Secure Degrees of Freedom for Gaussian Channels with Interference: Structured Codes Outperform Gaussian Signaling

Xiang He   Aylin Yener
Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802
xxh119@psu.edu   *yener@ee.psu.edu*

***Abstract*—In this work, we prove that a positive secure degree of freedom is achievable for a large class of real Gaussian channels as long as the channel is not degraded and the channel is fully connected. This class includes the MAC wiretap channel, the 2-user interference channel with confidential messages, the 2-user interference channel with an external eavesdropper. Best known achievable schemes to date for these channels use Gaussian signaling. In this work, we show that structured codes outperform Gaussian random codes at high SNR when channel gains are real numbers.**

I. Introduction

Information theoretic security, originally proposed by Shannon [1], seeks the fundamental limits of reliable transmission rates when the messages must be kept secret from a computation-power unlimited adversary whose observation of the transmitted signals contains some uncertainty. By now, it is well known that introducing interference into the channel in a proper manner may increase the uncertainty observed by the adversary and hence allow for a higher rate of secret messages [2]–[4]. The interference should be introduced in a way such that it is more harmful to the adversary than it is to the intended receiver of the messages. Hence, the key is to achieve a fine balance between secrecy against the adversary and the level of harmful interference to the system.

For these channel models, the achieved rate obtained so far is far from the outer bounds. For example, the genie outer bound from [4] increases with power P at the speed of $0.5\log_2(P)$ [5, (69)]. The achievable secrecy rate converges to a constant when P goes to ∞ [4, Theorem 2]. This means the gap between the achievable rate and the outer bound is unbounded and the trade-off between secrecy and interference is still not well-understood. In fact, once the channel model is such that the intended receiver is not harmed by the introduced interference, the achieved secrecy rate immediately comes within 0.5 bits/channel use of the capacity region, as was shown for the one sided interference channel in [6] and the orthogonal MAC wiretap channel in [7].

In this work, we consider the more general case where introducing interference will both confuse the eavesdropper and harm the intended receiver simultaneously. We show, for a large class of Gaussian channels with confidential messages where introducing interference effects both the intended receiver and the eavesdropper, that signaling using structured codes can out-perform signaling with i.i.d. Gaussian codebooks in high SNR. This class includes the Gaussian MAC-wiretap channel [2], the Gaussian interference channel with confidential messages [3] and the Gaussian interference channel with an external eavesdropper [7]. It has been a folk conjecture that the achievable rate regions with Gaussian codebooks in these works were likely optimal and efforts have been made in [4], [5], [7] to find outer bounds to prove this. A direct consequence of the result we report in this paper is that this is not so.

This insight comes from studying the secure degree of freedom of the interference assisted wiretap channel [4], which falls under the three channels mentioned above when only one source node has a confidential message to send. As mentioned before, reference [4] shows that the achieved rate using Gaussian codebooks converges to a constant as the power increases, which implies the obtained secure degree of freedom for this channel is 0. In contrast, we find that a positive degree of freedom is actually achievable for all channel gains as long as the channel is not degraded. The key to getting this result is the use of different types of structured codes for appropriate channel gains rather than Gaussian signaling.

In obtaining our results we consider *all* possible channel gain configurations with a *fully* connected channel model. A *partial alignment* scheme is introduced and used in Section III-E to produce the largest achieved secure degree of freedom, in which part of the interference is actually aligned with the intended signal. Also, integer lattices are utilized whenever necessary, as they can achieve a larger secure degree of freedom for a certain set of channel gain configurations.

II. System Model

Consider the Gaussian interference-assisted wiretap channel [4] shown in Figure 1. In this model, node S_1 sends a secret message W_1 via $\tilde{X}_1$ to node D_1, which must be kept secret from node D_2. We assume the channel is fully connected,

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

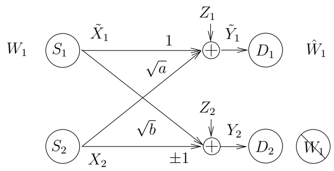

Fig. 1. Interference-assisted wiretap channel

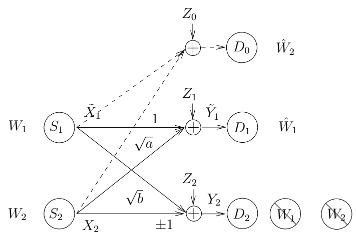

Fig. 2. Interference-assisted wiretap channel as a special case of the interference channel with an external eavesdropper

which means that no link's channel gain equals zero. This assumption is obviously valid for a wireless medium. Then after normalizing the channel gains of the two intended links to 1, the received signals at the two receiving nodes D_1 and D_2 can be expressed as

$$\begin{aligned}\tilde{Y}_1 &= \tilde{X}_1 + \sqrt{a}X_2 + Z_1 \\ Y_2 &= \sqrt{b}\tilde{X}_1 \pm X_2 + Z_2\end{aligned} \quad (1)$$

where $Z_i, i = 1, 2$ are zero-mean Gaussian random variables with unit variance. For now, we assume $\sqrt{a}$ and $\sqrt{b}$ are real numbers. The case with complex numbers will be briefly explained in Section II-B.

