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 secure transmission from Alice to Bob challenging. We present a method to exploit inherent vulnerabilities of the eavesdropper's receiver through the use of "cheap" cryptographic-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, 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 [7], and the technique proposed here can be used in conjunction with public discussion approaches when there exist two-way communications.

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 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 is obtained. However, the power modulation scheme of [7] is susceptible to being broken by an eavesdropper with a sophisticated receiver, as shown 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. 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, and assume that both Bob and Eve are at a unit distance from the transmitter by including variations of the path-loss in the noise variance; thus, the channel gain of both channels is unity. Both channels experience additive white Gaussian noise (AWGN). 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 \( \delta \). 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 is compromised. In the next section, a new approach to utilize
employ parallel receiver branches, each with a different
obtained. In this case, one countermeasure for Eve would be to
wait to obtain the key after completion of transmission and cancel the effect
of the jammer after her A/D.

Eve will not have recorded a reasonable version of the signal
and we will see that information-theoretic security can be
of 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
operation (the analog-to-digital converter) has processed the
signal at the input of Eve’s A/D, Alice should maximize
the span of her A/D 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 \(2n\sigma\), where \(n = 2^m\) is an arbitrary constant that
maximizes \(I(X; Z)\). Hence, the new resolution of Eve’s A/D
will be 
\[\delta_e' = \frac{2\sigma_m}{2c} = \frac{\sigma}{2^{m/2}} = \frac{\sigma_m}{2^{m/2}},\]
and since the jamming signal is uniformly distributed, she will miss a 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 \(m = k\).

III. ANALYSIS

Suppose that Eve has a \(b\) bit A/D and she sets the span of
the A/D to \(2\sigma\) 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 \(2n\sigma\), where \(n = 2^m\) is an arbitrary constant that
maximizes \(I(X; Z)\). Hence, the new resolution of Eve’s A/D
will be 
\[\delta_e' = \frac{2\sigma_m}{2c} = \frac{\sigma}{2^{m/2}} = \frac{\sigma_m}{2^{m/2}},\]
and since the jamming signal is uniformly distributed, she will miss a 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,

\[I(X; Z) = h(Z) - h(Z|X)\]

\[= \int_{-l\sigma}^{l\sigma} -f_Z(z) \log(f_Z(z))dz\]

\[+ \int_{-\infty}^{-l\sigma} f_X(z) \int_{-\infty}^{-l\sigma} -f_Z|X=x(z) \log(f_Z|X=x(z))dzdx,\]  

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 \(Z = J + X + n_x\). Suppose that after analog-to-digital
conversion, Eve can somehow obtain the key and cancel the

---

1We 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.
effect of the jamming signal. Hence, the eventual signal that 
Eve obtains is, $Z = X + n_c + n_{qe}$. For simplicity of presentation, we define the random variable $Z'$ as $Z' = X + n_c$. Since $X \sim \mathcal{N}(0, P)$ and $n_c \sim \mathcal{N}(0, \sigma_c^2)$, $Z'$ follows a normal distribution with zero mean and variance $P + \sigma_c^2$. Hence, the probability density function of $Z$ is,

$$f_Z(z) = f_{Z'}(z) * f_{n_{qe}}(z)$$

$$= \frac{1}{\delta_c} \int_{-\delta_c}^{\delta_c} f_{Z'}(s)U(-\delta'_c/2,\delta'_c/2)(z-s)ds$$

$$= \frac{1}{\delta_c} \int_{\min(-\delta_c, z-\delta'_c/2)}^{\max(-\delta_c, z-\delta'_c/2)} f_{Z'}(s)ds$$

$$= \frac{1}{\delta_c} \left[ Q \left( \frac{\max(-l\sigma, z-\delta'_c/2)}{\sqrt{P + \sigma_c^2}} \right) - Q \left( \frac{\min(l\sigma, z + \delta'_c/2)}{\sqrt{P + \sigma_c^2}} \right) \right]$$

(2)

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

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

$$f_{Z|X=x}(z) = f_{Z'|X=x}(z) * f_{n_{qe}}(z)$$

$$= \frac{1}{\delta_c} \int_{\min(l\sigma, z+\delta_c'/2)}^{\max(-l\sigma, z-\delta_c'/2)} f_{Z'|X=x}(s)ds$$

$$= \frac{1}{\delta_c} \left[ Q \left( \frac{\max(-l\sigma, z-\delta_c'/2)}{\sigma_c} - x \right) - Q \left( \frac{\min(l\sigma, z + \delta_c'/2)}{\sigma_c} - x \right) \right]$$

(3)

Hence, $I(X;Z)$ can be calculated by substituting (2) and (3) in (1). Similarly, $I(Y;Z)$ can be calculated by substituting $Z$ with $Y$, $\sigma_c$ with $\delta_k$, and $\delta'_c$ with $\delta_k$ (where $\delta_k$ is the resolution of Bob’s A/D) in (1), (2), and (3). The achievable secrecy rate can be found by substituting these expressions for 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 $\sigma_c^2 = 0$ in (2), and $h(Z|X)$ can be obtained as,

$$h(Z|X) = \int_{-\infty}^{\infty} h(Z|X = x)f_X(x)dx$$

$$= \int_{-\infty}^{\infty} h(X + n_{qe}|X = x)f_X(x)dx$$

$$= \int_{-\infty}^{\infty} h(n_{qe})f_X(x)dx = \log(\delta'_e)$$

(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 quantization range to $l = 2.5$ [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 ($2^{k+1}\sigma$).

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, is shown in Figure 5. In this figure, the transmitter power $P = 1$, where this does not include the jamming power (a total power constraint will be considered below). 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, 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. In Figure 6, the secrecy rate versus signal-to-noise ratio of both Bob and Eve’s channel ($\text{SNR}_B = \text{SNR}_E = \text{SNR}$) is shown. In this case, Bob has a 10 bit A/D while Eve has a much better (16 bit) A/D. It can be seen that even when Eve’s analog-to-digital conversion abilities are higher (i.e. either Eve’s A/D is 64 times better than Bob’s A/D, or she stacks 64 A/Ds of the same quality as Bob’s A/D), the proposed method can result in meaningful positive secrecy rates.

The secrecy rate versus the number of key bits per jamming symbol ($k$) for a total power constraint is shown in Figure 7. The total power $P + P_J = 1$, both Bob and Eve have 10 bit A/Ds, and the quality of both channels is the same. 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. Finally, 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 technique is effective. In Figure 8, it can be seen that by using the proposed method, positive secrecy rates are still available to the legitimate nodes.

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 suggest 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.

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