Faster than Nyquist Interference Assisted Secret Communication for OFDM Systems

Arsenia Chorti[†,*], *Member, IEEE*, H. Vincent Poor[†], *Fellow, IEEE*
[†]Department of Electrical Engineering, Princeton University, Princeton, New Jersey 08544, USA
[*] Institute of Computer Science (ICS) of the Foundation for Research and Technology - Hellas
N. Plastira 100, Vassilika Vouton, GR-700 13 Heraklion, Crete, Greece
{achorti, poor}@princeton.edu

***Abstract*—Physical layer security techniques have emerged as promising candidates in order to achieve perfect secrecy in wireless communication systems. In this framework, an approach is proposed to enhance secrecy, taking advantage of topological and mobility asymmetries between a legitimate user and potential eavesdroppers. As a specific example, an Alamouti Orthogonal Frequency Division Multiplexing (OFDM) system with distributed mobile transmitters is investigated for underwater acoustic and radio frequency applications. The mobile transmitters independently emit pre-equalized - in terms of Doppler shifts - Alamouti OFDM symbols. As a result, the legitimate receiver effortlessly receives Doppler shift free copies of the OFDM symbols with standard diversity gains. On the contrary, eavesdroppers experience diversity gain compression and cross-symbol interference. A positive ergodic secrecy capacity is achievable even in the absence of an SNR advantage at the legitimate user.**

I. Introduction

Physical layer security has recently become a focal point of research due to the importance of its potential applications. Security is becoming an increasingly crucial issue in wireless applications and physical layer approaches can offer alternatives for building perfectly secure systems. The pioneering works of Wyner [1] and Csiszár and Körner [2] have demonstrated that a noisy communication channel offers opportunities for secret communication as long as the legitimate user has an SNR advantage. In particular, they demonstrated that in situations where the eavesdropper's channel is on average a degraded version of the main channel, a positive secrecy capacity can be guaranteed. Extending these results, analyses for the wireless fading channel [3] and Multiple-Input Multiple-Output (MIMO) systems [4] establish positive secrecy capacities even when on average the eavesdropper's channel can be better than that of the legitimate user.

However, in the aforementioned scenarios, the transmitter needs to know the instantaneous Channel Impulse Response (CIR) between the transmitter, the legitimate receiver and the eavesdropper, so that the transmission rate can be adapted accordingly. In the presence of a passive eavesdropper this is a very stringent requirement as the eavesdropper channel can only be described statistically. Furthermore, even if this issue is dealt with using opportunistic approaches, the resulting highly variable transmission rates may be unsuitable for a number of applications.

In order to overcome such difficulties, more proactive approaches have been proposed, relying on the injection of artificial noise into the network. Numerous helping-interferer approaches [5], [6], [7], [8] have been presented, making use of the idea of intentionally degrading the eavesdropper's SNR. In the present paper, this idea is extended; instead of degrading the eavesdropper SNR, our aim is to degrade the eavesdropper channel eigenvalues. We extensively discuss a possible scenario, making use of topological and mobility asymmetries between a legitimate user and potential eavesdroppers. As a specific example, an Alamouti Orthogonal Frequency Division Multiplexing (OFDM) system with distributed transmitters is analyzed. In a sense, this work introduces a qualitatively different approach in helping interferer techniques; our focus is on the received signal properties rather than the channel SNR. The merits of the proposed system are demonstrated by evaluation of the system ergodic secrecy capacity. The paper is structured as follows: Section II summarizes the main points in physical layer security for OFDM systems, the proposed system is described in Section III, the ergodic secrecy capacity is evaluated in Section IV, while Section V concludes the present work.

