New Directions in Information Theoretic Security: Benefits of Bidirectional Signaling

Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802.
yener@ee.psu.edu

***Abstract*—The past decade has witnessed significant effort towards establishing reliable and information theoretically secure rates in communication networks, taking advantage of the properties of the communication medium. Such efforts include those in the wireless medium where simultaneous transmissions and the ensuing interference can prove advantageous from an information theoretic secrecy point of view. With the goal of obtaining a secrecy rate that scales with transmit power, structured signaling with simultaneous favorable signal alignment at the legitimate receiver(s) and unfavorable signal alignment at the eavesdropper(s) has proven particularly useful in multi-terminal Gaussian channels. Many challenges remain however in realizing the vision of absolute security provided by the wireless physical layer including handling more realistic models. In this paper, we provide a brief overview of the state of the art, the forward look and argue for an additional asset that could be utilized for secrecy, i.e., bidirectional signaling. Taking the bidirectional wiretap channel as an example, Gaussian signaling is demonstrated to be as good as structured signaling from the degrees of freedom point of view, while observed to be performing better with finite transmit power. Moreover, taking bidirectional signals explicitly into account for encoding performs even better and provides a way forward to synergistically combine physical layer based secrecy and encryption.**

I. Introduction

Information theoretic security by enlarge deals with providing reliable communication rates between legitimate parties with confidentiality (secrecy) guarantees from eavesdroppers irrespective of their computational power. Information theoretic security was first formalized by Shannon [1]. Shannon defined the notion of secure information transfer by comparing the entropy of the message to the entropy of the message given the observation of an eavesdropper (cryptanalyst). He showed that, if the eavesdropper were to observe the exact signal sent by a transmitter, then, in order to ensure no reduction in the entropy of the message, i.e., perfect secrecy, the transmitter and the receiver would have to share a key (presumably through a secure channel) whose rate equals that of the data to be sent. As such, achieving perfect secrecy against a computationally unbounded eavesdropper is impractical. This pessimistic observation arguably resulted in the shift in focus towards countering computationally-bounded adversaries, i.e., the broad field of cryptography.

It was not until three decades after Shannon's original classified work in the subject that Wyner had established the notion of *secrecy capacity* [2]. Wyner demonstrated that a positive reliable *and* secure communication rate between a transmitter and a receiver can be achieved in the presence of a wiretapper, when the channel between the transmitter and the wiretapper is a discrete memoryless channel cascaded to the discrete memoryless channel between the transmitter and the receiver. While Wyner's transformative work characterized the rate equivocation region for the degraded wiretap channel, reference [3] generalized Wyner's framework to a large class of (not necessarily degraded) channels. The secrecy capacity, i.e., the largest rate of reliable communication that can be kept confidential from an eavesdropper, of the Gaussian channel was established in [4]. Following these early works from four decades ago, the past decade has witnessed a significant research effort in information theoretic security, arguably owing to the advent of wireless communication networks, see for example [5]–[12], and also [13]. We will provide a (very) brief overview in the next section in an effort to motivate a forward look and articulate the remaining challenges in realizing the vision of information theoretic security, which promises provable confidential communication against computationally unbounded eavesdroppers.

II. State of the Art and Forward Look

Multi-terminal models where information theoretic secrecy can provide valuable insights are particularly relevant in wireless communication scenarios. This is due to the open medium where simultaneous transmissions and overhearing can take place. While such a scenario is arguably more vulnerable to eavesdropping attacks, it is also the broadcast nature of the medium that can provide advantages for legitimate entities of the network to implicitly or explicitly cooperate for improved secrecy. Effort in this realm includes study of the Gaussian multiple access channel in the presence of an eavesdropper, i.e., the multiple access wiretap channel, where superposing transmitted signals can provide implicit cooperation against the eavesdropper [5]. Moreover, terminals can explicitly cooperate to introduce intentional interference to the communication scenario [7]. Referred to as cooperative jamming, this intentional interference is introduced to the medium in order to induce a more detrimental channel for the eavesdropper(s) while impacting the reception capability of the legitimate receiver(s) the least. That is, one can readily observe cooperative jamming as a form of channel pre-fixing. A cooperative jammer can mimic noise or send a codeword. Earlier work has observed that cooperative jamming with Gaussian noise can help improve sum secrecy rates for the multiple access wiretap channel, with legitimate transmitter(s) with better channel quality to the eavesdropper taking the role of cooperative jammer [7]. That is to say that a cooperative jammer abandons sending secret messages, yet is helpful to improve for the secrecy rate of the remaining terminals.

