Secure Degrees of Freedom for the MIMO Wire-tap Channel with a Multi-antenna Cooperative Jammer

Mohamed Nafea, Member, IEEE, and Aylin Yener, Fellow, IEEE

Abstract—In this paper, a multiple antenna wire-tap channel in the presence of a multi-antenna cooperative jammer is studied. In particular, the secure degrees of freedom (s.d.o.f.) of this channel is established, with \( N_t \) antennas at the transmitter, \( N_e \) antennas at the legitimate receiver, and \( N_c \) antennas at the eavesdropper, for all possible values of the number of antennas, \( N_e \), at the cooperative jammer. In establishing the result, several different ranges of \( N_e \) need to be considered separately. The lower and upper bounds for these ranges of \( N_e \), are derived, and are shown to be tight. The achievable techniques developed rely on a variety of signaling, beamforming, and alignment techniques which vary according to the (relative) number of antennas at each terminal and whether the s.d.o.f. is integer valued. Specifically, it is shown that, whenever the s.d.o.f. is integer valued, Gaussian signaling for both transmission and cooperative jamming, linear precoding at the transmitter and the cooperative jammer, and linear processing at the legitimate receiver, are sufficient for achieving the s.d.o.f. of the channel. By contrast, when the s.d.o.f. is not an integer, the achievable schemes need to rely on structured signaling at the transmitter and the cooperative jammer, and joint signal space and signal scale alignment. The converse is established by combining an upper bound which allows for full cooperation between the transmitter and the cooperative jammer, with another upper bound which exploits the secrecy and reliability constraints.

Index Terms—MIMO wiretap channel, cooperative jamming, secure degrees of freedom, beamforming, structured signaling, real interference alignment.

I. INTRODUCTION

INFORMATION theoretically secure message transmission in noisy communication channels was first considered in the seminal work by Wyner [3]. Reference [4] subsequently identified the secrecy capacity of a general discrete memoryless wire-tap channel. Reference [5] studied the Gaussian wire-tap channel and its secrecy capacity. More recently, an extensive body of work was devoted to study a variety of network information theoretic models under secrecy constraint(s), see for example [6]–[23]. The secrecy capacity region for most of multi-terminal models remain open despite significant progress on bounds and associated insights. Recent work thus includes efforts that concentrate on characterizing the more tractable high signal-to-noise ratio (SNR) scaling behavior of secrecy capacity region for Gaussian multi-terminal models [21]–[26].

Among the multi-transmitter models studied, a recurrent theme in achievability is enlisting one or more terminals to transmit intentional interference with the specific goal of diminishing the reception capability of the eavesdropper, known as cooperative jamming [27]. For the Gaussian wire-tap channel, adding a cooperative jammer terminal transmitting Gaussian noise can improve the secrecy rate considerably [11], albeit not the scaling of the secrecy capacity with power at high SNR. Recently, reference [23] has shown that, for the Gaussian wire-tap channel, adding a cooperative jammer and utilizing structured codes for message transmission and cooperative jamming, provide an achievable secrecy rate scalable with power, i.e., a positive secure degrees of freedom (s.d.o.f.), an improvement from the zero degrees of freedom of the Gaussian wire-tap channel. More recently, reference [24] has proved that, for this channel, the s.d.o.f. \( \frac{1}{2} \), achievable by codebooks constructed from integer lattices along with real interference alignment, is tight. References [25], [26] have subsequently identified the s.d.o.f. region for multi-terminal Gaussian wire-tap channel models.

While the above development is for single-antenna terminals, multiple antennas have also been utilized to improve secrecy rates and s.d.o.f. for several channel models, see for example [7]–[9], [21], [28]–[33]. The secrecy capacity of the multi-antenna (MIMO) wire-tap channel, identified in [28], scales with power only when the legitimate transmitter has an advantage over the eavesdropper in the number of antennas. It then follows naturally to utilize a cooperative jamming terminal to improve the secrecy rate and scaling for multi-antenna wire-tap channels as well which is the focus of this work.

In this paper, we study the multi-antenna wire-tap channel with a multi-antenna cooperative jammer. We characterize the high SNR scaling of the secrecy capacity, i.e., the s.d.o.f., of the channel with \( N_t \) antennas at the cooperative jammer, \( N_t \) antennas at the transmitter, \( N_e \) antennas at the receiver, \( N_c \) antennas at the eavesdropper, under the assumption of known channel state information at all terminals. The achievability and converse techniques both are methodologically developed for ranges of the parameters, i.e., the number of antennas at each terminal. The upper and lower bounds for all parameter...
values are shown to match one another. Presenting this work in part, [1] and [2] are conference presentations reporting the resulting s.d.o.f. for $N_t = N_e$ only. Note that the s.d.o.f. results in this paper match the achievability results reported in [34], [35], which are special cases for \{$N_t = N_r = 1, N_c = N_e$\}, \{\$N_t = N_r = N_c = 2N, \$\}, \{\$N_t = N_r = N_e = N, N_c = 2N - 1\}, and with real channel gains.

We remark that secure degrees of freedom for single and multiple antenna wire-tap channels have recently been investigated under the assumption of unknown eavesdropper channel state information at the legitimate terminals. The secure degrees of freedom for the single-antenna wire-tap channel with multiple helpers, multiple-access wire-tap channel, and interference wire-tap channel, with unknown and static eavesdropper channel, have been derived in [36]. The strongly secure degrees of freedom of the multiple antenna wire-tap channel with unknown and varying eavesdropper channel is established in [32] by showing the existence of a universal scheme that can counter any eavesdropper state. [32] thus quantifies the reduction in degrees of freedom that results from universal immunity to eavesdropping. This paper, by contrast, addresses the improvement provided by adding a multi-antenna helper in the benchmark case that is the static and known channel state information for the MIMO wiretap channel.

The proposed achievable schemes for different ranges of the values for $N_c$, $N_t$, $N_r$, and $N_e$ all involve linear precoding and linear receiver processing. The common goal to all these schemes is to perfectly align the cooperative jamming signals at all terminals. The tools that enable the signal scale alignment are available in the field of transcendental number theory [38]–[40]. Throughout the paper, we use $j = \sqrt{-1}$ to denote the imaginary unit in a complex number. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, and $Z$ denote the sets of real, complex, rational, and real-valued integer numbers, respectively. $Z_c$ denotes the set of complex integers, i.e., $Z_c \triangleq \{ n + jm : n, m \in Z \}$. The set of integers $\{-Q, \ldots, Q\}$ is denoted by $(−Q, Q)_{Z_c}$. $0_{m \times n}$ denotes an $m \times n$ matrix of zeros, and $I_n$ denotes an $n \times n$ identity matrix. For matrix $A$, $N(A)$ denotes its null space, $\text{det}(A)$ denotes its determinant, and $||A||$ denotes its induced norm. For vector $V$, $||V||$ denotes its Euclidean norm, and $V^k_{i}$ denotes the $i$th to $k$th components in $V$. We use $V^n$ to denote the $n$-letter expansion of the random vector $V$, i.e., $V^n = [V(1) \cdots V(n)]$. The operators $T$, $H$, and $\dagger$ denote the transpose, Hermitian, and pseudo inverse operations. A circularly symmetric Gaussian random vector with zero mean and covariance matrix $K$ is denoted by $\mathcal{CN}(0, K)$.

As the channel model, we consider the MIMO wire-tap channel with an $N_t$-antenna transmitter, $N_r$-antenna receiver, $N_c$-antenna eavesdropper, and an $N_e$-antenna cooperative jammer as depicted in Fig. 1. The received signals at the receiver and eavesdropper, at the $n$th channel use, are given by

$$Y_r(n) = H_t X_t(n) + H_e X_e(n) + Z_r(n) \tag{1}$$

$$Y_e(n) = G_t X_t(n) + G_e X_e(n) + Z_e(n) \tag{2}$$

where $X_t(n)$ and $X_e(n)$ are the transmitted signals from the transmitter and the cooperative jammer at the $n$th channel use. $H_t \in \mathbb{C}^{N_r \times N_t}$, $H_e \in \mathbb{C}^{N_r \times N_e}$ are the channel gain matrices from the transmitter and the cooperative jammer to the receiver, while $G_t \in \mathbb{C}^{N_c \times N_t}$, $G_e \in \mathbb{C}^{N_c \times N_e}$ are the channel gain matrices from the transmitter and the cooperative jammer to the eavesdropper. It is assumed that the channel gains are drawn independently from a complex-valued continuous distribution. All channel gains are assumed to be known at all terminals. $Z_r(n)$ and $Z_e(n)$ are the complex Gaussian noise at the receiver and eavesdropper at the $n$th channel use, where $Z_r(n) \sim \mathcal{CN}(0, I_{N_r})$ and $Z_e(n) \sim \mathcal{CN}(0, I_{N_e})$ for all $n$. $Z_r(n)$ is independent from $Z_e(n)$ and both are independent

The distinction between matrices and random vectors is clear from the context.

II. CHANNEL MODEL AND DEFINITIONS

First, we remark the notation we use throughout the paper: Small letters denote scalars and capital letters denote random variables. Matrices are denoted by bold small letters, while matrices and random vectors are denoted by bold capital letters. Vectors are denoted by bold small letters, while matrices and random vectors are denoted by bold capital letters. Sets are denoted using calligraphic fonts. All logarithms are taken to be base 2. Throughout the paper, we use $j = \sqrt{-1}$ to denote the imaginary unit in a complex number. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, and $Z$ denote the sets of real, complex, rational, and real-valued integer numbers, respectively. $Z_c$ denotes the set of complex integers, i.e., $Z_c \triangleq \{ n + jm : n, m \in Z \}$. The set of integers $\{-Q, \ldots, Q\}$ is denoted by $(−Q, Q)_{Z_c}$. $0_{m \times n}$ denotes an $m \times n$ matrix of zeros, and $I_n$ denotes an $n \times n$ identity matrix. For matrix $A$, $N(A)$ denotes its null space, $\text{det}(A)$ denotes its determinant, and $||A||$ denotes its induced norm. For vector $V$, $||V||$ denotes its Euclidean norm, and $V^k_{i}$ denotes the $i$th to $k$th components in $V$. We use $V^n$ to denote the $n$-letter expansion of the random vector $V$, i.e., $V^n = [V(1) \cdots V(n)]$. The operators $T$, $H$, and $\dagger$ denote the transpose, Hermitian, and pseudo inverse operations. A circularly symmetric Gaussian random vector with zero mean and covariance matrix $K$ is denoted by $\mathcal{CN}(0, K)$.
and identically distributed (i.i.d.) across the time index\(^2 n\). The power constraints on the transmitted signals at the transmitter and the cooperative jammer are \(E(XX^H)\leq P\). The transmitter aims to send a message \(W\) to the receiver, and keep it secret from the external eavesdropper. A stochastic encoder, which maps the message \(W\) to the transmitted signal \(X^n\in X^n_{\epsilon}\), is used at the transmitter. The receiver uses its observation, \(Y^n_{r}\in Y^n_{r}\), to obtain an estimate \(\hat{W}\) of the transmitted message. Secrecy rate \(R_s\) is achievable if for any \(\epsilon > 0\), there is a channel code (2\(nR_s\), \(n\)) satisfying

\[
P_e \triangleq \Pr(\hat{W} \neq W) \leq \epsilon, \tag{3}
\]

\[
\frac{1}{n} H(W|Y^n_{r}) \geq \frac{1}{n} H(W) - \epsilon. \tag{4}
\]

The secrecy capacity of a channel, \(C_s(P)\), is defined as the closure of all its achievable secrecy rates. For a channel with complex-valued coefficients, the maximum secure degrees of freedom (s.d.o.f.) is defined as

\[
D_s \triangleq \lim_{n\to\infty} \frac{C_s(P)}{\log n}. \tag{5}
\]

The cooperative jammer transmits the signal \(X^n_{c}\in X^n_{c}\) in order to reduce the reception capability of the eavesdropper. However, this transmission affects the receiver as well, as interference. The jamming signal, \(X^n_{c}\), does not carry any information. Additionally, there is no shared secret between the transmitter and the cooperative jammer.

### III. Main Result

We first state the s.d.o.f. results for \(N_t = N_r = N\).

**Theorem 1:** The s.d.o.f. of the MIMO wire-tap channel with an \(N_c\)-antenna cooperative jammer, \(N\) antennas at each of the transmitter and receiver, and \(N_e\) antennas at the eavesdropper, is almost surely\(^4\) (a.s.)

\[
D_s = \begin{cases} 
[N + N_e - N_c]^{+}, & \text{if} \ 0 \leq N_e \leq N - \frac{\min\{N, N_c\}}{2} \\
N - \frac{\min\{N, N_c\}}{2}, & \text{if} \ \max\{N, N_c\} < N_e \leq \max\{N, N_c\} \\
N + N_e - N_c, & \text{if} \ \max\{N, N_c\} < N_e \leq N + N_e,
\end{cases} \tag{6}
\]

**Proof:** The proof for Theorem 1 is provided in Sections IV and V. \(\blacksquare\)

Next, in Theorem 2 below, we generalize the result in Theorem 1 to \(N_t \neq N_r\).

**Theorem 2:** The s.d.o.f. of the MIMO wire-tap channel with an \(N_c\)-antenna cooperative jammer, \(N_t\)-antenna transmitter, \(N_r\)-antenna receiver, and \(N_e\)-antenna eavesdropper, is a.s.

\[
D_s = \begin{cases} 
\min\{N_t, [N_c + N_t - N_c]^{+}\}, & \text{if} \ 0 \leq N_c \leq N_1 \\
\min\{N_t, N_r, \frac{N_c + N_t - N_c}{2}\}, & \text{if} \ N_1 < N_c \leq N_2 \\
\min\{N_t, N_r, \frac{N_c + N_t - N_c}{2}\}, & \text{if} \ N_2 < N_c \leq N_3, \\
\min\{N_t, N_r\}, & \text{if} \ N_c > N_3,
\end{cases} \tag{7}
\]

where,

\[
N_1 = \min\{N_c, \left[\frac{N_r}{2} + \frac{N_e - N_t}{2 - N_c} + N_e - N_t \right]^{+}\}, \quad 1_{N_c > N_t} = \begin{cases} 1, & \text{if} \ N_c > N_t \\
0, & \text{if} \ N_c \leq N_t \end{cases}
\]

\[
N_2 = N_r + [N_c - N_t]^{+}, \quad N_3 = \max\{N_2, 2 \min\{N_t, N_r\} + N_e - N_t\}.
\]

\(^4\)The subset of the channel gains for which the result does not hold has a Lebesgue measure zero.
Proof: The proof for Theorem 2 is provided in Section VI.