II. Secrecy Capacity of OFDM Systems

We assume an OFDM communication system with N carriers spaced $\Delta f = \frac{1}{T_s}$ Hz apart. The observation vectors at the Fast Fourier Transform (FFT) outputs in the legitimate and eavesdropping receivers can be described as

$$\mathbf{z}_{l/e} = \mathbf{H}_{l/e}\mathbf{d} + \mathbf{n}_{l/e}. \tag{1}$$

The indices l and e correspond to the legitimate receiver and the eavesdropper respectively, while the $N \times N$ matrices $\mathbf{H}_{l/e}$ denote the respective legitimate user and eavesdropper channel matrices; $\mathbf{d} = [d_1, \dots, d_N]^T$ is a sequence of independent and identically distributed (i.i.d.) symbols d_i and $\mathbf{n}_{l/e} = [n_{1,l/e}, \dots, n_{N,l/e}]^T$ are length N noise vectors of i.i.d. Gaussian random variables with variances $\sigma^2_{n,l/e} = \frac{N_{0,l/e}}{2}$. Due to the employment of cyclic prefixes and assuming slow fading environments, the matrices $\mathbf{H}_{l/e}$ are typically diagonal so that we have N parallel independent transmission channels.

This work was funded in part by the IOF "APLOE" (PIOF-GA-2010-274723) grant within the 7th Framework Program of the European Community and in part by the U. S. National Science Foundation Grant CNS-09-05398.

The OFDM system secrecy capacity can then be straightforwardly evaluated as [9], [10]

$$\begin{aligned} C_s &= (C_l - C_e)^+ \\ &= \left(\log\det(\mathbf{I} + \gamma_l \mathbf{H}_l \mathbf{H}_l^H) - \log\det(\mathbf{I} + \gamma_e \mathbf{H}_e \mathbf{H}_e^H)\right)^+ \\ &= \sum_{i=1}^{N} \left(\log \frac{1 + \gamma_l \lambda_i}{1 + \gamma_e \xi_i} \right)^+, \end{aligned} \tag{2}$$

with γ_l and γ_e denoting the SNR of the forward and wiretap channels respectively, λ_i and ξ_i denoting the eigenvalues of $\mathbf{H}_l \mathbf{H}_l^H$ and $\mathbf{H}_e \mathbf{H}_e^H$ respectively, $(\cdot)^H$ denoting the Hermitian of a matrix and $(\cdot)^+ = \max(\cdot, 0)$. Clearly, for those subchannels for which $\gamma_l \lambda_i > \gamma_e \xi_i$, we can transmit in perfect secrecy at a maximal rate of $\log \frac{1+\gamma_l \lambda_i}{1+\gamma_e \xi_i}$ if the i-th data symbol d_i is drawn from a Gaussian distribution.

III. Alamouti OFDM with Distributed Mobile Transmitters

Let us assume an Alamouti Space Time Block Coded (STBC) OFDM system [11]. In order to provide a systematic secrecy framework, we aim at generating asymmetries between the legitimate user and the eavesdropper. In the present case study, we assume ideally synchronized distributed mobile transmitters T_{x_0} and T_{x_1}, which independently choose their velocities and directions of movement, as shown in Fig. 1. At this stage, we further require that the transmitters' motions are completely random as perceived by the legitimate user R_x and the eavesdropper E_x and can be modeled as Brownian motions clocked at the OFDM symbol period T_s. As an example, the movement of the transmitters is controlled by the sampling of independent local random processes [12] or using hardware random number generators. The present paper is not concerned with the detailed design of such systems but rather with the proof of the concept presented, so the above idealizations are considered acceptable.

Under the above-mentioned scenario, each transmitter radiates a pre-equalized version of the Alamouti OFDM symbols, so that the Doppler shift at the legitimate receiver is canceled upon reception [13]. This fact does not necessarily mean that the legitimate receiver needs to be static, but rather that its movement pattern is a-priori known to the transmitters (and through abstraction to any eavesdropper). In summary, we make the following assumptions:

- At least in practical terms, no eavesdropper can predict the velocity and direction of movement of the mobile transmitters.
- All eavesdroppers can measure the relative velocities between the transmitters and the legitimate user and they can calculate their own Doppler shifts.
- The OFDM symbol duration is too short to allow any eavesdropper to adjust its velocity to match the Doppler shift at the legitimate receiver, implying that a residual Doppler shift will almost surely be present at any eavesdropper.