Since W_1 must be kept secret from D_2, we require

$$\lim_{n\to\infty} \frac{1}{n} H(W_1) = \lim_{n\to\infty} \frac{1}{n} H(W_1|Y_2^n) \quad (2)$$

The achieved secrecy rate R_e is defined as $\lim_{n\to\infty} \frac{1}{n} H(W_1)$ such that the condition (2) is fulfilled and W_1 can be reliably received by D_1.

Let $X_1 = \sqrt{b}\tilde{X}_1$ and $Y_1 = \sqrt{b}\tilde{Y}_1$. Then from (1), we have

$$\begin{aligned}Y_1 &= X_1 + \sqrt{ab}X_2 + \sqrt{b}Z_1 \\ Y_2 &= X_1 \pm X_2 + Z_2\end{aligned} \quad (3)$$

In the sequel, we will focus on this scaled model instead, as we find it more convenient to use it to explain our results.

Let the average power constraint of node S_i on X_i be $\bar{P}_i$. The secure degree of freedom of the secrecy rate is defined as

$$\limsup_{\bar{P}_i\to\infty, i=1,2} \frac{R_e}{\frac{1}{2}\log_2\left(\sum_{i=1}^{2} \bar{P}_i\right)} \quad (4)$$

It is clear that the secure degree does not change, whether the model is described via (1) or (3).

A. Relationship to Other Channels

The significance of the interference-assisted wiretap channel is that it can be considered as a special case of a large class of channel models with confidential messages, as shown below:

1) If node S_2 has a confidential message W_2 for D_1, which must be kept secret from D_2, then the channel is the MAC-wiretap channel considered in [2].
2) If node S_2 has a confidential message W_2 for D_2, and the message must be kept secret from D_1, then the channel is the interference channel with confidential messages considered in [3].
3) As shown in Figure 2, we can add another receiving node D_0 to Figure 1, to which node S_2 wants to sent a confidential message W_2. Again W_2 must be kept secret from D_2. Then the channel becomes the interference channel with an external eavesdropper in [7, Section VI].

Hence, any secrecy rate achieved in the the interference-assisted wiretap channel is an achievable *individual rate* for all the three multi-user channels mentioned above. Naturally, an achievable secrecy region can be obtained by time sharing.

B. Complex Channel Gains

Generally speaking, channels with complex channel gains may be of interest. The reason that we focus on the real case in the sequel is that the complex case is actually easier in terms of achieving positive secure degree of freedom, as explained below.

Since the channel is fully connected, after normalization of the channel gains and variable substitution, the received signals at nodes D_1 and D_2 can be expressed as [8]:

$$\begin{aligned}Y_1 &= X_1 + \sqrt{ab}e^{j\psi}X_2 + \sqrt{b}Z_1 \\ Y_2 &= X_1 + X_2 + Z_2\end{aligned} \quad (5)$$

where $Z_i, i = 1, 2$ are rotational invariant complex Gaussian random variables with unit variance. Then we have:

Theorem 1: A secure degree of freedom of 1 is achievable if $\psi \neq 0$ or $\pi \bmod 2\pi$.

Proof Outline: Let $\mathrm{Im}X_i = 0, i = 1, 2$. Let $\cot x = \cos x / \sin x$. Then since $\mathrm{Im}Y_2 = \mathrm{Im}Z_2$, $\mathrm{Im}Y_2$ does not provide any information about W_1 to the eavesdropper. Hence we can assume the eavesdropper receives $\mathrm{Re}Y_2$ only. Node D_1 computes $g(Y_1) = \mathrm{Re}Y_1 - \cot\psi \mathrm{Im}Y_1$. Then the channel can be expressed as

$$\begin{aligned}g(Y_1) &= \mathrm{Re}X_1 + \sqrt{b}\left(\mathrm{Re}Z_1 - \cot\psi \mathrm{Im}Z_1\right) \\ \mathrm{Re}Y_2 &= \mathrm{Re}X_1 + \mathrm{Re}X_2 + \mathrm{Re}Z_2\end{aligned} \quad (6)$$