Remark 1: Theorem 2 provides a complete characterization for the s.d.o.f. of the channel. The s.d.o.f. at $N_c = N_3$ is equal to $\min\{N_t, N_c\}$, which is equal to the d.o.f. of the $(N_t \times N_r)$ point-to-point MIMO Gaussian channel. Thus, increasing the number of antennas at the cooperative jammer, $N_c$, over $N_3$ cannot increase the s.d.o.f. over $\min\{N_t, N_c\}$.

Remark 2: For $N_t \geq N_r + N_c$, the s.d.o.f. of the channel is equal to $N_r$ at $N_c = 0$, i.e., the maximum s.d.o.f. of the channel is achieved without the help of the cooperative jammer.

Remark 3: The converse proof for Theorem 2 involves combining two upper bounds for the s.d.o.f. derived for two different ranges of $N_c$. These two bounds are a straightforward generalization of those derived for the symmetric case in Theorem 1. However, combining them is more tedious since more cases of the number of antennas at the different terminals should be handled carefully. Achievability for Theorem 2 utilizes similar techniques to those used for Theorem 1 as well, where handling more cases is required. For clarity of exposition, we derive the s.d.o.f. for the symmetric case first in order to present the main ideas, and then utilize these ideas and generalize the result to the asymmetric case of Theorem 2.

For illustration purposes, the s.d.o.f. for $N_t = N_r = N$ and $N_c$ varying from 0 to $2N$, is depicted in Fig. 2. The s.d.o.f. curves with $N$ even and odd are shown in Fig. 2a and Fig. 2b, respectively.

We provide the discussion of the results of this work in Section VII.

IV. CONVERSE FOR $N_t = N_r = N$

In Section IV-A, we derive the upper bound for the s.d.o.f. for $0 \leq N_c \leq N$. In Section IV-B, we derive the upper bound for $\max\{N, N_c\} \leq N_c \leq N + N_c$. The two bounds are combined in Section IV-C to provide the desired upper bound in (6).

A. $0 \leq N_c \leq N$

Allow for full cooperation between the transmitter and the cooperative jammer. This cooperation cannot decrease the s.d.o.f. of the channel, and yields a MIMO wire-tap channel with $N + N_c$-antenna transmitter, $N$-antenna receiver, and $N_c$-antenna eavesdropper. It has been shown in [28] that, at high SNR, i.e., $P \to \infty$, the secrecy capacity of this channel, $C_s(P)$, takes the asymptotic form

$$C_s(P) = \log \det \left( I_N + \frac{P}{p} \mathbf{H} \mathbf{G}^\dagger \mathbf{H}^H \right) + o(\log P),$$

(8)

where $\lim_{P \to \infty} \frac{o(\log P)}{\log P} = 0$, $\mathbf{H} \in \mathbb{C}^{N \times (N+N_c)}$ and $\mathbf{G} \in \mathbb{C}^{N_c \times (N+N_c)}$ are the channel gains from the combined transmitter to the receiver and eavesdropper, and $\mathbf{G}^\dagger$ is the projection matrix onto the null space of $\mathbf{G}$, $\mathcal{N}(\mathbf{G})$. $p$ is the number of antennas at the different terminals.

Thus, the s.d.o.f. of the original channel, for $0 \leq N_c \leq N$, is upper bounded as

$$D_s \leq \lim_{P \to \infty} \frac{C_s(P)}{\log P} = \lim_{P \to \infty} \frac{p \log P + o(\log P)}{\log P}$$

(14)

$$= \left[ N + N_c - N_e \right]^+.$$  

(15)
The upper bound we derive here is inspired by the converse of the single antenna Gaussian wire-tap channel with a single antenna cooperative jammer derived in [24], though as we will see shortly, the vector channel extension resulting from multiple antennas does require care. Let \( \phi_i, \) for \( i = 1, 2, \cdots, 10, \) denote constants which do not depend on the power \( P. \)

The secrecy rate \( R_s \) can be upper bounded as follows

\[
R_s = H(W) - H(W|Y^n) \leq n \epsilon \tag{16}
\]

where \( H(W) - H(W|Y^n) \leq n \epsilon \) by Fano’s inequality. Let \( H(W|Y^n) \geq H(W|Y^n, X^n) \) by the fact that conditioning does not increase entropy. (22) follows since \( Z^n \) is independent from \( \{W, Y^n, X^n, \}\), and \( \phi_i = \epsilon \). Let \( X_1 = X_t + Z_t \) and \( X_c = X_c + Z_c \), where \( Z_t \sim \mathcal{CN}(0, K_t) \) and \( Z_c \sim \mathcal{CN}(0, K_c). \)

The covariance matrices, \( K_t \) and \( K_c \), are chosen as \( K_t = \rho^2 I_N \) and \( K_c = \rho^2 I_{N_c} \), where \( 0 < \rho \leq 1. \)

Note that \( X_t \) and \( X_c \) are noisy versions of the transmitted signals \( X_t \) and \( X_c \), respectively. \( Z_t \) is independent from \( Z_c \), and both are independent from \( \{X_t, X_c, Z_t, Z_c\} \). \( Z^n_t \) and \( Z^n_c \) are i.i.d. sequences of the random vectors \( Z_t \) and \( Z_c \). Let \( Z_1 = -H(Z_t - H(Z_t + Z_c), and \( Z_2 = -G(Z_t - G(Z_t + Z_c). \)

Note that \( Z_1 \sim \mathcal{CN}(0, Z_1) \) and \( Z_2 \sim \mathcal{CN}(0, Z_2). \)

The choice of \( K_t \) and \( K_c \) above guarantees the finiteness of \( h(Z_1), h(Z_2), \) and \( h(Z_2) \) as shown in Appendix A. Starting from (22), we have

\[
R_s \leq h(Y^n_t, Y^n_c) - h(Y^n_t) + n \phi_2 \tag{23}
\]

\[
h(Y^n_t, Y^n_c, X^n_t, X^n_c) - h(Y^n_t, X^n_t) - h(Y^n_c, X^n_t) + n \phi_2 \tag{24}
\]

\[
h(Y^n_t, Y^n_c, X^n_t, X^n_c) - h(Y^n_t) + n \phi_2 \tag{25}
\]

\[
h(Y^n_t, Y^n_c, X^n_t, X^n_c) - h(Y^n_t, Y^n_c) + n \phi_2 \tag{26}
\]

\[
h(Y^n_t, Y^n_c, X^n_t, X^n_c) - h(Y^n_t, Y^n_c) + n \phi_2 \tag{27}
\]

\[
h(Y^n_t, Y^n_c, X^n_t, X^n_c) - h(Y^n_t, Y^n_c) + n \phi_2 \tag{28}
\]

where (26) follows since \( Z^n_t \) and \( Z^n_c \) are independent from \( \{X^n_t, Y^n_t, X^n_c, Y^n_c\}, \phi_2 = \phi_1 - h(Z_t), \phi_3 = \phi_2 - h(Z_c), \) and \( \phi_4 = \phi_3 + h(Z_1) + h(Z_2). \)

We have utilized the noisy versions \( X_t = X_t + Z_t \) and \( X_c = X_c + Z_c \) instead of \( X_t, X_c \) so that (24)-(29) hold whether \( X_t, X_c \) are continuous or discrete random vectors. This requires continuing the analysis with stochastically equivalent versions of \( Y_t, Y_c \) in which they are expressed as functions of \( X_t \) and/or \( X_c \). To do so, we divide the Gaussian noise \( Z_t, Z_c \) into sums of other independent Gaussian noise variables. The infinite divisibility of the Gaussian distribution ensures such division of \( Z_t, Z_c \). We now consider the following two cases.

**Case 1:** \( N_c \leq N \)

We first lower bound \( h(Y^n_c) \) in (29) as follows. Using the infinite divisibility of Gaussian distribution, we can express a stochastically equivalent form of \( Z^n_c \), denoted by \( Z^n_c' \), as

\[
Z^n_c' = G_t \tilde{Z}_t + \tilde{Z}_c. \tag{30}
\]

where \( \{\tilde{Z}_t, \tilde{Z}_c\} \) is independent from \( \{Z_t, Z_c, X_t, X_c, Z_t, Z_c\} \). \( \{\tilde{Z}_t, \tilde{Z}_c\} \) is an i.i.d. sequence of the random vectors \( Z_t, Z_c \). Using (30), a stochastically equivalent form of \( Y^n_c \) is

\[
Y^n_c = G_t X^n_t + G_c X^n_c + Z^n_c. \tag{31}
\]

Let \( X_t = [X_{t,1}, \cdots, X_{t,N}^T, \tilde{Z}_t = [\tilde{Z}_t, \cdots, \tilde{Z}_t] \), \( Y_t = [X_{t,1}, \cdots, X_{t,N}^T, \tilde{Z}_t = [\tilde{X}_{t,1}, \cdots, X_{t,N}^T, \tilde{Z}_t = \tilde{X}_{t,1}, \cdots, \tilde{X}_{t,N}^T, X_{t,k} = X_{t,k} + \tilde{Z}_{t,k} \}

\]

Let \( G_{t,k} = [G_{t,k}^t, G_{t,k}^c] \), where \( G_{t,k}^c \in \mathbb{C}_{N_c \times N_c} \), and \( G_{t,k}^t \in \mathbb{C}_{N_c \times (N-N_c)} \), and \( G_{t,k} = G_{t,k}^t + G_{t,k}^c \).

where the inequality in (33) follows since \( \{G_t \tilde{X}_t^t \} \) and \( \{G_c \tilde{X}_c^c \} \) are independent, as for two independent random vectors \( X_t \) and \( Y_t \), we have \( h(X_t + Y_t) \geq h(X_t) \).

Substituting (35) in (29) results in

\[
rR_s \leq h(X^n_t, X^n_c) + h(X^n_t) - h(X^n_t, Y^n_c) - n \log | \det (G_{t,k}) | + n \phi_5 \tag{36}
\]

\[
= h(X^n_t) + h(X^n_c) + h(Z^n_t) + h(Z^n_c) - h(Y^n_c) + n \phi_5 \tag{37}
\]

where \( \phi_5 = \phi_4 - \log | \det (G_{t,k}) |). \)

We now exploit the reliability constraint in (3) to derive another upper bound for \( R_s \), which we combine with the bound in (37) in order to obtain the desired bound for the s.d.o.f. when \( N_c \leq N \) and \( N < N_c \leq N + N_c \). The reliability constraint in (3) can be achieved only if \( [41] \)

\[
R_s \leq I(X^n_t; Y^n_c) = h(Y^n_c) - h(Y^n_c|X^n_t) \tag{38}
\]

\[
= h(Y^n_c) - h(H, X^n_c + Z^n_c). \tag{39}
\]

where \( \phi_5 = \phi_3 - \log | \det (G_{t,k}) | \) is a valid covariance matrix.

\[\text{Note that when } N_c = N, \text{ the vector } X^n_t \text{ and the matrix } G_{t,k} \text{ vanish and the analysis below holds in the same manner, by discarding } X^n_t \text{ and } G_{t,k}. \]
Similar to (30), a stochastically equivalent form of $Z_c$ is given by
\[ Z'_c = H_c \tilde{Z}_c + \tilde{Z}_e, \] (40)
where $\tilde{Z}_e \sim \mathcal{CN}(0, I_N - H_c K_c H_c^H)$ is independent from \{\tilde{Z}_t, \tilde{Z}_e, X_t, X_c, Z_c\}. $Z'^c$ is an i.i.d. sequence of the random vectors $Z_c$. Let $\tilde{X}_c = [X_{c,1}, \ldots, X_c, N] \in T$, $\hat{X}_c = [X_{c,1}, \ldots, X_c, N] \in T$, and $X_{c, k} = X_{c, k} + \tilde{Z}_{c, k}, k = 1, \ldots, N$. In addition, let $H_c = [H_{c1}, H_{c2}]$, where $H_{c1} \in \mathbb{C}^{N \times N}$ and $H_{c2} \in \mathbb{C}^{N \times (N - N)}$. Using (40), we have
\[ h(H_c X_c^n + Z'^c) = h(H_c X_c^n + \tilde{Z}_e^n) = h(H_c X_c^n + \tilde{Z}_e^n), \]
\[ \geq h(H_c X_c^n) = h(H_c X_c^n + \tilde{Z}_e^n) \]
\[ \geq h(H_c X_c^n | X_c^n), \]
\[ = h(X_c^n | X_c^n) + n \log |\det(H_c)|. \]

Substituting (44) in (39) yields
\[ n R_s \leq h(Y_e^n) - h(X_c^n) - n \log |\det(H_c)|. \] (45)
Let $Y_e = [Y_e, 1, \ldots, Y_e, N] \in T$. Summing (37) and (45) results in
\[ n R_s \leq \frac{1}{2} \left\{ h(Y_e^n) + h(X_c^n) \right\} + n \phi_6 \]
\[ \leq \frac{1}{2} \left\{ \sum_{i=1}^N h(Y_{e, k}(i)) + \sum_{i=1}^N h(X_{e, k}(i)) \right\} + n \phi_6, \]
where $\phi_6 = \frac{1}{2} (\phi_5 - \log |\det(H_c)|)$. In Appendix B, we show, for $i = 1, \ldots, n, k = 1, \ldots, N$, and $m = 1, \ldots, N$, that
\[ h(Y_{e, k}(i)) \leq \log 2^n e + \log(1 + h^2 P), \]
\[ h(X_{e, m}(i)) \leq \log 2^n e + \log(\rho^2 + P), \]
where $h^2 = \max_k (\|h_{e, k, k}\|^2 + \|h_{e, k, k}\|^2)$; $h_{e, k, k}$ and $h_{e, k, k}$ denote the transpose of the $k$th row vectors of $H_c$ and $H_c$, respectively. Using (47), (48), and (49), we have
\[ R_s \leq \frac{N}{2} \log(1 + h^2 P) + \frac{N - N_e}{2} \log(\rho^2 + P) + \phi_7, \]
where $\phi_7 = \phi_6 + \frac{N + N_e - N}{2} \log 2^n e$. Using (5), we get
\[ D_s \leq \lim_{P \to \infty} \frac{N}{2} \log(1 + h^2 P) + \frac{N - N_e}{2} \log(\rho^2 + P) + \phi_7 \]
\[ = \frac{N + N_e - N}{2}. \]
Thus, the s.d.o.f. for $N_e = N$ and $N < N_e \leq N + N_e$ is upper bounded by $\frac{N + N_e - N}{2}$.

