The Secrecy Capacity of Gaussian MIMO Channels With Finite Memory

Nir Shlezinger, *Student Member, IEEE*, Daniel Zahavi, *Student Member, IEEE*, Yonathan Murin, *Member, IEEE*, and Ron Dabora, *Senior Member, IEEE*

***Abstract*— In this paper, we study the secrecy capacity of Gaussian multiple-input multiple-output (MIMO) wiretap channels (WTCs) with a *finite memory*, subject to a per-symbol average power constraint on the MIMO channel input. MIMO channels with finite memory are very common in wireless communications as well as in wireline communications (e.g., in communications over power lines). To derive the secrecy capacity of the Gaussian MIMO WTC with finite memory, we first construct an asymptotically equivalent block-memoryless MIMO WTC, which is then transformed into a set of parallel, independent, memoryless MIMO WTCs in the frequency domain. The secrecy capacity of the Gaussian MIMO WTC with finite memory is obtained as the secrecy capacity of the set of parallel, independent, memoryless MIMO WTCs, and is expressed as maximization over the input covariance matrices in the frequency domain. Finally, we detail two applications of our result: First, we show that the secrecy capacity of the Gaussian *scalar* WTC with *finite memory* can be achieved by waterfilling, and obtain a closed-form expression for this secrecy capacity. Then, we use our result to characterize the secrecy capacity of narrowband powerline channels, thereby resolving one of the major open issues for this channel model.**

***Index Terms*— Physical layer security, MIMO channels, channels with memory, wiretap channels.**

I. Introduction

ONE of the main challenges in the design of communications schemes for shared channels is to reliably transmit information to a destination, while keeping potential eavesdroppers ignorant of the transmitted information. The fundamental model for studying secure physical-layer communications over shared mediums is the *wiretap channel* (WTC) model [1], which consists of three terminals: A transmitter (Tx), an intended receiver (Rx), and an eavesdropper (Ev). The secrecy capacity is defined as the maximum information rate for reliable Tx–Rx communications such that the rate of information leaked to the eavesdropper asymptotically vanishes. The initial study of WTCs detailed in [1], considered memoryless WTCs in which the channel inputs and the channel outputs are discrete random variables (RVs) with finite alphabets, and the Tx–Ev channel is a physically degraded version of the Tx–Rx channel. The general discrete memoryless WTC was studied in [2], which characterized its secrecy capacity by introducing a virtual channel, also referred to as *prefix channel* [3, Ch. 3.5].

Memoryless scalar WTCs with additive white Gaussian noise (AWGN) were first studied in [4], which made three important observations: (1) No prefix channel is required, (2) Gaussian codebooks are optimal, and (3) The secrecy capacity is zero when the noise power at the intended receiver is equal to or greater than the noise power at the eavesdropper. Several works studied the fundamental limits of secure communications over memoryless WTCs with AWGN and multiple antennas at the terminals, referred to as the multiple-input multiple-output (MIMO) WTC: The work [5] considered the scenario of two antennas at the Tx, two antennas at the Rx, and one antenna at the Ev, where the channel input is subject to a per-codeword average power constraint. The secrecy capacity of MIMO WTCs with an arbitrary number of antennas at each node was derived in [6] subject to a per-codeword average power constraint, and in [7] subject to a per-symbol average power constraint. An alternative derivation of the secrecy capacity of MIMO WTCs was carried out in [8], subject to a more general input covariance matrix constraint. In [8, Corollary 1] it is shown that the secrecy capacity subject to a per-codeword average power constraint on the input can be obtained as a corollary of the main result of [8]. The more general scenario of AWGN MIMO broadcast channels with confidential messages was studied in [9]–[11]. Similarly to the scalar Gaussian case, the secrecy capacity of MIMO WTCs with AWGN is achieved by using a Gaussian codebook without channel prefixing, where the secrecy capacity expression is stated as an optimization over all possible input covariance matrices which satisfy a specified power constraint. This optimization problem was shown to be non-convex [6], [12]–[14], and methods for approaching the maximizing input covariance matrix were proposed in several works. In particular, [12] proposed an algorithm based on alternating optimization for approaching the optimal covariance matrix, [13] studied the conditions for the covariance matrix to be full rank and characterized the optimal covariance matrix for this case, and in [14] rank deficient solutions for the optimal covariance matrix were proposed. Secrecy in the presence of temporally correlated Gaussian noise was studied in [15], which considered *scalar degraded*

Manuscript received August 9, 2015; revised October 26, 2016; accepted December 19, 2016. Date of publication January 4, 2017; date of current version February 14, 2017. This work was supported by the Ministry of Economy of Israel through the Israeli Smart Grid Consortium. This paper was presented at the 2015 IEEE International Symposium on Information Theory.

