Everlasting Secrecy in Disadvantaged Wireless Environments against Sophisticated Eavesdroppers

Azadeh Sheikholeslami, Dennis Goeckel and Hossein Pishro-nik
Electrical and Computer Engineering Department, University of Massachusetts, Amherst

***Abstract*—Secure communication over a wireless channel in the presence of a passive eavesdropper is considered. Our main interest is in the disadvantaged wireless environment, where the channel from the transmitter Alice to the eavesdropper Eve is (possibly much) better than that from Alice to Bob, hence making information-theoretic secrecy challenging. We present a method to exploit inherent vulnerabilities of the eavesdropper's receiver through the use of "cheap" cryptographically-secure key-bits, which only need be kept secret from Eve for the (short) transmission period of the message, to obtain information-theoretic (i.e. everlasting) secret bits at Bob. In particular, based on an ephemeral cryptographic key pre-shared between Alice and Bob, a random jamming signal with large variations is added to each symbol. The legitimate receiver Bob uses the key to subtract the jamming signal immediately, while Eve is forced to perform the inherently nonlinear operation of recording the signal; when Eve then obtains the key, which we assume pessimistically (for Alice) happens right after message transmission, Eve can then immediately subtract the jamming signal from the recorded signal. But, because of the intervening non-linear operation in Eve's receiver and the non-commutativity of nonlinear operations, Bob's channel and Eve's channel have different achievable rates and information-theoretic secrecy can be obtained, hence achieving the goal of converting the vulnerable cryptographic secret key into information-theoretic secure bits. The achievable secrecy rates for different settings are evaluated. Among other results, it is shown that, even when the eavesdropper has perfect access to the output of the transmitter (albeit through an imperfect analog-to-digital converter), the method can still achieve a positive secrecy rate.**

I. Introduction

The usual approach to provide secrecy is encryption of the message. Such cryptographic approaches rely on the assumption that the eavesdropper does not have access to the key, and the computational capabilities of the eavesdropper are limited [1]. However, if the eavesdropper can somehow obtain the key in the future, or the cryptographic system is broken, the secret message can be obtained from the recorded clean cipher [2], which is not acceptable in many applications requiring everlasting secrecy.

The desire for everlasting security motivates considering information-theoretic security methods, where the eavesdropper is unable to extract any information about the message from the received signal. Wyner showed that, for a discrete memoryless wiretap channel, if the eavesdropper's channel is degraded with respect to the main channel, adding randomness to the codebook allows a positive secrecy rate to be achieved [3]. This idea was extended to the more general case of a wiretap channel with a "more noisy" or "less capable" eavesdropper [4]. Hence, in order to obtain a positive secrecy rate in a one way communication system, having an advantage for the main channel with respect to the eavesdropper's channel is essential. However, in wireless systems, guaranteeing such an advantage is not always possible, as an eavesdropper that is close to the transmitter or with a directional antenna can obtain a very high signal-to-noise ratio. Furthermore, the location and channel state information of a passive eavesdropper is usually not known to the legitimate nodes, making it difficult to pick the secrecy rate to employ. Recently, approaches based on the cooperative jamming scheme of [5], which try to build an advantage for the legitimate nodes over the eavesdropper, have been considered extensively in the literature. However, these approaches require either multiple antennas, helper nodes, and/or fading and therefore are not robust across all operating environments envisioned for wireless networks. Other approaches to obtain information-theoretic security when such an advantage does not exist are schemes based on "public discussion" [6], which utilize two-way communication channels and a public authenticated channel. However, public discussion schemes result in low secrecy rates in scenarios of interest (this discussed in detail in [7]), and the technique proposed here can be used in conjunction with public discussion approaches when two-way communication is possible.