The channel then becomes an one-sided interference channel. By transmitting a i.i.d. Gaussian noise via $\mathrm{Re}X_2$, the channel is equivalent to a Gaussian wiretap channel. It is known that the following secrecy rate is achievable [9]:

$$C\left(\frac{P_1}{(b\csc^2\psi)/2}\right) - C\left(\frac{P_1}{P_2 + 1/2}\right) \quad (7)$$

where $C(x) = \frac{1}{2}\log_2(1+x)$. P_i is the average power constraint on X_i. Hence a secure degree of freedom of 1 is achievable for this channel. ■

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

C. Gaussian Signaling

In [4], an achievable rate is derived with Gaussian codebooks and power control. One implication of this achievable rate is the high SNR behavior as described by Theorem 2 therein. We re-state this result below:

Theorem 2: With Gaussian codebooks, the achievable secrecy rate R_1 converges to a constant when the power constraint of node D_1 and D_2 goes to ∞.

This means the achieved secure degree of freedom by the coding scheme in [4] is 0.

III. The Achievable Scheme

A. Results on Structured Codes

1) Nested Lattice: A nested lattice code is defined as an intersection of N-dimensional fine lattice Λ and the fundamental region of an N-dimensional "coarse" lattice Λ_c, denoted by $\mathcal{V}(\Lambda_c)$. We require that $\Lambda_c \subset \Lambda$. Let u_i^N be uniformly distributed over $\Lambda \cap \mathcal{V}(\Lambda_c)$. Let the dithering noise d_i^N be a continuous random vector which is uniformly distributed over $\mathcal{V}(\Lambda_c)$. Define modulus operation such that $x \bmod \Lambda_c = x - \arg\min_{u\in\Lambda_c} \|x-u\|$. Then the values of X_i over N channel uses are computed as

$$X_i^N = (u_i^N + d_i^N) \bmod \Lambda_c \tag{8}$$

$u_i^N, d_i^N, i=1,2$ are independent. We also assume $d_i^N, i=1,2$ are known by all receiving nodes. Hence they are not used to enhance secrecy.

As will be shown later, we are interested in upper-bounding the expression $I(u_1^N; X_1^N \pm X_2^N, d_1^N, d_2^N)$, which corresponds to the rate of information leaked to the eavesdropper. To do that, we need the following result. Its proof follows from the representation theorem introduced in [10] and is given in [8].

Theorem 3: There exists an integer T, such that $1 \le T \le 2^N$, and $X_1^N \pm X_2^N$ is uniquely determined by $\{T, X_1^N \pm X_2^N \bmod \Lambda_c\}$.

Using Theorem 3, we have

$$\begin{aligned}
&I(u_1^N; X_1^N \pm X_2^N, d_1^N, d_2^N)\\
=&I(u_1^N; X_1^N \pm X_2^N \bmod \Lambda_c, T, d_1^N, d_2^N) &(9)\\
\le&I(u_1^N; X_1^N \pm X_2^N \bmod \Lambda_c, d_1^N, d_2^N) + H(T) &(10)\\
=&I(u_1^N; u_1^N \pm u_2^N \bmod \Lambda_c) + H(T) &(11)\\
=&H(T) \le N &(12)
\end{aligned}$$

This means at most N bit per channel use is leaked to the eavesdropper over N channel uses.

2) Integer Lattice: An integer lattice code with parameter Q is composed of points in the set $[0,Q) \cap \mathbf{Z}$ where $\mathbf{Z}$ is the set of all integers. In this case, the rate of information leaked to the eavesdropper is given by $f(Q)$ defined as [8]:

$$f(Q) = I(X_1; X_1 \pm X_2) \tag{13}$$

where $X_i, i=1,2$ is uniformly distributed over $[0,Q) \cap \mathbf{Z}$. $f(Q)$ can be lower bounded by the following lemma:

Lemma 1: For a positive integer Q,

$$f(Q) \le \frac{1}{2}\log_2(2\pi e(\frac{1}{6} - \frac{1}{12Q^2})) < \frac{1}{2}\log_2(\frac{\pi e}{3}) < 0.8 \tag{14}$$

The proof follows from [11, Lemma 12] and is given in [8].

We next use these results to derive achievable secure degree of freedom for the interference assisted wiretap channel.

B. When $\sqrt{ab}$ is algebraic irrational

Theorem 4: A secure degree of freedom of $1/2$ is achievable when $\sqrt{ab}$ is an algebraic irrational number.