Case 2: $N_e > N$
Another stochastically equivalent form of $Z_c$ is
\[ Z'_c = G_c \tilde{Z}_c + G_c \tilde{Z}_e + Z'^c. \] (53)
where $\tilde{Z}_c \sim \mathcal{CN}(0, I_N - G_c K_c G_c^H)$ is independent from \{\tilde{Z}_t, \tilde{Z}_e, X_t, X_c, Z_c\}. $Z'^c$ is an i.i.d. sequence of the random vectors $Z_c$. Using (53), another stochastically equivalent form of $Y_e^n$ is given by
\[ Y_e^n = G_c \tilde{X}_t + G_c \tilde{X}_c^n + \tilde{Z}_e^n. \]

Let us rewrite $\tilde{X}_c$ and $H_c$ as follows. $\tilde{X}_c = [X_{c,1}, \ldots, X_c, N] \in T$, $\tilde{X}_c = [X_{c,1}, \ldots, X_c, N] \in T$, $X_{c, k} = X_{c, k} + \tilde{Z}_{c, k}$, $k = 1, \ldots, N$. In addition, let $H_c = [H_{c1}, H_{c2}]$, where $H_{c1} \in \mathbb{C}^{N \times (N - N)}$, $H_{c2} = [H_{c2}^1, H_{c2}^2]$, $H_{c2}^1 \in \mathbb{C}^{N \times (N - N)}$, and $H_{c2}^2 \in \mathbb{C}^{N \times (N - N)}$. Let $G_c = [G_{c1}, G_{c2}]$, where $G_{c1} \in \mathbb{C}^{N \times (N - N - N)}$ and $G_{c2} \in \mathbb{C}^{N \times (N + N - N - N)}$. Using (54), we have
\[ h(Y_e^n) = h(Y_e'^n) = h(G_c G_{c1}) \left[ \tilde{X}_c^n | \tilde{X}_c^n \right] + G_{c2} \tilde{X}_c^n + \tilde{Z}_e^n \]
\[ \geq h(\tilde{X}_c^n | \tilde{X}_c^n) + n \log |\det(G_c G_{c1})| \]
\[ = h(\tilde{X}_c^n) + h(\tilde{X}_c^n | \tilde{X}_c^n) + n \log |\det(G_c G_{c1})| \]
where (57) follows since $\tilde{X}_c^n$ and $\tilde{X}_c^n$ are independent. Substituting (57) in (29) gives
\[ n R_s \leq h(\tilde{X}_c^n) + n \phi_8, \]
where $\phi_8 = \phi_4 - \log |\det(G_c G_{c1})|$. In order to obtain another upper bound for $R_s$, which we combine with (58) to obtain the desired bound for $N_e > N$ and $N_e < N_e \leq N + N_e$, we proceed as follows. Consider a modified channel where the first $N_e - N$ antennas at the cooperative jammer are removed, i.e., the cooperative jammer uses only the last $N + N_e - N$ out of its $N_e$ antennas. The transmitted signals in the modified channel are $X_t^n$ and $X_{c2}^n$, and hence, the legitimate receiver receives
\[ \tilde{Y}_e^n = H_t X_t^n + H'_{c2} X_{c2}^n + Z_{e2}^n. \]
Let $R$ and $\tilde{R}$ denote reliable communication rates, i.e., the achievable rates without the secrecy constraint, for the original and the modified channels, respectively. Since the cooperative jamming signal is additive interference for the legitimate receiver, the reliable communication rate of the modified channel, $\tilde{R}$, is an upper bound for that of the original channel, $R$. Since $R_s$ satisfies the reliability and secrecy constraints in (3) and (4), we have that
\[ n R_s \leq n R \leq n \tilde{R} \]
\[ \leq I(\tilde{X}_t^n; \tilde{Y}_e^n) = h(\tilde{Y}_e^n) - h(H'_{c2} X_{c2}^n + Z_{e2}^n). \] (60)
\[ \tilde{Z}_{e2} = [\tilde{Z}_{e,1} N + \ldots, \tilde{Z}_{e,N_e}] \sim \mathcal{CN}(0, K_{e2}^H), \]
where $K_{e2} = \rho^2 I_{N_e + N_e}$. Another stochastically equivalent form

\[ \tilde{Z}_e \sim \mathcal{CN}(0, I_N - G_c K_c G_c^H). \]
The choice of $K_c$ and $K_{e2}$ guarantees that $I_N - G_c K_c G_c^H$ is a valid covariance matrix.
of $Z_c$ is $Z_c'' = H_{d_c}^c Z_{c_2} + Z_{t_c}'$, where $\bar{Z}_{t_c}' \sim \mathcal{CN}(0, I_N - H_{d_c}^c K_c H_{d_c}^c)$ is independent from $\{\bar{Z}_t, \bar{Z}_c, X_t, X_c, Z_c, Z_e\}$, and $Z_e''$ is an i.i.d. sequence of $\bar{Z}_e'$. Thus, using (60), we have

$$n R_s \leq h(\tilde{Y}_n) - h(H_{d_2}^c \tilde{X}_{c_2} + Z_{t_c}'' \bar{Z}_e')$$

$$\leq h(\tilde{Y}_n) - h(H_{d_2}^c \tilde{X}_{t_c}'' \bar{Z}_e')$$

$$\leq h(\tilde{Y}_n) - h(\bar{X}_{c_2}'' \bar{X}_{c_2}'' - n \log |\text{det}(H_{c_2}^c)|).$$

Let $\bar{Y}_t = [\bar{Y}_{t,1} \cdots \bar{Y}_{t,N}]^T$. Summing (58) and (63) yields

$$n R_s \leq \frac{1}{2} \left\{ h(\bar{Y}_n) + h(\bar{X}_{c_2}'' \bar{X}_{c_2}'') \right\} + n \phi_9$$

$$\leq \frac{1}{2} \sum_{i=1}^{N} \left\{ \sum_{k=1}^{N} h(\bar{Y}_{t,k}(i)) + \sum_{k=N_e+1}^{N} h(\bar{X}_{c,k}(i)) \right\} + n \phi_9,$$

where $\phi_9 = \frac{1}{2} (\phi_8 - \log |\text{det}(H_{c'}^e)|)$, In Appendix B, we also show that

$$h(\bar{Y}_{t,k}(i)) \leq 2 \pi e + \log(1 + \tilde{h}^2 P),$$

where $\tilde{h}^2 = \max \left( ||h_{t,k}^r||^2 + ||h_{c,k}^r||^2 \right)$; $h_{c,k}^r$ denotes the transpose of the $k$th row vector of $H_{c_2}^c$.

Similar to case 1, using (65), (66), and (49), the secrecy rate is bounded as

$$R_s \leq \frac{N}{2} \log(1 + \tilde{h}^2 P) + \frac{N_e - N_e}{2} \log(\rho^2 + P) + n \phi_{10},$$

where $\phi_{10} = \phi_9 + \frac{N + N_e - N_e}{2} \log 2 \pi e$. Thus, the s.d.o.f. for $N_e > N$ and $N_e < N_e \leq N + N_e$, is upper bounded as

$$D_s \leq \frac{N + N_e - N_e}{2}.$$

### C. Obtaining the Upper Bound

For $N_e \leq N$, the upper bound for the s.d.o.f. derived in Section IV-A is equal to $N + N_e - N_e$ for all $0 \leq N_e \leq N_e$. In addition, the upper bound derived in Section IV-B, at $N_e = N$, is equal to $N - \frac{N_e}{2}$, c.f. equations (15) and (52). As the upper bound is greater than the latter for all $\frac{N}{2} < N_e \leq N$, the s.d.o.f. is upper bounded by $N - \frac{N}{2}$ for all $\frac{N}{2} < N_e \leq N$. Combining these statements, we have the following upper bound for the s.d.o.f. for $N_e \leq N$:

$$D_s \leq \begin{cases} 
N + N_e - N_e, & \text{if } 0 \leq N_e \leq \frac{N}{2} \\
N - \frac{N}{2}, & \text{if } \frac{N}{2} < N_e \leq N \\
N_e, & \text{if } N_e > N + N_e.
\end{cases}$$

Similarly, when $N_e > N$ and for all $N_e - \frac{N}{2} < N_e \leq N_e$, the upper bound derivation for $0 \leq N_e \leq N_e$ in Section IV-A is greater than the upper bound derived in Section IV-B at $N_e = N$. Thus, the s.d.o.f. for $N_e - \frac{N}{2} < N_e \leq N_e$ is upper bounded by $N - \frac{N}{2}$. In addition, the upper bound in (15) is equal to

The choice of $K_c$ guarantees that $I_N - H_{d_2}^c K_c H_{d_2}^c$ is a valid covariance matrix.

0018-9448 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Remark 4: Note that integer-valued s.d.o.f. can also be achieved using structured signals. However, Gaussian signaling often outperforms structured signaling for finite SNR; see for example [42, Fig. 2]. Although our focus in this paper is on characterizing the s.d.o.f., i.e., secrecy rate scaling at high SNR, for the channel, we use Gaussian signaling whenever possible for the achievability for this reason.

In order to extend real interference alignment to complex channels, we need to utilize different results than those used for real channels. For real channels, to analyze the decoder performance, reference [43] proposed utilizing the convergence part of Khintchine-Groshev theorem in the field of Diophantine approximation [44], which deals with the approximation of real numbers with rational numbers. For complex channels, approximations [44], which deals with the approximation of part of Khintchine-Groshev theorem in the field of Diophantine independence over rational numbers of the channel gains, which increases the s.d.o.f. of the achievable scheme for this reason, when $N = 4$, $N_e = 2$, and $N_c = 1$, is depicted in Fig. 3.

Since $N_c \leq \frac{N}{2}$, the total number of superposed received streams at the receiver, $2N_e + N - N_c$, is less than or equal to the number of its available spatial dimensions, $N$. Thus, the receiver can decode all the information and cooperative jamming streams at high SNR. Using (1), (2), and (72), the received signals at the receiver and the eavesdropper are

$$Y_r = [H_t P_t \ H_c] [U_t] [V_{c}] + Z_r,$$  

$$Y_e = [G_t G_c \ 0_{N_e \times (N-N_c)}] [U_{t}^{l}] + G_c V_c + Z_e$$

$$= G_c (U_{t}^{l} + V_c) + Z_e.$$  

We lower bound the secrecy rate in (71) as follows. First, in order to compute $I(X_t;Y_e)$, we show that the matrix $[H_t P_t \ H_c] \in \mathbb{C}^{N \times (d+1)}$ in (74) is full column-rank a.s.

The columns of $P_{t,a} = G_t^H G_c$ are linearly independent a.s. due to the randomly generated channel gains, and the $N - N_e$ columns of $P_{t,a}$ are linearly independent as well, since they span an $N - N_e$-dimensional subspace. In addition, each of the columns of $P_{t,a}$ is linearly independent from the columns of $P_{t,a}$ a.s. since $G_t P_{t,a} = G_c$, and hence $G_t P_{t,i} \neq 0$ for all $i = 1, 2, \ldots, l$. Thus $P_c = [P_{t,a} \ P_{t,n}]$ is full column rank a.s. The matrix $[H_t P_t \ H_c]$ can be written as

$$[H_t P_t \ H_c] = [H_t \ H_c] \begin{bmatrix} P_t \ 0_{N \times d} \ I_l \end{bmatrix}.$$  

(77)

The matrix $[H_t \ H_c]$ has all of its entries independently and randomly drawn according to a continuous distribution, while the second matrix on the right hand side (RHS) of (77) is full column rank a.s. By applying Lemma 1 to (77), we have that the matrix $[H_t P_t \ H_c]$ is full column rank a.s. Thus, using (74), we obtain the lower bound

$$I(X_t;Y_r) \geq d \log P + o(\log P).$$  

(78)

Next, using (76), we upper bound $I(X_t;Y_e)$ as follows:

$$I(X_t;Y_e) = h(Y_e) - h(Y_e|X_t)$$

$$= h(G_c (U_{t}^{l} + V_c) + Z_e) - h(G_c V_c + Z_e)$$

$$= \log \frac{\det(I_{N_e} + 2P G_c G_c^H)}{\det(I_{N_e} + P G_c G_c^H)}$$

$$= \log \frac{\det(I_{l} + 2P G_c G_c^H)}{\det(I_{l} + P G_c G_c^H)}$$

$$= \log \frac{2\det(I_{l} + P G_c G_c^H)}{\det(I_{l} + P G_c G_c^H)}$$

$$\leq l.$$  

(84)

Substituting (78) and (84) in (71), we have

$$R_s \geq d \log P + o(\log P) - l$$  

(85)
and hence, using (5), we conclude that the achievable s.d.o.f. is
\( \mathcal{D}_a \geq N + N_c - N_e \).

**B. Case 2: \( N_c \leq N, \frac{N_t}{2} < N_c \leq N, \text{ and } N_c \text{ is even}**

Unlike case 1, the s.d.o.f. for this case does not increase by increasing \( N_c \). For all \( N_c \) in this case, the transmitter sends the same number of information streams, while the cooperative jammer utilizes a linear precoder which allows for discarding any unnecessary antennas. The s.d.o.f. here is integer valued, and we use Gaussian signaling for transmission and cooperative jamming.

In particular, for \( N_c \) is even, \( N_c = \frac{N_t}{2} \), and \( N_c \leq N \), the achievable s.d.o.f., using the scheme in Section V-A, is equal to \( N - \frac{N_t}{2} \). However, from (69), we observe that the s.d.o.f. is upper bounded by \( N - \frac{N_t}{2} \) for all \( \frac{N_t}{2} < N_e \leq N \). Thus, when \( N_c \leq N \) and \( N_c \) is even, the scheme for \( N_c = \frac{N_t}{2} \) in Section V-A can be used to achieve the s.d.o.f. for all \( \frac{N_t}{2} < N_c \leq N \) by discarding the remaining \( N_c - \frac{N_t}{2} \) antennas. That is, the cooperative jammer uses the precoder

\[
P_c = \begin{bmatrix} I_l \\ 0_{(N_c-l)\times l} \end{bmatrix},
\]

with \( l = \frac{N_t}{2} \), to utilize only \( \frac{N_t}{2} \) out of its \( N_c \) antennas, and the transmitter utilizes

\[
P_t = [P_{t,a} \ P_{t,n}],
\]

\( P_{t,a} = G_t^\dagger G_c P_e \in \mathbb{C}^{N \times l} \), \( P_{t,n} \in \mathbb{C}^{N \times (N-N_c)} \) is defined as in (73), in order to send \( d = N - \frac{N_t}{2} \) Gaussian information streams. Following the same analysis as in the previous case, the achievable s.d.o.f. is \( N - \frac{N_t}{2} \) for all \( \frac{N_t}{2} < N_c \leq N \), where \( N_c \) is even and \( N_c \leq N \).