A line of work developed in search for the secrecy capacity of various network models examines the high signal-to-noise ratio (SNR) behavior of secrecy capacity. The motivation behind this direction is certainly contributed by that which is identical to the non-secrecy counterpart of the literature: even when capacity results are not tractable, their high SNR behavior can be, delivering insightful design principles, interference alignment being a prominent example [14]. In addition, an important reason to pursue a *secure* degrees of freedom characterization is to show superiority of certain schemes over others with respect to secrecy rate scaling with power. In particular, this analysis has been used to show that structured signaling can be desirable from the secrecy perspective. The secure degrees of freedom of a Gaussian wiretap channel, where the secrecy capacity is the difference of the capacities of the channels between the transmitter and the legitimate receiver (the main channel), and between the transmitter and the eavesdropper (the eavesdropper channel) [4], is zero. A cooperative jammer that simply puts Gaussian noise into the channel can significantly enhance the secrecy rate but does not improve the secure degrees of freedom, due to the fact that the achievable rate is again a difference of two terms with the same scaling in power. In other words, introducing a noise term to both the main channel and the eavesdropper channel, while beneficial in finite SNR regime, is not helpful as the power grows to infinity. Reference [10] showed that structured signaling that aligns the signals transmitted from the legitimate transmitter and the cooperative jammer favorably at the legitimate receiver while simultaneously aligning unfavorably at the eavesdropper leads to positive secure degrees of freedom. The codebooks for transmission as well as cooperative jamming in this case were constructed either from integer lattices or nested lattices. Subsequently, reference [11] has shown that the secure degrees of freedom of the Gaussian wiretap channel with a cooperative jammer is equal to $\frac{1}{2}$ by proving the converse and showing achievability by signaling and alignment with integer lattices for almost all channel gains, i.e., real interference alignment (signal scale alignment). Further work on secure degrees of freedom analysis on wiretap channel with a cooperative jammer studies multiple antenna terminals [12], improving the secure degrees of freedom of the MIMO wiretap channel [9] from zero when the number of antennas at the eavesdropper is greater than or equal to the number of antennas at the transmitter, to a positive number depending on the number of antennas at the cooperative jammer. The achievability in this case requires careful orchestration of spatial alignment and signal scale alignment depending on the number of antennas available at each terminal.

While insightful as to what could be achieved in terms of secrecy rate scaling with power, and instructive in signaling schemes that are beneficial in this regard, alignment based schemes often require accurate channel state information of the involved parties. In fact, complete and accurate channel state information, even that of an external eavesdropper has been a standing assumption in all but very recent work in information theoretic security. In reality, the eavesdropper channel is unlikely to be known to the legitimate parties, unless the eavesdropper is part of the legitimate system perhaps untrusted with information, e.g. [6]. Understandably, this assumption on channels is a road block in making the information theoretic security based design approach practical. Recent efforts have thus emerged in relaxing this assumption and finding methods of providing secure rates irrespective of the eavesdropper channel state. These methods differ in the way they address this relaxation. For example, early work by Goppala et. al. on the single user fading wiretap channel considers only the distribution of the channel state to be known [8]. Recent work by Xie and Ulukus on blind cooperative jamming for the Gaussian wiretap channel with a cooperative jammer shows that the same secure degrees of freedom as with full channel state information is achievable for almost all channel gains as long as the channel gains to the eavesdropper are static and below an aggregate value [15]. Perhaps the strongest model is that of reference [16], which studies a MIMO wiretap channel where the secrecy guarantee is against any sequence of eavesdropper channel states that can materialize during the transmission and can vary in each channel use. This work requires no statistical model for the eavesdropper channel gains, in fact a proper distribution need not even exist. It is shown that universal secrecy, that is secrecy against any channel sequence, is possible, but at the expense of reduced secrecy rate as well as reduced secure degrees of freedom. This severe penalty suggests that an examination of what is practically relevant is needed. That is, while we strive for the strongest theoretical result, the design insight perhaps should rely on a practically relevant model. This area thus remains to be full of interesting questions towards realizing the vision offered by physical layer based unconditional security.