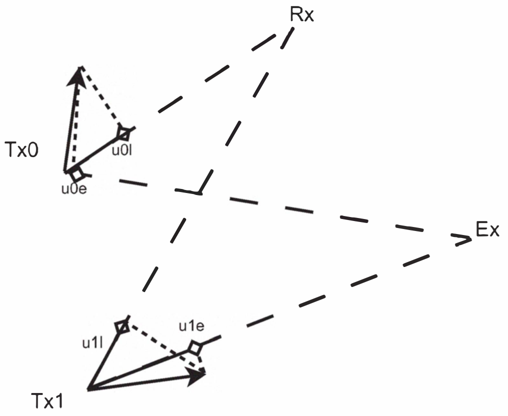

Fig. 1. Alamouti STBC OFDM system with distributed mobile transmitters.

A. System Description

In the following we employ a discrete (sampled) representation of the relevant analogue time domain signals. Matrices and vectors are denoted in bold upper and lower case letters respectively, $\mathbf{I}_n$ denotes the $n \times n$ identity matrix, $[\cdot]_{nm}$ denotes the n-th row and m-th column element of a matrix, while $(\cdot)^*$ denotes the conjugate operator. Furthermore, in order to render the notation as compact as possible, we use indices t, r to denote the transmitter-receiver pairs, with $t \in \{0, 1\}$ denoting the zeroth and first transmitter respectively and $r \in \{l, e\}$ denoting the legitimate and eavesdropping receiver respectively. Furthermore, we use $\tilde{(\cdot)}$ to distinguish quantities related to the 2nd Alamouti symbol from the respective quantities occurring during the 1st Alamouti symbol.

During the transmission of the 1st Alamouti symbol, the signals $\mathbf{s}_0$ and $\mathbf{s}_1$ emitted by the two mobile distributed transmitters T_{x_0} and T_{x_1} can be expressed as

$$T_{x_0} : \mathbf{s}_0 = \mathbf{F}^H \mathbf{\Phi}_{0,l}^H \mathbf{d}_0, \tag{3}$$

$$T_{x_1} : \mathbf{s}_1 = \mathbf{F}^H \mathbf{\Phi}_{1,l}^H \mathbf{d}_1, \tag{4}$$

where $\mathbf{F}^H$ denotes the Inverse Fourier Matrix (IFM) and $\mathbf{\Phi}_{t,r}$ are diagonal matrices modeling the Doppler frequency shifts along the subcarriers [14], i.e.

$$[\Phi_{t,r}]_{nm} = \delta_{nm} e^{2\pi j (1+\beta_{t,r})n}, \tag{5}$$

$$\beta_{t,r} = \cos\phi_{t,r} \frac{u_{t,r}}{c} \tag{6}$$

with δ_{ij} denoting Kronecker's delta. In the above equations, the effective relative velocities between T_{x_0} and T_{x_1} and the legitimate receiver R_x and the eavesdropper E_x are given by

$$\cos\phi_{t,r} u_{t,r}. \tag{7}$$

The quantities involved are depicted in Fig. 1.

For R_x and E_x to experience the same Doppler shifts, the following needs to hold:

$$u_{0,e} \cos\phi_{0,e} = u_{0,l} \cos\phi_{0,l}, \tag{8}$$

$$u_{1,e} \cos\phi_{1,e} = u_{1,l} \cos\phi_{1,l}. \tag{9}$$

We assume that in the general case (8) and (9) do not hold simultaneously.

Due to the use of the cyclic prefix and pre-equalization at the distributed transmitters, the legitimate receiver FFT output generates a length N observation vector

$$\mathbf{z}_l = \mathbf{H}_{0,l}\mathbf{d}_0 + \mathbf{H}_{1,l}\mathbf{d}_1 + \mathbf{w}_l \tag{10}$$

with the $\mathbf{H}_{t,r}$ being diagonal matrices of the frequency responses $h_{t,r_n}, n = 0, \dots, N-1$ in the two main channels and the two eavesdropping channels respectively, i.e.,

$$[H_{t,r}]_{nm} = \delta_{nm} h_{t,r_n}. \tag{11}$$

Furthermore, $\mathbf{w}_l$ is a vector of i.i.d. zero-mean Gaussian random variables.