In this work, we exploit *current* hardware limitations of the eavesdropper to achieve everlasting security. Prior work in this area includes the "bounded storage model" of Cachin and Maurer [8]. However, it is difficult to plan on memory size limitations at the eavesdropper, since not only do memories improve rapidly as described by the well-known Moore's Law [9], but they also can be stacked arbitrarily subject only to (very) large space limitations. Our approach, first presented in [10] and further developed in [7], rather than attacking the memory in the receiver back-end, attacks the analog-to-digital converter (A/D) in the receiver front-end, where the technology progresses slowly, and unlike memory, stacking cannot be done arbitrarily due to jitter considerations. Also, from a long-term perspective, there is a fundamental bound on the ability to perform A/D conversion [11]. Hence, we exploit the receiver analog-to-digital conversion processing effect on the received signal to obtain everlasting security. A rapid random power modulation instance of this approach was investigated in [7] and [10], where Alice modulates the signal

This work has been supported, in part, by the National Science Foundation under Grant CIF-1249275.

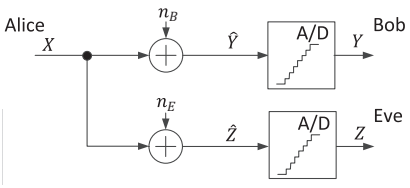

Fig. 1. Wiretap channel with A/Ds.

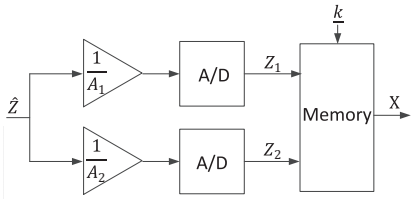

Fig. 2. Eve with sophisticated receiver. To break the power modulation approach of [7] and [10], she can record Z_1 and Z_2 and decode them later - when she obtains the key, the encryption system is broken, or she has access to an unlimited computational power - to obtain the secret message.

by two vastly different power levels. Bob, since he knows the key, can demodulate the signal before his A/D, while Eve fails to do such and information-theoretic security, for a class of attacker model, is obtained. However, the power modulation scheme is susceptible to being broken by an eavesdropper with a more sophisticated receiver than that in the attacker model of [7], as discussed in [7] and shown here in more detail in Section II. Hence, in this paper, Alice adds a random jamming signal to the secret message using the key. Since Bob knows the key, he can cancel the jamming signal before his A/D; on the other hand, Eve must store the signal and try to cancel the jamming signal after her A/D when she obtains the key (since storage of an analog signal is equivalent to a delay line, which is one of the classical weaknesses of analog signal processing). However, the jamming signal is designed such that Eve has already lost the information she would need to recover the secret message.

II. System Model and Approach

A. System Model

We consider a simple wiretap channel, which consists of a transmitter, Alice, a legitimate receiver, Bob, and an eavesdropper, Eve. The eavesdropper is assumed to be passive, i.e. it does not attempt to actively thwart (i.e. via jamming, signal insertion) the legitimate nodes. Thus, the location and channel state information of the eavesdropper is assumed to be unknown to the legitimate nodes. We consider a one-way communication system over AWGN channels, and we include variations of the path-loss in the noise variance. We consider line of sight communication; however, the scheme works similarly on fading channels and only achieves different secrecy rates. Let X denote the current code symbol, $\hat{Y}$ denote the received signal at Bob's receiver, and $\hat{Z}$ denote the received signal at Eve's receiver (Figure 1). We assume that X is taken from a standard Gaussian codebook where each entry has variance P, i.e. $X \sim \mathcal{N}(0, P)$.

The effect of the A/D on the received signal (quantization error) is modeled by both a quantization noise, which is due to the limitation in the size of each quantization level, and missed symbols due to the quantizer's overflow. The quantization noise in this case is (approximately) uniformly distributed [12], so we will assume it is uniformly distributed throughout the paper. For a *b*-bit quantizer (2^b gray levels) over the full dynamic range $[-r, r]$, two adjacent quantization levels are spaced by $\delta = 2r/2^b$, and thus the quantization noise is uniformly distributed over an interval of length δ. Quantizer overflow happens when the amplitude of the received signal is greater than the quantizer's dynamic range. We assume that Alice knows an upper bound on Eve's current A/D conversion ability (without any assumption on Eve's future A/D conversion capabilities).

