

Active Eavesdropping in Fast Fading Channels: A Block-Markov Wyner Secrecy Encoding Scheme

George T. Amariuca
Iowa State University, USA
E-mail: gamari@iastate.edu

Shuangqing Wei
Louisiana State University, USA
E-mail: swei@ece.lsu.edu

Abstract—This paper studies the problem of active eavesdropping in fast fading channels. The active eavesdropper (Eve-A) is a more powerful adversary than the classical eavesdropper. It can choose between two functional modes: eavesdropping (Ex mode), and jamming (Jx mode) – Eve-A cannot function in full duplex mode. We consider the most conservative scenario, when the Eve-A can choose her strategy based on the legitimate transmitter-receiver pair’s strategy – and thus the transmitter and legitimate receiver have to plan for the worst. We introduce a novel encoding scheme, based on very limited and unprotected feedback – the *Block-Markov Wyner (BMW) encoding scheme* – which outperforms any schemes currently available.

I. INTRODUCTION

The benefits of the ergodic-fading diversity upon the achievable secrecy rates have been exposed by [1], [2], [3]. A fast-fading eavesdropper channel is studied in [1] under the assumption that the main channel is a fixed-SNR additive white Gaussian noise (AWGN) channel. Although the secrecy capacity for fast-fading eavesdropper channels is still unknown, [1] provides achievable secrecy rates and shows that sometimes noise injection at the transmitter can improve these rates. The different approach of [2], [3] models both channels as ergodic-fading AWGN channels. However, the fading is assumed to be slow enough to be considered constant for infinitely long blocks of transmitted symbols, so that separate channel encoding can be used for each block.

Although the slow-fading-ergodic-channel model can be artificially created by a multiplexing/demultiplexing architecture [4], it still requires either coarse quantization or long delays (under fine quantization, for a channel state with low probability it may take forever to gather a large enough number of symbols to enable almost-error-free decoding). A different approach in [5] uses such an architecture to generate a secret key (no delay constraints), while the delay-constrained traffic uses the previously-generated keys as one-time-pads. In this paper, we focus on a scenario where both the main and the eavesdropper’s channel are affected by *fast* stationary fading. However, unlike [1], we are concerned with a much stronger sort of adversary: the *active eavesdropper* (Eve-A).

In our channel model, depicted in Figure 1, the eavesdropper (Eve-A) has two options: either to jam the conversation between the legitimate transmitter (Alice) and the legitimate receiver (Bob) – Jx mode – or to eavesdrop – Ex mode – (Eve-A cannot both transmit and receive on the same frequency, at the same time). Both Alice and Eve-A (in Jx mode) are

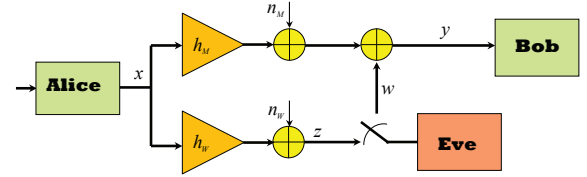


Fig. 1. Channel model

constrained by average (over each codeword) power budgets \mathcal{P} and \mathcal{J} , respectively. Eve-A’s purpose is to minimize the secrecy rate achievable by Alice, and to that extent she has to decide on the optimal alternation between Jx mode and Ex mode. The state of each of the main and eavesdropper channels, i.e. the absolute squared channel coefficients (or simply “the channel coefficients” hence forth), which we denote by h_M and h_W , respectively, are assumed to be available to the respective receivers. However, Bob does not know the exact state of Eve-A’s channel, nor has Eve-A any information about Bob’s channel, except its statistics. Each channel is further distorted by an independent additive white complex Gaussian noise of variance σ_N^2 . We assume the existence of a low-rate, unsecured feedback channel between Bob and Alice.

