Secure Degrees of Freedom for the MIMO Wiretap Channel with a Multiantenna Cooperative Jammer

Mohamed Nafea and Aylin Yener
Department of Electrical Engineering, The Pennsylvania State University, University Park, PA 16802

Abstract—A multiple antenna Gaussian wiretap channel with a multiantenna cooperative jammer (CJ) is considered and the secure degrees of freedom (s.d.o.f.), with \( N \) antennas at the sender, receiver, and eavesdropper, is derived for all possible values of the number of antennas at the cooperative jammer, \( K \). In particular, the upper and lower bounds for the s.d.o.f. are provided for different ranges of \( K \) and shown to coincide. Gaussian signaling both for transmission and jamming is shown to be sufficient to achieve the s.d.o.f. of the channel, when the s.d.o.f. is not an integer, structured signaling and joint signal space and signal scale alignment are employed to achieve the s.d.o.f.

I. INTRODUCTION

Information theoretic secrecy [1] guarantees secure communication in the presence of an eavesdropper. Information theoretic secrecy of multiterminal and multiantenna channels has been studied extensively, e.g., [2]–[9]. In particular, the Gaussian wiretap channel (WTC) with a cooperative jammer (CJ) was studied in [2]–[8]. A CJ can improve the secrecy rate and even the prelog factor of the secrecy rate, i.e., the secure degrees of freedom (s.d.o.f.) [5]. Relying on cooperative jamming and structured signaling, [6], [7] identified the s.d.o.f. secure degrees of freedom (s.d.o.f.), with \( K \) increasing over \( N \). For vector \( X \), \( V \) = \([V_1 \cdots V_j]^T \), where \( 1 \leq i < j \leq n \), and \( ||V|| \) denotes Euclidean norm, \( 0_{m \times n} \) denotes an \( m \times n \) matrix of zeros. The set of integers \( \{ -Q, \cdots, Q \} \) is denoted by \( \{ -Q, \cdots, Q \}_Z \), \( Z[j] \) denotes the set of complex integers.

II. CHANNEL MODEL AND DEFINITIONS

We consider a multiantenna Gaussian WTC composed of a transmitter, a receiver, an eavesdropper each with \( N \) antennas, and a \( K \)-antenna CJ, see Fig.1. The received signals at the receiver and eavesdropper at the \( n \)th channel use are given by

\[
Y_r(n) = H_t X_t(n) + H_c X_e(n) + Z_r(n) \tag{1}
\]

\[
Y_e(n) = G_c X_t(n) + G_c X_e(n) + Z_e(n), \tag{2}
\]

where \( X_t(n) \), \( X_e(n) \) are the transmitted signals from the transmitter and CJ, respectively, \( H_t, G_t \in \mathbb{C}^{N \times N} \) are the transmitter’s channel matrices to the legitimate receiver and to the eavesdropper, and \( H_c, G_c \in \mathbb{C}^{N \times K} \) are the channel matrices from the CJ to the legitimate receiver and eavesdropper. The channel gains are static, and \( \text{complex-valued}, \) \( Z_r(n) \) and \( Z_e(n) \) denote the complex Gaussian noise at the \( n \)th channel use, i.e., \( Z_r(n), Z_e(n) \sim \mathcal{C}N(0, I_N) \), are independent from one another and both are independent and identically

This work was supported by NSF Grants CCF 09-64362, 13-19338 and CNS 13-14719.
distributed (i.i.d.) across $n$. The power constraints at the transmitter and CJ are $E\{X^n_i X_i\}, E\{H^n X_i\} \leq P$.

