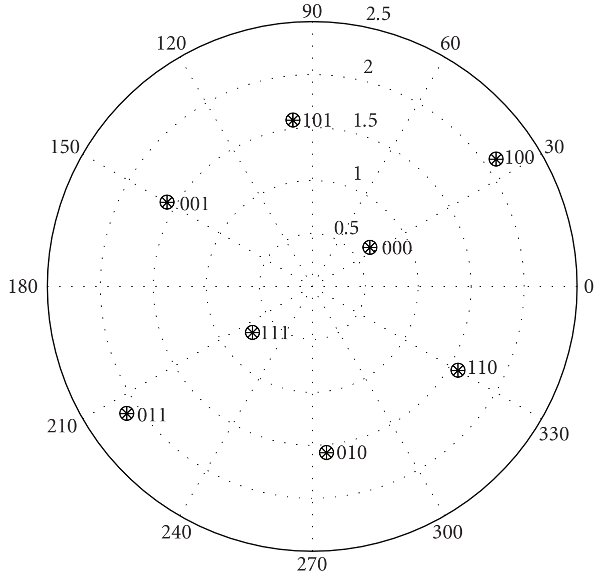

Figure 5: Joint constellation for the three transmitters scenario.

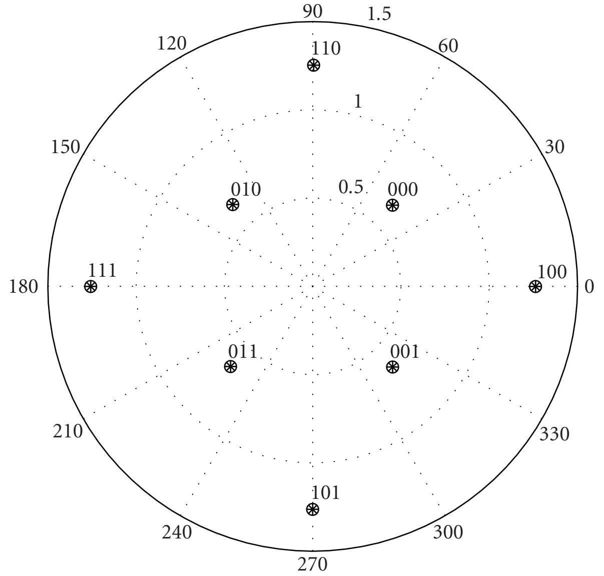

Figure 6: 8QAM constellation of TDMA reference system.

Figure 5. Each set of 3 bits represents the bits of TX1, TX2, and TX3 from left to right, respectively. Notice that the average energy of the received constellation is larger than 1. Interestingly, this joint constellation has the exact structure of a type of 8QAM constellation used in some industry standards for a single transmitter signal [43, page 53]. Note that the joint constellation is not Gray coded. Although this increases BER, it would be shown below that performance is satisfactory.

Next an efficient ML decoding algorithm is designed, based on constellation symmetries. The algorithm comprises three steps for decoding a received joint sample r.

(1) Rotate the received sample: $q = r\ \exp(-j\,0.1865\pi)$.

(2) Calculate

$$\begin{aligned} q_R &= \mathrm{Re}(q), \\ q_I &= \mathrm{Im}(q), \\ u_R &= \mathrm{Re}\left(q * \exp\left(-\frac{j\pi}{4}\right)\right), \\ u_I &= \mathrm{Im}\left(q * \exp\left(-\frac{j\pi}{4}\right)\right). \end{aligned} \tag{32}$$

(3) Use Table 1 for decoding.

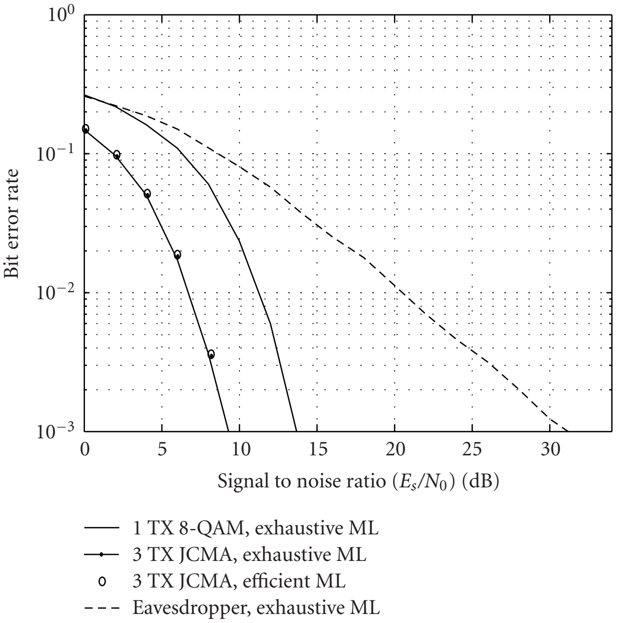

Figure 7: Performance curves for the three transmitters scenario.