This paper is limited to the following simplifying assumptions: i) Rayleigh fading: h_M and h_W are exponentially distributed, with parameters λ_M and λ_W respectively; ii) Eve-A uses white Gaussian noise for jamming [6], [7] (the most harmful uncorrelated jamming strategy [8]); iii) the channel that links Eve-A (when in Jx mode) and Bob is error-and-fading-free [7], [9]; this ensures that the statistics of the jamming signal, at Bob, are still Gaussian; iv) Eve-A’s exact jamming strategy (i.e. when and with what power she jams) is perfectly known to Bob (a posteriori) so that Bob can employ coherent detection and communicate Eve-A’s strategy to Alice at the end of the transmission, via the low-rate feedback link; v) the instantaneous state of the main channel cannot be known to Alice non-causally; vi) the codewords are long enough such that not only the channel fading, but also the combination of channel fluctuation and Eve-A’s alternation between jamming and eavesdropping display ergodic properties over the duration of a codeword; vii) Eve-A employs an ergodic strategy, i.e. she uses the same statistics for alternating between Jx mode and Ex mode for every codeword. Our contributions can be stated as follows: (a) We introduce the concept of “active

eavesdropper”; (b) we show that, under the most conservative scenario, Wyner’s scheme [10] performs poorly (if at all); (c) we provide a much-better-performing BMW secrecy encoding scheme, which only requires a low-rate, unprotected feedback transmission from Bob to Alice.

II. THE WORST-CASE SCENARIO

In this paper we assume, for simplicity, that Eve-A can know the exact value of her channel coefficient h_W only if and after she made her decision to eavesdrop (Ex mode), and has no information about the value of h_W while she is in Jx mode. This scenario models a situation where the training sequences, which are transmitted by Alice at a low rate, and are used by Bob to estimate the channel coefficient before the transmission of a block of symbols, are protected against eavesdropping. Nevertheless, Eve-A can eventually estimate her channel coefficient if more received data is available, i.e. at the end of a block. Hence Eve-A takes the decision to jam or to eavesdrop randomly. Denote $q = \Pr\{\text{Ex mode}\}$ the probability that Eve-A is in Ex mode. Since Eve-A’s strategy is not known in advance, a Wyner-type scheme designed for a specific parameter $q_0 = \Pr\{\text{Ex mode}\}$ may fail if Eve-A decides to use any different strategy. Instead, a Wyner-type scheme should have a forwarding rate low enough to protect against the most powerful attack on intelligibility (when Eve-A is in Jx mode all the time), and with a secrecy rate low enough protect against the most powerful attack on secrecy (when Eve-A is in Ex mode all the time). The achievable secrecy rate for this kind of scheme is

$$R_{s,wcs} = \left[\mathbf{E}_{h_M} \left[\log \left(1 + \frac{h_M \mathcal{P}}{\sigma_N^2 + \mathcal{J}} \right) \right] - \mathbf{E}_{h_W} \left[\log \left(1 + \frac{h_W \mathcal{P}}{\sigma_N^2} \right) \right] \right]^+. \quad (1)$$

The fact that both Alice and Eve-A (if she transmits) use constant powers \mathcal{P} and \mathcal{J} , respectively, follows since $R_{s,wcs}$ is a convex function of \mathcal{P} for fixed \mathcal{J} , and a concave function of \mathcal{J} for fixed \mathcal{P} , and will not be proved here for brevity. Note that the achievable secrecy rate in (1) is rarely strictly positive. In fact, under assumption i) of the previous section, $R_{s,wcs} > 0$ holds if and only if $\lambda_W > \lambda_M(1 + \frac{\mathcal{J}}{\sigma_N^2})$. For a large jamming-power-to-noise ratio \mathcal{J}/σ_N^2 , this implies that Eve-A’s channel needs to be impractically worse than Bob’s.

However, the above scheme does not take full advantage of the model characteristics. Recall the original assumption that Eve-A can function only as a half-duplex terminal. Therefore, whenever Eve-A is in Jx mode, she cannot eavesdrop – so the whole transmission remains perfectly secret to Eve-A – and conversely, if in Ex mode, Eve-A cannot simultaneously jam.