Let $X^n_\epsilon = [X_1(\cdots) X_\epsilon(n)]$, $Y^n_\epsilon, Y^n_\epsilon, Z^n_\epsilon, Z^n_\epsilon$ are defined similarly. The transmitter intends to send a secret message $W \in W$ to the legitimate receiver in the presence of the eavesdropper. $W$ is mapped into the transmitted signal $X^n_\epsilon \in \mathcal{X}^n_\epsilon$ by using a stochastic encoder $f : W \mapsto X^n_\epsilon$ at the transmitter. The receiver forms an estimate of $W$, denoted by $\hat{W}$. Secrecy rate $R_s$ is achievable if for any $\epsilon > 0$, there exists a channel code, $(2^n R_s, n)$, such that

$$\Pr\{\hat{W} \neq W\} \leq \epsilon, \quad \frac{1}{n} H(W|Y^n_\epsilon) \geq \frac{1}{n} H(W) - \epsilon.$$  

(3)

The achievable s.d.o.f. for a given secrecy rate, $R_s$, is

$$D_s = \lim_{P \to \infty} \frac{R_s}{\log_2 P}.$$  

(4)

The CJ transmits $X^n_\epsilon \in \mathcal{X}^n_\epsilon$. The jamming signal $X^n_\epsilon$ is not meant to convey a message. There is no common randomness between the transmitter and the CJ.

### III. Main Result

#### Theorem 1

The s.d.o.f. of the multiantenna Gaussian WTC with a K-antenna CJ and N antennas at each of its nodes is

$$D_s = \begin{cases} K, & \text{for } 0 \leq K \leq \frac{N}{2} \\ \frac{N}{2}, & \text{for } \frac{N}{2} < K \leq N \\ \frac{N}{2}, & \text{for } N < K \leq 2N. \end{cases}$$  

(5)

Theorem 1 provides a complete characterization for the s.d.o.f. of the channel. The s.d.o.f. for $K = 2N$ is equal to $N$, that is equal to the d.o.f. of the $N$-antenna Gaussian channel with no secrecy constraint. Thus, the s.d.o.f. can not be increased by increasing $K$ over 2N. Interestingly, Theorem 1 shows that the s.d.o.f. of the channel is not increased by increasing $K$ from $\left[ \frac{N}{2} \right]$ to $N$. In Sections IV and V, we provide the converse and achievability proofs for Theorem 1.

### IV. Converse

#### A. $0 \leq K \leq N$

We allow for cooperation between the transmitter and CJ, obtain, in effect a multiantenna Gaussian WTC with $N + K$-antenna transmitter, $N$-antenna receiver, and $N$-antenna eavesdropper. The secrecy rate of this channel is bounded as [9]

$$R_s \leq \log \det \left( I_N + \frac{P}{K} \mathbf{H}\mathbf{G}^\dagger \mathbf{H} \right) + o(\log P),$$  

(6)

where $\mathbf{H}, \mathbf{G} \in \mathbb{C}^{N \times N + K}$ are the channel matrices from the combined transmitter to the receiver and eavesdropper, and $\mathbf{G}^\dagger$ is the projection matrix onto $N(\mathbf{G})$. We also have [9]

$$\mathbf{H}\mathbf{G}^\dagger \mathbf{H} = \Psi \begin{bmatrix} 0_{N-K \times N-K} & 0_{N-K \times K} \\ 0_{K \times N-K} & \Omega \end{bmatrix} \Psi^H,$$  

(7)

where $\Psi$ is a unitary matrix and $\Omega$ is a non-singular matrix. By substituting (7) in (6), it can be easily shown that

$$R_s \leq K \log P + o(\log P).$$  

(8)

1 Throughout the paper, we omit index $n$ whenever possible.

The secrecy rate for the original channel, $R_s$, is upper bounded by $R_s$. Using (4), the s.d.o.f., $D_s$, is upper bounded by $K$.