As elaborated above, there has been a fair amount of work in structured signaling and signal alignment to provide secrecy rate scaling. Noting that secrecy capacity results are much less tractable for multi transmitter models, the secure degrees of freedom analyses provide the comfort of tight results but only in the high SNR. Indeed, structured signaling approaches may be less than favorable in low to moderate SNR. One than might wonder if there are models where such structured signaling is *not* advantageous. In the remainder of this short paper, we show such a case and argue that a road less traveled in non-secrecy problems, namely that of signaling with memory may offer a way forward. That is, we hypothesize, using the case study below, that bidirectionality of the wireless links may be an asset that secrecy based designs can tap into.

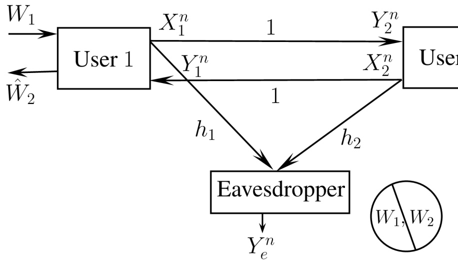

Fig. 1. The Gaussian two-way wiretap channel.

III. A case study: The Two-way Wiretap Channel

The simplest model where the bidirectional nature of the communication links can be taken advantage of is the two-way channel in the presence of an eavesdropper. We will study the secrecy rates, and for tight results, their high SNR behavior. The main observation is that, in this set up, structure does not buy us a secrecy advantage, utilizing the feedback link does.

A. The Channel Model

Consider a Gaussian two-way wiretap channel as depicted in Fig. 1. $X_k(i)$, $k = 1, 2$, is the transmitted signal from user k at the ith channel use. $Y_k(i)$, $Y_e(i)$ are the received signals at user k and the external eavesdropper. After removing self interference, the received signals at the two users and the eavesdropper, over the n channel uses, are given by

$$Y_1^n = X_2^n + N_1^n \tag{1}$$

$$Y_2^n = X_1^n + N_2^n \tag{2}$$

$$Y_e^n = h_1 X_1^n + h_2 X_2^n + N_e^n, \tag{3}$$

where h_k, $k = 1, 2$, is the channel gain from user k to the eavesdropper. N_1^n, N_2^n, N_e^n are the Gaussian noise at user 1, user 2, and the eavesdropper. $N_1, N_2, N_e \sim \mathcal{N}(0, 1)$ are independent and identically distributed (i.i.d.) across the time index. The power constraints for $k = 1, 2$ are

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \mathrm{E}\{X_k^2(i)\} \leq P. \tag{4}$$

User k intends to send a message W_k to user j, $k, j = 1, 2$, and $k \neq j$, and to keep its message W_k secret from the external eavesdropper. The decoder at user k uses Y_k^n to estimate user j's message, $\hat{W}_j$, $k \neq j$. The secrecy rate pair (R_{s_1}, R_{s_2}) is said to be achievable if for every $\epsilon > 0$, there exists a channel code $(2^{nR_{s_1}}, 2^{nR_{s_2}}, n)$ such that $P_e = \Pr\{(\hat{W}_1, \hat{W}_2) \neq (W_1, W_2)\} \leq \epsilon$ and $\frac{1}{n} I(W_1^n, W_2^n; Y_e^n) \leq \epsilon$. The achievable secure degrees of freedom (s.d.o.f.) for user k, for a given secrecy rate R_{s_k}, is defined as

$$d_k = \lim_{P\to\infty} \frac{R_{s,k}}{\frac{1}{2}\log_2 P}. \tag{5}$$

In the following, we will first present the upper bound for the sum s.d.o.f. for this channel and then present three schemes which achieves it.