III. THE BLOCK-MARKOV WYNER (BMW) ENCODING SCHEME FOR THE ACTIVE EAVESDROPPER CHANNEL

There are two main reasons why Wyner’s scheme [10] does not work in our model. First, Alice does not know the statistics of Bob’s channel in advance – Eve-A has control

over the signal-to-noise ratio of this channel. Therefore, the main channel can be modeled as a compound channel. In order to reliably transmit a message to Bob, Alice should use a special kind of encoding. It was shown in [11] that the same layered encoding technique that achieves the points on the boundary of the capacity region for broadcast channels can also be used for transmission over compound channels. Our scheme uses the broadcast layered encoding of [11] to ensure that reliable transmission is possible between Alice and Bob even in the most unfavorable conditions. However, even if such a scheme were used, Alice could not know in advance which messages will actually be decodable by Bob. The second reason is that Alice does not know the statistics of Eve-A’s channel in advance – due to the alternation between jamming and eavesdropping, Eve-A’s equivalent channel is actually weaker than her physical channel. Hence, Alice cannot directly transmit a secret message at a rate larger than $R_{s,wcs}$, because she is not sure whether the secrecy would be compromised.

Our novel BMW scheme solves both of these problems: it guarantees both the intelligibility and the secrecy of the message, for a transmission rate much larger than $R_{s,wcs}$.

An alternative to Wyner’s secrecy scheme for regular passive eavesdropper channels: a-posteriori binning

We begin by studying a scenario where, before the transmission takes place, Alice and Bob already share a secret key. In addition to the secret message that can be encoded by Wyner’s scheme, another secret message can be transmitted over the channel. This latter message is encrypted using the secret key. We provide two encoding schemes that can both achieve the simultaneous transmission of the two secret messages.

Denote the capacities of the channels from Alice to Bob and to Eve-A by C_M and C_E , respectively, the achievable secrecy rate (under Wyner’s original scheme) by R_k , the rate of the encrypted message by R_s and the codeword length by N .

Scheme 1: Wyner’s scheme with an encrypted message. Alice bins the codebook (containing $2^{N C_M}$ codewords) into $2^{N R_k}$ “super-bins”, such that $R_k \leq C_M - C_E$. The first secret message picks the index of a super-bin. The super-bin is then binned again into $2^{N(C_M - R_s - R_k)}$ bins (each containing $2^{N R_s}$ bin-words). One of the bins is picked randomly, while a specific codeword in that bin is picked according to the encrypted message.

Scheme 2: The alternative encoding scheme. The codebook is randomly binned into $2^{N(C_M - R_s)}$ bins – let us denote these as “pre-bins”. Each pre-bin consists of $2^{N R_s}$ bin-words. The bins are then randomly grouped into $2^{N R_k}$ “super-bins”, such that each super-bin consists of $2^{N(C_M - R_s - R_k)}$ bins, and where R_k is picked to satisfy $R_k \leq C_M - C_E$. The first secret message picks the index of a super-bin. A bin inside that super-bin is randomly picked, and the transmitted codeword is then picked by the encrypted message inside this bin. A similar strategy was discussed in [12].

The two schemes are equivalent. Recall that Wyner’s scheme [10] involves random binning of the codebook into bins, each of them a good code for Eve-A’s channel. The actual

transmission does not contain information about the binning itself. Hence, the same “random” binning is done separately at Alice (before the transmission) and at Bob (before he can begin decoding). The reason why Alice performs the binning of the codebook before transmitting is because she needs to send a *meaningful* secret message over the coming frame (so the transmitted codeword needs to belong to the particular bin indexed by this message). However, if the “secret message” had no meaning, both Alice and Bob could perform the binning after the transmission ends. The “secret message” generated this way could be thought of as a *secret key* for encrypting a meaningful message over the next frame.