Proof: We use the lattice codebook used in [11, Theorem 1]. Let $\Lambda_{P,\varepsilon}$ be the scalar lattice defined as:

$$\Lambda_{P,\varepsilon} = \left\{x : x = P^{1/4+\varepsilon} z, z \in \mathbf{Z}\right\} \tag{15}$$

The codebook $\mathcal{C}_{P,\varepsilon}$ is given by:

$$\mathcal{C}_{P,\varepsilon} = \Lambda_{P,\varepsilon} \cap \left[-\sqrt{P}, \sqrt{P}\right] \tag{16}$$

where $P = \min\{\bar{P}_1, \bar{P}_2\}$. It then can be verified that, for large enough P, we have

$$\log_2 |\mathcal{C}_{P,\varepsilon}| \ge \log_2\left(2P^{1/4-\varepsilon} - 1\right) \ge \log_2\left(P^{1/4-\varepsilon}\right) \tag{17}$$

The codebook is used for both node S_1 and node S_2. The codeword transmitted by node S_1 is chosen based on the secret message W_1. The codeword transmitted by node S_2 is chosen independently according to a uniform distribution.

Since the input from S_2 is i.i.d., the channel is then equivalent to a memoryless wiretap channel [12]. Let $[x]^+$ denote x if $x \ge 0$ and 0 otherwise. Then, according to [12], any secrecy rate R such that

$$0 \le R < [I(X_1; Y_1) - I(X_1; Y_2)]^+ \tag{18}$$

is achievable. Hence we need to find a lower bound to the right hand side of (18).

According to [11, Theorem 1], $p(X_1)$ is chosen to be a uniform distribution over $\mathcal{C}_{P,\varepsilon}$. Under this input distribution, following a similar derivation to [11, Theorem 1], it can be shown that when $P > \frac{1}{a^2b^2}$, we have

$$I(X_1; Y_1) \ge \left(1 - 2\exp\left(-\frac{P^{2\varepsilon}}{8b}\right)\right)\log_2(|\mathcal{C}_{P,\varepsilon}|) - 1 \tag{19}$$

For $I(X_1; Y_2)$, we have

$$I(X_1; Y_2) \le I(X_1; Y_2, Z_2) = I(X_1; X_1 \pm X_2) \le 0.8 \tag{20}$$

where (20) follows from Lemma 1. Using (19) (20), and (17), we find (18) is lower bounded by

$$[\left(1 - 2\exp\left(-\frac{P^{2\varepsilon}}{8b}\right)\right)\left(\frac{1}{4} - \varepsilon\right)\log_2(P) - 1.8]^+ \tag{21}$$

for sufficiently large P. From (17), ε can take any value between $(0, 1/4)$. Hence we have completed the proof. ■

Remark 1: When $\sqrt{ab} = 1$ and all channel gains are positive, the channel is degraded and from the outer bound in [4], the secure degree of freedom is 0. Since algebraic irrational numbers are dense on the real line, it follows that the secure degree of freedom is discontinuous at $\sqrt{ab} = 1$.

The result in Section III-B only applies when $\sqrt{ab}$ is algebraic irrational, which is a set of measure 0 on the real line. In the sequel we consider the case where $\sqrt{ab}$ is either rational or transcendental.

C. When $\sqrt{ab} \geq 2$ or $1/\sqrt{ab} \geq 1/2$

Here we use the Q-bit expansion scheme similar to the one in [13]. Let $Q = \sqrt{ab}$ if $\sqrt{ab} \geq 2$. Otherwise, let $Q = 1/\sqrt{ab}$. Let $\lfloor Q \rfloor$ denote the largest integer $\leq Q$.

Theorem 5: The following secure degree of freedom is achievable:

$$[\frac{1}{2}\frac{\log_2 \lfloor Q \rfloor}{\log_2 Q} - \frac{f(\lfloor Q \rfloor)}{2\log_2 Q}]^+ \tag{22}$$

where $f(Q)$ is defined in (13). (22) is lower bounded by

$$[\frac{1}{2}\frac{\log_2 \lfloor Q \rfloor}{\log_2 Q} - \frac{\log_2\left(2\pi e\left(\frac{1}{6}\right) - \frac{1}{12\lfloor Q \rfloor^2}\right)}{4\log_2(Q)}]^+ \tag{23}$$

For $Q = 2$, (22) equals 0.25.

Proof: We begin by considering the case when $\sqrt{ab} \geq 2$.

$$X_k = \sqrt{P_0}\sum_{i=0}^{M-1} a_{k,i} Q^{2i}, k = 1, 2 \tag{24}$$

where P_0 is a constant scaling factor. $a_{k,i}$ is uniformly distributed over $[0, \lfloor Q \rfloor - 1] \cap \mathbf{Z}$, hence $a_{k,i}$ is uniquely determined by X_k.

