A new jamming technique for secrecy in multi-antenna wireless networks

Omar Bakr[†] Raghuraman Mudumbai

Electrical Engineering and Computer Sciences, UC Berkeley, Berkeley, CA 94720
Electrical and Computer Engineering, University of Iowa, Iowa City, IA 52242
Email:ombakr@eecs.berkeley.edu, rmudumbai@engineering.uiowa.edu

***Abstract*— We consider the problem of secure wireless communication in the presence of an eavesdropper when the transmitter has multiple antennas, using a variation of the recently proposed artificial noise technique. Under this technique, the transmitter sends a pseudo-noise jamming signal to selectively degrade the link to the eavesdropper without affecting the desired receiver. The previous work in the literature focuses on ideal Gaussian signaling for both the desired signal and the noise signal. The main contribution of this paper is to show that the Gaussian signaling model has important limitations and propose an alternative "induced fading" jamming technique that takes some of these limitations into account. Specifically we show that under the Gaussian noise scheme, the eavesdropper is able to recover the desired signal with very low bit error rates when the transmitter is constrained to use constant envelope signaling. Furthermore, we show that an eavesdropper with multiple antennas is able to use simple, blind constant-envelope algorithms to completely remove the Gaussian artificial noise signal and thus defeat the secrecy scheme. We propose an alternative scheme that induces artificial fading in the channel to the eavesdropper, and show that it outperforms the Gaussian noise scheme in the sense of causing higher bit error rates at the eavesdropper and is also more resistant to constant modulus-type algorithms.**

I. Introduction

Wireless communication links are inherently vulnerable to eavesdropping because of the broadcast nature of the medium: any node within range of the transmitter is able to listen to any of its transmissions. However with the advent of multi-input multi-output (MIMO) spatial multiplexing techniques [1] a transmitter equipped with multiple antennas can selectively send different streams of data to different receivers simultaneously over the same frequency band; by carefully choosing the array weights, the transmitter can ensure that each data stream is received at its intended destination without interference from other data streams. Unfortunately this requires the knowledge of channel state information (CSI) to all receivers at the transmitter; since a hostile eavesdropper can hide its CSI (e.g. by simply remaining passive), it is not usually possible to hide the desired signal from an eavesdropper. However, it is possible to encode the desired "plain text" information in the desired signal in a suitable way to hide it from an eavesdropper.

One simple method for doing this has been recently developed and it is based on the concept of artificial noise [2]. In this method, the multi-antenna transmitter sends, along with the desired signal, an additional jamming signal that is designed in such a way that it does not interfere with the intended receiver (see Figure 1). On the other hand, the jamming signal will in general interfere with any eavesdropper and degrade its channel, and thus this technique can be used as the basis for a secure wireless link.

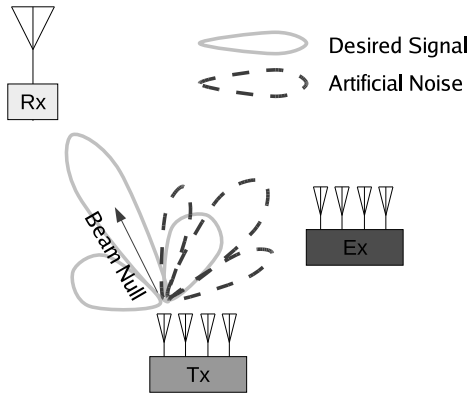

Fig. 1. Multi-antenna transmitter transmits artificial noise in directions that are orthogonal to the desired receiver.

Previous works on artificial noise focus almost exclusively on a Gaussian model where all the desired signals and artificial noise are chosen from Gaussian probability distributions. However this model has some important limitations. First, the Gaussian distribution is physically unrealizable because it requires unbounded amplitudes, and secrecy schemes that are optimal for Gaussian signaling are no longer optimal when such physical constraints are imposed. Second, the Gaussian distribution has the special property that a linear combination of Gaussian signals is still Gaussian, therefore deviations from the Gaussian distribution open up the possibility of an eavesdropper with multiple antennas using powerful statistical techniques such as independent component analysis [3] or constant modulus algorithms [4] to overcome the secrecy scheme.