B. Power Modulation Approach [7], [10]

In this scheme, a very short initial key is either pre-shared between Alice and Bob, or they use a standard key agreement scheme (e.g. Diffie-Hellman [13]) to generate it. This initial key will be used to generate a very long key-sequence by using a standard cryptographic method such as AES in counter mode (CTR) (for more details see [7], [14]). We assume that Eve cannot recover the initial key before the key renewal and during the transmission period. However, we assume (pessimistically) that Eve is handed the full key (and not just the initial key) as soon as transmission is complete. Thus, the goal is to use the cheap (and numerous) cryptographically secure bits of the key stream to obtain "expensive" information-theoretic secret bits at the legitimate receiver. Hence, unlike the cryptographic approaches, even if the encryption system is broken later, Eve will not have enough information to recover the secret message.

As a first step, in [7], [10], we considered a rapid power modulation instance of this approach, where the transmitted signal is modulated by two vastly different power levels at the transmitter. Since Bob knows the key, he can undo the effect of power modulator before his A/D, putting his signal in the appropriate range for analog-to-digital conversion, while Eve must compromise between larger quantization noise and more A/D overflows. Consequently, she will lose information she needs to recover the message, and information-theoretic security is obtained. However, a clear risk of the approach of [7], [10] is a sophisticated eavesdropper with multiple A/Ds. Suppose that Eve has two A/Ds, and she uses them in parallel with a gain in front of each A/D such that each gain cancels the effect of one of the gains that Alice uses to modulate the secret message; thus, she records Z_1 and Z_2 as shown in Figure 2. After completion of the transmission, if Eve obtains the key as we assume, she can use it to retain for each channel use only the element of $\{Z_1, Z_2\}$ from the branch of her receiver properly matched to the transmission gain. In the disadvantaged wireless scenario, Eve's recorded signal then contains more information than Bob's about the transmitted message from Alice, and thus the desired everlasting secrecy

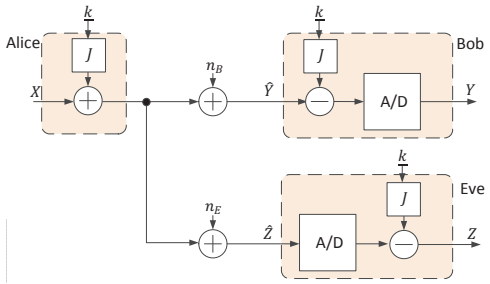

Fig. 3. Bob and Eve both receive the superposition of the message and the random jamming signal. Bob uses the key sequence to cancel the effect of jammer on his signal before the analog-to-digital conversion, while Eve has to wait to obtain the key after completion of transmission and cancel the effect of the jammer after her A/D.

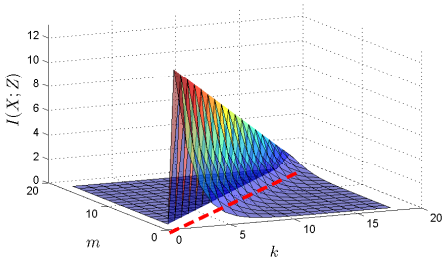

Fig. 4. $I(X;Z)$ versus k (the number of key bits per jamming symbol) and m (the span of Eve's A/D) where $b_e = 20$. It can be seen that when $m = k$ the mutual information is maximized (the red dashed line). Thus, Eve will set the span of her A/D to $2^{k+1}l\sigma$.

is compromised. In the next section, a new approach to utilize the key-bits to obtain everlasting secrecy in the case of an eavesdropper with sophisticated hardware is presented.