N. Shlezinger, D. Zahavi, and R. Dabora are with the Department of Electrical and Computer Engineering, Ben-Gurion University, Be'er-Sheva 8410501, Israel (e-mail: nirshl@post.bgu.ac.il; zahavida@post.bgu.ac.il; ron@ee.bgu.ac.il).

Y. Murin is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305, USA (e-mail: moriny@stanford.edu).

Communicated by A. Khisti, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2017.2648742

block-memoryless WTCs with additive colored Gaussian noise. Additional scenarios of physical-layer security in modern networks include fading WTCs, studied in [16]–[18], independent parallel channels, studied in [19], [20], and an achievable secrecy rate for multi-carrier systems, characterized in [21] and [22]. The wiretap framework was further extended to multi-user channels in [23]–[26] (see also detailed surveys in [27], [3, Ch. 8], and [28, Ch. 22]). The secrecy capacity of arbitrary wiretap channels was studied in [29], yet, the expression derived in [29, Thm. 1] is rather involved and does not identify the input distribution which maximizes the secrecy rate. Finally, we note that a suboptimal precoding scheme for block frequency-selective scalar WTCs with AWGN was proposed in [30].

In this paper we study the secrecy capacity of MIMO Gaussian WTCs with finite memory, i.e., MIMO Gaussian WTCs in which the channel introduces intersymbol interference (ISI) of a finite duration at each receive antenna, and the noise is an additive stationary colored Gaussian process whose temporal correlation has a finite length. This channel model applies to many communications scenarios, including wireless communications and power line communications. However, despite the importance of this model as a fundamental model for secure modern communications, the secrecy capacity of Gaussian *finite-memory* MIMO WTCs and also of Gaussian *finite-memory* scalar WTCs *has not been characterized to date*.

***Main Contributions*:** In this paper we derive the secrecy capacity of Gaussian MIMO WTCs with finite memory, subject to a per-MIMO symbol average power constraint on the channel input, where the transmitter knows both the Tx-Rx channel and the Tx-Ev channel. To this aim, we first construct a block-memoryless Gaussian MIMO WTC based on the characteristics of the original finite-memory Gaussian MIMO WTC, and prove that the two channel models are asymptotically equivalent. Then, we transform the block-memoryless channel into an equivalent set of parallel memoryless Gaussian MIMO WTCs, for which the secrecy capacity has been characterized in [19]. Our derivation uses concepts from the derivation of the (non-secure) capacity of finite-memory Gaussian point-to-point channels [31], multiple-access channels (MACs) [32], and broadcast channels (BCs) [33], as well as introduce novel techniques and schemes for the analysis of the information leakage rate at the eavesdropper. For the special case of the *scalar* Gaussian WTC with *finite memory*, we show that the secrecy capacity can be obtained via the waterfilling power allocation scheme, and demonstrate the resulting rate via a numerical example. Finally, we show how our result directly leads to the secrecy capacity of narrowband powerline communications (PLC) channels, which is a major challenge in smart grid communications networks [34]. Our results provide insights on the relationship between these seemingly different problems.

The rest of this paper is organized as follows: Section II introduces the problem formulation; Section III derives the secrecy capacity for finite-memory Gaussian MIMO WTCs; Section IV discusses the results and their application to PLC, and provides a numerical example; Lastly, Section V provides some concluding remarks.