[†]Omar Bakr's research is sponsored by a fellowship from King Abdullah University of Science and Technology. The authors would also like to acknowledge the students, faculty and sponsors of the Berkeley Wireless Research Center, and the National Science Foundation Infrastructure Grant No. 0403427.

Although a multiple-antenna eavesdropper can remove artificial noise even with Gaussian signaling, secrecy systems must be designed using the most conservative assumptions on the capabilities of the hostile nodes. Thus, the ease with which interference cancellation can be accomplished for non-Gaussian signals makes it necessary to consider the effect of non-Gaussian signaling to fully assess the vulnerabilities of an artificial noise system.

The focus of this paper is to motivate the need for non-Gaussian jamming techniques to overcome these limitations. We assume apriori that the transmitter is constrained to a constant envelope (QPSK) constellation. This can be thought of as an extreme case of non-Gaussian signaling and serves to highlight the above limitations of the Gaussian model. Our contributions are summarized as follows.

1) We study the bit error rate at the eavesdropper under Gaussian artificial noise and show that a significantly higher amount of power is necessary in the artificial noise signal in order to force high BERs at the eavesdropper than what is predicted for Gaussian signaling. In general secrecy systems will use coding and therefore a low bit error rate is not necessarily required for insuring a low probability of interception. However, for our purposes, the BER serves as a useful proxy for the strength of the secrecy provided by the jamming signal.
2) We consider the case when the eavesdropper has multiple antennas and show that it is possible to remove the artificial noise signal almost completely using a simple constant modulus algorithm.
3) As an alternative to Gaussian artificial noise we propose an "induced fading" scheme and show that it achieves a higher BER at the eavesdropper compared to the additive Gaussian noise scheme.
4) We show that the constant modulus algorithm is significantly less effective in overcoming the "induced fading" scheme for a multi-antenna eavesdropper than Gaussian artificial noise.

A. Previous work on secure multi-antenna channels

There is a long history of research into secure wireless links, and the previous work on the subject falls broadly into two categories. In the first category are investigations into coding techniques that can guarantee *perfect secrecy* in the information theoretic sense [5]. A second category of previous work is more recent and focuses on the design of practical schemes [6], [7], [8], [9] that use random fluctuations in the wireless channel itself as the basis for secrecy: the channel to the desired receiver sees different fluctuations than the channel to the eavesdropper, and this can be used as a shared key. Note that this type of scheme is an *encryption* technique whose cryptographic strength depends on the level of randomness and unpredictability of the channel and the ability to keep the CSI secret from the eavesdropper. In this paper, we focus only on the first category i.e. physical layer secrecy schemes that do not depend on keeping the channel state information secret from the eavesdropper.

The notion of *secrecy capacity* of a *wiretap* channel was first introduced in [10] for the special case where the eavesdropper's signal was a degraded version of the desired receiver's signal and later greatly generalized to arbitrary broadcast channels [11], [12], fading channels [13] and recently to multi-antenna channels [14], [15].

In addition, [14] considers a so-called "masked beamforming" scheme, and shows this scheme to be close to optimal in the asymptotic case of high SNR. This scheme involves transmitting an *artificial noise* signal to degrade the SNR of the eavesdropper without affecting the desired receiver. The idea of using artificial noise for secrecy was first proposed in [2], and is a special case of intentional jamming considered in this paper.

Intentional jamming has been considered in previous work in the information theoretic literature, where the channel coding problem is modeled as a non-cooperative game [16], [17] between a transmitter seeking to send a data signal and an interferer who seeks to disrupt the transmission by sending a jamming signal. (The receiver in this model is analogous to the eavesdropper considered in this paper.) The interferer can be either an actively hostile node, or merely a pessimistic model for passively generated noise. It has been shown [18] that the Gaussian interference model represents a mini-max solution ("saddle-point") of the non-cooperative game and is in this sense robust: the Gaussian distribution is the optimum choice for both the transmitter and the interferer given that the other player employs a Gaussian distributed signal.