#### B. $N \leq K \leq 2N$

Here, we extend the converse proof in [6] to the multiantenna channel. Let $\phi_i, i = 1, \cdots, 6$, denote constants that do not depend on the power $P$. $R_s$ can be upper bounded as

$$nR_s = H(W) \leq H(W|Y^n_\epsilon) + n\epsilon - H(W|Y^n_\epsilon) + n\delta$$  

(9)

$$\leq I(W; Y^n_\epsilon|Y^n_\epsilon) + n\phi_1$$  

(10)

$$= h(Y^n_\epsilon|Y^n_\epsilon) - h(Y^n_\epsilon|Y^n_\epsilon, X^n_\epsilon) + n\phi_1$$  

(11)

$$= h(Y^n_\epsilon|Y^n_\epsilon) - h(Y^n_\epsilon|Z^n_\epsilon, X^n_\epsilon) + n\phi_1.$$  

(12)

(9) follows from (3) and Fano’s inequality; $\phi_1 = \epsilon + \delta$.

Define $\tilde{X}_1 = X_1 + Z_1, \tilde{X}_n = X_n + Z_n$, where $Z_1 \sim \mathcal{CN}(0, \mathbf{K}_1)$ and $Z_n \sim \mathcal{CN}(0, \mathbf{K}_n)$. $\mathbf{K}_n$ are chosen as $\mathbf{K}_n = \rho \mathbf{I}_N$, $\mathbf{K}_n = \beta^2 \mathbf{I}_N$, where $0 < \rho \leq \frac{1}{\sqrt{1 - \rho^2}}$ and $0 < \beta \leq \frac{1}{\sqrt{1 - \rho^2}}$. $Z_1$ is independent from $Z_n$ and both are independent from $\{\tilde{X}_1, X_n, Z_n, Z_n\}$. $Z_1, Z_n$ are i.i.d. sequences of $Z_1, Z_n$, respectively. Let $Z_1 = -\tilde{X}_1, Z_n = -\tilde{X}_n, Z_n + Z_n$, where $Z_1 \sim \mathcal{CN}(0, \mathbf{K}_1)$, $Z_n \sim \mathcal{CN}(0, \mathbf{K}_n)$. $Z_1, Z_n$ are independent from $\{\tilde{X}_1, X_n, Z_n, Z_n\}$.

Using infinite divisibility of Gaussian distribution, a stochastic equivalence form of $Z_n$ is $Z^n_\epsilon = G_n X^n_n + G_n X^n_n + Z^n_\epsilon$. Since $G_n X^n_n, G_n X^n_n + Z^n_\epsilon$ are independent, we have

$$h(Y^n_\epsilon) = h(Y^n_\epsilon) \geq h(G_n X^n_n) + n\phi_3.$$  

(17)

$$= h(X^n_n) + n\log \det(G_n).$$  

(18)

Substituting (18) in (16) gives us

$$nR_s \leq h(X^n_n) + h(X^n_n|X^n_n) + n\phi_4,$$  

(19)

where $X^n_n = [X^n_1 \cdots \tilde{X}_n]^T, \tilde{X}_n = [X^n_1 \cdots \tilde{X}_n]^T$, and $\tilde{X}_n = X_n + Z_n$. Let $h_{c_k}$ be the $k$th column vector of $H_n = [H_{c_1} H_{c_2}]$. $h_{c_1} = \cdots \cdot h_{c_2}$ and $h_{c_2} = [h_{c_1} \cdots \cdot h_{c_2}]$. In order to reliably transmit the message $W$, we must have

$$nR_s \leq I(X^n_n; Y^n_\epsilon) = h(Y^n_\epsilon) - h(H_n X^n_n + Z^n_\epsilon)$$  

(20)

$$\leq h(Y^n_\epsilon) - h(H_n X^n_n + H_{c_2} X^n_2)$$  

(21)

$$\leq h(Y^n_\epsilon) - h(H_n X^n_n + H_{c_2} X^n_2).$$  

(22)
\[
\begin{align*}
\leq h(Y^n_r) - h(H, X^n_c | X^n_r, \bar{X}^n_r) 
\quad & = h(Y^n_r) - h(\bar{X}^n_r | X^n_r) - n \log \det(\mathbf{H}_c^i), \\
\end{align*}
\] 
where (21) follows similar to (17), and (22) follows since for correlated \( X \) and \( Y \), \( h(X + Y) \geq h(X + Y | Y) = h(X | Y) \).