II. Notations and Problem Formulation

A. Notations

We use upper-case letters to denote random variables (RVs), e.g., X, and calligraphic letters to denote sets, e.g., $\mathcal{X}$. We denote column vectors with boldface letters, e.g., $\mathbf{X}$; the k-th element of a vector $\mathbf{X}$ ($k \geq 0$) is denoted with $(\mathbf{X})_k$. Matrices are denoted with Sans-Sarif fonts, e.g., M; the element at the k-th row and the l-th column of a matrix M is denoted by $(\mathsf{M})_{k,l}$. We use I_a to denote the $a \times a$ identity matrix, and $\mathsf{0}_{a\times b}$ to denote the all-zero $a \times b$ matrix. Hermitian transpose, transpose, trace, complex conjugate, and stochastic expectation are denoted by $(\cdot)^H$, $(\cdot)^T$, $\mathrm{Tr}(\cdot)$, $(\cdot)^*$, and $\mathbb{E}\{\cdot\}$, respectively. We use $I(X;Y)$ to denote the mutual information between the RVs $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$, $H(X)$ to denote the entropy of a discrete RV X, $h(X)$ to denote the differential entropy of a continuous RV X, and $p(X)$ to denote the probability density function (PDF) of a continuous RV X. The symbol $\stackrel{d}{=}$ denotes equality in distribution, and we use j to denote $\sqrt{-1}$; All logarithms are taken to base 2. The sets of integers, non-negative integers, real numbers, and complex numbers are denoted by $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{R}$, and $\mathbb{C}$, respectively. We use $((a))_b$ to denote "a modulo b", i.e., writing $c = ((a))_b$ implies that c is satisfies the relationship $a = k \cdot b + c$, where $k \in \mathbb{Z}$ and $0 \leq c < b$. We use a^+ to denote $\max\{0, a\}$, and $|\cdot|$ to denote the magnitude when applied to scalars, and the determinant operator when applied to matrices.

For any sequence, possibly multivariate, $\mathbf{q}[i]$, $i \in \mathbb{Z}$, and for any pair of integers, a_1, a_2, satisfying $a_1 < a_2$, we use $\mathbf{q}_{a_1}^{a_2}$ to denote the column vector obtained by stacking $\left[\mathbf{q}[a_1]^T, \mathbf{q}[a_1+1]^T \ldots, \mathbf{q}[a_2]^T\right]^T$ and define $\mathbf{q}^{a_2} \equiv \mathbf{q}_0^{a_2}$. Lastly, we define the discrete Fourier transform (DFT) of a real multivariate sequence as follows: For some $n_q \in \mathbb{N}$, let $\left\{\hat{\mathbf{q}}[k]\right\}_{k=0}^{n-1}$ denote the n-point DFT of the multivariate sequence $\{\mathbf{q}[i]\}_{i=0}^{n-1}$, $\mathbf{q}[i] \in \mathbb{R}^{n_q}$. The sequence $\left\{\hat{\mathbf{q}}[k]\right\}_{k=0}^{n-1}$ is computed via

$$\hat{\mathbf{q}}[k] = \sum_{i=0}^{n-1} \mathbf{q}[i] e^{-j2\pi \frac{ik}{n}}, \tag{1}$$

$k \in \{0, 1, \ldots, n-1\} \triangleq \mathcal{N}$.

B. Channel Model

We consider the $n_t \times n_r \times n_e$ MIMO WTC with finite memory. Let m be a non-negative integer which denotes the *length of the memory of the channel*, and let $\mathbf{W}[i] \in \mathbb{R}^{n_r}$ and $\mathbf{U}[i] \in \mathbb{R}^{n_e}$ be two multivariate, zero-mean stationary real Gaussian processes with autocorrelation functions $\mathsf{C}_{\mathbf{W}}[\tau] \triangleq \mathbb{E}\left\{\mathbf{W}[i+\tau](\mathbf{W}[i])^T\right\}$ and $\mathsf{C}_{\mathbf{U}}[\tau] \triangleq \mathbb{E}\left\{\mathbf{U}[i+\tau](\mathbf{U}[i])^T\right\}$, respectively. We assume that $\mathbf{W}[i_1]$ and $\mathbf{U}[i_2]$ are uncorrelated $\forall i_1, i_2 \in \mathbb{Z}$, and that $\mathsf{C}_{\mathbf{W}}[\tau] = \mathsf{0}_{n_r\times n_r}$ and $\mathsf{C}_{\mathbf{U}}[\tau] = \mathsf{0}_{n_e\times n_e}$ for all $|\tau| > m$. We further assume that none of the samples of $\mathbf{W}[i]$ and $\mathbf{U}[i]$ are deterministically dependent, i.e., there is no index i_0 for which either $\mathbf{W}[i_0]$ or $\mathbf{U}[i_0]$ can be expressed as a linear combination of $\{\mathbf{W}[i]\}_{i\neq i_0}$ and $\{\mathbf{U}[i]\}_{i\neq i_0}$, respectively. Let $\{\mathsf{H}[\tau]\}_{\tau=0}^{m}$ denote the real $n_r \times n_t$ Tx–Rx channel transfer matrices and $\{\mathsf{G}[\tau]\}_{\tau=0}^{m}$ denote the real $n_e \times n_t$ Tx–Ev channel