In [19] the problem of finding the "worst-case" jamming signal was considered under different performance metrics including mutual information and BER, and it was shown that for discrete-valued input signals, the strongest interference signal is also discrete-valued. Thus, if we choose the input signals out of a discrete-valued distribution, the strongest noise is not Gaussian distributed but discrete-valued. This result, however, is fragile in the sense that, under some uncertainty in the channel model, e.g. in the precise values of the elements of the discrete set from which the input distribution is chosen, the strongest interference signal actually becomes the weakest, i.e. it allows perfect recovery of the transmitted signal. This fragility was recognized in [19], where it was proposed that a small continuous-valued noise be added to the discrete-valued interference to robustify the interference. However, this method is only suitable for small levels of channel uncertainty; in this paper, we assume that the channel to the eavesdropper is *completely unknown*.

The rest of the paper is organized as follows. In Section II-A, we present the system model; in Section II-B we analyze the limitations of the Gaussian artificial noise-based secrecy technique. We then present a bit error rate analysis in Section II-C and motivate an alternative "induced fading" jamming technique. Section II-D presents extensive simulation results of the Gaussian and induced fading schemes and Section III concludes with a summary and an outline of open issues for future work.

II. Bit Error Rate analysis

We now present a simple analysis of the bit error rate (BER) at the eavesdropper under additive Gaussian artificial noise and also under an induced-fading jamming signal.

A. Problem setup

As stated previously, we assume the transmitter has N antennas, and the receiver and eavesdropper have only one antenna. Let $\mathbf{h}_d \equiv a_d \mathbf{u}_d$ be the channel gain vector from the transmit array to the desired receiver and let $\mathbf{u}_i,\ i = 2 \dots N$ be an orthogonal set of vectors also orthogonal to $\mathbf{u_d}$, where $\mathbf{u_d},\ \mathbf{u_i}$ are all unit vectors. The channel vector $\mathbf{u}_d$ is assumed to be known to the transmitter either through reciprocity or through a secure feedback channel from the receiver. Furthermore let $\mathbf{u}_e$ be the unit vector proportional to the transmit array's channel $\mathbf{h}_e \equiv a_e \mathbf{u}_e$ to the eavesdropper. The basic idea behind all artificial noise schemes is to transmit

$$\mathbf{s}(t) = m(t)\mathbf{u}_d + \sum_{i=2}^{N} w_i(t)\mathbf{u}_i \tag{1}$$

where $m(t)$ is the message signal intended for the receiver and $w_i(t)$ are all pseudo-noise sequences that are intended to selectively degrade the SNR of the eavesdropper without affecting the intended receiver. The corresponding received signal at the desired receiver is $r_d(t) \equiv \mathbf{h}_d^H \mathbf{s}(t)$ and similarly for the eavesdropper. Clearly all the terms containing $w_i(t)$ in (1) are cancelled out of $r_d(t)$.

If the $w_i(t)$ are chosen $i.i.d.$ and if N_0 is the thermal noise power at the receiver and eavesdropper, the respective SNRs at the desired receiver and eavesdropper are given by

$$\mathrm{SNR_d} = \frac{a_d^2 P_m}{N_0} \tag{2}$$

$$\mathrm{SNR_e} = \frac{a_e^2 \alpha P_m}{N_0 + a_e^2(1-\alpha)P_w} \tag{3}$$

where $P_m = E[|m(t)|^2]$ and $P_w = E[|w_i(t)|^2]$ are respectively the power allocated to the signal transmission and artificial noise by the transmitter and $\alpha = |\mathbf{u}_d^H \mathbf{u}_e|^2$ is the parameter indicating the "alignment" between the receiver and eavesdropper. If the SNR at the desired receiver is large i.e. $\frac{P_m}{N_0} \gg 1$, then we can neglect the thermal noise component to obtain:

$$\mathrm{SNR_e} \approx \frac{\alpha P_m}{(1-\alpha)P_w} \tag{4}$$

The alignment parameter α depends on the relative location of the eavesdropper with respect to the transmitter and receiver and also on the statistics of the channel fading. In general, when the number of transmit antennas N increases, we expect the channels to the receiver and eavesdropper to be increasingly uncorrelated (i.e. less "aligned")[1].