For hard decoding, each table entry denotes the decoded bits of TX1, TX2, and TX3 from left to right, respectively. For soft decoding, the distance between q and the closest

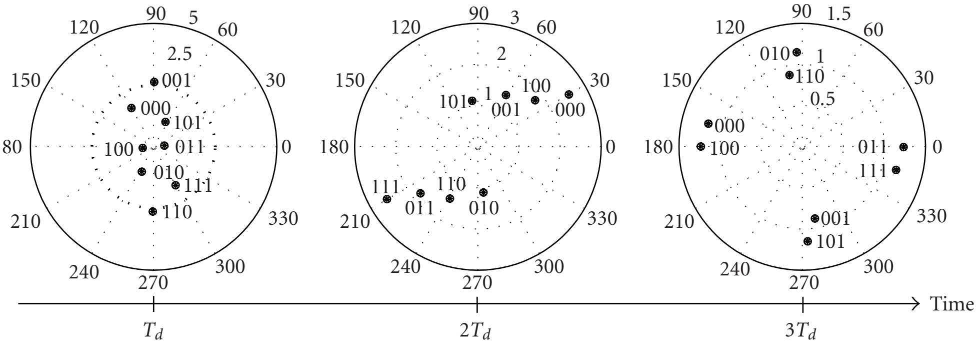

Figure 8: Consecutive joint constellations of eavesdropper.

joint constellation point has to be evaluated. This efficient decoding algorithm consists of three easy steps and its complexity is much lower than that of exhaustive ML decoding. The JCMA setting is compared to a TDMA transmitter using a power efficient circular 8-QAM constellation with the same power constraint. The 8-QAM constellation is depicted in Figure 6.

In Figure 7, hard decoding BER versus SNR (defined here as the ratio between the average energy per transmitter symbol and the noise variance at the receiver) is depicted for the JCMA setting and compared to TDMA. Results were obtained using computer simulation. A gain of 4.4 dB is achieved with JCMA while adhering to the transmitters' power constraint. This means that the increased overall energy invested in JCMA (3 times more than TDMA, equivalent to 4.7 dB) was successfully translated to performance gain. The marginal loss of 0.3 dB is attributed to the lack of Gray coding. Note that the efficient ML decoding algorithm performs as well as the exhaustive ML decoding algorithm.

To analyze the impact of security Factor 4 described in Section 4.2, BER of the receiver is also compared to that of an eavesdropper using a single MF and exhaustive ML hard decoding. Both receiver and eavesdropper experience a Rayleigh fading on all channels. It is clear that for the eavesdropper ML decoding BER is unsatisfactory for decoding the data. For example, if the receiver operates at E_s/N_0 of 9 dB, it would experience a BER of 10^{-3}, and the eavesdropper would experience a BER of 10^{-1}. It follows that for the given scenario the eavesdropper cannot effectively decode the messages from the nodes, even when the unicity distance has passed and security factors 1–3 described in Section 4.2 are compromised.

The eavesdropper can reduce BER by applying soft decoding instead of hard decoding and also apply multiple antennas reception. However, to match the receivers hard decoding BER of 10^{-3} the eavesdropper would need to achieve an SNR gain of 20 dB, and at least some of the gain achieved by the eavesdropper would be matched by implementing low complexity soft decoding at the receiver. It follows that the decoding complexity of the eavesdropper must be high enough to obtain an SNR gain of at least 20 dB. The SNR gain required at the eavesdropper for decoding is a clear indication of security by complexity.

To gain insight on the impact of security factors 1 and 3 described in Section 4.2 on decoding, representative joint constellations of the eavesdropper are depicted in Figure 8. Note how the joint constellation varies from pilot to pilot, implying the high decoding complexity. In addition, note how close the constellation points are to one another, implying the high probability for decoding errors.

7. Conclusion

A multiple access method for securing OFDM over wireless time-varying channels was proposed and analyzed. The method uses reverse piloting for implementing superposition modulation with joint decoding at the receiver. It makes use of channel randomness, reciprocity, and fast decorrelation in space to secure transmission with low overheads. Security strengths of the method were evaluated and practical means of implementation were suggested based on analytical analysis. Channel and system parameters were explicitly derived for achieving information theoretic security of entire transmission bursts, and features of security by complexity were assessed and demonstrated. Means for generating and efficiently decoding joint constellations were presented. It was proven that in addition to security, the method also offers decoding gain for power-limited transmitters. The effects of imperfections due to mobility, power control errors, and synchronization errors were analyzed and practical means for addressing them were given. It was proven and demonstrated that both security strength and decoding gain increase with the number of transmitters and that information theoretic security with low overheads is achievable for mobile scenarios in practical communication systems. Implementing the method requires the same computational complexity as a standard point-to-point communication system, and mitigating the effects of mobility, power control errors, and synchronization errors reduces to a simple piloting rule. The low computational complexity and feasibility of implementation make the method a good solution for securing OFDM transmission in wireless systems where the complexity associated with implementing traditional security algorithms is prohibitive.