**C. Case 3: \( N_c \leq N, \frac{N_t}{2} < N_c \leq N, \text{ and } N_c \text{ is odd}**

The s.d.o.f. for this case is equal to \( N - \frac{N_t}{2} \), which is not an integer. As Gaussian signaling cannot achieve fractional s.d.o.f. for the channel, we utilize structured signaling both for transmission and cooperative jamming for this case. In particular, we propose utilizing joint signal space alignment and the complex field equivalent of real interference alignment [37], [38].

The decoding scheme at the receiver is as follows. The receiver projects its received signal over a direction that is orthogonal to all but one information and one cooperative jamming streams. Then, the receiver decodes these two streams from the projection using complex field analogy of real interference alignment. Finally, the receiver removes the decoded information and cooperative jamming streams from its received signal, leaving \( N - 1 \) spatial dimensions for the other \( N - \frac{N_t+1}{2} \) information and \( \frac{N_t+1}{2} \) cooperative jamming streams.

Before continuing with the details for the achievability scheme for this case, we provide the following example, which illustrates the ideas utilized for this case.

**Example 1:** Consider a multi-antenna wire-tap channel with 4-antenna transmitter, 4-antenna receiver, 3-antenna eavesdropper, and 2-antenna cooperative jammer as shown in Fig. 4.

The transmitter sends 3 structured information streams, \( U_1, U_2, U_3 \), and the cooperative jammer sends 2 structured jamming streams, \( V_1, V_2 \). The streams \( U_1, V_1 \) are integer valued, while the streams \( U_2, U_3, V_2 \) are complex integers. That is, \( U_2 = U_{2,Re} + jU_{2,Im} \), \( U_3 = U_{3,Re} + jU_{3,Im} \), and \( V_2 = V_{2,Re} + jV_{2,Im} \). where \( \{U_{1},U_{2,Re},U_{2,Im},U_{3,Re},U_{3,Im},V_{1},V_{2,Re},V_{2,Im}\} \) are i.i.d. random variables uniform over a set of integer that scales with the transmit power as it will be explained later in (89). The transmitter chooses its precoder as in (88) so that \( U_3 \) is sent over \( \mathcal{N}(G_t) \), and hence \( U_3 \) is invisible to the eavesdropper, and that \( U_1, V_1 \) and \( U_2, V_2 \) are perfectly aligned at the eavesdropper. The cooperative jammer chooses its precoder as in (87) so that it utilizes only 2 out of its 3 antennas to send \( V_1, V_2 \). The legitimate receiver projects its received signal over a single dimension that is orthogonal to \( \{U_2, U_3, V_2\} \), and hence, only \( U_1 \) and \( V_1 \) remain in this dimension. The received signal after projection is of the form \( f_1 U_1 + f_2 V_1 + Z \), where \( f_1, f_2 \) are the coefficients resulting from multiplying the channel gains with the projection matrix, and \( Z \) is the projection of the Gaussian noise over

---

**Fig. 3:** An example for the achievability scheme for Case 1, when \( N = 4, N_c = 2, \text{ and } N_e = 1 \).
the single dimension. The receiver utilizes a hard decision decoder which maps \( f_1 U_1 + f_2 V_1 + Z \) to the nearest point in the constellation of \( f_1 U_1 + f_2 V_1 \). It has been shown in [43] that \( U_1, V_1 \) can be uniquely decoded from \( f_1 U_1 + f_2 V_1 \). Thus, the receiver decodes \( U_1, V_1 \), subtracts them from its original received signal, and then utilizes the remaining 3 dimensions in its signal space to decode \( U_2, U_3, V_2 \). Thus, the receiver utilizes 2.5 dimensions to decode the information streams, i.e., 2.5 useful dimensions, where each of \( U_2 \) and \( U_3 \) is decoded from a separate dimension while both \( U_1 \) and \( V_1 \) are decoded from a single dimension (each occupies half of that dimension), leading to 2.5 achievable s.d.o.f. for the channel.

Now, we continue with the detailed explanation for the achievability scheme for this case. The transmitted signals are given by (72), with \( d = N - N_0 + 1, l = \frac{N_2 + 1}{2} \), \( P_e, P_t \) are defined as in (87) and (88), and \( U_i = U_i,Re + jU_i,Im \), \( V_k = V_k,Re + jV_k,Im \), \( i = 2, 3 \), and \( k = 2, 3, \cdots, l \). The random variables \( U_1, V_1 \), \( \{U_i,Re\}_{i=2}^l \), \( \{U_i,Im\}_{i=2}^l \), \( \{V_i,Re\}_{i=2}^l \), and \( \{V_i,Im\}_{i=2}^l \) are i.i.d. uniform over the set \( \{a(-Q, Q)z\} \).

The values for \( a \) and the integer \( Q \) are chosen as
\[
Q = \left\lfloor \frac{1}{2} \frac{P}{\nu} \right\rfloor = \frac{P}{\nu} \bmod 2 - \nu
\]
\[a = \gamma P \frac{\nu}{\nu^2 + \nu},
\]
in order to satisfy the power constraints, where \( \epsilon \) is an arbitrarily small positive number, and \( \nu, \gamma \) are constants that do not depend on the power \( P \). Justification for the choice of \( a \) and \( Q \) is provided in Appendix D.

The received signal at the eavesdropper is
\[
Y_e = \tilde{G}_e(U_{t,1} + V_e) + Z_e,
\]
where \( \tilde{G}_e = G_eP_e \). We upper bound the second term in (71), \( I(X_t; Y_e) \), as follows:
\[
I(X_t; Y_e; Z_e) \leq I(X_t; Y_e) + I(Z_e; X_t | Y_e)
\]
\[= H(Y_e | Z_e) - H(Y_e | Z_e) + H(X_t | Z_e) - H(X_t | Z_e) = H \left( \tilde{G}_e(U_{t,1} + V_e) \right) - H \left( \tilde{G}_e V_e \right)
\]
\[= H(U_{t,1} + V_e) - H(V_e) \leq \left( \frac{1}{2^{2l-1}} \log(4Q + 1) \right) \leq 2l - 1,
\]
where (93) follows since \( X_t \) and \( Z_e \) are independent, and (98) follows since the entropy of a uniform random variable over the set \( \{a(-2Q, 2Q)z\} \) upper bounds the entropy of each of \( U_1 + V_1 \), \( U_2,Re + V_2,Re + V_2,Im + V_2,Im \), \( \cdots, U_{l,Im} + V_{l,Im} \). Equation (96) follows since the mappings \( U_{t,1} + V_e \mapsto \tilde{G}_e(U_{t,1} + V_e) \) and \( V_e \mapsto \tilde{G}_e V_e \) are injective. The reason for this is that the entries of \( \tilde{G}_e \) are rationally independent, as illustrated in Definition 1 below, and that \( (U_{t,1} + V_e) \) and \( V_e \) belong to \( \mathbb{Z}_N^2 \).

Definition 1: A set of complex numbers \( \{c_1, c_2, \cdots, c_L\} \) are rationally independent, i.e., linearly independent over \( \mathbb{Q} \), if there is no set of rational numbers \( \{r_i\} \), \( r_i \neq 0 \) for all \( i = 1, 2, \cdots, L \), such that \( \sum_{i=1}^L r_i c_i = 0 \).

Next, we derive a lower bound for \( I(X_t; Y_e) \). The received signal at the legitimate receiver is given by
\[
Y_r = A U_t + H'_c V_c + Z_r,
\]
where \( A = H'_c P_t = [a_1 \ \alpha_2 \cdots \ a_d] \) and \( H'_c = H_c P_c = [h_{c,1} \ h_{c,2} \cdots h_{c,l}] \). The receiver chooses \( b \in \mathbb{C}^N \) such that \( b \perp \text{span} \{a_2, \cdots, a_d, h_{c,2}, \cdots, h_{c,l}\} \) and obtains
\[
\tilde{Y}_r = D Y_r
\]
where
\[
D \triangleq \begin{bmatrix} 0_{(N-1) \times 1} & I_{N-1} \end{bmatrix}.
\]
Note that \( (d-1) - (l-1) = N - \frac{N_0 - 1}{2} - \frac{N_2 + 1}{2} = N - 1 \), and hence the dimension of \( \text{span} \{a_2, \cdots, a_d, h_{c,2}, \cdots, h_{c,l}\} \) is at most \( N - 1 \). This shows the existence of a vector \( b \in \mathbb{C}^N \) such that \( b \perp \text{span} \{a_2, \cdots, a_d, h_{c,2}, \cdots, h_{c,l}\} \). Thus, we have
\[
\tilde{Y}_r = \begin{bmatrix} \tilde{Y}_{r,1} \ \\ \tilde{Y}_{r,2} \end{bmatrix} = \begin{bmatrix} b^H a_1 \ 0_{1 \times (d-1)} \end{bmatrix} U_{t,1} \begin{bmatrix} A \end{bmatrix} + \begin{bmatrix} b^H h_{c,1} \ 0_{1 \times (l-1)} \end{bmatrix} V_1 \begin{bmatrix} H_c \end{bmatrix} + b^H Z_c \begin{bmatrix} 1 \ \\ Z_r^2 \end{bmatrix},
\]
where \( \tilde{A} = [a_1 \ a_2 \cdots a_d] \in \mathbb{C}^{(N-1) \times d} \), \( \hat{a}_i = a_i^H N_1 \) for all \( i = 1, 2, \cdots, d \). Similarly, \( \tilde{H}_{c} = [h_{c,1} \ h_{c,2} \cdots h_{c,l}] \in \mathbb{C}^{(N-1) \times l} \), where \( \hat{h}_{c,i} = h_{c,i}^H N_2 \) for all \( i = 1, 2, \cdots, l \).

Next, the receiver uses \( \tilde{Y}_{r,1} \) to decode the information stream \( U_1 \) and the cooperative jamming stream \( V_1 \) as follows. Let \( Z' = b^H Z_c \sim \mathcal{CN}(0, |b|^2) \), \( f_1 = b^H a_1 \), and \( f_2 = b^H h_{c,1} \).

Thus, \( \tilde{Y}_{r,1} \) is given by
\[
\tilde{Y}_{r,1} = f_1 U_1 + f_2 V_1 + Z' \tag{105}
\]
Once again, with randomly generated channel gains, \( f_1 = b^H a_1 \) and \( f_2 = b^H h_{c,1} \) are rationally independent a.s. Thus, the mapping \( (U_1, V_1) \mapsto f_1 U_1 + f_2 V_1 \) is invertible [43]. The receiver employs a hard decision decoder which maps \( Y_{r,1} \in \{r_{y,1}\} \) to the nearest point in the constellation \( Y_{r,1} = f_1 U_1 + f_2 V_1 \), where \( U_1, V_1 = \{a(-Q, Q)z\} \). Then, the receiver passes the output of the hard decision decoder through the bijective mapping \( f_1 U_1 + f_2 V_1 \mapsto (U_1, V_1) \) in order to decode both \( U_1 \) and \( V_1 \).

The receiver can now use
\[
\tilde{Y}_r = \tilde{Y}_{r,1} - \hat{a}_1 U_1 - \hat{h}_{c,1} V_1 \tag{106}
\]
\[= \begin{bmatrix} a_2 & \cdots & \hat{a}_d \end{bmatrix} U_{t,1}^d + [\hat{h}_{c,2} \cdots \hat{h}_{c,l}] V_c \tag{107}
\]
\[= B \begin{bmatrix} U_{t,1}^d \ \\ V_c \end{bmatrix} + Z_r^N,
\]
to decode $U_2, \ldots, U_d$, where,
\[
B \triangleq [\tilde{a}_2 \cdots \tilde{a}_d \tilde{h}_{c,2} \cdots \tilde{h}_{c,t}] \in \mathbb{C}^{(N-1) \times (N-1)},
\]
is full rank a.s. To show that $B$ is full rank a.s., let $\tilde{H}_t$ and $\tilde{H}_c$ be generated by removing the first row from $H_t$ and $H_c$, and let $\tilde{P}_t$ and $\tilde{P}_c$ be generated by removing the first column from $P_t$ and $P_c$, respectively. $B$ can be rewritten as
\[
B = [\tilde{H}_t \tilde{H}_c] \begin{bmatrix} \tilde{P}_t & 0_{N \times (l-1)} \end{bmatrix}. \tag{110}
\]
Note that $[\tilde{H}_t \tilde{H}_c]$ has all of its entries independently and randomly drawn from a continuous distribution, and the second matrix in the RHS of (110) is full column rank. Using Lemma 1, the matrix $B$ is full rank a.s.

Hence, by zero forcing, the receiver obtains
\[
\tilde{Y}_r = B^{-1}\tilde{Y}_r = \begin{bmatrix} U_{t_1}d_{i_1} & 0_{N \times (l-1)} \end{bmatrix} + Z_r, \tag{111}
\]
where $Z_r = B^{-1}Z_r^N \sim \mathcal{CN}(0, B^{-1}B^{-H})$. Thus, at high SNR, the receiver can decode the other information streams, $U_2, \ldots, U_d$, from $\tilde{Y}_r$.

The mutual information between the transmitter and receiver is lower bounded as follows:
\[
I(X_t; Y_r) \geq I(U_1; \tilde{Y}_r) \geq I(U_1, U_{t_2}; \tilde{Y}_{r_1}) + I(U_1, U_{t_2}; \tilde{Y}_{r_2} | \tilde{Y}_{r_1}) \geq I(U_1; \tilde{Y}_{r_1}) + I(U_{t_2}; \tilde{Y}_{r_2} | U_1, \tilde{Y}_{r_1}) \tag{112}
\]
where (112) follows since $U_t - X_t - Y_r - \tilde{Y}_r$ forms a Markov chain. We next lower bound each term in the RHS of (112).