[1]In a rich scattering Rayleigh environment, the channel responses from each antenna on transmitter to the receiver and eavesdropper become $i.i.d$ complex Gaussian random variables, in which case the alignment is $\frac{1}{N}$ on average [20], [21].

B. Importance of the Gaussian signaling assumption

In the remainder of this paper, we consider a running example of a system where the nominal SNR $\frac{P_m}{N_0} = 40\mathrm{dB}$, and the alignment $\alpha = 0.5$. Also we assume that the eavesdropper's channel is 10 dB weaker compared to the desired receiver i.e. $a_d^2 = 10 a_e^2$. Even under these favorable assumptions, we show that it is more difficult to achieve secrecy from the eavesdropper than we might expect from a Gaussian analysis.

In the example system described above, let the power allocated to the artificial noise be 10% of the power in the desired signal i.e. $P_w = \frac{1}{10} P_m$ Then, if ideal complex Gaussian signaling is used for both signal and artificial noise, the secrecy rate of the channel is given by [11]:

$$C_{\mathrm{sec}} = \log\big(1 + \frac{P_m}{N_0}\big) - \log\big(1 + \frac{\alpha P_m}{(1-\alpha)P_w}\big) \approx 9.8\mathrm{bits} \tag{5}$$

where we used the approximation for SNR_e in (4). Thus, it is possible to transmit up to 9.8 bits/symbol on this channel to the desired receiver without the eavesdropper being able to decode the message bits. This, of course, assumes ideal Gaussian signaling. If, instead of Gaussian signaling, we constrain ourselves to a QPSK constellation, the eavesdropper is able to decode the bits with a BER given by

$$\mathrm{BER}_e = Q(\sqrt{\mathrm{SNR}_e}) \approx 7.8 \times 10^{-4} \tag{6}$$

In other words, even when signaling at only 2 bits/symbol over a channel with a secrecy capacity of 9.8 bits/symbol, the eavesdropper is still able to recover the transmitted bits with a BER of less than 10^{-3}. This example illustrates the importance of the Gaussian signaling assumption for effective secrecy: when the transmitter is constrained to use a constant envelope signaling such as QPSK, much more of the transmitted power needs to be allocated to the jamming signal in order to cause substantial BER at the eavesdropper than under Gaussian signaling. We show later that under these conditions, an alternative "induced fading" jamming technique works better compared to Gaussian artificial noise in the sense of causing higher BER at the eavesdropper.

Now we consider an eavesdropper with N antennas i.e. the same number of antennas as the transmitter (or equivalently N single antenna eavesdroppers collaborating with each other). Assume that the channels to the eavesdropper antennas are given by $\mathbf{h}_{e,k} = a_e \mathbf{u}_{e,k},\ k = 1 \dots N$, where $a_e = \frac{1}{\sqrt{10}} a_d$ and the alignment parameters $|\mathbf{u}_d^H \mathbf{u}_{e,k}|^2 = 0.5,\ k = 1 \dots N$ as before for each eavesdropper antenna. Thus the eavesdropper antenna k receives the scalar signal

$$\begin{aligned} r_{e,k}(t) &= \mathbf{h}_{e,k}^H \mathbf{s}(t) \\ &\equiv a_e \Big((\mathbf{u}_{e,k}^H \mathbf{u}_d) m(t) + \sum_{i=2}^{N} (\mathbf{u}_{e,k}^H \mathbf{u}_i) w_i(t) \Big) \end{aligned} \tag{7}$$

In Section II-D we present simulation results that show that the eavesdropper is able to use a blind constant modulus algorithm to compute complex weights $c_k,\ k = 1 \dots N$ such that the

artificial noise signals $w_i(t)$ are completely removed from the linear combination $r_e(t) = \sum_{k=1}^{N} c_k r_{e,k}(t)$.