C. Random Jamming for Secrecy

In this paper, we propose adding random jamming with large variation to the signal to obtain secrecy (Figure 3). Suppose that Alice employs her cryptographically-secure key bits to select a signal from a uniform discrete distribution to add to the transmitted signal. Now, since Bob knows the key, he can simply subtract off the jamming signal and continue normal decoding with an A/D converter well-matched to the span of the signal. However, Eve does not have knowledge of the key and thus has difficulty matching the span of her A/D to the received signal. If she does not change the span of her A/D, she will lose information due to overflows. On the other hand, if she increases the span of her A/D to contain all of the received signal, the width of each quantization level will increase and thus she will lose information due to higher quantization noise. As before, we assume that the key is handed to Eve as soon as transmission is complete, and obviously Eve could simply subtract the jamming signal off of her *recorded* samples in memory. But, as before, a nonlinear operation (the analog-to-digital converter) has processed the signal, hence allowing the possibility of information-theoretic secrecy *even when the secret key is handed to Eve immediately after the transmission.*[1] Indeed, with her poorly matched A/D, Eve will not have recorded a reasonable version of the signal and we will see that information-theoretic security can be obtained. In this case, one countermeasure for Eve would be to employ parallel receiver branches, each with a different fixed voltage offset; however, this is precisely a higher-resolution A/D over a larger span and thus is captured by the standard A/D model and technology trend lines. In this paper, we will show that, through such a scheme, "cheap" cryptographically-secure key bits can be used to greatly increase the transmission rate of the desired "expensive" information-theoretic secure bits.

[1]We put the previous phrase in italics so that the reader does not confuse the proposed approach with a number of schemes in the information-theoretic secrecy literature that look similar, but must presume that the key (or secret) on which the jamming sequence is based is kept secret from Eve forever.

III. Analysis

Suppose that Eve has a b_e bit A/D and she sets the span of the A/D to $2l\sigma$ to cover $[-l\sigma, l\sigma]$, where l is a constant that maximizes $I(X;Z)$, and $\sigma = \sqrt{P}$ is the standard deviation of the transmitted signal X. Now, suppose that Alice adds a random jamming signal J to X (Figure 3). The amplitude of the jamming signal is random and is chosen based on the pre-shared key between Alice and Bob. In particular, J follows a discrete uniform distribution with 2^k levels between $-c$ and c, where k is the number of key bits per jamming symbol, and c (maximum amplitude of the jamming signal) is an arbitrary constant. In order to maximize the degradation of Eve's A/D, Alice should maximize c. Thus, given that k key bits per jamming symbol is available at Alice, the relationship between k and c is: $(2^k - 1) \times 2l\sigma = 2c$. On the other hand, Eve, in order to maximize $I(X;Z)$, expands the span of her A/D to $2nl\sigma$, where $n = 2^m$ is an arbitrary constant that maximizes $I(X;Z)$. Hence, the new resolution of Eve's A/D will be $\delta'_e = \frac{2l\sigma n}{2^{b_e}} = \frac{2l\sigma}{2^{b_e-m}}$, and since the jamming signal is uniformly distributed, she will miss a $\frac{2^k-2^m}{2^k}$ fraction of the information due to her A/D overflows. In the numerical results, we will show that the best strategy that Eve can take to maximize her mutual information is to set the span of her A/D to $[-c-l\sigma, c+l\sigma]$, or equivalently $m = k$. Hence, in the remainder of this section, we assume the dynamic range of Eve's A/D is $2^{k+1}l\sigma$, and thus no A/D overflow happens. In order to calculate the achievable secrecy rates, $I(X;Y)$ and $I(X;Z)$ are needed. We just show the calculations for the latter here, as $I(X;Y)$ can be obtained in a similar way. The mutual information between X and Z can be written as,

$$\begin{aligned} I(X;Z) &= h(Z) - h(Z|X) \\ &= \int_{-l\sigma}^{l\sigma} -f_Z(z)\log(f_Z(z))dz \\ &\quad - \int_{-\infty}^{\infty} f_X(x) \int_{-l\sigma}^{l\sigma} -f_{Z|X=x}(z)\log(f_{Z|X=x}(z))dzdx, \end{aligned} \quad (1)$$

Hence, we need to calculate the probability density functions (pdf) of Z and $Z|X = x$. The signal at the input of Eve's receiver is $\hat{Z} = J+X+n_e$. Suppose that after analog-to-digital conversion, Eve can somehow obtain the key and cancel the

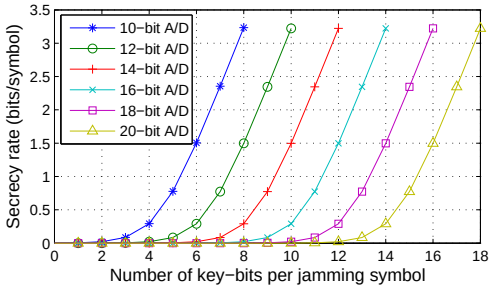

Fig. 5. Achievable secrecy rates versus the number of key bits for 10-bit A/D at Bob and various qualities of Eve's A/D. $P = 1$, $l = 2.5$, and the signal-to-noise ratio of both Eve's and Bob's channels is 30 dB.