We lower bound the first term, $I(U_1; \tilde{Y}_{r_1})$ as follows, see also [37], [43]. Let $P_{e_1}$ denote the probability of error in decoding $U_1$ at the receiver, i.e., $P_{e_1} \triangleq \Pr(\tilde{U}_1 \neq U_1)$, where $\tilde{U}_i, i = 1, 2, \ldots, d$, is the estimate of $U_i$ at the legitimate receiver. Thus, using Fano’s inequality, we have
\[
I(U_1; \tilde{Y}_{r_1}) = H(U_1) - H(U_1 | \tilde{Y}_{r_1}) \geq H(U_1) - 1 - P_{e_1} \log |U_1| \tag{113}
\]
\[
\geq (1 - P_{e_1}) \log(2Q + 1) - 1. \tag{114}
\]
From (105), since the mapping $(U_1, V_1) \mapsto f_1U_1 + f_2V_1$ is invertible, the only source of error in decoding $U_1$ from $\tilde{Y}_{r_1}$ is the additive Gaussian noise $Z'$. Note that, since $Z' \sim \mathcal{CN}(0, |b|^2)$, $\text{Re}[Z']$ and $\text{Im}[Z']$ are i.i.d. with $N(0, |b|^2)$ distribution, and $|Z'| \sim \text{Rayleigh}(\frac{|b|}{\sqrt{2}})$. Thus, we have
\[
P_{e_1} \triangleq \Pr(\tilde{U}_1 \neq U_1) \tag{115}
\]
\[
\leq \Pr(\tilde{U}_1 \neq U_1, V_1) \tag{116}
\]
\[
\leq \Pr(|Z'| \geq d_{\text{min}}^2), \tag{117}
\]
where $d_{\text{min}}$ is the minimum distance between the points in the constellation $\mathcal{X}_1 = f_1U_1 + f_2V_1$.

In order to upper bound $P_{e_1}$, we lower bound $d_{\text{min}}$. To do so, similar to [37], we extend real interference alignment [43] to complex channels. In particular, we utilize the following results from number theory:

**Definition 2:** [38] The Diophantine exponent $\omega(\mathbf{z})$ of $\mathbf{z} \in \mathbb{C}^n$ is defined as
\[
\omega(\mathbf{z}) \triangleq \sup \left\{ v : |p + \mathbf{z}q| \leq (||q||_\infty)^{-v} \text{ for infinitely many } q \in \mathbb{Z}^n, p \in \mathbb{Z} \right\}, \tag{120}
\]
where $\mathbf{q} = [q_1 q_2 \cdots q_n]^T$ and $||q||_\infty = \max_i |q_i|$.  

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig4}
\caption{An example for the achievability scheme for Case 3, when $N = 4$, $N_c = 3$, and $N_e = 2$.}
\end{figure}
Lemma 2: [38] For almost all $z \in \mathbb{C}^n$, the Diophantine exponent $\omega(z)$ is equal to $\frac{n-1}{2}$.

Lemma 2 implies the following:

Corollary 1: For almost all $z \in \mathbb{C}^n$ and for all $\epsilon > 0$,
\begin{equation}
|p + z \cdot q| > (\max_i |q_i|)^{-\frac{n+\epsilon}{2}}, \quad (125)
\end{equation}
holds for all $q \in \mathbb{Z}^n$ and $p \in \mathbb{Z}$ except for finitely many of them.

Since the number of integers that violate the inequality in (125) is finite, there exists a constant $\kappa$ such that, for almost all $z \in \mathbb{C}^n$ and all $\epsilon > 0$, the inequality
\begin{equation}
|p + z \cdot q| > \kappa (\max_i |q_i|)^{-\frac{n+\epsilon}{2}}, \quad (126)
\end{equation}
holds for all $q \in \mathbb{Z}^n$ and $p \in \mathbb{Z}$.

Thus, for almost all channel gains, the minimum distance $d_{\text{min}}$ is lower bounded as follows:
\begin{equation}
d_{\text{min}} = \inf_{Y_{r_1}, Y_{r_1}'} \frac{|Y_{r_1}' - Y_{r_1}|}{d_{\text{bf}}(Y_{r_1})} \geq \kappa \frac{|f_1|}{(2Q)^{\frac{n}{2}}} \geq \kappa |f_1| 2^{-\frac{1}{2} \frac{n}{2} \epsilon P^2}, \quad (130)
\end{equation}
where (130) follows from (126), and (131) follows by substituting (89) and (90) in (130). Substituting (131) in (123) gives the following bound on $P_{e_1}$,
\begin{equation}
P_{e_1} \leq \exp(-\mu P^\epsilon), \quad (132)
\end{equation}
where $\mu = \frac{\sigma^2 |f|^2}{d_{\text{bf}}} - \epsilon$ is a constant which does not depend on the power $P$. Thus, using (119) and (132), we have
\begin{equation}
I(U_1; Y_{r_1}) \geq (1 - \exp(-\mu P^\epsilon)) \log(2Q + 1) - 1. \quad (133)
\end{equation}

Next, we lower bound the second term in the RHS of (116), $I(U_{r_2}^d; Y_{r_2}^r)$. Let $B = [0_{(N-1) \times 1} \ I_{N-1}] - \frac{1}{f_2} \bar{h}_{e_1} b_{1}^H$, and
\begin{equation}
\tilde{Y}_{r}^r = B^{-1} \tilde{Y}_{r}^r = \left[ \begin{array}{c} U_{t_2}^d \ V_{c_2}^r \end{array} \right] + B^{-1} \bar{B} \mathbf{Z}_r, \quad (134)
\end{equation}
where $B$ is defined as in (109). Thus, we have
\begin{equation}
I(U_{r_2}^d; Y_{r_2}^r | U_1, Y_{r_1}) \geq I(U_{t_2}^d; A U_1 + \bar{h}_e V_c + Z_{r_2}^N | U_1, f_2 V_1 + Z') \geq I(U_{t_2}^d; \bar{h}_e^H \mathbf{Z}_r f_2 V_1 + Z') \geq I(U_{t_2}^d, \tilde{Y}_{r}^r) \geq I(U_{t_2}^d, \tilde{Y}_{r}). \quad (135)
\end{equation}

Using the upper bound in (100) and the lower bound in (152), we get
\begin{equation}
R_s \geq \frac{1 - \epsilon}{2 + \epsilon} \left[ 2d - 1 - \exp(-\mu P^\epsilon) \right] \log P + o(\log P) - (2l - 1) \quad (153)
\end{equation}
Thus, it follows that the s.d.o.f. is lower bounded as
\[ D_s \geq \frac{(1 - \epsilon)(2N - N_e)}{2 + \epsilon}. \]  
Since \( \epsilon > 0 \) can be chosen arbitrarily small, we can achieve s.d.o.f. of \( N - \frac{N}{2} \).

D. Case 4: \( N_e \leq N, N < N_e \leq N + N_e, \) and \( N + N_e - N_e \) is even

Since \( N_e > N \) for this case, the cooperative jammer, unlike the previous three cases, chooses its precoder such that \( N_i - N \) of its jamming streams are sent invisible to the receiver, in order to allow for more space for the information streams at the receiver. The s.d.o.f. for this case is integer valued, which we can achieve using Gaussian information and cooperative jamming streams.

The transmitted signals are given by (72), with \( d = \frac{N + N_e - N_e}{2}, l = \frac{N + N_e - N_e}{2}, \) \( U_t \sim \mathcal{CN}(0, \Pi_d), V_c \sim \mathcal{CN}(0, \Pi_l), \)

\[ P_c = [P_{c,1} P_{c,n}], \]  
where \( P_{c,1} \) is given by

\[ g = \frac{N + N_e - N_e}{2}, \text{ and } P_{c,n} \in \mathbb{C}^{N_e \times (N_e - N)} \text{ is a matrix whose columns span } \mathcal{N}(H_c), P_t \text{ is defined as in Section V-B, and } P = \alpha'P, \text{ where } \alpha' = \max \left\{ \sum_{i=1}^{d} ||p_{t,i}||^2, g + \sum_{i=g+1}^{l} ||p_{c,i}||^2 \right\}. \]

At high SNR, the receiver can decode the \( d \) information and the \( g \) cooperative jamming streams, where \( d + g = N \).

The received signals at the legitimate receiver and the eavesdropper are given by

\[ Y_r = H_r P_t U_t + [H_r P_{c,1} 0_{N \times (N_e - N)}] \left[ V_{l,c}^{-1} \right] [V_{c,0}^{-1}] + Z_r \]  
(158)

\[ Y_e = \tilde{G}_c(U_t^l + V_c) + Z_e, \]  
(159)

where \( \tilde{G}_c = G_r P_c \).

The matrix \( [H_r P_t H_r P_{c,1}] \in \mathbb{C}^{N \times N} \) in (159) can be rewritten as

\[ [H_r P_t H_r P_{c,1}] = [H_r \ H_c] \left[ \begin{array}{c} P_t \\ 0_{N \times d} \end{array} \right] \left[ \begin{array}{c} P_{c,1} \\ P_{c,1} \end{array} \right]. \]  
(161)

By applying Lemma 1 on (161), the matrix \( [H_r P_t H_r P_{c,1}] \) is full rank a.s. Thus,

\[ I(X_t; Y_r) \geq d \log P + o(\log P). \]  
(162)

Using similar steps as from (79) to (84), we can show that

\[ I(X_t; Y_e) = \log \frac{\det(I_2 + 2PG_r^H G_c)}{\det(I_2 + PG_r^H G_c)} \leq l. \]  
(163)

Thus, the achievable secrecy rate in (71) is lower bounded as

\[ R_s \geq d \log P + o(\log P) - l \]  
(164)

\[ = \frac{N + N_e - N_e}{2} \log P + o(\log P) - \frac{N_e + N_e - N}{2}, \]  
(165)

and, using (5), the s.d.o.f. is lower bounded as

\[ D_s \geq \frac{N + N_e - N_e}{2}. \]  
(166)

E. Case 5: \( N_e \leq N, N < N_e \leq N + N_e, \) and \( N + N_e - N_e \) is odd

As in case 3, the s.d.o.f. for this case is not an integer, and as in case 4, we have \( N_i > N \), which allows the cooperative jammer to send some signals invisible to the receiver. Consequently, the achievable scheme for this case combines the techniques used in Sections V-C and V-D.

The transmitted signals are given by (72) with \( d = \frac{N + N_e - N_e + 1}{2}, l = \frac{N + N_e - N_e + 1}{2}, P_t \) and \( P_c \) are defined as in Section V-D with \( g = \frac{N + N_e - N_e + 1}{2}, \) \( U_t, V_c \) are defined as in Section V-C. Similar to the proof in Appendix D, the values of \( Q \) and \( \nu \) are chosen as in (89) and (90), with

\[ \gamma = \frac{1}{\left( \max \left\{ ||p_{t,1}||^2 + 2 \sum_{i=2}^{d} ||p_{t,i}||^2, 2g - 1 + 2 \sum_{i=g+1}^{l} ||p_{c,i}||^2 \right\} \right)^{\frac{1}{2}}}, \]  
(167)

and \( \nu \) are constants that do not depend on the power \( P \).

The legitimate receiver uses the projection and cancellation technique described in Section V-C in order to decode the information streams. The received signal at the eavesdropper is the same as in (160), with \( l = \frac{N + N_e - N_e + 1}{2} \). Similar to the derivation from (92) to (100), we have

\[ I(X_t; Y_e) \leq 2l - 1. \]  
(168)

Let \( A = H_r P_t = [a_1 \ldots a_d], \) and \( H_c' = H_r P_{c,1} = [h_{c,1} \ldots h_{c,g}]. \) The received signal at the legitimate receiver is

\[ Y_r = \begin{bmatrix} A & H_r' \\ U_t & V_{c,1} \end{bmatrix} + Z_r. \]  
(169)

As in case 3, we have that \( d + g - 2 = N - 1 \), and hence the dimension of \( \{a_2, \ldots, a_d, h_{c,2}, \ldots, h_{c,g}\} \) is at most \( N - 1 \), and there exists \( b \in \mathbb{C}^N \) such that \( b \) is orthogonal to span \( \{a_2, \ldots, a_d, h_{c,2}, \ldots, h_{c,g}\} \). The receiver chooses such \( b \) and multiplies its received signal by the matrix \( D \) given in (103) to obtain \( \tilde{Y}_r = \begin{bmatrix} \tilde{Y}_{r_1} \ \tilde{Y}_{r_2} \end{bmatrix}^T \), where

\[ \tilde{Y}_{r_1} = f_1 U_t + f_2 V_1 + Z_r', \]  
(170)

\[ \tilde{Y}_{r_2} = \tilde{A} U_t + \tilde{H}_r V_{c,1} + Z_{r_2}, \]  
(171)

\( f_1, f_2, Z', \tilde{A}, \) and \( \tilde{H}_r \) are defined as in Section V-C. In order to decode \( U_t \) and \( V_1 \), the receiver passes \( \tilde{Y}_{r_1} \) through a hard decision decoder, \( \tilde{Y}_{r_1} \rightarrow f_1 U_t + f_2 V_1 \), and passes the output of the hard decision decoder through the bijective map \( f_1 U_t + f_2 V_1 \rightarrow (U_1, V_1) \), where \( f_1 \) and \( f_2 \) are rationally independent.
Using similar steps to the derivation from (112) to (152) in Section V-C, we obtain
\[
I(X_t; Y_r) \geq \frac{1 - \epsilon}{2 + \epsilon} \left[ 2d - 1 - \exp(-\mu P^t) - 2(d - 1)^2 \exp(-\mu' P'^t) \right] \log P + o(\log P),
\]
where \(\epsilon > 0\) is arbitrarily small, \(\epsilon' = \frac{3c}{2t+1}\), and \(\mu, \mu'\) are constants which do not depend on \(P\).

Thus, the achievable secrecy rate in (71) is lower bounded as
\[
R_s \geq \frac{1 - \epsilon}{2 + \epsilon} \left[ 2d - 1 - \exp(-\mu P^t) - (d - 1)^2 \exp(-\mu' P'^t) \right] \log P + o(\log P) - (2d - 1) \tag{173}
\]
and hence the s.d.o.f is lower bounded as
\[
D_s \geq \frac{(1 - \epsilon)(N + N_e - N_e)}{2 + \epsilon}. \tag{175}
\]
Since \(\epsilon > 0\) can be chosen arbitrarily small, \(D_s = \frac{N+N_e-N_e}{2}\) is achievable for this case, which completes the achievability of (69). Next, we show the achievability of (70), where \(N_e > N\), i.e., the eavesdropper has more antennas than the legitimate receiver.