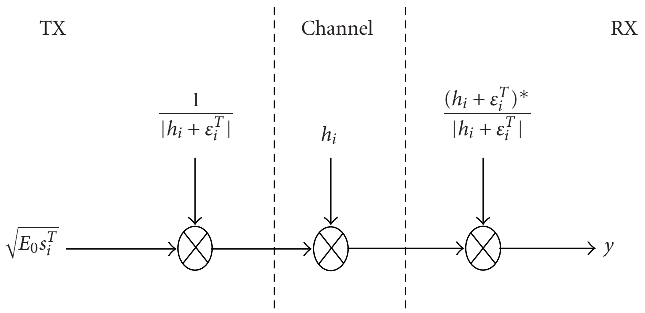
TX
Channel
RX
$\frac{1}{|h_i+\varepsilon_i^T|}$
h_i
$\frac{(h_i+\varepsilon_i^T)^*}{|h_i+\varepsilon_i^T|}$
$\sqrt{E_0}s_i^T$
y

Figure 9: Single transmitter in TDMA.

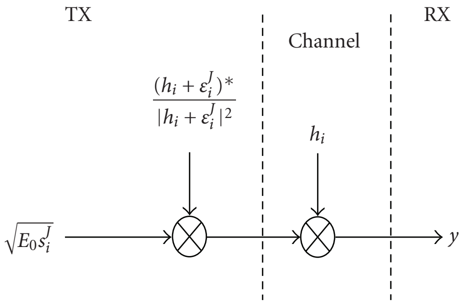

Figure 10: Single transmitter in JCMA.

Appendix

A. Effects of Imperfections on Performance

A.1. Synchronization and Power Control Errors

TDMA reference system. The TDMA BB model for a single transmitter (indexed i) with CSI errors and power control is depicted in Figure 9, where E_0 is the energy per symbol needed at the receiver to achieve a certain performance level, h_i is the complex valued channel fading coefficient, s_i^T is the TDMA symbol, and ε_i^T is the channel estimation error.

Since the transmitters are required to be simple in design, we assume that a linear estimator is used at each transmitter for estimating the channel coefficient, such as a linear MMSE estimator. For MMSE estimators, ε_i^T is modeled as a complex normal random variable with zero mean and arbitrary variance [44–49], and ε_i^T is uncorrelated with h_i.

At RX, the channel is estimated and compensated for phase by an erroneous estimate of the channel $(h_i+\varepsilon_i^T)^*/|h_i+\varepsilon_i^T|$. The channel estimated at RX is fed back to the transmitter for allowing the transmitter to compensate for channel fading before performing power control. It is assumed this is done without error. It follows that, $1/|h_i+\varepsilon_i^T|$ represents the TX compensation for fading.

Power control is achieved by setting $\sqrt{E_0}$ and compensating for the fading $|h_i|$. It follows that

$$y = \sqrt{E_0}s_i^T\frac{h_i}{\left(h_i+\varepsilon_i^T\right)}. \tag{A.1}$$

Since channel estimation has to be fairly accurate, the pilot energy is such that high SNR is achieved for channel estimation. It follows that ε_i^T is expected to be much smaller in magnitude than h_i and so $\Pr(|h_i| \ll |\varepsilon_i|) \approx 1$. Using this assumption (A.1) reduces to

$$\begin{aligned} y &= \sqrt{E_0}s_i^T h_i\left(\frac{1}{h_i\left(1+\varepsilon_i^T/h_i\right)}\right) \approx \sqrt{E_0}s_i^T h_i\frac{1}{h_i}\left(1-\frac{\varepsilon_i^T}{h_i}\right) \\ &= \sqrt{E_0}s_i^T - \sqrt{E_0}s_i^T\frac{\varepsilon_i^T}{h_i}. \end{aligned} \tag{A.2}$$

The term $z^T \overset{\text{def}}{=} \sqrt{E_0}s_i^T(\varepsilon_i^T/h_i)$ represents the synchronization error and its variance is with relation to δ.

JCMA System. The JCMA BB model for a single transmitter with CSI errors and power control is depicted in Figure 10, where s_i^J and ε_i^J are the JCMA transmitted symbol and channel estimation error of transmitter i, respectively.