The signal received by node D_1 is given by

$$Y_1 = \sqrt{P_0}(\sum_{i=0}^{M-1} a_{1,i} Q^{2i} + \sum_{i=0}^{M-1} a_{2,i} Q^{2i+1}) + \sqrt{b} Z_1 \tag{25}$$

We then derive a lower bound to $I(X_1; Y_1) - I(X_1; Y_2)$ as we did for Theorem 4.

Following a similar derivation to [11, Theorem 1], with Fano's inequality, it can be shown that $I(X_1; Y_1)$ is lower bounded as:

$$I(X_1; Y_1) \geq \left(1 - 2e^{\left(-\frac{P_0}{8b}\right)}\right) H(X_1) - 1 \tag{26}$$

For $I(X_1; Y_2)$, we have:

$$I(X_1; Y_2) \leq I(X_1; X_1 \pm X_2) \tag{27}$$

$$\leq \sum_{i=0}^{M-1} I(a_{1,i}; a_{1,i} \pm a_{2,i}) = Mf(\lfloor Q \rfloor) \tag{28}$$

Therefore, the following secrecy rate is achievable

$$R_e = M(1 - 2e^{(-\frac{P_0}{8b})})(\log_2 \lfloor Q \rfloor) - 1 - Mf(\lfloor Q \rfloor) \tag{29}$$

It can be verified that the transmission power is given by:[1]

$$Var[X_i] = P_0\left(\frac{\lfloor Q \rfloor^2 - 1}{12}\right)\frac{Q^{4M} - 1}{Q^4 - 1} \quad i = 1, 2 \tag{30}$$

[1]In case it is desired for X_k to have zero mean, we can simply shift X_k by a constant, which will not change the secrecy rate.

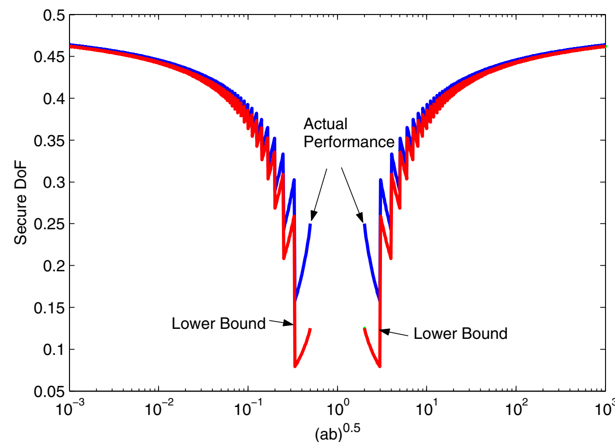

Fig. 3. Secure degree of freedom

The secure degree of freedom is hence given by by:

$$\lim_{M\to\infty} \frac{\left(\left(1 - 2\exp\left(-\frac{P_0}{8b}\right)\right)\log_2 \lfloor Q \rfloor - f(\lfloor Q \rfloor)\right) M}{\frac{1}{2}\log_2(Q^{4M})} \tag{31}$$

$$= \frac{1}{2}\left(1 - 2\exp\left(-\frac{P_0}{8b}\right)\right)\frac{\log_2 \lfloor Q \rfloor}{\log_2 Q} - \frac{f(\lfloor Q \rfloor)}{2\log_2(Q)} \tag{32}$$

which can be made arbitrarily close to (22) by choosing a large enough P_0. (23) then follows from (22) via Lemma 1.

When $Q = 2$, it can be verified that $f(\lfloor Q \rfloor) = 0.5$, and (32) can be made to be arbitrarily close to $1/4$.

The case of $1/\sqrt{ab} \geq 2$ can be proved in a similar fashion. Details can be found in [8]. ■

In Figure 3, we plot the secure degree of freedom achieved by Theorem 5. We observe that as $\sqrt{ab}$ moves away from 1, the lower bound given by (23) becomes tighter, and the secure degree of freedom converges to 0.5.

D. When $\sqrt{ab} = 1$ or $\sqrt{ab} = 1.5$

When $Y_2 = X_1 + X_2 + Z_2$, the channel is degraded. The secure degree of freedom is known to be 0 [4]. When $Y_2 = X_1 - X_2 + Z_2$, we have the following result:

Theorem 6: The secure degree of freedom of 0.0548 is achievable.