Combining (19) and (24), we get
\[
\begin{align*}
nR_s & \leq \frac{1}{2} \sum_{i=1}^{2n} \left( \sum_{k=1}^{N} h(Y_{rk}(i)) + \sum_{k=N+1}^{K} h(\bar{X}_{ck}(i)) \right) + n\phi_6, \\
\end{align*}
\] 
Using Cauchy-Schwarz inequality and the power constraints, we can show that the variance of \( Y_{rk}(i) \) is bounded as
\[
\Var(Y_{rk}(i)) \leq 1 + h^2P, 
\] 
where \( h^2 = \max \left( \|h_r^T\|^2 + \|h_c^T\|^2, \|h_r^T\|^2 \right) \), and \( h_r^T, h_c^T \) are the \( k \)th row vectors of \( H_r \) and \( H_c \). Thus, \( h(Y_{rk}(i)) \leq \log 2\pi e(1 + h^2P) \). Similarly, we can show that \( h(\bar{X}_{ck}(i)) \leq \log 2\pi e(\beta^2 + P) \). Thus,
\[
R_s \leq \frac{N}{2} \log(1 + h^2P) + \frac{K - N}{2} \log(\beta^2 + P) + \phi_6, 
\] 
and the s.d.o.f. is upper bounded as \( D_s \leq \frac{K}{2} \).

C. Obtaining the upper bound for all \( K \)

We use the upper bound obtained in Section IV-A for \( 0 \leq K \leq \frac{N}{2} \), and the upper bound obtained in Section IV-B for \( N \leq K \leq 2N \). By comparing the two, it is evident that the upper bound from Section IV-A is greater than \( \frac{N}{2} \) for \( \frac{N}{2} < K \leq N \). Since we know, from Section IV-B, that at \( K = N \), the upper bound is \( \frac{N}{2} \), we can use \( \frac{N}{2} \) as the upper bound for \( \frac{N}{2} < K \leq N \). Combining these statements, we get (5). Next, we shall see the achievability of (5).

V. Achievable Schemes

We divide the range \( 0 \leq K \leq 2N \) into five cases and propose an achievable scheme for each case. For all the achievable schemes, we have the \( n \)-letter signals, \( X^n_r \) and \( X^n_c \), as i.i.d. sequences. Since \( X^n_r \) is independent from \( X^n_c \), we have in effect a memoryless WTC, and the following secrecy rate is achievable by stochastic encoding [1]:
\[
R_s = [I(X_t; Y_r) - I(X_t; Y_e)]^+. 
\] 
A. Case 1: \( 0 \leq K \leq \frac{N}{2} \)

The transmitter sends \( K \) independent Gaussian information streams and the CJ sends \( K \) independent Gaussian jamming streams. Since \( 2K \leq N \), the legitimate receiver can decode all the information and jamming streams at high SNR. The transmitter chooses a precoder, \( P_t \), which aligns its information streams over the jamming streams at the eavesdropper. The signals transmitted by the transmitter and the CJ are
\[
X_t = P_t U_t, \quad X_c = J_c V_c, 
\] 
where \( U_t, V_c \sim \mathcal{CN}(0, P I_K) \). \( U_t \) and \( V_c \) are the information and jamming streams, respectively. \( P_t = G_t^{-1} G_c \) and \( J_c = I_K \). \( P = \frac{1}{2\alpha} P_t \), where \( \alpha = \max \{K, \sum_{k=1}^{K} ||p_k||^2 \} \) to satisfy the power constraints. The received signals are expressed as
\[
\begin{align*}
Y_r &= [H_r G_t^{-1} G_c, H_c] [U_t^T, V_c^T]^T + Z_r, \\
Y_e &= G_c (U_t + V_c) + Z_e. 
\end{align*}
\] 
We lower bound (27) as follows. First, \([H_r G_t^{-1} G_c, H_c]\) is almost surely (a.s.) full column-rank. Thus,
\[
I(X_t; Y_r) \geq K \log P + o(\log P). 
\] 
Next, we upper bound the term \( I(X_t; Y_e) \) as follows:
\[
I(X_t; Y_e) = \log \det(I_K + 2P G_c^H G_c) \leq K. 
\] 
By substituting (31) and (32) in (27), we have
\[
R_s \geq K \log P + o(\log P) - K. 
\]
Hence, the achievable s.d.o.f. is lower bounded as \( D_s \geq K \).