Here the channel is estimated at TX alone and is compensated prior to transmission. In the same manner as in (A.2) it follows that for a single transmitter,

$$\begin{aligned} y &= \sqrt{E_0}s_i^J\frac{\left(h_i+\varepsilon_i^J\right)^* h_i}{\left|h_i+\varepsilon_i^J\right|^2} = \sqrt{E_0}s_i^J\frac{h_i}{\left(h_i+\varepsilon_i^J\right)} \\ &\approx \sqrt{E_0}s_i^J + \sqrt{E_0}s_i^J\frac{\varepsilon_i^J}{h_i}. \end{aligned} \tag{A.3}$$

The last estimation in (A.3) is given using a Taylor expansion with $|\varepsilon_i^J| \ll |h_i|$. The synchronization error of a single transmitter in JCMA $z^J \overset{\text{def}}{=} \sqrt{E_0}s_i^J(\varepsilon_i^J/h_i)$ has the same statistics as that of TDMA.

Now consider the entire JCMA system:

$$y = \sum_{i=1}^{N}\left(\sqrt{E_0}s_i^J + \sqrt{E_0}s_i^J\frac{\varepsilon_i^J}{h_i}\right) = \sum_{i=1}^{N}\left(\sqrt{E_0}s_i^J\right) + \sum_{i=1}^{N}\left(\sqrt{E_0}s_i^J\frac{\varepsilon_i^J}{h_i}\right). \tag{A.4}$$

The JCMA synchronization error is $Z^J \overset{\text{def}}{=} \sum_{i=1}^{N}(\sqrt{E_0}s_i^J(\varepsilon_i^J/h_i))$.

The estimation errors ε_i^J; $i = 1, 2, \ldots, N$ are uncorrelated and identically distributed. The same is true for the channels h_i and information symbols s_i^J. It follows that

$$\operatorname{var}\left(Z^J\right) = N\operatorname{var}\left(z^J\right). \tag{A.5}$$

The channel is estimated at TX using a pilot signal from RX. Channel estimation using pilot signaling is well established in theory and practice [44–49], and an "efficient estimate" as defined in [50] is obtained. This means that the *Cramer Rao Bound* (CRB) for the channel estimation error is achievable.

It is assumed that all transmitters are able to compensate for the channel fading $|h_i|$ with their limited peak power. This means that $|h_i|$ is higher than some threshold value. If $|h_i|$ falls beneath this threshold the transmitter fails to compensate for it and the connection between this transmitter and the receiver cannot be maintained. This phenomenon occurs in all multiple access methods in fading channels and is usually solved at a high level protocol. In cellular telephony, for example, a failing transmitter roams to a different *Base Station* (BS) for service.

The CRB for efficient ML estimation of a random variable in AWGN is given by [50]

$$\operatorname{var}(\varepsilon) = \operatorname{var}(h)\left(\frac{2\operatorname{var}(h)E_p}{N_0}\right)^{-1}, \tag{A.6}$$

where E_p is the energy of the pilot symbol, and N_0 is the AWGN noise variance.

Using (A.6), it is possible to calculate the needed increase in pilot energy for JCMA in order to achieve the same synchronization/power control error as that of TDMA. For this the error variances must be equated:

$$\operatorname{var}\left(Z^J\right) = \operatorname{var}\left(z^T\right). \tag{A.7}$$

Since the variance of a sum is the sum of variance, (A.7) is also

$$N\operatorname{var}\left(z^J\right) = \operatorname{var}\left(z^T\right) \tag{A.8}$$

Equivalently, in accordance with (A.2), (A.4):

$$N\ \operatorname{var}\left(\sqrt{E_0}s_i^J\frac{\varepsilon_i^J}{h_i}\right) = \operatorname{var}\left(\sqrt{E_0}s_i^T\frac{\varepsilon_i^T}{h_i}\right), \tag{A.9}$$

where $s_i^J, \varepsilon_i^J, s_i^T, \varepsilon_i^T, h_i$; $i = 1,\ldots,N$ are all uncorrelated and have zero mean, so (A.9) is also

$$\begin{aligned} &NE_0E\left(\left|s_i^J\right|^2\right)E\left(\left|\varepsilon_i^J\right|^2\right)E\left(\left|\frac{1}{h_i}\right|^2\right) \\ &\quad = E_0E\left(\left|s_i^T\right|^2\right)E\left(\left|\varepsilon_i^T\right|^2\right)E\left(\left|\frac{1}{h_i}\right|^2\right). \end{aligned} \tag{A.10}$$