The eavesdropper receives a signal that in the general case is distorted due to Doppler shifts, so that the observation vector at the FFT output of E_x is given by

$$\mathbf{z}_e = \mathbf{H}_{0,e}\boldsymbol{\Theta}_0\mathbf{d}_0 + \mathbf{H}_{1,e}\boldsymbol{\Theta}_1\mathbf{d}_1 + \mathbf{w}_e \tag{12}$$

where $[\Theta_0]_{nm} \doteq \theta_{0_n} = \delta_{nm} e^{2\pi j \Delta\beta_0 n}$ with $\Delta\beta_0 = \beta_{0,e} - \beta_{0,l}$. Similarly, $[\Theta_1]_{nm} \doteq \theta_{1_n} = \delta_{nm} e^{2\pi j \Delta\beta_1 n}$ with $\Delta\beta_1 = \beta_{1,e} - \beta_{1,l}$.

The transmission of the 2nd Alamouti symbol involves the emission of

$$\begin{aligned} T_{x_0} : \tilde{\mathbf{s}}_0 &= -\mathbf{F}^H \tilde{\boldsymbol{\Phi}}_{0,l}^H \mathbf{d}_1^*, & (13)\\ T_{x_1} : \tilde{\mathbf{s}}_1 &= \mathbf{F}^H \tilde{\boldsymbol{\Phi}}_{1,l}^H \mathbf{d}_0^*, & (14) \end{aligned}$$

where $\tilde{\boldsymbol{\Phi}}_{t,r}$ are diagonal matrices modeling the Doppler frequency shifts along the subcarriers during the second Alamouti symbol, i.e

$$\begin{aligned} [\tilde{\Phi}_{t,r}]_{nm} &= \delta_{nm} e^{2\pi j (1+\tilde{\beta}_{t,r}) n}, & (15)\\ \tilde{\beta}_{t,r} &= \cos\tilde{\phi}_{t,r} \frac{\tilde{u}_{t,r}}{c}. & (16) \end{aligned}$$

For simplicity, we assume that the channels are slowly varying so that they remain unchanged during the transmission of the two Alamouti symbols. As a result, the observation vectors at the FFT outputs of R_x and E_x respectively are expressed during the second Alamouti symbol as

$$\begin{aligned} \tilde{\mathbf{z}}_l &= -\mathbf{H}_{0,l}\mathbf{d}_1^* + \mathbf{H}_{1,l}\mathbf{d}_0^* + \tilde{\mathbf{w}}_l, & (17)\\ \tilde{\mathbf{z}}_e &= -\mathbf{H}_{0,e}\tilde{\boldsymbol{\Theta}}_0\mathbf{d}_1^* + \mathbf{H}_{1,e}\tilde{\boldsymbol{\Theta}}_1\mathbf{d}_0^* + \tilde{\mathbf{w}}_e & (18) \end{aligned}$$

where $[\tilde{\Theta}_0]_{nm} = \delta_{nm} e^{2\pi j \Delta\tilde{\beta}_0 n}$ with $\Delta\tilde{\beta}_0 = \tilde{\beta}_{0,e} - \tilde{\beta}_{0,l}$, and $[\tilde{\Theta}_1]_{nm} = \delta_{nm} e^{2\pi j \Delta\tilde{\beta}_1 n}$ with $\Delta\tilde{\beta}_1 = \tilde{\beta}_{1,e} - \tilde{\beta}_{1,l}$.

The output of the combiner at the legitimate user produces

$$\mathbf{H} \begin{bmatrix} \mathbf{d}_0 \\ \mathbf{d}_1 \end{bmatrix} + \begin{bmatrix} \mathbf{n}_0 \\ \mathbf{n}_1 \end{bmatrix}, \tag{19}$$

where

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}_{0,l} + \mathbf{A}_{1,l} & 0 \\ 0 & \mathbf{A}_{0,l} + \mathbf{A}_{1,l} \end{bmatrix}, \tag{20}$$

while at the eavesdropper, the combiner output produces

$$\boldsymbol{\Lambda} \begin{bmatrix} \mathbf{d}_0 \\ \mathbf{d}_2 \end{bmatrix} + \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \end{bmatrix}, \tag{21}$$