transfer matrices. The channel transfer matrices, $\{\mathsf{H}[\tau]\}_{\tau=0}^{m}$ and $\{\mathsf{G}[\tau]\}_{\tau=0}^{m}$, and the autocorrelation functions of the noises, $\mathsf{C}_{\mathbf{W}}[\tau]$ and $\mathsf{C}_{\mathbf{W}}[\tau]$, $\tau \in \mathbb{Z}$, are assumed to be a-priori known at the transmitter. We refer to this assumption as Tx-CSI. The input-output relationships for the linear time-invariant (LTI) Gaussian MIMO WTC (LGMWTC) are given by

$$\mathbf{Y}[i] = \sum_{\tau=0}^{m} \mathsf{H}[\tau]\mathbf{X}[i-\tau] + \mathbf{W}[i] \tag{2a}$$

$$\mathbf{Z}[i] = \sum_{\tau=0}^{m} \mathsf{G}[\tau]\mathbf{X}[i-\tau] + \mathbf{U}[i], \tag{2b}$$

$i \in \{0, 1, \ldots, l-1\}$, $l \in \mathbb{N}$, where the channel inputs are subject to a per-MIMO symbol power constraint (hereafter referred to as per-symbol power constraint for brevity)

$$\mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\} \leq P, \tag{3}$$

$i \in \{0, 1, \ldots, l-1\}$. We note that restricting the power of the information symbols at all time instants, rather than over the entire codeword, is very common in the design of practical communications systems, since the dynamic range of practical power amplifiers is limited [35, Ch. 09], rendering it impossible for transmitters to "store" power for later channel uses. This constraint is therefore a natural model for energy-constrained channels [31, Sec. I-A]. It should also be noted that similar constraints were used in related works, e.g., the derivation of the secrecy capacity of memoryless MIMO channels in [7], as well as in the derivation of some major information theoretic results including [31], [36, Section VII], and [37].

In this work we characterize the secrecy capacity of the LGMWTC.

C. Definitions

The framework used in this study is based on the following definitions:

Definition 1: A MIMO WTC with memory, in which the transmitter has n_t antennas, the intended receiver has n_r antennas, and the eavesdropper has n_e antennas, abbreviated as the $n_t \times n_r \times n_e$ MIMO WTC, consists of an input stream $\mathbf{X}[i] \in \mathbb{R}^{n_t}$, two output streams $\mathbf{Y}[i] \in \mathbb{R}^{n_r}$ and $\mathbf{Z}[i] \in \mathbb{R}^{n_e}$, observed by the intended receiver and by the eavesdropper, respectively, $i \in \mathbb{N}$, an initial state $\mathbf{S}_0 \in \mathcal{S}_0$, and a sequence of transition probabilities $\left\{p\left(\mathbf{Y}^{l-1}, \mathbf{Z}^{l-1} | \mathbf{X}^{l-1}, \mathbf{S}_0\right)\right\}_{l=1}^{\infty}$.

In this work we focus on the LGMWTC, which is an instance of the general class of MIMO WTCs with memory defined above. From Def. 1 it follows that the initial state of the LGMWTC is given by $\mathbf{S}_0 = \left[\left(\mathbf{X}_{-m}^{-1}\right)^T, \left(\mathbf{W}_{-m}^{-1}\right)^T, \left(\mathbf{U}_{-m}^{-1}\right)^T\right]^T$. Note that complex MIMO WTCs with memory can be accommodated by the setup of Def. 1 by representing all complex vectors using real vectors having twice the number of elements and, representing the complex channel matrices using real matrices having four times the number of elements, corresponding to the real parts and the imaginary parts of the entries, see, e.g., [37, Sec. I].