Proof outline: Here we let $X_k = \sqrt{P_0}\sum_{i=0}^{M-1} a_{k,i}Q^{2i}$. $Q = 2$. The difference is that $a_{k,i}$ is not uniformly distributed over $\{0, 1\}$. Instead we choose its distribution to maximize

$$I(a_{1,i}; a_{1,i} + a_{2,i}) - I(a_{1,i}; a_{1,i} - a_{2,i}) \tag{33}$$

which is about 0.1095 when $\Pr(a_{1,i} = 1) = 0.1443$, $\Pr(a_{2,i} = 1) = 0.8557$. The theorem follows by deriving a lower bound to $[I(X_1; Y_1) - I(X_1; Y_2)]^+$. The details are provided in [8]. ■

Theorem 7: When $\sqrt{ab} = 1.5$, a secure degree of freedom of $1/6$ is achievable.

Proof outline: Let X_i be:

$$X_k = \sqrt{P_0}\sum_{i=0}^{3M-1} a_{k,i} Q^i, k = 1, 2 \tag{34}$$

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

where $Q = 2$. M is a positive integer and P_0 is a positive constant as defined in the proof of Theorem 5. Choose $a_{k,i}$ such that $a_{k,i} = 0$, if $i \bmod 3 = 1$ or 2. Otherwise $a_{k,i}$ is uniformly distributed over $\{0, 1\}$. Here $a_{k,i}$ is forced to be zero at $i \bmod 3 = 1$ or 2 to make room for $0.5a_{2,j}, \forall j \bmod 3 = 0$ and the carry-over from $a_{1,j} + a_{2,j}, \forall j \bmod 3 = 0$.

The theorem then follows by deriving a lower bound to $[I(X_1; Y_1) - I(X_1; Y_2)]^+$. The details are provided in [8]. ■

E. When $1 < \sqrt{ab} < 2$ or $1/2 < \sqrt{ab} < 1$, and $\sqrt{ab} \neq 1.5$

Let $\sqrt{ab} = p/q + \gamma/q$, where p, q are positive integers, and $-1 < \gamma < 1, \gamma \neq 0$. In this case, the channel can be expressed as:

$$qY_1 = qX_1 + (p + \gamma) X_2 + q\sqrt{b}Z_1 \tag{35}$$

$$Y_2 = X_1 \pm X_2 + Z_2 \tag{36}$$

Theorem 8: The following secure degree of freedom is achievable using nested lattice codes when $0 < |\gamma| < 0.5$:

$$\left[\frac{0.25 \log_2 (\alpha) - 1}{\frac{1}{2} \log_2 (\alpha\beta + 1)}\right]^+ \tag{37}$$

where

$$\alpha = \frac{1 - 2\gamma^2 + \sqrt{1 - 4\gamma^2}}{2\gamma^4} \tag{38}$$

and

$$\beta = q^2 + (p + \gamma)^2 \tag{39}$$

Proof outline: Here we use a layered coding scheme, which means the signal send by user k, X_k^N, is the sum of codewords from M layers: $X_k^N = \sum_{i=1}^{M} X_{k,i}^N$, $k = 1, 2$. For the ith layer, we use the nested lattice code described in Section III-A1, where the fine lattice and the coarse lattice used in layer i are Λ_i and $\Lambda_{c,i}$ respectively. Hence the signal $X_{k,i}^N$ is given by: $X_{k,i}^N = \left(u_{k,i}^N + d_{k,i}^N\right) \bmod \Lambda_{c,i}$, where $d_{k,i}^N$ is the dithering noise and $u_{k,i}^N$ is the lattice point. $u_{k,i}^N \in \mathcal{V}(\Lambda_{c,i}) \cap \Lambda_i$,$k = 1, 2$. For the nested codebook for the ith layer, we use R_i and P_i to denote its rate and average power per dimension respectively.

The interference is *partially aligned* with the intended signal at D_1. This means the decoding at layer i is carried out as follows: Node D_1 first decodes $qu_{1,i}^N + pu_{2,i}^N \bmod \Lambda_{c,i}$, then decodes $u_{2,i}^N$. In details, the decoder first computes

$$\hat{Y}_i^N = [\left(qu_{1,i}^N + pu_{2,i}^N\right) + \gamma X_{2,i}^N + \sum_{t=1}^{i-1} \left(qX_{1,t}^N + (p + \gamma) X_{2,t}^N\right) + q\sqrt{b}Z_1^N] \bmod \Lambda_{c,i} \tag{40}$$

It then decodes $qu_{1,i}^N + pu_{2,i}^N \bmod \Lambda_{c,i}$ from $\hat{Y}_i^N$. Define A_i as $A_i = \sum_{t=1}^{i-1} \left(q^2 + (p + \gamma)^2\right) P_t + q^2 b$. In order for node D_1 to decode correctly, we require [8]:

$$R_i \leq \frac{1}{2} \log_2 \left(\frac{P_i}{\gamma^2 P_i + A_i}\right) \tag{41}$$