with

$$\boldsymbol{\Lambda} = \begin{bmatrix} \mathbf{A}_{0,e}\boldsymbol{\Theta}_0 + \mathbf{A}_{1,e}\tilde{\boldsymbol{\Theta}}_1^* & \mathbf{H}_{0,e}^*\mathbf{H}_{1,e}(\boldsymbol{\Theta}_1 - \tilde{\boldsymbol{\Theta}}_0^*) \\ \mathbf{H}_{0,e}\mathbf{H}_{1,e}^*(\boldsymbol{\Theta}_0 - \tilde{\boldsymbol{\Theta}}_1^*) & \mathbf{A}_{0,e}\tilde{\boldsymbol{\Theta}}_0^* + \mathbf{A}_{1,e}\boldsymbol{\Theta}_1 \end{bmatrix}. \tag{22}$$

In the above, we denote the diversity gain matrices as $\mathbf{A}_{t,r} = \mathbf{H}_{t,r}\mathbf{H}_{t,r}^*$ while $\mathbf{n}_0$, $\mathbf{n}_1$, $\mathbf{w}_0$ and $\mathbf{w}_1$ are vectors of i.i.d. zero-mean Gaussian random variables.

B. Relation to Faster than Nyquist Signaling

Based on the properties of the reception matrices $\mathbf{H}$ and $\boldsymbol{\Lambda}$, we can establish a potential advantage at the legitimate user in respect to the eavesdropper; $\mathbf{H}$ is a diagonal matrix and has maximal eigenvalues as opposed to $\boldsymbol{\Lambda}$ which includes gain compression coefficients $\boldsymbol{\Theta}_{0/1}$, $\tilde{\boldsymbol{\Theta}}_{0/1}$ and cross-symbol interference terms. Due to Doppler shifts at E_x, the combiner output involves copies of the two Alamouti OFDM symbols offset by a residual frequency drift. Essentially, this situation is similar to receiving signals transmitted at a rate higher than the nominal Inter-Symbol Interference (ISI) free Nyquist rate.

It has been demonstrated that a receiver's capability to cope with the induced ISI in faster than Nyquist signaling scenarios depends on the dimensionality of the signal space as well as the excess transmission rate and is limited by the so-called Mazo limit [15]. For large dimensionality signal spaces, this limit practically tends to the Nyquist rate, so that no excess transmission rate can be achieved [16]. This case is particularly relevant to the wireless scenario of the proposed system [17] where the matrices $\boldsymbol{\Theta}_{0/1}$ and $\tilde{\boldsymbol{\Theta}}_{0/1}$ would not be diagonal and as a result cross-carrier interference would further degrade the eavesdropper reception.

From a communication theory point of view, the previous discussion can be related to the system error performance through the signal space minimum distance. The transmitted symbols are typically M-ary Quadrature Amplitude Modulation (M-QAM) symbols drawn from uniform distributions over lattices in the complex plane. The reception matrix $\mathbf{H}$ at the legitimate user simply corresponds to the Alamouti diversity gains and does not alter the shape of the data lattice, simply scaling the minimum distance. On the other hand, the eavesdropper reception matrix $\boldsymbol{\Lambda}$ has degraded eigenvalues with respect to $\mathbf{H}$. The signal space minimum distances d_l and d_e at the legitimate user and the eavesdropper respectively are (tightly) upper bounded by the Minkowski bound [18]:

$$\begin{aligned} d_l &\leq \sqrt{N}\det(\mathbf{H}\mathbf{H}^H)^{1/N} = \sqrt{N} \prod_{i=0,\dots,N-1} \lambda_i^{1/N}, & (23)\\ d_e &\leq \sqrt{N}\det(\boldsymbol{\Lambda}\boldsymbol{\Lambda}^H)^{1/N} = \sqrt{N} \prod_{i=0,\dots,N-1} \xi_i^{1/N}. & (24) \end{aligned}$$

The above bounds imply that the potential advantage - in terms of error rates - established at the legitimate user is independent of the eavesdropper receiver complexity.