B. Case 2: \( \frac{N}{2} < K \leq N \) is even

The s.d.o.f. is upper bounded by \( \frac{N}{2} \) for all \( \frac{N}{2} < K \leq N \). When \( N \) is even, the achievable scheme for \( K = \frac{N}{2} \) can be used to achieve the s.d.o.f. of the channel for all \( \frac{N}{2} < K \leq N \). The transmitted signals are given by (28), with \( J_c = [I_{2N} 0] \). \( P_t = G_t^{-1} G_c, U_t, V_c \sim \mathcal{CN}(0, P I_K) \). Using the same analysis as in the previous case, the achievable s.d.o.f. is \( \frac{N}{2} \) for any \( \frac{N}{2} < K \leq N \), where \( N \) is even.

C. Case 3: \( \frac{N}{2} < K \leq N \) is odd

For this case, we utilize structured signaling both at the transmitter and the CJ. In particular, we propose to use joint signal space alignment and the complex field equivalent of real interference alignment [10], [11]. The transmitter and CJ send \( \frac{N}{2} + 1 \) streams each. The transmitter aligns its information streams over the jamming at the eavesdropper. The legitimate receiver projects its received signal over a direction orthogonal to all but one information and one jamming stream, decodes these two streams from the projection, and subtracts their effect from its received signal, leaving \( N - 1 \) spatial dimensions for the other streams. For notational simplicity, let \( d = \frac{N}{2} + 1 \).

The transmitted signals are given by (28) with \( J_c = [I_{2d} 0_{d \times K - d}]^T \), \( P_t = G_t^{-1} G_c, U_t = [U_1 \cdots U_d]^T, V_c = [V_1 \cdots V_d]^T \), \( U_i = U_{it} + jU_{it}^*, V_i = V_{it} + jV_{it}^* \), for \( i = 2, \ldots, d \), and \( U_1, V_1, \{U_{it}, i \neq 2\}, \{V_{it}, i \neq 2\} \) are i.i.d. uniform over the set \( \{a(-Q, Q)\} \). The values for \( a \) and the integer \( Q \) are chosen as
\[
Q = P^{\frac{1}{d+1}} - \nu, \quad a = \gamma P^{\frac{1}{d+1}}, 
\] 
where \( \epsilon > 0 \) can be arbitrarily small, and \( \nu, \gamma \) are constants.

Let \( G_c = G_c J_c \). The received signal at the eavesdropper is
\[
Y_e = \tilde{G}_c (U_t + V_c) + Z_e. 
\]
We upper bound \( I(X_t; Y_e) \) as follows:
\[
I(X_t; Y_e) \leq I(X_t; Y_e, Z_e) = I(X_t; Y_e Z_e) 
\] 
\[
= H \left( \tilde{G}_c (U_t + V_c) \right) - H \left( \tilde{G}_c V_c \right). 
\]
where (38) follows since the mappings $U_t + V_e \mapsto G_c(U_t + V_e)$. The received signal at the legitimate receiver is

$$Y_r = AU_t + \hat{H}_e V_e + Z_r,$$

(40)

where $A = H_c G_c^{-1} G_c J_e$ and $\hat{H}_e = H_e J_e$. Let $a_i$ and $h_{ci}$ be the $i$th column vectors of $A$ and $\hat{H}_e$, respectively. The legitimate receiver chooses $b \in \mathbb{C}^n$ such that $b \perp \text{span} \{a_2, \ldots, a_d, h_{c2}, \ldots, h_{cd}\}$ and multiplies its received signal by the decoding matrix,

$$D = \begin{bmatrix} b^H & 0_{N-1 \times 1} \end{bmatrix},$$

(41)

to obtain $\tilde{Y}_r = DY_r = [\tilde{Y}_{r1} \ (\tilde{Y}_{r2})^T]^T$, where

$$\tilde{Y}_{r1} = f_1 U_t + f_2 V_1 + Z',$$

(42)

$$\tilde{Y}_{r2} = A U_t + \hat{H}_e V_e + Z_r^N,$$

(43)