Definition 2: An $[R, l]$ code with rate R and blocklength $l \in \mathbb{N}$ for the WTC consists of: (1) A source of local randomness at the encoder represented by the RV $D \in \mathcal{D}$ with PDF $p(D)$. (2) An encoder e_l which maps a message M, uniformly distributed over $\mathcal{M} \triangleq \{0, 1, \ldots, 2^{lR} - 1\}$, and a realization of D into a codeword $\mathbf{X}^{l-1} \in \mathcal{X}^l$, i.e.,

$$e_l : \mathcal{M} \times \mathcal{D} \mapsto \mathcal{X}^l.$$

(3) A decoder d_l which maps the channel output $\mathbf{Y}^{l-1} \in \mathcal{Y}^l$ into a message $\hat{M} \in \mathcal{M}$. i.e.,

$$d_l : \mathcal{Y}^l \mapsto \mathcal{M}.$$

The source of local randomness D facilitates the random nature of the encoder, and it is emphasized that the realization of D is known only to the encoder.

Note that we follow the standard setup for channels with memory and let the encoder and decoder operate using only the l symbols corresponding to the currently transmitted codeword [31]–[33], [38, Ch. 5.9], [39]. The encoder is assumed to be independent of the initial state $\mathbf{S}_0$.

Definition 3: The average probability of error of an $[R, l]$ code, when the initial state is $\mathbf{s}_0$, is defined as:

$$P_e^l(\mathbf{s}_0) = \frac{1}{2^{lR}} \sum_{\tilde{m}=0}^{2^{lR}-1} \Pr\left(d_l\left(\mathbf{Y}^{l-1}\right) \neq \tilde{m} \,\middle|\, M = \tilde{m}, \mathbf{S}_0 = \mathbf{s}_0\right).$$

Definition 4: A secrecy rate R_s is achievable for a WTC if for every positive triplet $\epsilon_1, \epsilon_2, \epsilon_3 > 0$, $\exists l_0 > 0$ such that $\forall l > l_0$ there exists an $[R, l]$ code which satisfies:

$$\sup_{\mathbf{s}_0 \in \mathcal{S}_0} P_e^l(\mathbf{s}_0) \leq \epsilon_1, \tag{4a}$$

$$\sup_{\mathbf{s}_0 \in \mathcal{S}_0} \frac{1}{l} I\left(M; \mathbf{Z}^{l-1} \,\middle|\, \mathbf{S}_0 = \mathbf{s}_0\right) \leq \epsilon_2, \tag{4b}$$

and

$$R \geq R_s - \epsilon_3. \tag{4c}$$

Def. 4 extends the definition of codes for memoryless WTCs stated in [3, Ch. 3.5], [28, Ch. 22.1] to finite-memory WTCs. The term $\frac{1}{l} I\left(M; \mathbf{Z}^{l-1} \,\middle|\, \mathbf{S}_0 = \mathbf{s}_0\right)$ represents the maximum achievable information rate at the eavesdropper, while *the eavesdropper knows the initial state*. This achievable rate is referred to as the *information leakage rate* [3, Ch. 3.4].

Definition 5: The secrecy capacity is defined as the supremum of all achievable secrecy rates.

Definition 6: A WTC is said to be memoryless if for every non-negative integer i

$$p\left(\mathbf{Y}[i], \mathbf{Z}[i] \,\middle|\, \mathbf{Y}^{i-1}, \mathbf{Z}^{i-1}, \mathbf{X}^{i}, \mathbf{S}_0\right) = p\left(\mathbf{Y}[i], \mathbf{Z}[i] \,\middle|\, \mathbf{X}[i]\right).$$

Def. 6 corresponds to the general notion of memoryless channels as in, e.g., [41, Sec. II-A]. Note that if there is no feedback to the transmitter, it follows that $p\left(\mathbf{X}[i] \middle| \mathbf{X}^{i-1}, \mathbf{Y}^{i-1}, \mathbf{Z}^{i-1}, \mathbf{S}_0\right) = p\left(\mathbf{X}[i] \middle| \mathbf{X}^{i-1}\right)$. Then, Def. 6 implies that for every positive integer l,

$$p\left(\mathbf{Y}^{l-1}, \mathbf{Z}^{l-1} | \mathbf{X}^{l-1}, \mathbf{S}_0\right) = \prod_{i=0}^{l-1} p\left(\mathbf{Y}[i], \mathbf{Z}[i] \middle| \mathbf{X}[i]\right), \tag{5}$$

which also coincides with the definition of memoryless WTCs stated in [3, Ch. 3.5]. We henceforth assume that no feedback is present in any of the channels considered.