IV. Secrecy Capacity Analysis

The secrecy capacity of the proposed system during two Alamouti symbols is given as

$$C_s = \left(\log\det(\mathbf{I}_N + \gamma_l \mathbf{H}\mathbf{H}^H) - \log\det(\mathbf{I}_N + \gamma_e \boldsymbol{\Lambda}\boldsymbol{\Lambda}^H)\right)^+ \tag{25}$$

In the simplistic scenario where the Doppler spread is very narrow compared to the intercarrier spacing, we can approximate all submatrices involved in (25) as being diagonal and the system can be decomposed into N parallel subsystems, corresponding to the respective N OFDM subchannels during two Alamouti symbols. Equivalently, reducing all submatrices involved to scalars and dropping the index n corresponding to the n-th carrier, the combiner outputs at the legitimate user and eavesdropper subchannels are respectively given in (26) and (27)

$$\mathbf{h}\begin{bmatrix} d_0 \\ d_1 \end{bmatrix} + \begin{bmatrix} n_0 \\ n_1 \end{bmatrix}, \tag{26}$$

$$\lambda\begin{bmatrix} d_0 \\ d_1 \end{bmatrix} + \begin{bmatrix} w_0 \\ w_1 \end{bmatrix}, \tag{27}$$

with

$$\mathbf{h} \;=\; \begin{bmatrix} |h_{0,l}|^2 + |h_{1,l}|^2 & 0 \\ 0 & |h_{0,l}|^2 + |h_{1,l}|^2 \end{bmatrix}, \tag{28}$$

and

$$\lambda = \begin{bmatrix} |h_{0,e}|^2\theta_0 + |h_{1,e}|^2\tilde{\theta}_1^* & h_{0,e}^* h_{1,e}(\theta_1 - \tilde{\theta}_0^*) \\ h_{0,e}h_{1,e}^*(\theta_0 - \tilde{\theta}_1^*) & |h_{0,e}|^2\tilde{\theta}_0^* + |h_{1,e}|^2\theta_1 \end{bmatrix}. \tag{29}$$

The capacity C_l^* of the legitimate user in a subchannel is evaluated as

$$\begin{aligned} C_l^* &= \log\det(\mathbf{I}_2 + \gamma_l \mathbf{h}\mathbf{h}^H) \\ &= 2\log(1 + \gamma_l(|h_{0,l}|^2 + |h_{1,l}|^2)^2) \end{aligned} \tag{30}$$

during the transmission of two Alamouti symbols. The capacity C_e^* of the eavesdropper in a subchannel on the other hand can be evaluated as

$$\begin{aligned} C_e^* &= \log\det(\mathbf{I}_2 + \gamma_e\lambda\lambda^H) \\ &= \log\Bigg\{\bigg[1 + \gamma_e\Big(\big||h_{0,e}|^2\theta_0 + |h_{1,e}|^2\tilde{\theta}_1\big|^2 \\ &+ |h_{0,e}|^2|h_{1,e}|^2|\tilde{\theta}_0 - \theta_1|^2\Big)\bigg] \\ &\times \bigg[1 + \gamma_e\Big(\big||h_{0,e}|^2\tilde{\theta}_0 + |h_{1,e}|^2\theta_1\big|^2 \\ &+ |h_{0,e}|^2|h_{1,e}|^2|\theta_0 - \tilde{\theta}_1|^2\Big)\bigg] \\ &- \gamma_e|h_{0,e}|^2|h_{1,e}|^2\big|(\theta_0^* - \tilde{\theta}_1)(|h_{0,e}|^2\theta_0 + |h_{1,e}|^2\tilde{\theta}_1^*) \\ &- (\theta_1 - \tilde{\theta}_0^*|)(|h_{0,e}|^2\tilde{\theta}_0 + |h_{1,e}|^2\theta_1^*)\big|^2\Bigg\} \\ &\leq \log\big(1 + \gamma_e\big||h_{0,e}|^2\theta_0 + |h_{1,e}|^2\tilde{\theta}_1\big|^2\big) \\ &+ \log\big(1 + \gamma_e\big||h_{0,e}|^2\tilde{\theta}_0 + |h_{1,e}|^2\theta_1\big|^2\big). \end{aligned} \tag{31}$$