Suppose that Eve-A’s channel is unknown to Alice and Bob until the end of the codeword. The first codeword is randomly selected from the whole un-binned codebook. After transmission ends, Alice and Bob realize that the secrecy capacity was R_s . Both Bob and Alice can now proceed to the (same) binning of the codebook – the same single bin will be identified by both as containing the transmitted message, and its index will be secret to Eve-A. The secret message conveyed by this index has no meaning, but can be used over the next frame, as a secret key. Over the second frame, Alice and Bob use *Scheme 2* above. At the end of the second frame, Alice and Bob determine what the secrecy capacity was, and a new secret key is agreed upon.

Three observations are in order. First, the secret key (decided upon at the end of the frame) and the encrypted message (carried by the frame) cannot overlap and maintain the same equivocation at Eve-A [13]. Hence, it is required that $R_s + R_k \leq C_M$. Second, the key is used as a one-time pad to encrypt the secret message of the next frame, therefore, if $R_s < C_M/2$, the transmission of the meaningful secret message can be done at almost the secrecy capacity, with a small initial penalty (since the first frame does not carry an encrypted message) which becomes negligible as the number of transmitted frames increases. Third, our new protocol can be used whenever Alice does not have a good description of Eve-A’s channel until the transmission of the codeword ends, which is precisely the case with our current model.

Detailed description of the BMW encoding scheme

Eve-A’s strategy consists of choosing the parameter $q = \Pr\{\text{Ex mode}\}$. Once the transmission of a codeword (we shall denote the span of a codeword by “frame”) is finished, Bob can accurately evaluate the parameter q used by Eve-A over that frame. Bob can then feed this value back to Alice. Note that the knowledge of q provides Alice with the statistical description of both the main channel – determined by $(1 - q)$ – and the eavesdropper’s channel – determined by q . Before learning Eve-A’s strategy, the channel between Alice and Bob appears like a compound channel to the legitimate parties. The possible states of this channel are given by Eve-A’s strategy q , which takes values in the interval $[0, 1]$. To transform this uncountable set of possible channel states into a finite set, we divide the interval $[0, 1]$ to which q belongs into subintervals such that $[0, 1] = [q_0, q_1) \cup [q_1, q_2) \dots \cup [q_{n-1}, q_n]$, where

$q_0 = 0$ and $q_n = 1$. To convey a message to Bob, Alice uses an n -level broadcast-channel-type codebook, as in [11]. Level i is allocated power $(1 - \alpha_i)\alpha_{i-1} \dots \alpha_1 P$ (with $\alpha_j \in [0, 1] \forall j = 1, \dots, n-1$ and $\alpha_n = 0$) and is designed to deal with a jammer which is on with probability $1 - q_{i-1}$ over each channel use. Note that $q_0 < q_1 < \dots < q_n$. In the remainder of this section, we shall say that level i is “stronger” than level j if $i < j$, i.e. if level i can deal with a jammer which is on more often. The notation is fully justified by Lemma 1 below.

Denote the rates of the different encoding levels as:

$$R_1 = \mathbf{E}_{h_M} \left[\log \left(1 + \frac{(1 - \alpha_1)Ph_M}{\sigma_N^2 + \alpha_1 Ph_M + \mathcal{J}} \right) \right] \quad (2)$$

for the strongest level, which can deal with the case when Eve-A is always in Jx mode, i.e. $q = q_0 = 0$,

$$R_{i+1} = \mathbf{E}_{h_M} \left[q_i \log \left(1 + \frac{(1 - \alpha_{i+1})\alpha_i \dots \alpha_1 Ph_M}{\sigma_N^2 + \alpha_{i+1} \dots \alpha_1 Ph_M} \right) + (1 - q_i) \log \left(1 + \frac{(1 - \alpha_{i+1})\alpha_i \dots \alpha_1 Ph_M}{\sigma_N^2 + \alpha_{i+1} \dots \alpha_1 Ph_M + \frac{\mathcal{J}}{1 - q_i}} \right) \right], \quad (3)$$