Note that $E(|1/h_i|^2) < \infty$ because it is assumed that the transmitter can compensate for fading, so $|h_i|^2$ is higher than some threshold. According to the peak power constraint, $E(|s_i^J|^2) = E(|s_i^T|^2)$, and (A.10) reduces to

$$NE\left(\left|\varepsilon_i^J\right|^2\right) = E\left(\left|\varepsilon_i^T\right|^2\right). \tag{A.11}$$

Now using (A.6),

$$N\operatorname{var}(h)\left(\frac{2\operatorname{var}(h)E_p^J}{N_0}\right)^{-1} = \operatorname{var}(h)\left(\frac{2\operatorname{var}(h)E_p^T}{N_0}\right)^{-1}. \tag{A.12}$$

Equation (A.12) reduces to the compact expression:

$$E_p^J = NE_p^T. \tag{A.13}$$

Equation (A.13) gives the required energy of the JCMA pilot signal sent by the receiver to achieve the same degradation in decoding as for an equivalent TDMA system.

A.2. Mobility and Channel Decorrelation. Channel decorrelation manifests itself in a shift of the joint constellation points from their original position. The probability for a more significant shift increases as time passes from the last channel estimation time (pilot transmission time). It follows that channel decorrelation directly influences the shift in constellation points over time. We evaluate this influence by deriving the expected shift of a constellation point over time. A closely related approach is used when evaluating transmitter performance in the presence of linear and nonlinear distortions using *Error Vector Magnitude* (EVM) [51–53]. EVM is a well-founded parameter used to characterize the quality of communication and is closely related to BER [51–53].

An EVM-like approach is used here for JCMA. Disregarding the additive noise and errors in the channel estimate at the receiver, the received constellation points of any communication system are supposed to remain constant over time. However, as the channel decorrelates the points shift randomly, due to a discrepancy between the last channel estimate and the true value of the time-varying channel.

The shift of a specific constellation point over time is a stochastic process defined as

$$\Delta y_0(t) = y_0(t) - y_0(t_0), \tag{A.14}$$

where $t_0 \leq t$ is the last time the channel was estimated (a pilot signal was sent) and $y_0(t_0) \in y$, where y denotes the constellation set. For ease of notation the ^{J} index is dropped from the following derivation. There is a one to one mapping between $\underline{x} \equiv [x_1, x_2, \ldots, x_N]$; $x_i \equiv s_ih_i(t_0)$ and $y_0(t)$ given by

$$y_0(t) = \sum_{i=1}^{N}[x_ih_i(t)]. \tag{A.15}$$

It follows that

$$\Delta y_0(t) = \sum_{i=1}^{N}[x_ih_i(t)] - \sum_{i=1}^{N}[x_ih_i(t_0)] = \sum_{i=1}^{N}[x_i(h_i(t) - h_i(t_0))]. \tag{A.16}$$

In a classical EVM approach, the variance of $\Delta y_0(t)/\max_{y_0(t_0)}(|y_0(t_0)|^2)$ should be averaged over all points in the constellation. Because the focus of analysis is performance degradation of a communication link due to channel decorrelation, it would be biased in favor of JCMA to normalize $\Delta y_0(t)$, since higher overall energy is invested in the JCMA constellation. In the following analysis the conditional variance of $\Delta y_0(t)$ is evaluated without normalization and then averaged over all points in the constellation:

$$\begin{aligned}
&E(\Delta y_0(t) \mid \underline{x}) \\
&\quad = \sum_{i=1}^{N} [x_i(E(h_i(t)) - E(h_i(t_0)))] = 0,
\end{aligned} \tag{A.17}$$

$$\begin{aligned}
&\operatorname{var}(\Delta y_0(t) \mid \underline{x}) \\
&\quad = E\left(\left| (\Delta y_0(t) \mid \underline{x}) \right|^2 \right) \\
&\quad = E\left(\left\{ [y_0(t) \mid \underline{x} - y_0(t_0) \mid \underline{x}][y_0(t) \mid \underline{x} - y_0(t_0) \mid \underline{x}]^* \right\} \right) \\
&\quad = E\left(\left| (y_0(t) \mid \underline{x}) \right|^2 \right) + E\left(\left| (y_0(t_0) \mid \underline{x}) \right|^2 \right) \\
&\qquad - E(\{(y_0(t) \mid \underline{x})(y_0^*(t_0) \mid \underline{x})\}) \\
&\qquad - E(\{(y_0(t_0) \mid \underline{x})(y_0^*(t) \mid \underline{x})\}),
\end{aligned} \tag{A.18}$$

$$\begin{aligned}
&E\left(\left| y_0(t) \mid \underline{x} \right|^2 \right) \\
&\quad = E\left(\sum_{i=1}^{N} [x_i h_i(t)] \sum_{j=1}^{N} \left[x_j^* h_j^*(t) \right] \right) \\
&\quad = \sum_{i=1}^{N} \left[\sum_{j=1}^{N} \left[x_i x_j^* E\left(h_i(t) h_j^*(t) \right) \right] \right].
\end{aligned} \tag{A.19}$$