Node D_1 is then left with the following:

$$[\gamma X_{2,i}^N + \sum_{t=1}^{i-1} \left(qX_{1,t}^N + (p + \gamma) X_{2,t}^N\right) + q\sqrt{b}Z_1^N] \bmod \Lambda_{c,i} \tag{42}$$

As long as

$$P_i > \gamma^2 P_i + A_i \tag{43}$$

(42) can be approximated with high probability [8] by the following:

$$\tilde{Y}_i^N = \gamma X_{2,i}^N + \sum_{t=1}^{i-1} \left(qX_{1,t}^N + (p + \gamma) X_{2,t}^N\right) + q\sqrt{b}Z_1^N \tag{44}$$

Otherwise a decoding error is said to occur. Node D_1 then evaluates the following expression from (44):

$$\left[k\tilde{Y}_i^N - \gamma d_{2,i}^N\right] \bmod \gamma\Lambda_{c,i} = [\gamma u_{2,i}^N + (k - 1) \gamma X_{2,i}^N + k(\sum_{t=1}^{i-1} \left(qX_{1,t}^N + (p + \gamma) X_{2,t}^N\right) + q\sqrt{b}Z_1^N)] \bmod \gamma\Lambda_{c,i} \tag{45}$$

where k is a scalar which functions as the α in [14, (13)]. In order for node D_1 to decode $u_{2,i}^N$ from this signal correctly, we require [8]:

$$R_i \leq \frac{1}{2} \log_2 \left(1 + \frac{\gamma^2 P_i}{A_i}\right) \tag{46}$$

Then node D_1 can recover the following signal from (44):

$$\sum_{t=1}^{i-1} \left(qX_{1,t}^N + (p + \gamma) X_{2,t}^N\right) + q\sqrt{b}Z_1^N \tag{47}$$

which will be fed to the decoder at lower layers.

We next determine the R_i and P_i for each layer. Let the right hand side of (41) equal to the right hand side of (46):

$$\frac{P_i}{\gamma^2 P_i + A_i} = 1 + \frac{\gamma^2 P_i}{A_i} \tag{48}$$

which gives us:

$$P_i = \alpha A_i \tag{49}$$

where $\alpha = \frac{1-2\gamma^2+\sqrt{1-4\gamma^2}}{2\gamma^4}$. This leads to (38) in Theorem 8. For α to be real, we require $1 - 4\gamma^2 \geq 0$, which means $|\gamma| \leq 0.5$.

Substituting the definition of A_i into (49) and solving for P_i, we find:

$$P_i = \alpha (\alpha\beta + 1)^{i-1} q^2 b \tag{50}$$

where $\beta = q^2 + (p + \gamma)^2$. This leads to (39).

Substituting (50) into the definition of A_i, we get:

$$A_i = (\alpha\beta + 1)^{i-1} q^2 b \tag{51}$$

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

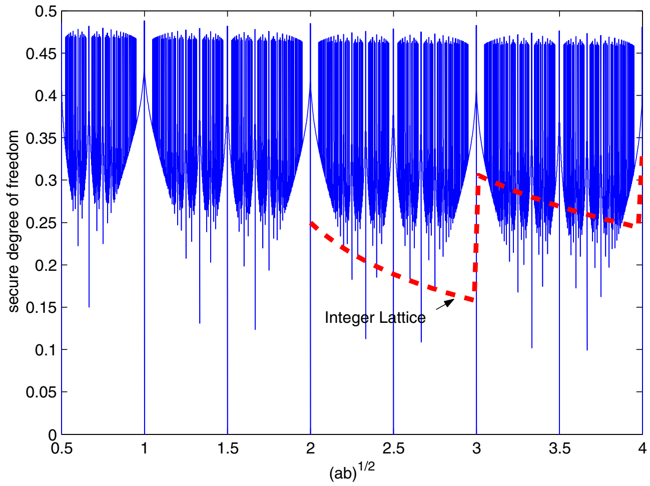

Fig. 4. Secure degree of freedom

Due to (48), R_i can be found by averaging (41) and (46) and substituting (50) and (51) into the result. It can be verified that R_i is given by:

$$R_i = 0.25 \log_2(\alpha) \tag{52}$$

It can also be verified that the requirement (43) is fulfilled automatically when $|\gamma| < 0.5$ [8].