$f_1 = b^H a_1$, $f_2 = b^H h_{c2}$, $Z' = b^H Z_r$, $\tilde{A} = [\tilde{a}_1 \ldots \tilde{a}_d]$, $\hat{H} = [\tilde{h}_{c2} \ldots \hat{h}_{cd}]$, and $\tilde{h}_{c2} = \hat{h}_{c2}$. The legitimate receiver uses $\tilde{Y}_{r1}$ to decode $U_1$ and $V_1$. Since $f_1, f_2$ are a.s. rationally independent, the mapping $(U_1, V_1) \mapsto f_1 U_t + f_2 V_1$ is bijective (i.e., invertible) [10]. The legitimate receiver employs a hard decision decoder which maps $\tilde{Y}_{r1} \in \tilde{Y}_{r1}$ to the nearest point in the constellation $R_1 = f_1 U_t + f_2 V_1$, where $U_t, V_1 = \{a(-Q, Q)\}_2$. Then, the legitimate receiver passes the output of the hard decision decoder through the bijective map $f_1 U_t + f_2 V_1 \mapsto (U_1, V_1)$ to decode both $U_1, V_1$, and subtracts the signal from $\tilde{Y}_{r2}^N$ to obtain

$$Y_r = B [U_{t2}^d V_{c2}^d]^T + Z_r^N,$$

(44)

where $B = [\tilde{a}_2 \ldots \tilde{a}_d \ \tilde{h}_{c2} \ldots \hat{h}_{cd}] \in \mathbb{C}^{N-1 \times N-1}$ is a.s. full rank due to the random generation assumption on the channel gains. Finally, by zero forcing, the receiver obtains $U_{t2}^d$ from $Y_r$. The term $I(X_t; Y_r)$ is lower bounded as follows:

$$I(X_t; Y_r) \geq I(U_t; \tilde{Y}_{r1}) + I(U_{t2}^d; \tilde{Y}_{r2}^N|U_t, \tilde{Y}_{r1}),$$

(46)

where (45) follows since $U_t \rightarrow X_t \rightarrow Y_r \rightarrow Y_e$ forms a Markov chain. The term $I(U_t; \tilde{Y}_{r1})$ can be bounded as

$$I(U_t; \tilde{Y}_{r1}) = H(U_t) - H(U_t|\tilde{Y}_{r1}) \geq H(U_t) - 1 - P_{e_1} \log |U_t| = (1 - P_{e_1}) \log (2Q + 1) - 1,$$

(47)

(49)

where $P_{e_1} = \Pr(\hat{U}_1 \neq U_1)$, and (48) follows from Fano's inequality. Since the mapping $(U_1, V_1) \mapsto f_1 U_t + f_2 V_1$ is invertible, the only source for error is the Gaussian noise $Z'$. Hence

$$P_{e_1} \leq \Pr \left\{ \hat{U}_1 \neq U_1, V_1 \right\} \leq \Pr \left\{ |Z'| \geq d_{\min}^2 \right\} = \exp \left( -\frac{d_{\min}^2}{2|b|^2} \right),$$

(51)

where $|Z'| \sim \text{Rayleigh}(|b|)$ and $d_{\min}$ is the minimum distance between points in the constellation $R_1$, which can be lower bounded using the following lemma [10], [11].

**Lemma 1** For almost all $z \in \mathbb{C}^n$ and for all $\epsilon > 0$,

$$|p + z| > \left( \max_i q_i \right)^{-\left( \frac{a-1+\epsilon}{\epsilon} \right)},$$

(52)

holds for all $q \in \mathbb{Z}^n, p \in \mathbb{Z}$ except for finitely many of them.