The channels are i.i.d, therefore,

$$\begin{aligned}
&E\left(\left| y_0(t) \mid \underline{x} \right|^2 \right) \\
&\quad = \sum_{i=1}^{N} \left(\sum_{j=1}^{N} \left(x_i x_j^* \delta_{i,j} \operatorname{var}(h) \right) \right) \\
&\quad = \operatorname{var}(h) \sum_{i=1}^{N} \left(|x_i|^2 \right),
\end{aligned} \tag{A.20}$$

where $\operatorname{var}(h) \equiv E(|h_i(t)|^2)$ for all $(i, t.)$,

$$\begin{aligned}
&E(\{y_0(t) y_0^*(t_0)\} \mid \underline{x}) \\
&\quad = E\left(\sum_{i=1}^{N} [x_i h_i(t)] \sum_{j=1}^{N} \left[x_j^* h_j^*(t_0) \right] \right) \\
&\quad = \sum_{i=1}^{N} \left(\sum_{j=1}^{N} \left(x_i x_j^* E\left(h_i(t) h_j^*(t_0) \right) \right) \right) \\
&\quad = \sum_{i=1}^{N} \left(|x_i|^2 E(h_i(t) h_i^*(t_0)) \right) \\
&\quad = \sum_{i=1}^{N} \left(|x_i|^2 R(t) \right),
\end{aligned} \tag{A.21}$$

where $R(t) \overset{\text{def}}{=} E(h_i(t) h_i^*(t_0))$ is the channel autocorrelation function and depends on the channel fading statistics. Notice that since the in-phase and quadrature components of all channels are uncorrelated, $R(t)$ is a real function and, therefore, $R(t) = E(h_i(t) h_i^*(t_0)) = E(h_i(t_0) h_i^*(t))$. It follows that

$$E(\{y_0(t_0) y_0^*(t)\} \mid \underline{x}) = \sum_{i=1}^{N} \left(|x_i|^2 R(t) \right). \tag{A.22}$$

Using (A.20), (A.21), (A.22) in (A.18) yields

$$\begin{aligned}
&\operatorname{var}\left(\Delta y_0^J(t) \mid \underline{x}^J \right) \\
&\quad = 2 \sum_{i=1}^{N} \left(\left| x_i^J \right|^2 \right) (\operatorname{var}(h) - R(t)) \overset{\text{def}}{=} \operatorname{var}\left(\Delta y_0^J(t) \right),
\end{aligned} \tag{A.23}$$

where the superscript J was reintroduced.

For TDMA this variance is given by

$$\begin{aligned}
&\operatorname{var}\left(\Delta y_0^T(t) \mid x_i^T \right) \\
&\quad = \operatorname{var}\left(\Delta y_0^J(t) \mid \underline{x}^J \right)|_{N=1} = 2 \left| x_i^T \right|^2 (\operatorname{var}(h) - R(t)),
\end{aligned} \tag{A.24}$$

where $x_i^T \equiv s_i^T h_i(t_0)$. Obviously, $\operatorname{var}(\Delta y_0^T(t)) < \operatorname{var}(\Delta y_0^J(t))$ and $\operatorname{var}(\Delta y_0^J(t))$ increases with N. It is easy to show that if normalization of $\Delta y_0(t)/|y_0(t_0)|^2$ was initially introduced to (A.18), the result would have been the same for TDMA and JCMA.

To compare decorrelation times (A.23) and (A.24) should be equated. Let t_p^J and t_p^T be the time passed between consecutive pilots in JCMA and TDMA respectfully. Equating (A.23) and (A.24) yields

$$\operatorname{var}\left(\Delta y_0^T\left(t_p^T \right) \mid x_i^T \right) = \operatorname{var}\left(\Delta y_0^J\left(t_p^J \right) \mid \underline{x}^J \right). \tag{A.25}$$

Now, using (A.23) and (A.24) in (A.25),

$$2 \left| x_i^T \right|^2 \left(\operatorname{var}(h) - R\left(t_p^T \right) \right) = 2 \sum_{i=1}^{N} \left| x_i^J \right|^2 \left(\operatorname{var}(h) - R\left(t_p^J \right) \right). \tag{A.26}$$