We assume that the random variables $h_{t,r}$, $\theta_{t,r}$ and $\beta_{t,r}$ share the same statistics as the random variables $\mathfrak{H}$, $\mathfrak{F}$ and $\mathfrak{B}$ respectively. Due to symmetry in the expressions involved, the ergodic secrecy capacity can be evaluated as

$$\begin{aligned} \langle C_s\rangle &= \big\langle (C_l^* - C_e^*)^+ \big\rangle \\ &\geq \big\langle 2\log(1 + 4\gamma_l|\mathfrak{H}|^4) - 2\log\big(1 + 4\gamma_e|\mathfrak{H}|^4|\mathfrak{F}|^2\big)\big\rangle, \end{aligned} \tag{32}$$

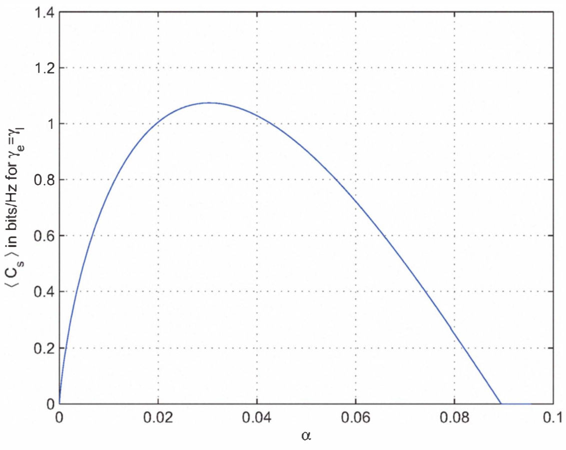

Fig. 2. Ergodic secrecy capacity when the legitimate user has the same SNR as a potential eavesdropper.

where $\langle\cdot\rangle$ denotes ensemble expectation. We can further simplify (32) by using the series expansion of $\log(x)$ for $0 < x \leq 2$ which would require that

$$\gamma_e \leq \frac{1 + 8\gamma_l|\mathfrak{H}|^4}{4|\mathfrak{H}|^4|\mathfrak{F}|^2}. \tag{33}$$

If (33) is true then (32) becomes

$$\begin{aligned} \langle C_s\rangle &= -2\Bigg\langle \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\bigg(\frac{1 + 4\gamma_e|\mathfrak{H}|^4|\mathfrak{F}|^2}{1 + 4\gamma_l|\mathfrak{H}|^4} - 1\bigg)^n\Bigg\rangle \\ &= -2\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\frac{4^n\langle|\mathfrak{H}|^{4n}\rangle\gamma_l^n\langle(\frac{\gamma_e}{\gamma_l}|\mathfrak{F}|^2 - 1)^n\rangle}{\langle(1 + 4\gamma_l|\mathfrak{H}|^4)^n\rangle} \\ &\simeq 2\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\langle(1 - \frac{\gamma_e}{\gamma_l}|\mathfrak{F}|^2)^n\rangle \\ &= -2\Big\langle \log\Big(\frac{\gamma_e}{\gamma_l}|\mathfrak{F}|^2\Big)\Big\rangle \\ &\simeq 2\log\Big(\frac{\gamma_l}{\gamma_e}\Big) + 2\Big\langle \log\frac{1}{1 - 4\pi^2 n^2\Delta f^2\Delta\mathfrak{B}^2}\Big\rangle, \end{aligned} \tag{34}$$

where we have assumed that $4\gamma_l|\mathfrak{H}|^2 \gg 1$ and that $\mathfrak{F}$ takes small values so that $|\mathfrak{F}|^2 \simeq 1 - (2\pi n\Delta\mathfrak{B})^2$. (34) reveals that even if the eavesdropper has a small SNR advantage, it is still possible to achieve a positive secrecy capacity.