B. Upper bound

The sum secrecy rate of the channel in (1)-(3), can be upper bounded as follows. The bound is readily obtained as a special case of the bound derived in reference [17].

$$\begin{aligned} &R_{s_1} + R_{s_2} \leq \\ &\frac{1}{2} \min \left\{ \left\{ \log_2 \left(1 + \frac{P}{1 + h_1^2 P}\right) + \log_2 \left(1 + (1 + h_2^2)P\right) \right\}, \right. \\ &\left. \left\{ \log_2 \left(1 + \frac{P}{1 + h_2^2 P}\right) + \log_2 \left(1 + (1 + h_1^2)P\right) \right\} \right\}. \end{aligned} \tag{6}$$

Using (6), the sum s.d.o.f. is upper bounded as

$$\begin{aligned} d_1 + d_2 &\leq \lim_{P\to\infty} \frac{R_{s_1} + R_{s_2}}{\frac{1}{2}\log_2 P} \qquad (7) \\ &\leq \lim_{P\to\infty} \frac{\frac{1}{2}\left\{\log_2\left(1 + \frac{P}{1+h_1^2 P}\right) + \log_2\left(1 + (1 + h_2^2)P\right)\right\}}{\frac{1}{2}\log_2 P} = 1 \end{aligned}$$

C. Achievability Using Structured Signaling

First, let us consider an achievable scheme using signal scale alignment, i.e., amplitude modulation [11]. The scheme is as follows. Transmitter k sends a combination of an information signal, U_k, which carries message W_k, and a jamming signal, V_k, which is intended to mask the other transmitter's information signal at the eavesdropper. U_k and V_k, $k = 1, 2$, are independently and uniformly drawn from the constellation $a\{-Q, -Q+1, \cdots, Q-1, Q\}$, where Q is a positive integer, and a is a real number which is chosen to satisfy the power constraint at each user.

The transmitted signals are given by

$$X_1 = \frac{\alpha}{h_1} U_1 + \frac{\beta}{h_1} V_1 \tag{8}$$

$$X_2 = \frac{\beta}{h_2} U_2 + \frac{\alpha}{h_2} V_2, \tag{9}$$

where α and β are chosen to be rationally independent.

The transmitted signals X_1^n, X_2^n are i.i.d. over the channel uses and the encoder is memoryless. Denoting $[x]^+ = \max\{0, x\}$, for user k, $k = 1, 2$, the secrecy rate

$$R_{s_k} = \left[I(U_k; Y_j) - I(U_k; Y_e)\right]^+, \tag{10}$$

is achievable by stochastic encoding at user k, where $j = 1, 2$, and $j \neq k$ [3]. Thus, we bound the sum rate as follows.

$$\begin{aligned} &R_{s_1} + R_{s_2} \\ &\geq I(U_1; Y_2) + I(U_2; Y_1) - [I(U_1; Y_e) + I(U_2; Y_e|U_1)] \qquad (11) \\ &= I(U_1; Y_2) + I(U_2; Y_1) - I(U_1, U_2; Y_e), \qquad (12) \end{aligned}$$

where (11) follows since

$$\begin{aligned} I(U_2; Y_e) &= H(U_2) - H(U_2|Y_e) \qquad (13) \\ &\leq H(U_2|U_1) - H(U_2|Y_e, U_1) = I(U_2; Y_e|U_1). \qquad (14) \end{aligned}$$