**F. Case 6: \(N_e > N\) and \(N_e - N < N_e \leq N_e - \frac{N}{2}\)**

Unlike the previous five cases, since \(N_e > N\), no information streams can be sent invisible to the eavesdropper. In fact, the precoder at the transmitter is not adequate for achieving the alignment of the information and cooperative jamming streams at the eavesdropper. We need to design both precoders at the transmitter and the cooperative jammer to take part in achieving the alignment condition. The s.d.o.f. here is integer valued, and hence we can utilize Gaussian streams.

The transmitted signals are given by (72), with \(d = l = N + N_e - N_e\), and \(U_t, V_c \sim \mathbb{CN}(0, P_{t}, P_{c})\). The matrices \(P_t\) and \(P_c\) are chosen as follows. Let \(G = [G_t - G_c] \in \mathbb{C}^{N_e \times (N+N_e)}\), and let \(Q \in \mathbb{C}^{(N+N_e) \times d}\) be a matrix whose columns are randomly chosen to span \(\mathbb{N}(G)\). Write the matrix \(Q\) as \(Q = [Q_t^T, Q_c^T]^T\), where \(Q_t \in \mathbb{C}^{N \times d}\) and \(Q_2 \in \mathbb{C}^{N_e \times d}\). Set \(P_t = Q_1\) and \(P_c = Q_2\). \(P = \frac{1}{\alpha''} P_t\), where \(\alpha'' = \max\{\sum_{i=1}^{d} ||P_{t,i}||^2, \sum_{i=1}^{d} ||P_{c,i}||^2\}\).

The choice of \(P_t\) and \(P_c\) results in \(G_t P_t = G_c P_c\). Thus, the eavesdropper receives
\[
Y_c = G_c P_c (U_t + V_c) + Z_c. \tag{176}
\]

Similar to going from (79) to (84), it follows that we have
\[
I(X_t; Y_c) \leq N + N_e - N_e. \tag{177}
\]

The received signal at the receiver in turn is given by
\[
Y_r = [H_t P_t \ H_c P_c] [U_t | V_c] + Z_r. \tag{178}
\]

Note that, without conditioning on \(G_t\) and \(G_c\), the matrix \(Q\) has all of its entries independently and randomly drawn according to a continuous distribution. Thus, each of \(P_t\) and \(P_c\) is full column rank a.s. Hence, using Lemma 1, we can show that the matrix \([H_t P_t \ H_c P_c]\) is full column rank a.s. Using (178), we have
\[
I(X_t; Y_r) \geq (N + N_e - N_e) \log P + o(\log P). \tag{179}
\]

Hence, using (177), (179), (71), and (5), the s.d.o.f. is lower bounded as \(D_s \geq N + N_e - N_e\).

**G. Case 7: \(N_e > N\), \(N_e - \frac{N}{2} < N_e \leq N_e\), and \(N\) is even**

The s.d.o.f. for this case does not increase by increasing \(N_e\). The scheme in Section V-F for \(N_e = N_e - \frac{N}{2}\), i.e., \(d = \frac{N}{2}\), can be used to achieve the s.d.o.f. for all \(N_e - \frac{N}{2} < N_e \leq N_e\), when \(N_e > N\) and \(N\) is even. However, since \(\min(\mathbb{N}(G)) = N + N_e - N_e > \frac{N}{2}\), the \(d = \frac{N}{2}\) columns of the matrix \(Q\) are randomly chosen as linearly independent vectors from \(\mathbb{N}(G)\). Following the same analysis as in Section V-F, we can show that the s.d.o.f. is lower bounded as \(D_s \geq \frac{N}{2}\).

**H. Case 8: \(N_e > N\), \(N_e - \frac{N}{2} < N_e \leq N_e\), and \(N\) is odd**

The difference here from Section V-G is that the s.d.o.f. is not an integer, and hence, structured signaling for transmission and cooperative jamming is needed, and the difference from V-C is that \(N_e > N\), and hence both the precoders at the transmitter and cooperative jammer have to participate in achieving the alignment condition at the eavesdropper.

The transmitted signals are given by (72), with \(d = l = \frac{N+1}{2}\), \(U_t\) and \(V_c\) are defined as in Section V-C, and the values for \(Q\) and \(\alpha\) are chosen as in (89) and (90), with
\[
\gamma = \frac{1}{\max \left\{ \left( \sum_{i=1}^{d} ||P_{t,i}||^2 \right)^{\frac{1}{2}}, \left( \sum_{i=1}^{d} ||P_{c,i}||^2 \right)^{\frac{1}{2}} \right\}}, \tag{180}
\]
and \(\nu\) are constants which do not depend \(P\). \(P_t\) and \(P_c\) are chosen as in Section V-G, with \(d = \frac{N+1}{2}\). The eavesdropper’s received signal is the same as in (176). Similar to (92)-(100), we have
\[
I(X_t; Y_c) \leq N. \tag{181}
\]

The receiver employs the decoding scheme in Sections V-C and V-E. Following similar steps as in Sections V-C and V-E, we have
\[
I(X_t; Y_r) \geq \frac{(1 - \epsilon)N}{2 + \epsilon} \log P + o(\log P). \tag{182}
\]

Using (181), (182), (71), and (5), the s.d.o.f. is lower bounded as \(D_s \geq \frac{(1-\epsilon)N}{2+\epsilon}\), and since \(\epsilon > 0\) is arbitrarily small, the s.d.o.f. of \(\frac{N}{2}\) is achievable for this case.
I. Case 9: \( N_c > N \), \( N_c < N_c \leq N + N_c \), and \( N + N_c - N_c \) is even

In Sections V-G and V-H, we observe that the flat s.d.o.f. range extends to \( N_c = N_c \), and not \( N_c = N \) as in Sections V-B and V-C. Achieving the alignment of information and cooperative jamming at the eavesdropper requires that \( N_c > N_c \) in order for the cooperative jammer to begin sending some jamming signals invisible to the legitimate receiver. For this case, in addition to choosing its precoding matrix jointly with the transmitter to satisfy the alignment condition, the cooperative jammer chooses its precoder to send \( N_c - N_c \) jamming streams invisible to the receiver. The s.d.o.f. here is integer valued, for which we utilize Gaussian streams.

The transmitted signals are given by (72) with \( d = \frac{N + N_c - N_c}{2} \), and \( U_t, V_c \) are defined as in Section V-F. Let \( P_t = [P_{t,1} P_{t,2}] \) and \( P_c = [P_{c,1} P_{c,2}] \), where \( P_{t,1} \in C^{N \times g} \), \( P_{t,2} \in C^{N \times (N_c - N_c)} \), \( P_{c,1} \in C^{N_c \times g} \), \( P_{c,2} \in C^{N_c \times (N_c - N_c)} \), and \( g = \frac{N + N_c - N_c}{2} \). The matrices \( P_t \) and \( P_c \) are chosen as follows. Let \( G = [G_t - G_c] \in C^N \times (N + N_c) \), and let \( G' \in C^N \times (N + N_c) \) be expressed as

\[
G' = \begin{bmatrix} G_t & -G_c \\ N \times N & H_c \end{bmatrix}.
\] (183)

Let \( Q' \in C^{(N + N_c) \times (N_c - N_c)} \) be randomly chosen such that its columns span \( N(G') \), and let the columns of the matrix \( Q \in C^{(N + N_c) \times g} \) be randomly chosen as linearly independent vectors in \( N(G) \), and not in \( N(G') \). Write the matrix \( Q \) as \( Q = [Q'_1 Q'_2] \), and the matrix \( Q' \) as \( [Q'_1 Q'_2] \), where \( Q'_1 \in C^{N \times g} \), \( Q'_2 \in C^{N_c \times g} \), \( Q'_1 \in C^{N \times (N_c - N_c)} \), and \( Q'_2 \in C^{N_c \times (N_c - N_c)} \). Set \( P_{t,1} = Q_{1t} \), \( P_{t,2} = Q_{1t}' \), \( P_{c,1} = Q_{2c} \), and \( P_{c,2} = Q_{2c}' \).

This choice of \( P_t \) and \( P_c \) results in \( G_t P_t = G_c P_c \) and \( H_t P_{c,2} = 0 \times (N_c - N_c) \). Thus, the received signals at the receiver and eavesdropper are given by

\[
Y_r = [H_t P_t \ H_t P_{c,1}] \begin{bmatrix} U_t \\ V_c \end{bmatrix} + Z_r \] (184)

\[
Y_e = G_c P_c (U_t + V_c) + Z_e. \] (185)

Using (185), and similar to going from (79) to (84), we have

\[
I(X;Y) \leq \frac{N + N_c - N_c}{2}. \] (186)

Because of the assumption of randomly generated channel gains, each of \( P_t \) and \( P_c \) is full column rank a.s. Using Lemma 1, we have the matrix \([H_t P_t \ H_t P_{c,1}]\) is full column rank a.s., and hence, using (184), we have

\[
I(X;Y) \geq \frac{N + N_c - N_c}{2} \log P + o(\log P). \] (187)

Thus, using (186), (187), (71), and (5), the s.d.o.f. is lower bounded as \( D_s \geq \frac{N + N_c - N_c}{2} \).

J. Case 10: \( N_c > N \), \( N_c < N_c \leq N + N_c \), and \( N + N_c - N_c \) is odd

The s.d.o.f. for this case is not an integer, and we have \( N_c > N_c \), and hence, we utilize here precoding as in Section V-I, and signaling and decoding scheme as in Section V-H; \( U_t, V_c \) are defined as in Section V-H, and \( P_t, P_c \) are chosen as in Section V-I, with \( d = \frac{N + N_c - N_c + 1}{2} \) and \( g = \frac{N + N_c - N_c + 1}{2} \). Using the same decoding scheme as in Section V-H, we obtain that the s.d.o.f. is lower bounded as \( D_s \geq \frac{N + N_c - N_c}{2} \) for this case, which completes the achievability proof of (70). Thus, we have completed the proof for Theorem 1.

VI. EXTENDING TO THE GENERAL CASE: THEOREM 2

The converse and achievability proofs for Theorem 2 involve the same techniques as those utilized for Theorem 1. However, one needs to carefully handle the antenna configurations when \( N_t \neq N_r \). In the following, we summarize how to extend the main ideas presented in Sections IV and V in order to prove Theorem 2.

A. Converse

The converse proof for Theorem 2 follows similar steps as in Section IV. In particular, we derive the following two upper bounds which hold for two different ranges of \( N_c \).

1) \( 0 \leq N_c \leq N_e \): When \( N_t \neq N_t \), the range of \( N_c \) for which the first upper bound holds is the same as in the case when \( N_t = N_r = N \) in Section IV-A. However, unlike in Section IV-A, when \( N_t \neq N_r \), this range of \( N_c \) is further subdivided into two ranges. The first upper bound on the s.d.o.f. we derive here is again \( D_s \leq [N_c - N_c - N_c] + \), yet, the maximum s.d.o.f. for the channel is equal to \( \min[N_t, N_r] \). Hence, for the case \( N_t < N_t + N_c - N_r \), the maximum s.d.o.f., \( N_r \), is reached at an \( N_c \) that is smaller than \( N_c \). In particular, using similar analysis as in Section IV-A, we have

\[
R_s \leq C_s(P) = \rho \log P + o(\log P), \] (188)

where, for \( 0 \leq N_c \leq [N_c - N_c + N_t] \), \( \rho = [N_c + N_t - N_c] \). Since \( [N_c + N_c - N_c] \leq N_c \) for \( [N_c - N_c + N_t] \leq N_c \), we have, for \( 0 \leq N_c \leq N_c \),

\[
D_s \leq \min[N_t, [N_c + N_c - N_c]]. \] (189)

2) \( N_c + [N_c - N_c] \leq N \leq 2 \min[N_t, N_r] + N_c - N_t \): Following similar steps as in Section IV-B, where the two cases we consider here are \( N_c \leq N_t \) and \( N_c > N_t \), the s.d.o.f. for this range of \( N_c \) is upper bounded as

\[
D_s \leq \frac{N_c + N_c - N_c}{2}. \] (190)

It easy to see that, when \( N_t = N_r = N \), the range of \( N_c \) for which the second upper bound in (190) holds is reduced to the range \( \max[N_t, N_r] \leq N_c \leq N + N_r \) in Section IV-B. However, when \( N_t \neq N_r \), the range of \( N_c \) is different. In particular, we have that \( N_c > N_r + [N_c - N_t] \) because, when \( N_r > N_t \), (190) holds only when \( N_r > N_c + N_t \) so that the number of antennas at the cooperative jammer in the modified channel, c.f. (59), is greater than \( N_r \). We also have that \( N_c \leq 2 \min[N_t, N_r] + N_t - N_t \). This because, when \( N_t < N_r \), we have \( N_c + N_t - N_c = N_t \) at \( N_c = N_t + N_c \), and when \( N_t > N_r \), we have \( N_c + N_t - N_c = N_t \) at \( N_c = 2N_c + N_c - N_t \).
3) Obtaining the upper bound: For each of the following cases, we use the two bounds in (189) and (190) to obtain the upper bound for the s.d.o.f.

i) \( N_t \geq N_r + N_c \)

For this case, we use the trivial bound for the s.d.o.f., \( D_s \leq N_r \) for all the values of \( N_c \).

ii) \( N_c \geq N_t \geq N_r \) and \( N_r \geq N_t + N_c \)

Using the bound in (189), we have

\[
D_s \leq N_r + N_t - N_c, \quad \text{for } 0 \leq N_c \leq N_r,
\]

where at \( N_c = N_r \), we have \( D_s \leq N_t \), which is the maximum achievable s.d.o.f. for this case.

iii) \( N_t \geq N_c \) and \( N_t - N_c < N_c < N_t + N_c \)

Combining the bounds in (189) and (190), as in Section IV-C, yields

\[
D_s \leq \begin{cases} 
N_c + N_t - N_c, & \text{if } 0 \leq N_c \leq \frac{N_t + N_c - N_r}{2} \\
N_r + \frac{N_r - N_t}{2}, & \text{if } \frac{N_r + N_t - N_c}{2} < N_c \leq N_r \\
N_r + \frac{N_r - N_t}{2}, & \text{if } N_r < N_c \leq 2 \min \{N_t, N_r\} + N_c - N_t.
\end{cases}
\]

(191)

(192)

iv) \( N_c > N_t \) and \( N_r \geq 2N_t \)

Using the bound in (189), we have

\[
D_s \leq \lfloor N_c + N_t - N_c \rfloor^+, \quad \text{for } 0 \leq N_c \leq N_r.
\]

v) \( N_c > N_t \) and \( N_r < 2N_t \)

By combining the bounds in (189) and (190), we have

\[
D_s \leq \begin{cases} 
\lfloor N_c + N_t - N_c \rfloor^+, & \text{if } 0 \leq N_c \leq \frac{N_c + N_r - N_t}{2} + N_c - N_t \\
\frac{N_r}{2}, & \text{if } \frac{N_r}{2} + N_c - N_t < N_c \leq N_r + N_c - N_t \\
\frac{N_r + N_c - N_t}{2}, & \text{if } N_r + N_c - N_t < N_c \leq 2 \min \{N_t, N_r\} + N_c - N_t.
\end{cases}
\]

One can easily verify that the cases cited above cover all possible combinations of number of antennas at various terminals. By merging the upper bounds for these cases in one expression, we obtain (7) as the upper bound for the s.d.o.f. of the channel.