for $i = 1, 2, \dots, n-2$, and finally

$$R_n = \mathbf{E}_{h_M} \left[q_{n-1} \log \left(1 + \frac{\alpha_{n-1} \dots \alpha_1 Ph_M}{\sigma_N^2} \right) + (1 - q_{n-1}) \log \left(1 + \frac{\alpha_{n-1} \dots \alpha_1 Ph_M}{\sigma_N^2 + \frac{\mathcal{J}}{1 - q_{n-1}}} \right) \right], \quad (4)$$

for the weakest level, corresponding to the case when Eve-A is in Jx mode with probability $1 - q_{n-1}$. Note that the encoding levels are designed such that Bob decodes the stronger levels first, and treats the remaining un-decoded messages as white noise. The codebook for level i contains 2^{NR_i} codewords of length N , generated such that each component of each codeword represents an independent realization of a Gaussian random variable of mean 0 and variance $(1 - \alpha_i)\alpha_{i-1} \dots \alpha_1 P$. The relative strength of the encoding levels is established by the following intuitive lemma, the proof of which [14] is omitted here for brevity.

Lemma 1: If Eve-A uses a parameter $q \in [q_{i-1}, q_i)$ over a frame, then the messages encoded in levels $1, 2, \dots, i$ are intelligible by Bob at the end of the frame. Thus the forwarding rate from Alice to Bob is $R_{M,i} = R_1 + R_2 + \dots + R_i$.

Consider the first frame, for which the transmitted message carries no useful information, but rather its symbols are selected in a random, i.i.d. fashion. Once Alice receives the feedback sequence from Bob at the end of the frame, describing Eve-A’s strategy (i.e. the value of q – actually, as we shall see shortly, only the interval $[q_{i-1}, q_i)$ that contains q is enough information for Alice), Alice and Bob can separately agree on the same secret message, as described in the protocol above. This message will function as a secret key for encrypting a meaningful secret message over the next frame. In turn, the secret message agreed upon at the end of the second frame can function as a secret key for the third frame, and so on.

To formalize the intuitive description above, we begin by stating several definitions: (1) The “encrypted message” is a meaningful secret message, encrypted with the help of a secret key that was generated in the previous frame. (2) The “secret key” is a meaningless random message, which is perfectly secret to Eve-A, is agreed upon by both Alice and Bob at the end of the frame, and can be used for the encryption of a secret message (of at most the same length) over the next frame. (3) The term “secret key rate” refers to the rate at which a secret key is generated at the end of a frame – the correspondent of Wyner’s “secrecy capacity”. (4) The term “achievable secrecy rate” refers to the rate of transmission of the encrypted message.

Our encoding scheme works as follows. First, the n codebooks, indexed by i , with $i \in \{1, 2, \dots, n\}$ are generated as described above, and are made available to all parties. On a given frame, Alice transmits an encrypted message, at a rate $R_s \leq 0.5R_1$ (we show in Theorem 3 below that this constraint does not incur any loss of performance) – note that the *encrypted message* is encrypted with the help of a secret key generated over a previous frame. To transmit the encrypted message, Alice randomly bins codebook 1 into $2^{N(R_1-R_s)}$ bins. One of the bins (each containing 2^{NR_s} codewords) will be picked randomly (uniformly), and the encrypted message will pick a codeword from this bin for transmission. Recall that the reason why Alice cannot directly bin the codebook for generating the secret key is because Eve-A’s strategy (hence her equivalent channel) is unknown until the end of the frame. An additional $n-1$ codewords are also chosen randomly, one from each of the remaining codebooks. Alice’s transmitted sequence is the sum of the n codewords.

At the end of the frame, Bob feeds back to Alice the exact value of Eve-A’s strategy q over that frame. To agree on a secret key, Alice and Bob first need to know which encoding levels are decodable by Bob, and which are decodable by Eve-A. Only the information encoded in those levels that are decodable by Bob, but are not perfectly decodable by Eve-A, can contribute to the generation of the secret key.