Definition 7: A WTC is said to be n-block memoryless if for every positive integer b

$$p\left(\mathbf{Y}^{n\cdot b-1},\mathbf{Z}^{n\cdot b-1}|\mathbf{X}^{n\cdot b-1},\mathbf{S}_0\right) = \prod_{\tilde{b}=1}^{b} p\left(\mathbf{Y}_{n\cdot(\tilde{b}-1)}^{n\cdot\tilde{b}-1},\mathbf{Z}_{n\cdot(\tilde{b}-1)}^{n\cdot\tilde{b}-1}|\mathbf{X}_{n\cdot(\tilde{b}-1)}^{n\cdot\tilde{b}-1}\right).$$

Def. 7 corresponds to the definition of n-block memoryless BCs stated in [33, Eq. (8)]. Note that codewords of any length can be transmitted over n-block memoryless channels, however, when the length of the codeword is an integer multiple of the channel block memory n, then the average probability of error is independent of the initial state $\mathbf{S}_0$ [33, Sec. II], and similarly, the information leakage rate is also independent of $\mathbf{S}_0$. This follows since the outputs of the channels at the receiver and at the eavesdropper corresponding to the transmitted codeword are independent of the initial channel state, by the definition of the channel.

III. The Secrecy Capacity of the LGMWTC

Our main result is the characterization of the secrecy capacity of the LTI Gaussian MIMO WTC with finite memory, defined in Subsection II-B. This secrecy capacity is stated in the following theorem:

Theorem 1: Consider the LGMWTC defined in (2) *subject to the per-symbol power constraint* (3) *and with Tx-CSI. Define* $\mathsf{C}'_{\mathbf{W}}(\omega) \triangleq \sum_{\tau=-m}^{m} \mathsf{C}_{\mathbf{W}}[\tau]\, e^{-j\omega\tau}$, $\mathsf{C}'_{\mathbf{U}}(\omega) \triangleq \sum_{\tau=-m}^{m} \mathsf{C}_{\mathbf{U}}[\tau]\, e^{-j\omega\tau}$, $\mathsf{H}'(\omega) \triangleq \sum_{\tau=0}^{m} \mathsf{H}[\tau]\, e^{-j\omega\tau}$, *and* $\mathsf{G}'(\omega) \triangleq \sum_{\tau=0}^{m} \mathsf{G}[\tau]\, e^{-j\omega\tau}$.

Let $\mathcal{C}_P$ denote the set of $n_t \times n_t$ positive semi-definite Hermitian matrix functions $\mathsf{C}'_{\mathbf{X}}(\omega)$, defined over the interval $\omega \in [0,\pi)$, such that

$$\frac{1}{\pi}\int_{\omega=0}^{\pi} \mathrm{Tr}\left(\mathsf{C}'_{\mathbf{X}}(\omega)\right) d\omega \le P, \tag{6a}$$

and define $\psi(\omega)$ as:

$$\psi(\omega) \triangleq \frac{\left|\mathsf{I}_{n_r} + \mathsf{H}'(\omega)\mathsf{C}'_{\mathbf{X}}(\omega)\left(\mathsf{H}'(\omega)\right)^H\left(\mathsf{C}'_{\mathbf{W}}(\omega)\right)^{-1}\right|}{\left|\mathsf{I}_{n_e} + \mathsf{G}'(\omega)\mathsf{C}'_{\mathbf{X}}(\omega)\left(\mathsf{G}'(\omega)\right)^H\left(\mathsf{C}'_{\mathbf{U}}(\omega)\right)^{-1}\right|}. \tag{6b}$$

Then, the secrecy capacity of the LGMWTC is given by

$$C_s = \max_{\mathsf{C}'_{\mathbf{X}}(\omega)\in\mathcal{C}_P} \frac{1}{2\pi}\int_{\omega=0}^{\pi} \log\psi(\omega)\, d\omega. \tag{6c}$$

In the proof we use elements from the capacity derivation for the finite-memory MAC [32] and BC [33], as well as novel approach and techniques for analyzing the information leakage rate.