C. BER at the eavesdropper

Let us denote by ρ the proportion of the total power at the transmitter allocated to the noise signal i.e. $\rho \doteq \frac{P_w}{P_m+P_w}$. Then we can rewrite (4) as:

$$\mathrm{SNR}_e \approx \frac{\alpha(1-\rho)}{(1-\alpha)\rho} \tag{8}$$

The corresponding BER under Gaussian artificial noise is given by

$$\mathrm{BER}_{an} = Q\big(\sqrt{\mathrm{SNR}_e}\big) \approx Q\Big(\sqrt{\frac{\alpha(1-\rho)}{(1-\alpha)\rho}}\Big) \tag{9}$$

Note that we are interested in the high BER regime with its correspondingly low SNR_e values, and asymptotic approximations of the $Q(.)$ function with exponentials are thus not appropriate here.

Consider now an alternative jamming scheme, where instead of random additive noise, the transmitter sends a randomly scaled version of the signal itself. Specifically, in (1), we set $w_i(t) = c_i(t)m(t)$, where $c_i(t)$ is randomly chosen so that the jamming part of the transmitted signal is $m(t) \times \mathbf{v}_\perp(t)$, where $\mathbf{v}_\perp(t) \doteq \sum_{i=2}^{N} c_i(t)\mathbf{u}_i$ is a random vector in the subspace orthogonal to $\mathbf{u}_d$, such that $|\mathbf{v}_\perp(t)|^2 \equiv \sum_{i=2}^{N} |c_i(t)|^2 = \frac{\rho}{1-\rho}$.

The corresponding signal received at the eavesdropper is given by (neglecting the thermal noise):

$$r_e(t) = a_e m(t)\Big(\sqrt{\alpha} + (\mathbf{u}_e^H \mathbf{v}_\perp(t))\Big) \tag{10}$$

where we assumed without loss of generality that $\angle(\mathbf{u}_e^H \mathbf{u}_d) = 0$ and set $|(\mathbf{u}_e^H \mathbf{u}_d)|^2 = \alpha$. Thus the effective channel to the eavesdropper looks like a fading channel, and the effect of the jamming signal is to induce artificial fading in the channel to the eavesdropper. Let us denote $x_1(t) + jx_2(t) \doteq (\mathbf{u}_e^H \mathbf{v}_\perp(t))$. Then, the induced fading will cause an error in the QPSK symbol whenever $|\angle\sqrt{\alpha} + x_1(t) + jx_2(t)| \geq \frac{\pi}{4}$ i.e. if the fading "rotates" the received signal by at least $\frac{\pi}{4}$. This requires $|x_2(t)| \geq \sqrt{\alpha} + x_1(t)$. We show in Section II-D that the BER of the induced fading scheme exceeds BER_{an} in (9) for large values of ρ which corresponds to large BER at the eavesdropper. We also show that a multi-antenna eavesdropper will have a more difficult time blocking the jamming signal under induced fading than Gaussian artificial noise.

D. Simulation results

In this section, we provide numerical results that verify the analysis of this paper, and compare the performance of the jamming schemes. The graphs in Figures 2a-d plot the fraction of transmit power allocated for jamming (ρ) that is required to achieve a given bit error rate at a *single antenna* eavesdropper for both the Gaussian noise and induced fading jamming schemes. In Figure 2a, the complex channel response vectors to the desired receiver and eavesdropprer are generated independently from Rayleigh distributions. In Figures 2b-d, the alignment α between the two channels was fixed at 0.1, 0.5, 0.1 respectively. In Figures 2a-c The transmitter has 5 antennas, and 20 antennas in Figure 2d. These graphs show that the induced fading technique can achieve the same BER (for high BERs) at the eavesdropper as Gaussian noise using up to 15% less power (smaller ρ). However, the figures also show that Gaussian noise outperforms induced fading in small regions in the graphs where ρ is small. This is due to the unbounded nature of Gaussian noise. This region also grows as we increase the alignment (α). However, as we pointed out in Section II-A, we expect the alignment to be inversely proportional to the number of antennas in rich scattering Rayleigh environments, which increases the likelihood of induced fading outperforming Gaussian noise.