Assuming that $\mathfrak{B}$ is uniformly distributed in the range $(-\alpha, \alpha)$ with $0 < \alpha < 1$, (34) becomes

$$\begin{aligned} \langle C_s\rangle &= 2\log\Big(\frac{\gamma_l}{\gamma_e}\Big) + 4\alpha\ln 2 + 2\alpha\log(\alpha^2 - 1 - 2\alpha) \\ &+ 2\log\Big(\frac{1+\alpha}{1-\alpha}\Big). \end{aligned} \tag{35}$$

In Fig. 2 the ergodic secrecy capacity is evaluated when the legitimate user and the eavesdropper experience on average the same channel conditions, i.e. $\gamma_e = \gamma_l$. For underwater acoustic OFDM systems the velocity of sound is approximately $c = 1500$ m/sec; for a reasonable velocity of 10 km/h, we obtain $\beta \simeq 2 \times 10^{-3}$ [14]. On the other hand, for RF systems $c = 3 \times 10^8$ m/sec so that for a velocity $u = 100$ km/h we obtain

$\beta \simeq 10^{-7}$ [14]. Therefore, we can argue that in such typical scenarios, a small positive secrecy capacity can be inferred and Wyner's concept can be achieved even when the legitimate user has no SNR advantage over the eavesdropper.

V. Conclusions and Future Work

In this paper we have investigated an alternative approach in the framework of physical layer security relying on topological and mobility network asymmetries. We have proposed an Alamouti STBC OFDM system with distributed mobile transmitters. A reception advantage can be established at the legitimate user with respect to a potential eavesdropper based on pre-equalization - in terms of Doppler shifts - of the transmitted symbols. Even in the simple scenario where the Doppler spread is narrow compared to the OFDM inter-carrier spacing, it can be demonstrated that a positive ergodic secrecy capacity can be achieved even when the legitimate user has no SNR advantage over the eavesdropper. The underlying system concept is closely related to the reception of signals transmitted at rates higher than the Nyquist rate. In such scenarios, the reception matrices' eigenvalues explicitly determine both the signal space minimum distance (and therefore the error rate) and the secrecy capacity.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1385–1357, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Information Theory*, vol. 54, no. 10, pp. 4687–5403, Oct. 2008.

[4] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple antenna wiretap channel," *IEEE Trans. Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[5] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, Jul. 2008, pp. 389–393.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[7] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer.* New York: Springer, 2010.

[8] N. Marina, H. Yagi, and H. V. Poor, "Improved rate-equivocation regions for secure cooperative communication," in *Proc. IEEE International Symposium on Information Theory*, St Petersbourg, Russia, Jul. 2011, pp. 2871 – 2875.

[9] F. Renna, N. Laurenti, and H. V. Poor, "High SNR secrecy rate with OFDM signaling over fading channels," in *Proc. IEEE Personal Indoor and Mobile Radio Communications*, Istanbul, Turkey, Sep. 2010, pp. 2692 – 2697.

[10] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications.* Hanover MA: Now Publishers Inc., 2004.

[11] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.

[12] F. Galton, "Dice for statistical experiments," *Nature*, vol. 42, no. 1070, pp. 13–14, May 1870.

[13] P. Baracca, N. Benvenuto, and L. Vangelista, "A frequency domain pre-equalizer for MIMO-OFDM mobile communication systems employing Alamouti coding," in *Proc. IEEE 12th Int. Workshop on Signal Proc. Advances in Wireless Com.*, 2011.

[14] A. Salberg and A. Swami, "Doppler and frequency-offset synchronization in wideband OFDM," *IEEE Trans. Wireless Communications*, vol. 4, no. 6, pp. 2870–2881, Nov. 2005.

[15] J. E. Mazo, "Faster than Nyquist signalling," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1451–1462, Oct. 1975.

[16] A. Chorti, "Masked-OFDM: A physical layer encryption for future OFDM applications," in *Proc. IEEE Globecom 2010 Workshop on Mobile Computing and Emerging Communication Networks*, Miami, FL, Dec. 2010, pp. 1254 – 1258.

[17] X. Zhao, T. Peng, M. Yang, and W. Wang, "Doppler spread estimation by tracking the delay-subspace for OFDM systems in doubly selective fading channels," *IEEE Signal Proc. Letters*, vol. 16, no. 3, pp. 212–215, Mar. 2009.

[18] V. Lyubashevsky and D. Micciancio, "On bounded distance decoding, unique shortest vectors, and the minimum distance problem," in *Proc. Advances in cryptology - Crypto 2009.* Santa Barbara, CA: Springer, Aug. 2009, pp. 577–594.