The solution to (A.26) depends on the channel fading instance and the symbols being transmitted. Averaging over all channel instances and symbol types on both sides of (A.26) gives

$$\begin{aligned}
&2E\left(\left| x_i^T \right|^2 \right) \left(\operatorname{var}(h) - R\left(t_p^T \right) \right) \\
&\quad = 2 \sum_{i=1}^{N} E\left(\left| x_i^J \right|^2 \right) \left(\operatorname{var}(h) - R\left(t_p^J \right) \right),
\end{aligned} \tag{A.27}$$

$$\begin{aligned}
&E\left(\left| s_i^T \right|^2 \right) E\left(|h_i|^2 \right) \left(\operatorname{var}(h) - R\left(t_p^T \right) \right) \\
&\quad = \sum_{i=1}^{N} \left[E\left(\left| s_i^J \right|^2 \right) E\left(|h_i|^2 \right) \right] \left(\operatorname{var}(h) - R\left(t_p^J \right) \right).
\end{aligned} \tag{A.28}$$

However, $E(|s_i^T|^2) = E(|s_i^J|^2)$, $E(|h_i|^2) = \text{var}(h)$ for all i, so (A.28) reduces to

$$R\left(t_p^J\right) = \frac{R\left(t_p^T\right) + \text{var}(h)(N-1)}{N}. \qquad \text{(A.29)}$$

The functions $R(t_p^J)$ and $R(t_p^T)$ are monotonic decreasing functions until full decorrelation is reached for the first time, so if the inverse of (A.29) is taken and noting that $R(t=0) = \text{var}(h)$, we get

$$t_p^J = R^{-1}(\mu), \qquad \mu = \frac{R\left(t_p^T\right) + R(0)(N-1)}{N}. \qquad \text{(A.30)}$$

Rearranging μ gives

$$\mu = R\left(t_p^T\right) + \frac{(N-1)}{N}\left(R(0) - R\left(t_p^T\right)\right). \qquad \text{(A.31)}$$

Since $R(0) > R(t_p^T)$, $\mu > R(t_p^T)$ which means that $t_p^J < t_p^T$. It follows that JCMA effectively shortens the decorrelation time of the channel.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[2] U.S. National Bureau of Standards (NBS), "Data Encryption Standard," Federal Information Processing Standards Publication 46 (FIPS-46), 1977.

[3] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill, New York, NY, USA, 2002.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[5] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128–143, 2006.

[6] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38–47, 2004.

[7] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 122–130, 2006.

[8] G. Guimarães, E. Souto, D. Sadok, and J. Kelner, "Evaluation of security mechanisms in wireless sensor networks," in *Proceedings of the IEEE Systems Communications (ISWCS '05)*, pp. 428–433, August 2005.

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

[10] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell System Technical Journal*, vol. 63, pp. 2135–2157, 1984.

[11] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[12] A. O. Hero III, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, 2003.

[13] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[14] Y. Liang and H. V. Poor, "Secure communication over fading channels," in *Proceedings of the 44th Annual Allerton Conference on Communication Control, and Computing*, Monticello, Ill, USA, September 2006.

[15] Y. Liang, H. V. Poor, and S. Shamai, "Secrecy capacity region of fading broadcast channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '07)*, pp. 1291–1295, Nice, France, June 2007.

[16] Y. Liang, H. V. Poor, and S. Shamai, "Secrecy capacity region of parallel broadcast channels," in *Proceedings of the IEEE Information Theory and Applications Workshop (ITA '07)*, pp. 245–250, San Diego, Calif, USA, February 2007.

[17] M. Debbah and M. Kobayashi, "On the secrecy capacity of frequency-selective fading channels: a practical vandermonde approach," in *Proceedings of IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '08)*, pp. 1–5, Cannes, France, September 2008.

[18] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, no. 1, pp. 3–6, 1995.

[19] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, Alexandria, Va, USA, October 2007.

[20] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[21] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Communications Letters*, vol. 4, no. 2, pp. 52–55, 2000.

[22] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[23] G. R. Tsouri and D. Wulich, "Reverse piloting protocol for securing time varying wireless channels," in *Proceedings of the 7th Annual Wireless Telecommunications Symposium (WTS '08)*, pp. 125–131, Pomona, Calif, USA, April 2008.

[24] G. R. Tsouri and D. Wulich, "Joint Constellation Multiple Access—PCT patent pending," SigNexT Comm., (WO/2007/039908), http://www.wipo.int/pctdb/en/wo.jsp?IA=WO2007039908.

[25] A. Goldsmith, *Wireless Communications*, Cambridge University Press, Cambridge, UK, 2006.

[26] S. Verdu, *Multiuser Detection*, Cambridge University Press, Cambridge, UK, 1998.

[27] E. G. Larsson and B. R. Vojcic, "Cooperative transmit diversity based on superposition modulation," *IEEE Communications Letters*, vol. 9, no. 9, pp. 778–780, 2005.

[28] F. N. Brännström, T. M. Aulin, and L. K. Rasmussen, "Constellation-constrained capacity for trellis code multiple access systems," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '01)*, vol. 2, pp. 791–795, San Antonio, Tex, USA, December 2001.