The next simulation shows that fast random fluctuations in the channel response from the transmitter to eavesdropper can easily be absorbed when the eavesdropper is equipped with at least the same number of antennas as the transmitter using a constant modulus algorithm (CMA). In Figure 2e, we ran the constant modulus algorithm with $N = 5$ antennas at the transmitter, $M = 6$ antennas at the eavesdropper, 30dB SNR at the eavesdropper, and $\rho = 0.5$. The graph shows that the constant modulus algorithm achieves up to 30dB artifical noise rejection. We repeated the same simulation with the induced fading scheme using a slow fading rate (Doppler rate = 1/500 the symbol rate) in Figure 2f. The graph clearly shows little or no interference rejection by the constant modulus algorithm despite the high SNR at the eavesdropper (60dB). Thus the induced fading scheme is more difficult to overcome for a multi-antenna eavesdropper compared to Gaussian artificial noise. This can be intuitively explained as follows. From (10), the overall channel gain seen by each antenna at the eavesdropper is $a_e\big(\sqrt{\alpha} + (\mathbf{u}_e^H \mathbf{v}_\perp(t))\big)$, and this gain can be made to remain roughly constant over several symbols if $\mathbf{v}_\perp(t)$ is varied very slowly. Thus, by using a fading rate slow compared to the convergence rate of the constant modulus algorithm, it is possible to fool the CMA to effectively train to the wrong value of the channel gain. Even though this might suggest that slow fading is a superior jamming technique for dealing with multi-antenna eavesdroppers, if the fading is too slow, the eavesdropper can easily track slow channel variations. Therefore, there is a tradeoff in choosing the fading rate. A detailed analysis of this tradeoff and its generalization for algorithms other than the CMA are interesting topics for future works.

III. Conclusion

In this paper, we considered the idea of using multiple antennas at the transmitter to achieve a secure wireless link by artificially degrading the channel to an eavesdropper. Previous work on this topic has shown that a Gaussian artificial noise scheme can achieve rates close to the secrecy capacity. We show in this paper that the performance of this scheme can be fragile in the sense that it depends strongly on the special properties of the Gaussian distribution. We show that when the transmitter is constrained to use constant envelope signaling,