The received signal at the eavesdropper is given by

$$Y_e = h_1 X_1 + h_2 X_2 + N_e \tag{15}$$

$$= \alpha(U_1 + V_2) + \beta(U_2 + V_1) + N_e. \quad (16)$$

We upper bound $I(U_1, U_2; Y_e)$ as follows:

$$\begin{aligned} I(U_1, U_2; Y_e) &\leq I(U_1, U_2; Y_e, N_e) && (17)\\ &= I(U_1, U_2; Y_e|N_e) && (18)\\ &= H(\alpha(U_1 + V_2) + \beta(U_2 + V_1)) - H(\alpha V_2 + \beta V_1) && (19)\\ &\leq \log_2(4Q + 1)^2 - \log_2(2Q + 1)^2 \leq 2 && (20) \end{aligned}$$

where (18) follows since (U_1, U_2) and N_e are independent, and (20) follows since the entropy of a uniform random variable over the set $a\{-2Q, \cdots, 2Q\}$ upper bounds the entropy of $U_1 + V_2$, and $U_2 + V_1$.

Choosing $Q = P^{\frac{1-\epsilon}{2(2+\epsilon)}} - \nu$ and $a = \gamma P^{\frac{1+2\epsilon}{2(2+\epsilon)}}$, where γ, ν are constants that do not depend on P, satisfies the power constraints. For user 1, we lower bound $I(U_1; Y_2)$ as follows:

$$\begin{aligned} I(U_1; Y_2) &= H(U_1) - H(U_1|Y_2) && (21)\\ &\geq H(U_1) - 1 - P_{e_1} \log_2(|\mathcal{U}_1|) && (22)\\ &= (1 - P_{e_1}) \log_2(2Q + 1) - 1, && (23) \end{aligned}$$

where $\mathcal{U}_1 = a\{-Q, \cdots, Q\}$, $P_{e_1} = \Pr\{\hat{U}_1 \neq U_1\}$, $\hat{U}_1$ is the estimate of U_1 at the receiver of user 2.

Using results from [18], P_{e_1} can be upper bounded as $P_{e_1} \leq \exp(-\mu P^{\epsilon})$, where the minimum distance between the received constellation points at user 2 is lower bounded using Khintchine-Groshev theorem; μ is a constant which does not depend on P. Note that choosing α and β to be rationally independent enables user k to decode U_j, $j \neq k$ [18]. Thus, we have

$$\begin{aligned} I(U_1; Y_2) &\geq (1 - \exp(-\mu P^{\epsilon})) \log_2(2Q + 1) - 1 && (24)\\ &\geq \frac{(1 - \epsilon)}{2(2 + \epsilon)} \log_2 P + o(\log_2 P). && (25) \end{aligned}$$

Following the same analysis as for $I(U_1; Y_2)$, we obtain

$$I(U_2; Y_1) \geq \frac{(1 - \epsilon)}{2(2 + \epsilon)} \log_2 P + o(\log_2 P). \quad (26)$$

Thus, substituting (20), (25), and (26) in (12) gives

$$R_{s_1} + R_{s_2} \geq \frac{(1 - \epsilon)}{2 + \epsilon} \log_2 P + o(\log_2 P), \quad (27)$$

and the sum s.d.o.f. is lower bounded as

$$d_1 + d_2 \geq \lim_{P \to \infty} \frac{R_{s_1} + R_{s_2}}{\frac{1}{2} \log_2 P} = \frac{2(1 - \epsilon)}{2 + \epsilon}. \quad (28)$$

Since ϵ can be arbitrarily small, $d_1 + d_2 = 1$ is achievable.

D. Achievability Using Gaussian Signaling

In the previous section, we have shown that the sum secure degrees of freedom is achievable by real interference alignment. In this section, we will see that alignment is not necessary at all. Specifically, we will simply employ Gaussian signaling and cooperative jamming with Gaussian noise. It suffices to show the achievability of the pair $(d_1, d_2) = (1, 0)$. It follows then that the pair $(0, 1)$ is also achievable and sum s.d.o.f. of 1 is then achievable by time sharing.