Due to the code construction (see Lemma 1), under any jamming/ eavesdropping strategy, Bob will be able to decode the strongest level first, treating the other levels as white noise, and then perform successive interference cancellation to decode increasingly weaker levels. However, the same does not hold for Eve-A. Eve-A’s channel is quite different from Bob’s. While the code is designed to handle Bob’s unknown-length interference channel, Eve-A sees an interference-free channel that is totally interrupted $(1-q)$ of the time. In the general case, it is thus possible that the order of strength of the encoding levels, from Eve-A’s perspective, is not the same as that from Bob’s perspective. For example, for a code with 7 levels Bob might be able to decode only levels 1, 2, 3, 4, while Eve-A may be able to perfectly decode only levels 1, 4, 6, 7. In this case, we can re-order the levels from Eve-A’s perspective, as 1, 4, 6, 7, 2, 3, 5. The first four levels are decodable by Eve-A perfectly, the next two are decodable by Bob, but not by Eve-A, and the last level is decodable by neither. Only levels

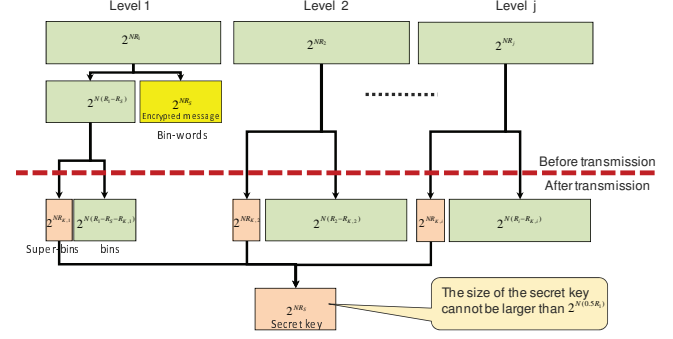


Fig. 2. BMW encoding method – most general case, when $1 \in \mathcal{I}_{ne}$.

2 and 3 can be used for generating the secret key.

For the general case, we shall denote the ordered set of indices corresponding to the encoding levels specified by their rates in (2)-(4) by \mathcal{J} , and the set of indices corresponding to the order of strength of the encoding levels from Eve-A’s perspective by $\widehat{\mathcal{J}}$. There exists a bijection (i.e. a re-ordering) $\mathbb{B} : \mathcal{J} \rightarrow \widehat{\mathcal{J}}$, defined as follows: (1) the set of indices (in arbitrary order) corresponding to levels that are perfectly decodable by Eve-A is denoted \mathcal{J}_e ; (2) the set of indices corresponding to levels that are not perfectly decodable by Eve-A, but perfectly decodable by Bob is denoted \mathcal{J}_k ; (3) the set of indices corresponding to levels that are not perfectly decodable by either Eve-A or Bob is denoted \mathcal{J}_n ; (4) the ordered set $\widehat{\mathcal{J}}$ is defined as $\widehat{\mathcal{J}} = \{\mathcal{J}_e, \mathcal{J}_k, \mathcal{J}_n\}$. Furthermore, we define $\mathcal{I}_{ne} = \{\mathcal{J}_k, \mathcal{J}_n\}$ as the set of indices corresponding to encoding levels which are not perfectly decodable by Eve-A. The method of encoding is described in Figure 2. Theorem 2 below provides the achievable secret key rate for the general case. Its proof is given in [14].

Theorem 2: Suppose that Eve-A picks a strategy $q \in [q_{i-1}, q_i)$ over a frame. Then an achievable secret key rate is

$$R_{k,i} = \sum_{j \in \mathcal{J}_k} [R_j - R_{E,j}], \quad (5)$$

where R_j are defined as in (2)-(4) for $j = 1, 2, \dots, n$, and $R_{E,j}$ are selected such that they satisfy the following conditions:

$$R_{E,1} \geq 0.5R_1, \text{ if } 1 \in \mathcal{I}_{ne}, \quad (6)$$

$$R_{E,l} \leq R_l \quad \forall l \in \mathcal{I}_{ne} \quad (7)$$

$$\sum_{l \in \mathcal{J}} R_{E,l} \leq q \mathbf{E}_{h_W} \left[\log \left(1 + \frac{\sum_{l \in \mathcal{J}} (1 - \alpha_l) \alpha_{l-1} \dots \alpha_1 P h_W}{\sigma_N^2} \right) \right] - \epsilon, \quad (8)$$

for any subset \mathcal{S} of \mathcal{I}_{ne} , and with equality for $\mathcal{S} = \mathcal{I}_{ne}$, where ϵ is positive and arbitrarily close to zero. The expression in (8) uses the convention $\alpha_n = 0$. Note that the bijection \mathbb{B} defined above also depends on Eve-A’s strategy q , and hence

on the interval i to which q belongs. Therefore, the set of indices \mathcal{S}_k depends on i .

We have seen the best achievable secret key rate if $q \in [q_{i-1}, q_i]$. The next theorem provides Eve-A's optimal strategy under our assumption that Eve-A knows Alice's strategy in advance, and also Alice's best achievable secrecy rate.

Theorem 3: (1) If Eve-A chooses a strategy $q \in [q_{i-1}, q_i]$, then it is optimal for her to choose q arbitrarily close to q_i .

(2) Eve-A's optimal strategy is the same over all frames.

(3) Denote the achievable secret key rates by $\{R_{k,i} : i = 1, 2, \dots, n\}$, where $R_{k,i}$ is the best achievable secret key rate given by Theorem 2, under $q = q_i$. Then Eve-A's optimal strategy is $q_{i_{opt}} = \arg \min_{q_i} \{R_{k,i}\}$, if $\min_{q_i} \{R_{k,i}\} < 0.5R_1$, and $q_{i_{opt}} = q_1$, otherwise.

(4) Under Eve-A's optimal strategy, the maximum achievable secrecy rate (under the current setup) is $R_s = \min\{0.5R_1, R_{k,i_{opt}}\}$.

(5) There is no loss of performance incurred by restricting the rate of the encrypted message to $R_s \leq 0.5R_1$.

Proof: (1) Using Theorem 2, it is easy to check that, given $q \in [q_{i-1}, q_i]$, the achievable secret key rate is a decreasing function of q . Therefore, if $q \in [q_{i-1}, q_i]$, Eve-A's optimal strategy is to pick q arbitrarily close to q_i .

(2),(3),(4) We have already seen that the rate at which the encrypted message is transmitted is restricted to $R_s \leq 0.5R_1$. If $\min_{q_i} \{R_{k,i}\}$ is achieved by $q_{i_{opt}}$ and is less than $0.5R_1$, then switching to a different Eve-A's strategy q_d will only increase the rate of generation of the secret key, and hence the rate of transmission of the encrypted message. On the other hand, if $\min_{q_i} \{R_{k,i}\} \geq 0.5R_1$, then no matter what Eve-A's strategy is, the secrecy rate will always equal $0.5R_1$.

(5) Alice has to protect the encrypted message against jamming. But if Eve-A chooses to constantly play $q \in [0, q_1]$, Bob will only be able to decode level 1 of the code. This message, transmitted at a maximum rate of R_1 , has to carry an encrypted message and generate a secret key, simultaneously. But if Eve-A's strategy remains in $[0, q_1]$ over next frames, the rate of the encrypted message cannot exceed $0.5R_1$ – not enough secret key bits to encrypt it. Therefore, the strategy $q \in [0, q_1]$ can function as a “default” state for Eve-A, where she could take refuge if the achievable secrecy rate under any other strategy exceeded $0.5R_1$. ■

IV. NUMERICAL RESULTS AND CONCLUSIONS

In Figure 3 we show the significant improvement of our BMW scheme over the worst-case scenario approach (a passive receiver or equivalently $n = 1$ in our scenario) of (1), when $\lambda_W > \lambda_M(1 + \frac{\sigma_N^2}{\sigma_M^2})$.