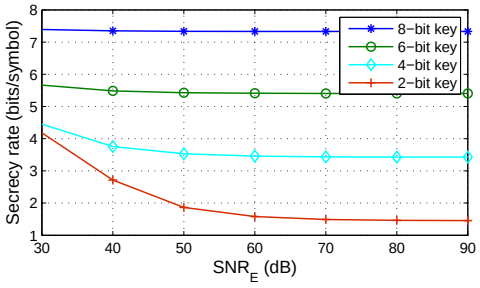

Fig. 6. Achievable secrecy rates versus the signal-to-noise ratio of Eve's channel (SNR_E) for various number of key-bits per jamming symbol at the jammer, when SNR of Bob's channel is 60dB. $P = 1$, $l = 2.5$, and both Bob and Eve use 10-bit A/Ds. Even when the quality of Eve's channel is much better than that of Bob's channel, positive secrecy rates can be achieved.

effect of the jamming signal. Hence, the eventual signal that Eve obtains is, $Z = X + n_e + n_{qe}$. For simplicity of presentation, we define the random variable Z' as $Z' = X + n_e$. Since $X \sim \mathcal{N}(0, P)$ and $n_e \sim \mathcal{N}(0, \sigma_e^2)$, Z' follows a normal distribution with zero mean and variance $P + \sigma_e^2$. Hence, the probability density function of Z is,

$$\begin{aligned} f_Z(z) &= f_{Z'}(z) * f_{n_{qe}}(z) \\ &= \frac{1}{\delta'_e} \int_{-l\sigma}^{l\sigma} f_{Z'}(s) U_{[-\delta'_e/2, \delta'_e/2]}(z-s) ds \\ &= \frac{1}{\delta'_e} \int_{\max(-l\sigma, z-\delta'_e/2)}^{\min(l\sigma, z+\delta'_e/2)} f_{Z'}(s) ds \\ &= \frac{1}{\delta'_e} \left[Q\left(\frac{\max(-l\sigma, z-\delta'_e/2)}{\sqrt{P+\sigma_e^2}} \right) - Q\left(\frac{\min(l\sigma, z+\delta'_e/2)}{\sqrt{P+\sigma_e^2}} \right) \right] \end{aligned} \quad (2)$$

where $U_{[-\delta'_e/2, \delta'_e/2]}(.)$ is the rectangle function on $[-\delta'_e/2, \delta'_e/2]$, i.e. the value of the function is 1 on the interval $[-\delta'_e/2, \delta'_e/2]$ and is zero elsewhere.

The random variable Z' given $X = x$ has a Gaussian distribution with mean x and variance σ_e. Thus, the probability density function of $Z|X = x$ is,

$$\begin{aligned} f_{Z|X=x}(z) &= f_{Z'|X=x}(z) * f_{n_{qe}}(z) \\ &= \frac{1}{\delta'_e} \int_{\max(-l\sigma, z-\delta'_e/2)}^{\min(l\sigma, z+\delta'_e/2)} f_{Z'|X=x}(s) ds = \\ &\frac{1}{\delta'_e} \left[Q\left(\frac{\max(-l\sigma, z-\frac{\delta'_e}{2}) - x}{\sigma_e} \right) - Q\left(\frac{\min(l\sigma, z+\frac{\delta'_e}{2}) - x}{\sigma_e} \right) \right] \end{aligned} \quad (3)$$

Hence, $I(X;Z)$ can be calculated by substituting (2) and (3) in (1). Similarly, $I(X;Y)$ can be calculated by substituting Z with Y, σ_e with σ_b, and δ'_e with δ_b (where δ_b is the resolution of Bob's A/D) in (1), (2), and (3). The achievable secrecy rate can be found by substituting these expressions of the mutual information into $R_s = I(X;Y) - I(X;Z)$.