We transmit i.i.d. signals, X_1^n, X_2^n, over n. In addition, at the ith channel use, user k does not utilize any of the previously received signals $[Y_k(1) \cdots Y_k(i - 1)]$ for encoding X_k. The transmitter at user 1 maps its message W_1 to X_1^n, where $X_1 \sim \mathcal{N}(0, P)$, using a stochastic encoder. Simultaneously, user 2 sends a cooperative jamming signal X_2^n, where $X_2 \sim \mathcal{N}(0, P)$, which carries no information. Since X_2^n is independent from X_1^n, and the encoding function at user 1 does not depend on its previous received signals, we have a memoryless Gaussian wiretap channel, and the following secrecy rate is achievable using stochastic encoding [3]:

$$\begin{aligned} R_{s_1} &= [I(X_1; Y_2) - I(X_1; Y_e)]^+ && (29)\\ &= \frac{1}{2} \left[\log_2(1 + P) - \log_2(1 + \frac{h_1^2 P}{1 + h_2^2 P})\right]^+. && (30) \end{aligned}$$

Thus, $d_1 = \lim_{P \to \infty} \frac{R_{s_1}}{\frac{1}{2} \log_2 P} = 1$, and $(1, 0)$ is achievable.

E. Achievability Using Gaussian Signaling with a Twist

In this section, we will present the achievable scheme from [17] which utilizes the backward channel signaling explicitly and combines cooperative jamming and encryption in a two phase scheme. During the first phase, with time sharing factor $1 - a$, $0 \leq a \leq 1$, user 2 sends a key, K, to user 1 using a Gaussian codebook of i.i.d. sequences drawn from $\mathcal{N}(0, P)$, and user 1 jams the eavesdropper by transmitting an i.i.d. Gaussian noise sequence with power P, in order to help secure the key from the eavesdropper. During the second phase, user 1 uses K in encrypting its message W_1, and sends the encoded signal using a Gaussian codebook with i.i.d. components drawn from $\mathcal{N}(0, P)$, to user 2, while user 2 performs cooperative jamming by sending i.i.d. Gaussian noise sequences with power P. The rate of the key, R_K, transmitted by user 2 in the first phase is chosen as

$$R_K < \frac{1}{2} \min \left\{ \left[\log_2(1 + P) - \log_2\left(1 + \frac{h_2^2 P}{1 + h_1^2 P}\right)\right]^+, \log_2\left(1 + \frac{h_1^2 P}{1 + h_2^2 P}\right) \right\}. \quad (31)$$

Note that the key rate is chosen to be less than $\frac{1}{2}[\log_2(1 + P) - \log_2(1 + \frac{h_2^2 P}{1 + h_1^2 P})]^+$ in order to keep the key secret from the eavesdropper, by utilizing a stochastic encoder at user 2. In addition, the key rate is chosen to be smaller than $\frac{1}{2} \log_2(1 + \frac{h_1^2 P}{1 + h_2^2 P})$ since the key is utilized at user 1 to compensate for the rate loss of the forward channel due to the existence of the eavesdropper, which is equal to $\frac{1}{2} \log_2(1 + \frac{h_1^2 P}{1 + h_2^2 P})$. User 1 generates $2^{(1-a)nR_K}$ codebooks, each corresponds to a particular K and is composed of $2^{(an \log_2(1+P))/2}$ codewords. Upon estimating the value of K from the first phase, user 1 chooses the codebook that corresponds to this estimate, and performs stochastic encoding to encode its message W_1.

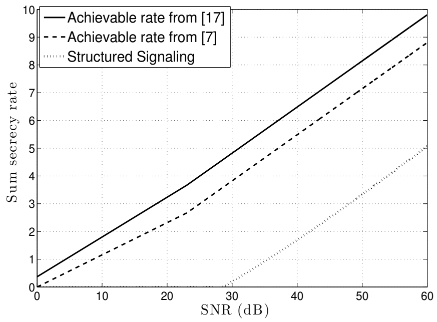

Fig. 2. Achievable secrecy rates from Sections III-C-III-E. $h_1 = 2, h_2 = 1$.