The achievable secrecy rates when either a pure jammer or a passive eavesdropper replaces Eve-A (and Alice and Bob are aware of this change) are given for comparison. Note the disastrous effect of the active eavesdropper. Also note how the improvement in the secrecy rate for the transition from $n = 1$ to $n = 2$ is larger than that for the transition from $n = 2$ to $n = 3$. Additional comments on the behavior of the secrecy rate as $n \rightarrow \infty$, as well as about the complexity and a possible

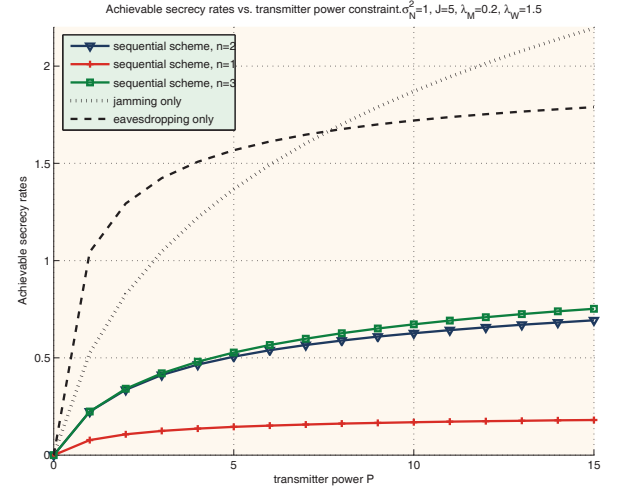


Fig. 3. Achievable secrecy rates with our BMW secrecy encoding scheme for $J = 5$, $\sigma_N^2 = 1$. Exponentially distributed channel coefficients with $\lambda_M = 0.2$, $\lambda_W = 1.5$

simplification of the numerical algorithm required to find the optimal $\{(\alpha_i, q_i) : i = 1, 2, \dots, n\}$ can be found in [14].

REFERENCES

- [1] Z. Li, R. Yates, and W. Trappe, “Secret communication with a fading eavesdropper channel,” *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, June 2007.
- [2] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.
- [3] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, pp. 2470–2492, June 2008.
- [4] A. J. Goldsmith and P. P. Varaiya, “Capacity of fading channels with channel state information,” *IEEE Trans. Inform. Theory*, vol. 43, pp. 1986–1992, Nov. 1997.
- [5] K. Khalil, O. O. Koiluglu, H. E. Gamal, and M. Youssef, “Opportunistic secrecy with a strict delay constraint,” *Submitted to IEEE Transactions on Information Theory*, 2009.
- [6] E. Altman, K. Avrachenkov, and A. Garnaev, “A jamming game in wireless networks with transmission cost,” *Proceedings of Net-Coop, Avignon, France*, June 2007.
- [7] S. Shafiee and S. Ulukus, “Capacity of multiple access channels with correlated jamming,” *Military Communications Conference, MILCOM*, vol. 1, pp. 218–224, Oct. 2005.
- [8] S. N. Diggavi and T. Cover, “The worst additive noise under a covariance constraint,” *IEEE Trans. Inform. Theory*, vol. 47, pp. 3072–3081, Nov. 2001.
- [9] A. Kashyap, T. Basar, and R. Srikant, “Correlated jamming on mimo Gaussian fading channels,” *IEEE Trans. Inform. Theory*, vol. 50, pp. 2119–2123, Sept. 2004.
- [10] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.
- [11] T. M. Cover, “Broadcast channels,” *IEEE Trans. Inform. Theory*, vol. 18, pp. 2–14, Jan. 1972.
- [12] A. E. G. Y.-K. Chia, “Wiretap channel with causal state information,” *arXiv:1001.2327*, 2010.
- [13] B. Schneier, *Applied cryptography*. John Wiley & Sons, 1996.
- [14] G. Amariuca and S. Wei, “Half-duplex active eavesdropping in fast fading channels: A block-markov wyner secrecy encoding scheme,” *Submitted to IEEE Transactions on Information Theory*, available on *arXiv:1002.1313*, 2010.