In the case that the channel between Alice and Eve is noiseless, $I(X;Z)$ can be obtained from (1) by substituting $h(Z)$ and $h(Z|X)$, given that the channel noise is zero. $h(Z)$ can be found by setting $\sigma_e^2 = 0$ in (2), and $h(Z|X)$ can be obtained as,

$$\begin{aligned} h(Z|X) &= \int_{-\infty}^{\infty} h(Z|X=x) f_X(x) dx \\ &= \int_{-\infty}^{\infty} h(X + n_{qe}|X=x) f_X(x) dx \\ &= \int_{-\infty}^{\infty} h(n_{qe}) f_X(x) dx = \log(\delta'_e) \end{aligned} \quad (4)$$

Numerical results are presented in the next section.

IV. Numerical Results

In this section, first we show that $I(X;Z)$ is maximized when Eve sets the span of her A/D to avoid overflow, and then we study the achievable secrecy rates of the proposed method for various scenarios. In order to maximize the mutual information ($I(X;Y)$ or $I(X;Z)$), we set the quantization range by $l = 2.5$ [7]. Since $I(X;Z)$ is an intricate function of the span of Eve's A/D (m) and the number of key bits employed per jamming symbol (k), we find the maximum of this function numerically. In Figure 4, $I(X;Z)$ versus m and k for $b_e = 20$ is shown. It can be seen that the value of $I(X;Z)$ for various numbers of key bits per jamming symbol is maximized when $m = k$. Thus, Eve will set the dynamic range of her A/D to avoid overflow ($2^{k+1} l\sigma$).

In order to see how many cheap bits (cryptographic key bits) per symbol are needed to achieve secrecy, the curves of achievable secrecy rates versus the number of key bits per jamming symbol, for various qualities of Eve's A/D, are shown in Figure 5. In this figure, the transmitter power $P = 1$ (this does not include the jamming power). Although the quality of both channels are the same (signal-to-noise ratio of both channels is 30 dB) and thus the secrecy capacity of the corresponding wiretap channel is zero, by using this method positive secrecy rates are achievable. Further, even in the case that Eve has an A/D of much better quality than Bob's A/D (or she stacked multiple A/Ds of the same quality as Bob's A/D), by utilizing more key bits per jamming symbol, which are "cheap" cryptographic bits and can be obtained at little cost [7], positive secrecy rates (i.e. "expensive" information-theoretically secure bits) can be achieved. Achievable secrecy

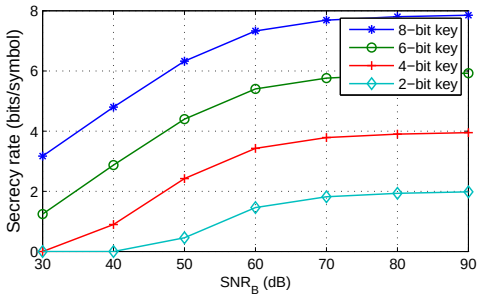

Fig. 7. Achievable secrecy rates versus signal-to-noise ratio of Bob's channel, for various numbers of key-bits per jamming symbol, when Eve's channel is noiseless, i.e. Eve has perfect access to what the transmitter sends and receives and thus no other classical technique is effective. $P = 1$, $l = 2.5$, and both Bob and Eve use 10-bit A/Ds.

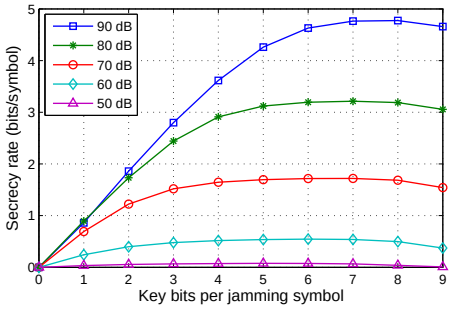

Fig. 8. Secrecy rate versus the number of key bits per jamming symbol (k) for various values of the total SNR, when $P + P_J = 1$, both Bob and Eve have 10 bit A/Ds, and the quality of both channels is the same.