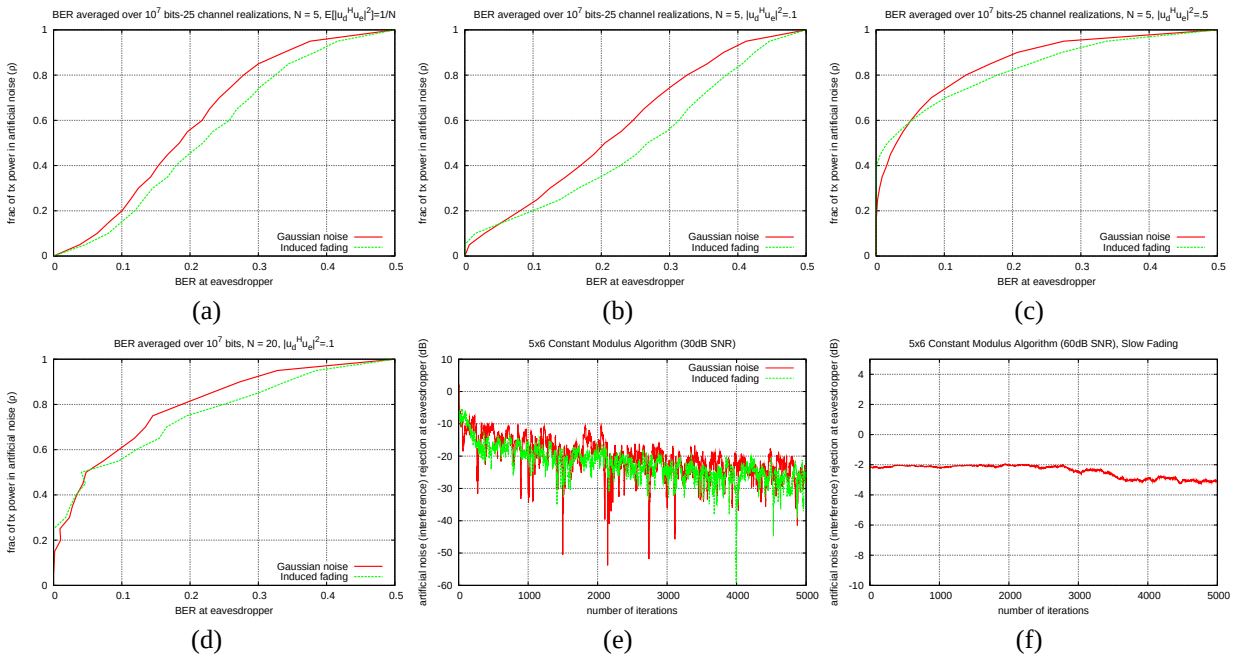

Fig. 2. (a)-(f)Comparing the performance of two signal jamming techniques: induced fading and Gaussian noise.

the amount of power required in the artificial noise signal is substantially greater than for Gaussian signaling. Furthermore, an eavesdropper with multiple antennas is able to use very simple constant modulus techniques to blindly remove all the artificial noise and thereby defeat the secrecy measures. These observations open up interesting issues for future work. One fundamental question is a precise characterization of how deviations from Gaussian signaling affect the strength of the secrecy scheme. Other open issues include the design of optimum jamming signals for non-Gaussian message signals, and the design of robust signaling schemes that are immune to constant-modulus-like non-linear algorithms. Our preliminary results indicate that "induced fading" schemes offer some advantages and this suggests an exploration of a larger family of jamming schemes beyond additive noise.

REFERENCES

[1] I. E. Telatar, "Capacity of multi-antenna Gaussian channels," *European transactions on telecommunications*, 1999.

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

[3] A. Hyvärinen and E. Oja, "Independent component analysis: algorithms and applications," *Neural networks*, vol. 13, no. 4-5, pp. 411–430, 2000.

[4] J. Johnson, R., P. Schniter, T. Endres, J. Behm, D. Brown, and R. Casas, "Blind equalization using the constant modulus criterion: a review," *Proceedings of the IEEE*, vol. 86, no. 10, pp. 1927–1950, Oct 1998.

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

[6] T. Kitano, A. Kitaura, H. Iwai, and H. Sasaoka, "A private key agreement scheme based on fluctuations of ber in wireless communications," in *Advanced Communication Technology, The 9th International Conference on*, vol. 3, Feb. 2007, pp. 1495–1499.

[7] J. Wallace, C. Chen, and M. Jensen, "Key Generation Exploiting MIMO Channel Evolution: Algorithms and Theoretical Limits."

[8] T. Ohira, "Esparski: Encryption scheme parasite array radiator secret key implementation," in *International Conference on Microwaves, Radar & Wireless Communications (MIKON)*, May 2006, pp. 1065–1070.

[9] A. Babakhani, D. Rutledge, and A. Hajimiri, "A near-field modulation technique using antenna reflector switching," in *IEEE International Solid-State Circuits Conference (ISSCC)*, Feb. 2008, pp. 188–605.

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

[11] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[12] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

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

[14] A. Khisti and G. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel."

[15] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *IEEE International Symposium on Information Theory*, 2008, pp. 524–528.

[16] N. Blachman, "Communication as a game," in *Proc. IRE WESCON Conf*, 1957, pp. 61–66.

[17] R. Dobrushin, "Optimum information transmission through a channel with unknown parameters," *Radio Eng. Electron*, vol. 4, no. 12, pp. 1–8, 1959.

[18] J. Borden, D. Mason, and R. McEliece, "Some information theoretic saddlepoints," *SIAM Journal on Control and Optimization*, vol. 23, p. 129, 1985.

[19] S. Shamai and S. Verdu, "Worst-case power-constrained noise for binary-input channels," *IEEE Transactions on Information Theory*, vol. 38, no. 5, pp. 1494–1511, 1992.

[20] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*. Cambridge University Press, 2005.

[21] O. Bakr, M. Johnson, R. Mudumbai, and U. Madhow, "Interference suppression in the presence of quantization errors," in *Allerton Conference on Communication, Control, and Computing*, September 2009.