B. Achievability

The s.d.o.f. for the channel when \( N_t \) is not equal to \( N_c \), given in (7), is achieved using techniques similar to what we presented in Section V. There are few cases, of the number of antennas, where the achievability is straightforward. One such case is when \( N_r \geq N_c + N_r \), where the transmitter can send \( N_c \) Gaussian information streams invisible to the eavesdropper, and the maximum possible s.d.o.f. of the channel, i.e., \( N_c \), is achieved without the help of the cooperative jammer, i.e., \( N_c = 0 \). Another case is when \( N_c \geq N_t + \min \{N_t, N_r\} \), where the receiver’s signal space is sufficient for decoding the information and jamming streams, at high SNR, for all \( 0 \leq N_c \leq N_c \), arriving at the s.d.o.f. of \( N_c \) (the maximum possible s.d.o.f.) at \( N_c = N_c \). Thus, there is no constant period in the s.d.o.f. characterization for this case where the s.d.o.f. keeps increasing by increasing \( N_c \), and Gaussian signaling and cooperative jamming are sufficient to achieve the s.d.o.f. of the channel.

We consider the five cases of the number of antennas at the different terminals listed in Section VI-A3. In the following, we summarize the achievable schemes for these cases. Let \( d \) and \( l \) denote the number of information and cooperative jamming streams. \( \mathbf{P}_t, \mathbf{P}_c \) are the precoding matrices at the transmitter and the cooperative jammer.

i) \( N_t \geq N_r + N_c \)

The transmitter sends \( N_r \) Gaussian information streams over \( N(\mathbf{G}_t) \). \( D_s = N_r \) is achievable at \( N_c = 0 \).

ii) \( N_r \geq N_c \geq N_r \) and \( N_r \geq N_t + N_c \)

For \( 0 \leq N_c \leq N_r \), \( d = N_r + N_t - N_c \) and \( l = N_c \) Gaussian streams are transmitted. Choose \( \mathbf{P}_t \) to send \( N_c - N_r \) information streams over \( N(\mathbf{G}_t) \) and align the remaining information streams over cooperative jamming streams at the eavesdropper. \( D_s = N_c + N_t - N_r \).

iii) \( N_t \geq N_c \) and \( N_t - N_c < N_c < N_t + N_c \)

1) For \( 0 \leq N_c \leq \frac{N_t + N_c - N_r}{2} \):

The same scheme as in case (ii) is utilized. \( D_s = N_c + N_t - N_r \).

2) For \( \frac{N_r + N_c - N_t}{2} < N_c \leq N_r \) and \( N_r + N_t - N_c \) is even:

The same scheme as in case (iii-1), with \( d = \frac{N_r + N_c - N_t}{2} \) and \( l = \frac{N_r + N_c - N_t}{2} \), is utilized. The cooperative jammer uses only \( \frac{N_r + N_c - N_t}{2} \) of its \( N_c \) antennas. \( D_s = \frac{N_r + N_c - N_t}{2} \).

3) For \( \frac{N_r + N_c - N_t}{2} \) odd:

The same scheme as in case (iii-2), with \( d = \frac{N_r + N_c - N_t}{2} + 1 \) and \( l = \frac{N_r + N_c - N_t}{2} + 1 \), is utilized. The cooperative jammer uses only \( \frac{N_r + N_c - N_t}{2} + 1 \) of its \( N_c \) antennas. \( \mathbf{P}_t \) is chosen as in case (ii). The legitimate receiver uses the projection and cancellation technique, as in Section V-C. \( D_s = \frac{N_r + N_c - N_t}{2} \).

4) For \( N_r < N_c \leq \lfloor 2 \min \{N_t, N_r\} \rfloor + N_c - N_t \) and \( N_r + N_t - N_c \) is even:

\[
d = \frac{N_r + N_c - N_t}{2}
\]

5) For \( N_r < N_c \leq 2 \min \{N_t, N_r\} + N_c - N_t \) and \( N_r + N_t - N_c \) is odd:

\[
d = \frac{N_r + N_c - N_t}{2} + 1
\]
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2017.2738011, IEEE Transactions on Information Theory

even:
\[ d = l = \frac{N_e}{2} \] Gaussian streams are transmitted. \( P_t, P_c \)
are chosen as in case (iv). \( D_s = \frac{N_e}{2} \).

3) For \( \frac{N_e}{2} + N_t - N_e < N_c \leq N_r + N_e - N_t \) and \( N_r \) is odd:
\[ d = l = \frac{N_e + t - 1}{2} \] structured streams are transmitted.
\( P_t, P_c \) are as in case (iv). The legitimate receiver uses the projection and cancellation technique. \( D_s = \frac{N_e}{2} \).

4) For \( N_c + N_t - N_e < N_c \leq 2 \min \{N_t, N_r\} + N_e - N_t \) and \( N_r + N_e - N_t \) is even:
\[ d = l = \frac{N_e + N_r - N_t}{2} \] Gaussian streams are transmitted.
Both \( P_t, P_c \) are chosen to align the information and the cooperative jamming streams at the eavesdropper. \( P_c \) is also chosen to send \( N_c - N_r \) cooperative jamming streams over \( N(\mathbf{H}_e) \) as in Section VI. \( N_c > N_r + N_e - N_t \) achieves the above two conditions.
\[ D_s = \frac{N_e + N_r - N_t}{2} \]

Using the achievable schemes described above for the different cases of the number of antennas, and their analysis as in Section V, we have (7) as the achievable s.d.o.f., which completes the proof for Theorem 2.

VII. DISCUSSION

At this point, it is useful to discuss the results and the implications of this work. Theorem 1, c.f. (6), shows the behavior of the s.d.o.f., for an \((N \times N \times N_c)\) multi-antenna Gaussian wire-tap channel with an \(N_c\)-antenna cooperative jammer, associated with increasing \(N_c\) from 0 to \(N + N_c\). The s.d.o.f. first increases linearly by increasing \(N_c\) from 0 to \(N_c = \frac{\min \{N_t, N_r\}}{2} \), that is to say adding one antenna at the cooperative jammer provided the system to have one additional degrees of freedom. The s.d.o.f. remains constant in the \(N_c\) range of \(N_c = \frac{\min \{N_t, N_r\}}{2} \) to \( \max \{N_c, N_t\} \), and starts to increase again for \(N_c\) from \( \max \{N_c, N_t\} \) to \( N + N_c\), until the s.d.o.f. arrives at its maximum value, \(N\), at \(N_c = N + N_c\). This behavior transpires both when the eavesdropper antennas are fewer or more than that of the legitimate receiver.

The reason for the flat s.d.o.f. range is as follows: At high SNR, achieving the secrecy constraint requires i) the entropy of the cooperative jamming signal, \(X_o^c\), to be greater than or equal to that of the information signal visible to the eavesdropper, and ii) \(X_o^b\) to completely cover the information signal, \(X_o^b\), at the eavesdropper. For \(N_c \leq N_t\), part of \(X_o^b\) can be sent invisible to the eavesdropper, and the information signal visible to the eavesdropper can be covered by jamming for all \(N_c\). For \(0 \leq N_c \leq \frac{N_t}{2}\), the spatial resources at the receiver are sufficient, at high SNR, for decoding information and jamming signals which satisfy the above constraints. Thus, increasing the possible entropy of \(X_o^b\) by increasing \(N_c\) from 0 to \(\frac{N_t}{2}\) allows for increasing the entropy of \(X_o^b\), and hence, the achievable secrecy rate and the s.d.o.f. increase. At \(N_c = \frac{N_t}{2}\), the possible entropy of \(X_o^c\) and, correspondingly, the maximum possible entropy of \(X_o^b\), result in information and jamming signals which completely occupy the receiver’s signal space. Thus, increasing the possible uncertainty of \(X_o^c\) by increasing \(N_c\) from \(\frac{N_t}{2}\) to \(N\) is useless, since, in this range, \(X_o^b\) is totally observed by the receiver which has its signal space already full at \(N_c = \frac{N_t}{2}\).

Increasing \(N_c\) over \(N\) increases the possible entropy of \(X_o^b\) and simultaneously increases the part of \(X_o^b\) that can be transmitted invisible to the receiver, leaving more space for \(X_o^b\) at the receiver. This allows for increasing the secrecy rate, and hence, the s.d.o.f. starts to increase again. For \(N_c > N\), the s.d.o.f. is equal to zero for all \(0 \leq N_c \leq N_r - N_t\), since \(X_o^c\) cannot cover the information at the eavesdropper for this case. The s.d.o.f. starts to increase again, after the flat range, at \(N_r > N_c\), since sending jamming signals invisible to the receiver while satisfying the covering condition at the eavesdropper requires that \(N_r > N_c\).

The difference in the slope for the increase in the s.d.o.f. in the ranges before and after the flat range, for both \(N_r \leq N\) and \(N_r > N\), can be explained as follows. For \(0 \leq N_c \leq N_r - \min \{N_t, N_r\} \), each additional antenna at the cooperative jammer allows for utilizing two more spatial dimensions at the receiver; one spatial dimension is used for the jamming signal and the other is used for the information signal. By contrast, for \(\max \{N_r, N_c\} \leq N_r \leq N_c\), each additional antenna at the cooperative jammer sets one spatial dimension at the receiver free from jamming, and this spatial dimension is shared between the extra cooperative jamming and information streams.

It is important to note that the result that suggests that increasing the cooperative jammer antennas is not useful in the range \(N_r - \min \{N_t, N_r\} \leq N_c \leq \max \{N_r, N_c\}\) applies only to the log of the secrecy capacity, i.e., is specific to the high SNR behavior. This should not be taken to mean that additional antennas do not improve secrecy rate, but only the secrecy rate scaling with power in the high SNR.

Theorem 2 generalizes the results above to the case where the number of transmit antennas at the transmitter, \(N_t\), is not equal to the number of receive antennas at the legitimate receiver, \(N_r\). Although the maximum possible s.d.o.f. of the channel for this case is limited to \(\min \{N_t, N_r\} = N_d\), increasing \(N_r\) over \(N_d\), or increasing \(N_r\) over \(N_r\), do change the behavior of the s.d.o.f. associated with increasing \(N_r\), until the maximum possible s.d.o.f. is reached. Let us start at \(N_t = N_r = N_d\). For \(N_t \geq N_r\), increasing \(N_t\) over \(N_d = N_r\) increases the number of the information streams that can be sent invisible to the eavesdropper, and hence the s.d.o.f. without the help of the cooperative jammer, i.e., \(N_e = 0\), increases. This results in increasing the range of \(N_c\) for which the s.d.o.f. remains constant by increasing \(N_t\), since the receiver’s signal space gets full at a smaller \(N_r\) and remains full until \(N_r\) is larger than \(N_d = N_r\). In addition, increasing \(N_t\) over \(N_r\), when \(N_t \geq N_r\), results in decreasing the value of \(N_r\) at which the maximum s.d.o.f. of the channel, \(N_{td}\), is achievable, arriving at \(N_t \geq N_r + N_c\), where the s.d.o.f. of \(N_{td}\) is achievable without the help of the cooperative jammer. Fig. 5 illustrates this behavior. When \(N_c > N_t\), increasing \(N_t\) over...
\( N_d \) decreases the value of \( N_e \), at which the s.d.o.f. is positive, and decreases the value of \( N_e \), at which the s.d.o.f. of \( N_d \) is achievable, arriving at \( N_t > N_e \), where the channel renders itself to the previous case. This behavior is demonstrated in Fig. 6. For both the cases \( N_t \geq N_e \) and \( N_t < N_e \), increasing \( N_r \) over \( N_d = N_t \), results in increasing the available space at the receiver's signal space, and hence the constant period decreases, arriving at \( N_r \geq N_t + N_e \) when \( N_t \geq N_e \), or at \( N_r \geq 2N_t \) when \( N_e > N_t \), where the constant period vanishes. Fig. 7 illustrates the behavior of the s.d.o.f. curve associated with increasing \( N_r \) over \( N_t \).

VIII. CONCLUSION

In this paper, we have studied the multi-antenna wire-tap channel with a \( N_e \)-antenna cooperative jammer, \( N_t \)-antenna transmitter, \( N_t \)-antenna receiver, and \( N_e \)-antenna eavesdropper. We have completely characterized the s.d.o.f. for this channel for all possible values of the number of antennas at the cooperative jammer, \( N_e \). We have shown that when the s.d.o.f. of the channel is integer valued, it can be achieved by linear precoding at the transmitter and cooperative jammer, Gaussian signaling both for transmission and jamming, and linear processing at the legitimate receiver. By contrast, when the s.d.o.f. is not an integer, we have shown that a scheme which employs structured signaling both at the transmitter and the cooperative jammer, along with joint signal space and signal scale alignment achieves the s.d.o.f. of the channel. We have seen that, when \( N_t \geq N_e \), the transmitter uses its precoder to send a part of its information signal invisible to the eavesdropper, and to align the remaining part over jamming at the eavesdropper, while the cooperative jammer uses its precoder to send a part of its jamming signal invisible to the receiver, whenever possible. When \( N_e > N_t \), more intricate precoding at the transmitter and cooperative jammer is required, where both the transmitter and cooperative jammer choose their precoders to achieve the alignment of information and jamming at the eavesdropper, and simultaneously, the cooperative jammer designs its precoder, whenever possible, to send a part of the jamming signal invisible to the receiver.