***Proof Outline*:** First, for $n > 2m$, we define the n-block memoryless circular Gaussian MIMO wiretap channel (n-CGMWTC) as follows: Let $\underset{\sim}{\mathbf{W}}[i]$ and $\underset{\sim}{\mathbf{U}}[i]$ be zero mean multivariate Gaussian processes, whose autocorrelation functions, denoted $\mathsf{C}_{\underset{\sim}{\mathbf{W}}}[\tau]$ and $\mathsf{C}_{\underset{\sim}{\mathbf{U}}}[\tau]$, respectively, are defined by

$$\mathsf{C}_{\underset{\sim}{\mathbf{W}}}[\tau] \triangleq \mathsf{C}_{\mathbf{W}}[\tau] + \mathsf{C}_{\mathbf{W}}[\tau+n] + \mathsf{C}_{\mathbf{W}}[\tau-n], \tag{7a}$$

$$\mathsf{C}_{\underset{\sim}{\mathbf{U}}}[\tau] \triangleq \mathsf{C}_{\mathbf{U}}[\tau] + \mathsf{C}_{\mathbf{U}}[\tau+n] + \mathsf{C}_{\mathbf{U}}[\tau-n], \tag{7b}$$

when the noise samples belong to the same n-block. Noise samples that belong to different n-blocks are independent since the channel is n-block memoryless. The outputs of the n-CGMWTC over any given n-block, i.e., for $i = 0, 1, \ldots, n-1$, are defined as

$$\underset{\sim}{\mathbf{Y}}[i] = \sum_{\tau=0}^{m} \mathsf{H}[\tau]\mathbf{X}\left[((i-\tau))_n\right] + \underset{\sim}{\mathbf{W}}[i] \tag{8a}$$

$$\underset{\sim}{\mathbf{Z}}[i] = \sum_{\tau=0}^{m} \mathsf{G}[\tau]\mathbf{X}\left[((i-\tau))_n\right] + \underset{\sim}{\mathbf{U}}[i]. \tag{8b}$$

The n-CGMWTC is subject to the same per-symbol average power constraints as the LGMWTC, stated in (3). Note that the definition of the n-CGMWTC is a natural extension of the definition of the n-block memoryless circular Gaussian channel (without secrecy), defined in [33, Sec. II], to secure communications.

The proof now proceeds in the following steps:

- In Subsection III-A, we prove that the secrecy capacity of the LGMWTC can be obtained from the secrecy capacity of the n-CGMWTC by taking $n \to \infty$. Note that while the asymptotic relationship between finite-memory channels and their circular block-memoryless counterparts has been used in the (non-secure) capacity analysis of finite-memory Gaussian channels in, e.g., [31], [32], and [33], to the best of our knowledge, this is the first time this approach is applied in the study of the secrecy capacity, and in such scenarios analyzing the *information leakage* presents a substantial challenge, as is evident from the analysis in Appendix A.
- Next, in Subsection III-B, we derive a closed-form expression for the secrecy capacity of the n-CGMWTC for a finite n.
- Lastly, in Subsection III-C, we let $n \to \infty$ and use the capacity expression derived for the n-CGMWTC in Subsection III-B, to obtain an explicit optimization problem whose maximal solution is the secrecy capacity of the LGMWTC.

A. Equivalence Between the Secrecy Capacity of the LGMWTC and the Asymptotic Secrecy Capacity of the n-CGMWTC

We now show that the secrecy capacity of the finite-memory LTI Gaussian MIMO WTC can be obtained as the secrecy capacity of the n-CGMWTC, by taking $n \to \infty$. Letting C_s^{n-CG} denote the secrecy capacity of the n-CGMWTC, the result is summarized in the following proposition:

Proposition 1: The secrecy capacity of the LGMWTC defined in (2)*, subject to the power constraint* (3) *can be*