[29] F. N. Brännström, T. M. Aulin, and L. K. Rasmussen, "Capacity considerations for trellis code multiple access systems," in *Proceedings of the IEEE Information Theory Workshop*, pp. 153–155, Cairns, Australia, September 2001.

[30] F. N. Brännström, T. M. Aulin, and L. K. Rasmussen, "Iterative detectors for trellis-code multiple-access," *IEEE Transactions on Communications*, vol. 50, no. 9, pp. 1478–1485, 2002.

[31] J. A. F. Ross and D. P. Taylor, "Vector assignment scheme for M+N users in N-Dimensional global additive channel," *IEEE Electronic Letters*, vol. 28, no. 17, pp. 1634–1636, 1992.

[32] J. A. F. Ross and D. P. Taylor, "Multiuser signaling in the symbol-synchronous AWGN channel," *IEEE Transactions on Information Theory*, vol. 41, no. 4, pp. 1174–1178, 1995.

[33] W. C. Lee, *Mobile Communication Engineering*, McGraw-Hill, New York, NY, USA, 1982.

[34] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.

[35] J. G. Proakis, *Digital Communication*, McGraw Hill, New York, NY, USA, 2000.

[36] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, McGraw-Hill, New York, NY, USA, 3rd edition, 1991.

[37] G. R. Tsouri and D. Wulich, "Wireless channel access through jointly formed signal constellations," in *Proceedings of the IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '06)*, pp. 1–5, San Diego, Calif, USA, September 2006.

[38] E. A. Lee and D. G. Messerschmitt, *Digital Communication*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1988.

[39] F. Vanhaverbeke, *Digital communications through oversaturated channels*, Ph.D. thesis, Ghent University, Ghent, Belgium, 2005, http://telin.ugent.be/~fv/eigen_publicaties.html.

[40] G. R. Tsouri and D. Wulich, "A Physical transmission security layer for wireless multiple access communication systems," in *Proceedings of the European Signal Processing Conference (EUSIPCO '07)*, Poznan, Poland, September 2007.

[41] S. Verdú, "Capacity region of gaussian CDMA channels: the symbol- synchronous case," in *Proceedings of 24th Allerton Conference on Communication, Control and Computing*, pp. 1025–1034, Urbana, Ill, USA, October 1986.

[42] IEEE, "Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications," IEEE Standard 802.16e, November 2005.

[43] ANSI/SCTE 79-1, "Data Over Cable Systems 2.0, Part 1: Radio Frequency Interface," 2003.

[44] Y. Li, "Pilot-symbol-aided channel estimation for OFDM in wireless systems," *IEEE Transactions on Vehicular Technology*, vol. 49, no. 4, pp. 1207–1215, 2000.

[45] O. Edfors, M. Sandell, J. J. D. Beek, S. K. Wilson, and P. O. Borjesson, "OFDM channel estimation by singular value decomposition," *IEEE Transactions on Communications*, vol. 46, no. 7, pp. 931–939, 1998.

[46] L. Berriche, K. Abed-Meraim, and J. C. Belfiore, "Cramer-rao bounds for MIMO channel estimation," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '04)*, vol. 4, pp. 397–400, Montreal, Canada, May 2004.

[47] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?" *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 951–963, 2003.

[48] M. Dong and L. Tong, "Optimal design and placement of pilot symbols for channel estimation," *IEEE Transactions on Signal Processing*, vol. 50, no. 12, pp. 3055–3069, 2002.

[49] X. Tang, M. S. Alouini, and A. J. Goldsmith, "Effect of channel estimation error on MQAM BER performance in rayleigh fading," *IEEE Transactions on Communications*, vol. 47, no. 12, pp. 1856–1864, 1999.

[50] H. L. Van Trees, *Detection, Estimation, and Modulation Theory—Part I*, John Wiley & Sons, New York, NY, USA, 2001.

[51] A. Georgiadis, "Gain, phase imbalance, and phase noise effects on error vector magnitude," *IEEE Transactions on Vehicular Technology*, vol. 53, no. 2, pp. 443–449, 2004.

[52] R. A. Shafik, M. S. Rahman, A. H. M. R. Islam, and N. S. Ashraf, "On the error vector magnitude as a performance metric and comparative analysis," in *Proceedings of the 2nd International Conference on Emerging Technologies (ICET '06)*, pp. 27–31, Islamabad, Pakistan, November 2006.

[53] J. L. Pinto and I. Darwazeh, "Error vector magnitude relation to magnitude and phase distortion in 8-PSK systems," *Electronics Letters*, vol. 37, no. 7, pp. 437–438, 2001.