The total power of S_i can be computed from (50) and is given by

$$\sum_{t=1}^{M} P_t = \frac{(\alpha\beta+1)^M - 1}{\beta} q^2 b \tag{53}$$

From (12), each layer leaks at most N bit to the eavesdropper over N channel uses. Since there are M layers, at most MN bits are leaked over N channel uses. From it, it can be shown that a secrecy rate of $R_e = \sum_{i=1}^{M} R_i - M$ is achievable [8]. The secure degree of freedom is therefore given by

$$\lim_{P\to\infty} \frac{R_e}{\frac{1}{2}\log_2 P} = \lim_{M\to\infty} \frac{[\sum_{i=1}^{M} R_i - M]^+}{\frac{1}{2}\log_2 \sum_{t=1}^{M} P_t} \tag{54}$$

which equals (37) in Theorem 8. ■

Remark 2: In Figure 4, we plot the achieved secure degree of freedom by the nested lattice coding scheme in this section. The figure shows that the secure degree of freedom is positive whenever $2\sqrt{ab}$ is not an integer. This, along with the results in the previous sections, proves that *the secure degree of freedom is positive everywhere except when the channel is degraded.*

Remark 3: Plotted with dashed lines in Figure 4 is the performance of the integer lattice from previous section. Comparing it with the performance of the scheme in this section, we find that neither scheme dominates the other in performance uniformly.

IV. Conclusion

In this work, we have proved that a positive secure degree of freedom is achievable for the fully connected interference assisted wiretap channel when the channel is not degraded. As a consequence of this high SNR result, we are able to claim that, in contrast to common belief, Gaussian signaling is not optimal for a large class of two user Gaussian channels with secrecy constraints.

The result here provides another example that structured codes are useful in proving information theoretic results. Examples where structured codes outperform random codes in non-secrecy problems can be found in [15]. Using structured codes in secrecy problems was first proposed by the authors in [10]. Up to date, for secrecy problems, structured codes proved to be useful for secrecy in multi-hop relay channels due to the possibility of compute-and-forward [10], or for interference channels with more than two users due to interference alignment [16]. The result here provides the example that structured codes are indeed useful for two user Gaussian channels as well.

References

[1] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, September 1949.
[2] E. Tekin and A. Yener. The General Gaussian Multiple Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, June 2008.
[3] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions. *IEEE Transactions on Information Theory*, 54(6):2493–2507, June 2008.
[4] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. The Gaussian Wiretap Channel With a Helping Interferer. In *IEEE International Symposium on Information Theory*, July 2008.
[5] X. He and A. Yener. A New Outer Bound for the Gaussian Interference Channel with Confidential Messages. In *43rd Annual Conference on Information Sciences and Systems*, March 2009.
[6] Z. Li, R. D. Yates, and W. Trappe. Secrecy Capacity Region of a Class of One-Sided Interference Channel. In *IEEE International Symposium on Information Theory*, July 2008.
[7] E. Ekrem and S. Ulukus. On the Secrecy of Multiple Access Wiretap Channel. In *46th Allerton Conference on Communication, Control, and Computing*, September 2008.
[8] X. He and A. Yener. Providing Secrecy With Structured Codes: Tools and Applications to Gaussian Two-user Channels. Submitted to IEEE Transactions on Information Theory, April, 2009, Available online at http://arxiv.org/abs/0907.5388.
[9] S. Leung-Yan-Cheong and M. Hellman. The Gaussian Wire-tap Channel. *IEEE Transactions on Information Theory*, 24(4):451–456, July 1978.
[10] X. He and A. Yener. Providing Secrecy with Lattice Codes. In *46th Allerton Conference on Communication, Control, and Computing*, September 2008.
[11] R. Etkin and E. Ordentlich. On the Degrees-of-Freedom of the K-User Gaussian Interference Channel. Submitted to IEEE Transactions on Information Theory, June, 2008.
[12] I. Csiszár and J. Körner. Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.
[13] V. R. Cadambe, S. A. Jafar, and S. Shamai. Interference Alignment on the Deterministic Channel and Application to Fully Connected AWGN Interference Networks. *IEEE Transactions on Information Theory*, 55(1):269–274, January 2009.
[14] U. Erez and R. Zamir. Achieving 1/2 log (1+ SNR) on the AWGN Channel with Lattice Encoding and Decoding. *IEEE Transactions on Information Theory*, 50(10):2293–2314, October 2004.
[15] B. Nazer and M. Gastpar. The Case for Structured Random Codes in Network Capacity Theorems. *European Transactions on Telecommunications, Special Issue on New Directions in Information Theory*, 19(4):455–474, June 2008.
[16] X. He and A. Yener. K-user Interference Channels: Achievable Secrecy Rate and Degrees of Freedom. In *IEEE Information Theory Workshop*, June 2009.