Thus, for almost all channel gains, $d_{\min}$ is

$$d_{\min} = \inf_{U_1, V_1 \in \mathbb{C}^{-2Q, 2Q(2Q)_1}} |f_1 U_1 + f_2 V_1| \geq \frac{a |f_1|}{(2Q)^{\frac{a}{2}}} \geq \gamma |f_1|^{2^{-a}} p^2.$$  

(53)

(54)

Substituting (54) in (51) gives $P_{e_1} \leq \exp(-\mu P')$, where $\mu = \frac{\gamma^2 |f_1|^{2^{-a}}}{|b|^2}$. Using (34) and (49), we have

$$I(U_1; \tilde{Y}_{r1}) \geq \frac{1 - \epsilon}{2 + \epsilon} \log P + o(\log P).$$

(55)

Next, we lower bound the term $I(U_{t2}^d; \tilde{Y}_{r2}^N|U_t, \tilde{Y}_{r1})$. Define $\hat{B} = [0_{N-1 \times 1} I_{N-1}] - \frac{1}{\sqrt{2}} \hat{h}_{c2} b^H$, $Y_{r}' = \hat{B} [U_{t2}^d V_{c2}^d]^T + \hat{B} Z_r$: $\tilde{Y}_r' = B^{-1} Y_r' = [U_{t2}^d V_{c2}^d]^T + B^{-1} \hat{B} Z_r$, and $P_{e2}^d = \Pr(U_{t2}^d \neq U_{t2}^d)$. Thus, we have

$$I(U_{t2}^d; \tilde{Y}_{r2}^N|U_t, \tilde{Y}_{r1}) = I(U_{t2}^d; \tilde{Y}_{r2}^N|U_t, f_2 V_1 + Z') = I(U_{t2}^d; \tilde{Y}_{r2}^N|f_2 V_1 + Z) \geq I(U_{t2}^d; \tilde{Y}_{r2}^N) \geq 1 - (P_{e2}^d) \log (2Q + 1)^{N-1} - 1.$$

(56)

(57)

(58)

(59)

Let $\hat{Z}_r = \Xi Z_r = [\hat{Z}_{r2} \ldots \hat{Z}_{rN}]^T$, where $\Xi = \mathbb{B}^{-1} \hat{B}$. Thus, $\hat{Z}_r \sim \mathcal{CN}(0, \Xi H)$ and $|\hat{Z}_r| \sim \text{Rayleigh}(\sigma_i)$, where $\sigma_i^2 = \Xi H(i, i)$. Using the union bound, we have

$$P_{e2}^d \leq \sum_{i=2}^d \Pr \left\{ U_{t2}^d \neq U_{t2}^d \right\} \leq \sum_{i=2}^d \Pr \left\{ |\hat{Z}_{r2}| \geq \frac{a}{2} \right\} \leq \frac{N - 1}{2} \exp(-\mu P'),$$

(60)

(61)

where $\mu' = \frac{a^2}{2\sigma_{\max}^2}$, $\sigma_{\max} = \max \sigma_i$, and $\epsilon' = \frac{a}{2\sigma_{\max}}$. Thus,

$$I(U_{t2}^d; \tilde{Y}_{r2}^N|U_t, \tilde{Y}_{r1}) \geq \frac{1 - \epsilon}{2 + \epsilon} (N - 1) \log P + o(\log P).$$

(62)

Thus, substituting (55) and (62) in (46) gives us

$$I(X_t; Y_r) \geq \frac{1 - \epsilon}{2 + \epsilon} N \log P + o(\log P),$$

(63)
and using (4), (27), (39), and (63) results in $D_s \geq \frac{1 + \epsilon}{\epsilon} N$. Since $\epsilon > 0$ is arbitrarily small, we can achieve s.d.o.f. of $\frac{N}{2}$.