The converse was established by allowing for full cooperation between the transmitter and cooperative jammer for a certain range of \( N_t \), and by incorporating both the secrecy and reliability constraints, for the other values of \( N_e \). We note that while this paper settles the degrees of freedom of this channel, its secrecy capacity is still open. Additionally, while the model considered here assumes channels to be known, universal secrecy as in [32] should be considered in the future.

APPENDIX A

CHOICE OF \( K_t \) AND \( K_c \)

The covariance matrices \( K_t \) and \( K_c \) are chosen so that they are positive definite, i.e., \( K_t, K_c \succ 0 \), and hence non-singular, in order to guarantee the finiteness of \( h(\tilde{Z}_t) \) and \( h(\tilde{Z}_e) \) in (26). In addition, positive definite \( K_t \) and \( K_c \) result in positive definite \( \Sigma_{\tilde{Z}_t} \) and \( \Sigma_{\tilde{Z}_e} \), and hence, \( h(\tilde{Z}_t) \) and \( h(\tilde{Z}_e) \) are also finite.

For \( I_{N_e} - G_t K_t G_t^H \) to be a valid covariance matrix for \( \tilde{Z}_c \) in (30), \( K_t \) has to satisfy \( G_t K_t G_t^H \leq I_{N_e} \), which is equivalent to

\[
\| K_t^\dagger G_t^H \| \leq 1. \tag{193}
\]

Recall that \( \| K_t^\dagger G_t^H \| \) is the induced norm for the matrix \( K_t^\dagger G_t^H \).
Similarly, for $I_N - H_r K_c H_c^H$, $I_N - G_t K_c G_t^H - G_c$, $G_c^H$, and $I_N - H_r' K_c' H_c'^H$ to be valid covariance matrices for $Z_r, Z_c'$, and $Z_r'$, in (40), (53), (62), $K_t, K_c, K_c'$ have to satisfy

$$||K_t^2 H_t|| \leq 1, \quad ||K_c^2 G_t^H||^2 + ||K_c^2 G_c^H||^2 \leq 1,$$

and $||K_c'^2 H_c'^H|| \leq 1$. (194)

In order to satisfy the conditions (193) and (194), we choose $K_t = \rho^2 I_N$, $K_c = \rho^2 I_K$, where

$$0 < \rho \leq \frac{1}{\max \left\{ \frac{||G_t^H||, ||H_t||, ||H_c^H||}{\sqrt{||G_t^H||^2 + ||G_c^H||^2}} \right\}}$$

(195)

In order to upper bound $h(Y_{r,k}(i))$, for all $i = 1, 2, \cdots, n$ and $k = 1, 2, \cdots, N$, we first upper bound the variance of $Y_{r,k}(i)$, denoted by $\text{Var}(Y_{r,k}(i))$. Let $h_{r,k}$ and $h_{c,k}$ denote the transpose of the $k$th row vectors of $H_r$ and $H_c$, respectively. Let $Z_r(i) = [Z_{r,1}(i) \cdots Z_{r,N}(i)]^T$. Using (1), $Y_{r,k}(i)$ is expressed as

$$Y_{r,k}(i) = h_{r,k}^T X_t(i) + h_{c,k}^T X_c(i) + Z_{r,k}(i).$$

(197)
Thus, $\text{Var}(Y_{r,k}(i))$ can be bounded as
\[
\text{Var}(Y_{r,k}(i)) \leq E(Y_{r,k}(i)Y_{r,k}^*(i)) = E\left(\left|h_{r,k}^T X_1(i)\right|^2 + E\left(\left|h_{r,k}^T X_{c}(i)\right|^2\right) + E\left(\left|Z_{r,k}(i)\right|^2\right)\right)
\]
(198)
\[
\leq \left|\left|h_{r,k}^T\right|^2\right| E\left(\left|X_1(i)\right|^2\right) + \left|\left|h_{r,k}^T\right|^2\right| E\left(\left|X_{c}(i)\right|^2\right) + 1
\]
(199)
\[
\leq 1 + \left(\left|h_{r,k}^T\right|^2 + \left|h_{c,k}^T\right|^2\right) P,
\]
(200)
where (200) follows from Cauchy-Schwarz inequality and monotonicity of expectation, and (201) follows from the power constraints at the transmitter and cooperative jammer.

Define $h^2 = \max_k \left(\left|h_{r,k}^T\right|^2 + \left|h_{c,k}^T\right|^2\right)$. Since $h(Y_{r,k}(i))$ is upper bounded by the entropy of a complex Gaussian random variable with the same variance, we have, for all $i = 1, 2, \ldots, n$ and $k = 1, 2, \ldots, N$,
\[
h(Y_{r,k}(i)) \leq \log 2\pi e \left(1 + \left(\left|h_{r,k}^T\right|^2 + \left|h_{c,k}^T\left|\right|^2\right)\right) P
\]
(202)
\[
\leq \log 2\pi e + \log(1 + h^2 P).
\]
(203)
Similarly, we have
\[
\overline{Y}_{r,k}(i) = h_{r,k}^T X_1(i) + h_{r,k}^T X_{c}(i) + Z_{r,k}(i),
\]
(204)
where $h_{r,k}^T$ is the transpose of the $k$-th row vector of $H_{c}$. Thus, we have,
\[
h(\overline{Y}_{r,k}(i)) \leq \log 2\pi e + \log(1 + h^2 P),
\]
(205)
where $\bar{h}^2 = \max \left(\left|h_{r,k}^T\right|^2 + \left|h_{c,k}^T\right|^2\right)$.

Next, we upper bound $h(\bar{X}_{1,i}(i))$. The power constraint at the transmitter, for $i = 1, 2, \ldots, n$, is $E\left(\left|X_{1}(i)\right|^2\right) = \sum_{k=1}^{N} E\left(\left|X_{t,k}(i)\right|^2\right) \leq P$. Thus, $E\left(\left|X_{t,k}(i)\right|^2\right) \leq P$ for all $i = 1, 2, \ldots, n$, and $k = 1, 2, \ldots, N$. Recall that $\bar{X}_{1,i}(i) = X_{t,k}(i) + \bar{Z}_{t,k}(i)$, where $X_{t,k}(i)$ and $\bar{Z}_{t,k}(i)$ are independent, and the covariance matrix of $\bar{Z}_i$ is $K_t = \rho^2 I_N$, where $0 < \rho \leq \min \left\{\frac{1}{\left|\left|H_{c}^T\right|\right|^2 + \left|\left|G_{c}\right|\right|^2}\right\}$. Thus, $\text{Var}\left(\bar{X}_{t,k}(i)\right)$ is upper bounded as
\[
\text{Var}\left(\bar{X}_{t,k}(i)\right) = \text{Var}(X_{t,k}(i)) + \text{Var}(Z_{t,k}(i)) \leq E\left(\left|X_{t,k}(i)\right|^2\right) + \rho^2 \leq P + \rho^2.
\]
(206)
(207)
Thus, for $i = 1, 2, \ldots, n$ and $k = 1, 2, \ldots, N$, we have
\[
h(\bar{X}_{t,k}(i)) \leq \log 2\pi e + \log(\rho^2 + P).
\]
(208)
Similarly, using the power constraint at the cooperative jammer, we have, for $i = 1, \ldots, n$ and $m = 1, \ldots, K$,
\[
h(\bar{X}_{c,m}(i)) \leq \log 2\pi e + \log(\rho^2 + P).
\]
(209)

**Appendix C**

**Proof of Lemma 1**

Consider two matrices $Q \in C^{M \times K}$ and $W \in C^{K \times N}$ such that $Q$ is full row-rank and $W$ has all of its entries independently drawn from a continuous distribution, where $K > N, M$. Let $L = \min\{N, M\}$. We show that $QW$ has a rank $L$ a.s. The matrices $Q$ and $W$ can be written as
\[
Q = \begin{bmatrix} q_1 & q_2 & \cdots & q_K \end{bmatrix},
\]
(210)
\[
W = \begin{bmatrix} w_1 & w_2 & \cdots & w_N \end{bmatrix},
\]
(211)
where $q_1, q_2, \ldots, q_K$ are the $K$-length-$M$ column vectors of $Q$, and $w_1, w_2, \ldots, w_N$ are the $N$ length-$K$ column vectors of $W$.

Let $w_{m,i}$ denotes the entry in the $m$th row and $i$th column of $W$. Let $QW = [s_1, s_2, \ldots, s_N]$, where $s_i$ is a length-$M$ column vector, $i = 1, 2, \ldots, N$. When $M \geq N$, $QW = [s_1, s_2, \ldots, s_L]$, and when $M < N$, $\{s_1, s_2, \ldots, s_L\}$ are the first $L$ columns of $QW$. In order to show that the matrix $QW$ has rank $L$, we show that, in either case, $\{s_1, s_2, \ldots, s_L\}$ are a.s. linearly independent, i.e.,
\[
\sum_{i=1}^{L} \lambda_i s_i = 0_{M \times 1}
\]
(212)
and if only if $\lambda_i = 0$ for all $i = 1, 2, \ldots, L$.

Each $s_i$, for $i = 1, 2, \ldots, L$, can be viewed as a linear combination of the $K$ columns of $Q$ with coefficients that are the entries of the $i$th column of $W$, i.e.,
\[
s_i = \sum_{m=1}^{K} w_{m,i} q_m.
\]
(213)
Using (213), we can rewrite (212) as
\[
\sum_{m=1}^{K} \varphi_m q_m = 0_{M \times 1}
\]
(214)
where, for $m = 1, 2, \ldots, K$,
\[
\varphi_m = \sum_{i=1}^{L} \lambda_i w_{m,i}.
\]
(215)
The $K$ columns of $Q$ are linearly dependent since each of them is of length $M$ and $K > M$. Thus, equation (214) has infinitely many solutions for $\{\varphi_m\}_{m=1}^{K}$.

Each of these solutions for $\varphi_m$’s constitutes a system of $K$ linear equations $\{\varphi_m = \sum_{i=1}^{L} \lambda_i w_{m,i}, m = 1, 2, \ldots, K\}$. The number of unknowns in this system, i.e., $\lambda$’s, is $L$. Since the number of equations in this system, $K$, is greater than the number of unknowns, $L$, this system has a solution for $\{\lambda_i\}_{i=1}^{L}$ only if the elements $\{w_{m,i} : m = 1, 2, \ldots, K, \text{ and } i = 1, 2, \ldots, L\}$ are dependent. Since the entries of $W$ are all randomly and independently drawn from some continuous distribution, the probability that these entries are dependent is zero.

Moreover, consider the set with infinite cardinality, where each element in this set is a structured $W$ that causes the system of equations in (215) to have a solution for $\{\lambda_i\}_{i=1}^{L}$ for one of the infinitely many solutions of $\{\varphi_m\}_{m=1}^{K}$ to (214). This set with infinite cardinality has a measure zero in the space $C^K \times L$, since this set is a subspace of $C^K \times L$ with a dimension strictly less than $K \times L$. We conclude that (212) a.s. has no non-zero solution for $\{\lambda_i\}_{i=1}^{L}$. Thus, $QW$ has rank $L$ a.s.

If $QW$ has rank $L$ a.s., then so does $(QW)^T = W^T Q^T$. 0018-9448 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Setting $E_1 = W^T$ and $E_2 = Q^T$, we have $E_i \in \mathbb{C}^{N \times K}$ has all of its entries independently drawn from some continuous distribution, $E_2 \in \mathbb{C}^{K \times M}$ is full column-rank, $K > N, M$, and $E_1 E_2$ has rank $L = \min\{N, M\}$ a.s. Thus, Lemma 1 is proved.

**APPENDIX D**

**DERIVATION OF (89) AND (90)**

The power constraints at the transmitter and cooperative jammer are $E \left( X_t^H X_t \right) \leq P$ and $E \left( X_c^H X_c \right) \leq P$. Using (72), we have

$$E \left( X_t^H X_t \right) = E \left( U_t^H U_t \right) \leq P$$

(216)

$$= \sum_{i=1}^d \sum_{m=1}^d p_{t,i}^H p_{t,i} E \left( U_{m,i}^* U_{m,i} \right)$$

(217)

$$= \sum_{i=1}^d \| p_{t,i} \|^2 E \left( | U_{i} |^2 \right)$$

(218)

$$= \| p_{t,1} \|^2 E \left( | U_{1} |^2 \right) + \sum_{i=2}^d \| p_{t,i} \|^2 \left( E \left( U_{i,1}^2 \right) + E \left( U_{i,1m}^2 \right) \right)$$

(219)

$$\leq \left( \| p_{t,1} \|^2 + 2 \sum_{i=2}^d \| p_{t,i} \|^2 \right) a^2 Q^2,$$

(220)

where (218) follows since $U_i$ and $U_m$, for $i \neq m$, are independent, and (220) follows since $E \left( U_{1,i}^2 \right)$, $E \left( U_{2,i}^2 \right)$, $E \left( U_{1,1m}^2 \right)$ $\leq a^2 Q^2$, for $i = 2, 3, \ldots, d$.

Similarly, using (72) and (87), we have

$$E \left( X_c^H X_c \right) = E \left( V_c^H P_c^H P_c V_c \right) = \sum_{i=1}^l E \left( | V_i |^2 \right)$$

(221)

$$= E \left( V_1^2 \right) + \sum_{i=2}^l E \left( V_{i,1}^2 \right)$$

(222)

$$\leq \left( 2l - 1 \right) a^2 Q^2.$$  

(223)

From (220) and (223), in order to satisfy the power constraints, we need that

$$a^2 Q^2 \leq \gamma^2 P,$$

(224)

where

$$\gamma = \frac{1}{\max \left\{ 2l - 1, \| p_{t,1} \|^2 + 2 \sum_{i=2}^d \| p_{t,i} \|^2 \right\}}.$$  

(225)

Let us choose the integer $Q$ as

$$Q = \left\lfloor \frac{P}{a^2 Q^2 \gamma} \right\rfloor = P^* \frac{1}{2} - \nu,$$

(226)

where $\nu$ is a constant which does not depend on the power $P$. Thus,

$$a = \gamma P^* \frac{1}{2},$$

(227)

satisfies the condition in (224). Thus, the power constraints at the transmitter and cooperative jammer are satisfied.

**REFERENCES**