Using this two phase scheme, the rate pair $(R_{s,1}, 0)$, where

$$R_{s,1} = \frac{1}{2}\max_{0\le a\le 1} a\Bigg[\log_2(1+P) - \Bigg[\log_2\left(1+\frac{h_1^2P}{1+h_2^2P}\right) - \frac{1-a}{a}\Bigg[\log_2(1+P) - \log_2\left(1+\frac{h_2^2P}{1+h_1^2P}\right)\Bigg]^+\Bigg]^+\Bigg]^+, \tag{32}$$

is achievable [17]. Similarly, by exchanging the roles of user 1 and user 2 and correspondingly exchanging h_1 with h_2 in (32), we obtain that the resulting rate pair $(0, R_{s_2})$ is achievable. Thus, the convex hull of $(0, 0)$, $(R_{s_1}, 0)$, $(0, R_{s_2})$ is achievable by time sharing, and we have that

$$d_1 + d_2 = \lim_{P\to\infty}\max_{0\le b\le 1}\frac{bR_{s_1} + (1-b)R_{s_2}}{\frac{1}{2}\log_2 P} \tag{33}$$

$$= \lim_{P\to\infty}\frac{\frac{1}{2}\max_{0\le a\le 1} a\log_2(1+P)}{\frac{1}{2}\log 2P} = 1, \tag{34}$$

where b is the time sharing factor for the scheme that achieves the pair $(R_{s_1}, 0)$. Thus $d_1 + d_2 = 1$ is achievable.

F. Comparison

We have seen that all three schemes achieve the same secrecy rate scaling with power. It is also instructive to compare their finite SNR performance. Figure 2 shows the achievable rate vs SNR and while the slope of secrecy rate for the three schemes are identical, Gaussian signaling and cooperative jamming outperforms discrete signaling. Further, the scheme that explicitly utilizes the signals heard on the back channel performs the best. This supports the notion that utilizing bidirectionality for jamming and encryption could be an alternative for alignment in some multi-transmitter models.

IV. Conclusion

In this paper, we have provided a brief overview of the state of the art in information theoretic secrecy, and challenges for bringing the promise of unconditional security at the foundation of (wireless) network design. We have also provided a case study with the two-way wiretap channel where careful signal alignment at the legitimate receiver and the eavesdropper is not necessary thanks to the availability of bidirectional communication between the two legitimate communicating nodes. The take away points of the paper are (i) while the high SNR studies are insightful as to proving an advantage of a signaling scheme, finite SNR performance, which likely is of more relevance in practical scenarios, also needs to be examined carefully; (ii) channel assumptions are a main concern for information theoretic security and a practically relevant scenario for eavesdropper channels needs to be brought upon that balances the concerns regarding the robustness of information theoretic secrecy methods to eavesdropper channel quality and of severe secrecy rate penalties; and (iii) utilizing backward channels and designing secrecy encoders accordingly enable synergistic combining of information theoretic security with private key encryption and may be a bridge between the two communities that emerged from Shannon's original work [1].

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

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

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

[5] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *39th Asilomar Conference on Signals, Systems and Computers*, Nov. 2005.

[6] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in *IEEE Int. Symp. on Info. Theory*, Jul. 2006.

[7] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. on Info. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

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

[9] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-part II: The MIMOME wiretap channel," *IEEE Trans. on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[10] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. on Info. Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.

[11] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. on Info. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[12] M. Nafea and A. Yener, "Secure degrees of freedom for the MIMO wiretap channel with a multiantenna cooperative jammer," in *IEEE Information Theory Workshop*, Nov. 2014.

[13] M. Bloch and J. Barros, *Physical Layer Security From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[14] V. Cadambe and S. Jafar, "Interference alignment and the degrees of freedom of the K user interference channel," *IEEE Trans. on Info. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[15] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Conf. on Information Sciences and Systems*, Mar. 2013.

[16] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. on Info. Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.

[17] ——, "The role of feedback in two-way secure communication," *IEEE Trans. on Info. Theory*, vol. 59, no. 12, pp. 8115–8130, Dec. 2013.

[18] A. S. Motahari, S. O. Gharan, M.-A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Trans. on Info. Theory*, vol. 60, no. 8, pp. 4799– 4810, Aug. 2014.