**D. Case 4: $N < K \leq 2N$ and $K$ is even**

The achievable scheme for this case involves transmitting $\frac{K}{2}$ Gaussian information and $\frac{K}{2}$ Gaussian jamming streams. The CJ sends $K-N$ out of its $\frac{K}{2}$ streams over the null space of $H_c$, $\mathcal{N}(H_c)$, leaving only $N - \frac{K}{2}$ streams visible to the legitimate receiver. At high SNR, the legitimate receiver can decode the $\frac{K}{2}$ information and the $N - \frac{K}{2}$ jamming streams. The transmitted signals are given by (28), with $P_t = G_t^{-1} G_c J_c$, $J_c = [J_1, J_n]$, $J_1 = [I_g h_{gK-N}^T]$, and $J_n = [n_1, \ldots, n_{K-N}]$ span $\mathcal{N}(H_c)$. The transmitted signals are received over a direction orthogonal to all $\mathcal{N}(H_c)$. Using similar analysis as in Section V-C, we have $I(U_{t2}, Y_{r2}^N | U_{t2}) \geq I(U_{t2}, Y_r^N)$, where $Y_r^N$ is arbitrarily small, we can achieve s.d.o.f. of $\frac{N}{2}$ is achievable, which completes the proof for Theorem 1.

**VI. CONCLUSION**

We have characterized the s.d.o.f. of the multi-antenna Gaussian wiretap channel with a $K$-antenna cooperative jammer (CJ) and $N$ antennas at each of its nodes for all possible values of $K$. We have shown that when the s.d.o.f. of the channel is integer-valued, the s.d.o.f. can be achieved by a scheme which involves linear precoding, Gaussian signaling both for transmission and jamming, and linear receiver processing. In contrast, we have proved that, when the s.d.o.f. is non-integer, a scheme which employs structured signaling along with joint signal space and signal scale alignment achieves the s.d.o.f. of the channel. The converse was proved by allowing for cooperation between the transmitter and CJ for a certain range of $K$, and by incorporating both the secrecy and reliability constraints, for the other values of $K$. Although we identify its prelog factor, the secrecy capacity of this model remains open and deserves further attention.

**REFERENCES**

1. A. D. Wyner, “The wire-tap channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975.
2. E. Tekin and A. Yener, “Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy,” in 44th Annual Allerton Conf. On Communication, Control, and Computing, Sep. 2006.
3. E. Tekin and A. Yener, “The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” IEEE Trans. Info. Theory, vol. 54, no. 6, pp. 2735–2751, 2008.
4. X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, “Interference assisted secret communication,” IEEE Trans. Info. Theory, vol. 57, no. 5, pp. 3153–3167, 2011.
5. X. He and A. Yener, “Providing secrecy with structured codes: Two-user Gaussian channels,” IEEE Trans. Info. Theory, vol. 60, no. 4, pp. 2121–2138, 2014.
6. J. Xie and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks,” IEEE Trans. Info. Theory, vol. 60, no. 6, pp. 3359–3378, 2014.
7. J. Xie and S. Ulukus, “Secure degrees of freedom of K-user Gaussian interference channels: A unified view,” Submitted to IEEE Trans. Info. Theory, 2013, arXiv preprint arXiv:1305.7214.
8. M. Nafea and A. Yener, “How many antennas does a cooperative jammer need for achieving the degrees of freedom of multiple antenna Gaussian channels in the presence of an eavesdropper,” in 51st Annual Allerton Conference on Communication, Control, and Computing, Oct. 2013.
9. A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas-Part II: The MIMO-MET wiretap channel,” IEEE Trans. Info. Theory, vol. 56, no. 11, pp. 5515–5532, 2010.
10. M. A. Maddah-Ali, “On the degrees of freedom of the compound MIMO broadcast channels with finite states,” 2009, arXiv preprint arXiv:0909.5006.
11. D. Kleinbock, “Baker-sprindzhuk conjectures for complex analytic manifolds,” 2002; arXiv preprint math/0210369.