rates versus the signal-to-noise ratio of Eve's channel (SNR_E) for various number of key-bits per jamming symbol at the jammer, when the SNR of Bob's channel is 60dB are depicted in Figure 6. It can be seen that even in the disadvantaged environments that the quality of Eve's channel is better than the quality of Bob's channel, positive secrecy rate can be achieved. In Figure 7, we look at the extreme case that Eve is able to receive exactly what Alice transmits and receives, e.g. the adversary is able to pick up the transmitter's radio and hook directly to the antenna, but the channel between Alice and Bob is noisy and hence no other classical technique[2] is effective. The secrecy rate versus the number of key bits per jamming symbol (k) for a total power constraint is shown in Figure 8. The total power $P+P_J = 1$, both Bob and Eve have 10 bit A/Ds, and both channels have the same quality. When $k = 0$, there is no jamming and all the power is allocated to the signal; thus, the secrecy rate is zero. As the number of key bits (and hence the power allocated to the jamming signal) increases, the secrecy rate increases, until it eventually, as the power allocated to the signal becomes very small, tapers at high jamming powers.

V. Conclusion

In this paper, an approach to utilize ephemeral "cheap" cryptographic key bits to achieve everlasting security in disadvantaged wireless environments is introduced. A random jamming signal chosen from a discrete uniform random ensemble based on a key pre-shared between Alice and Bob is added to each transmitted symbol. The intended receiver uses the key sequence to subtract the jamming signal, while the eavesdropper Eve, in order to prevent A/D overflows, needs to enlarge her A/D span and thus degrade the resolution of her A/D, thus resulting in information loss even if Eve is handed the key at the conclusion of transmission and is able to modify her recorded signal to attempt to remove the jamming effect. The results show that this method can provide secrecy even in the case that the eavesdropper has perfect access to the output of the transmitter's radio and an A/D of much better quality than that of the intended receiver.

[2]Quantum-cryptography techniques [15] are exempt from this.

This work has effectively focused on narrowband channels, where Eve knows the bandwidth employed by the legitimate nodes. For future work, we are interested in the game that arises between the legitimate nodes and Eve when both have access to a wideband channel, where the legitimate nodes might use their cryptographic key bits to try to hide the location of the signal from Eve. With this extra degree of freedom, Eve will be forced to make an additional tradeoff between A/D resolution and sampling frequency.

References

[1] D. Stinson, *Cryptography: Theory and practice*. CRC press, 2006.

[2] R. Benson, "The verona story," *National Security Agency Central Security Service, Historical Publications (available via WWW)*.

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

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

[5] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 62, p. 1906, 2005.

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

[7] A. Sheikholeslami, D. Goeckel, and H. Pishro-nik, "Everlasting secrecy by exploiting non-idealities of the eavesdroppers receiver," *IEEE Journal of Selected Areas in Communication*, vol. 31, no. 9, pp. 1828–1839, 2013.

[8] C. Cachin and U. Maurer, "Unconditional security against memory-bounded adversaries," *Advances in Cryptology*, pp. 292–306, 1997.

[9] R. Kuchibhatla, "IMFT 25-nm MLC NAND: technology scaling barriers broken," *EE Times News and Analysis*, 2010.

[10] A. Sheikholeslami, D. Goeckel, and H. Pishro-nik, "Exploiting the non-commutativity of nonlinear operators for information-theoretic security in disadvantaged wireless environments," *Proc. IEEE Allerton Conference*, pp. 233–240, 2012.

[11] S. Krone and G. Fettweis, "A fundamental physical limit to data transmission and processing," *IEEE Signal Processing Letters*, vol. 17, no. 3, pp. 305–307, 2010.

[12] B. Widrow and I. Kollár, *Quantization noise*. Cambridge University Press, 2008.

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

[14] A. Sheikholeslami, D. Goeckel, and H. Pishro-nik, "Artificial intersymbol interference (ISI) to exploit receiver imperfections for secrecy," in *Proc. IEEE ISIT*, pp. 2950–2954, 2013.

[15] C. H. Bennett, G. Brassard, *et al.*, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, p. 8, 1984.