written as

$$C_s = \lim_{n\to\infty} C_s^{n-CG}. \tag{9}$$

Proof: We provide here an outline of the proof; The detailed proof is provided in Appendix A. First, recall that the n-CGMWTC is defined for $n > 2m$. Next, for $n > 2m$ we define the n-block memoryless Gaussian MIMO wiretap channel (n-MGMWTC) as follows: The n-MGMWTC is obtained from the LGMWTC by considering the last $n - m$ vector channel outputs out of each n-block at both the eavesdropper and the receiver, i.e., the outputs of the n-MGMWTC are defined as the outputs of the LGMWTC for $0 \leq ((i))_n \geq m$, while for $((i))_n < m$ the outputs of the n-MGMWTC are not defined, see, e.g., [40]. The n-MGMWTC is subject to the power constraint (3) on the channel input, similarly to the LGMWTC. With this definition, we formulate the secrecy capacity of the n-MGMWTC in the form of the result of Csiszár and Körner [2, Eq. (11)]. Note that since the LGMWTC is transformed into the n-MGMWTC by setting the first m vector channel outputs out of each n-block of channel outputs to be "undefined" (see also, e.g., [33, Appendix A]), then by construction the codeword transmission starts at the beginning of an n-block, i.e., an n-block begins at time $i = 0$. Next, we show that the secrecy capacity of the LGMWTC can be obtained as the secrecy capacity of the n-MGMWTC by taking $n \to \infty$. For non-secure communications over BCs, it immediately follows that the capacity of the n-block memoryless Gaussian BC is not larger than the capacity of the LTI Gaussian BC, as the n-block memoryless Gaussian BC is a special case of the LTI Gaussian BC, obtained by letting the intended receiver discard m channel outputs out of every block of n received channel outputs, as was already shown in [33, Appendix A]. However, in the secure setup, this no longer holds, as the decoder at the eavesdropper *cannot be forced to discard m vector channel outputs out of every block of n received channel outputs*, and we conclude that such an inequality relationship between the secrecy capacities of the n-MGMWTC and of the LGMWTC can be proved only for the asymptotic case $n \to \infty$. This presents a fundamental difference from non-secure scenarios as will be elaborated in Comment A.2 in Appendix A. Lastly, we show that in the asymptotic regime of $n \to \infty$, the n-MGMWTC and the n-CGMWTC have the same secrecy capacity, from which we conclude that C_s is the secrecy capacity of the n-CGMWTC, in the limit $n \to \infty$. ■

Comment 1: In the proof of Proposition 1 in Appendix A, the secrecy capacity of the n-MGMWTC is obtained from the secrecy capacity of a memoryless Gaussian MIMO channel in which the number of antennas is set to be an integer multiple of n. Consequently, the computation of the secrecy capacity of the n-MGMWTC for $n \to \infty$ becomes prohibitive, and the expression for the secrecy capacity of the n-MGMWTC provides only little insight on the characterization of the channel inputs that achieve the secrecy capacity. However, the secrecy capacity of the n-CGMWTC for $n \to \infty$ can be obtained as a maximization problem with a closed-form objective, as will be shown in the sequel. For this reason, the n-MGMWTC is only an intermediate step, and in order to obtain a useful characterization of C_s we consider the secrecy capacity of the n-CGMWTC.

Comment 2: As the secrecy capacity of the n-MGMWTC is independent of the initial channel state, we conclude that the secrecy capacity of the finite-memory Gaussian MIMO WTC is also independent of the initial state. This is intuitive as the finite-memory property of the channel makes the impact of the initial state vanish when considering very large blocklengths.

Comment 3: The coding scheme that achieves the secrecy capacity of the n-MGMWTC does not require a prefix channel. In Lemma A.5 it is shown that every achievable rate R_s for the LGMWTC can be approached by applying codes for the n-MGMWTC which approach the same R_s after adding a fixed number of zero symbols at the beginning of each codeword. Since in Lemma A.3 it is shown that the coding scheme that achieves the secrecy capacity for the n-MGMWTC does not require a prefix channel, it follows from this code construction that the coding scheme that achieves the secrecy capacity of the LGMWTC does not require a prefix channel. This conclusion simplifies the design of secure coding schemes for such channels.

B. Characterizing the Secrecy Capacity of the n-CGMWTC

Next, we derive C_s^{n-CG} for a fixed and finite $n > 2m$. The derivation begins with applying the DFT to each n-block of the n-CGMWTC. Let $\left\{\hat{\underset{\sim}{\mathbf{W}}}[k]\right\}_{k=0}^{n-1}$ and $\left\{\hat{\underset{\sim}{\mathbf{U}}}[k]\right\}_{k=0}^{n-1}$ be the n-point DFTs of $\{\underset{\sim}{\mathbf{W}}[i]\}_{i=0}^{n-1}$ and $\{\underset{\sim}{\mathbf{U}}[i]\}_{i=0}^{n-1}$, respectively, i.e., $\hat{\underset{\sim}{\mathbf{W}}}[k] \triangleq \sum_{i=0}^{n-1} \underset{\sim}{\mathbf{W}}[i] e^{-j2\pi\frac{ik}{n}}$ and $\hat{\underset{\sim}{\mathbf{U}}}[k] \triangleq \sum_{i=0}^{n-1} \underset{\sim}{\mathbf{U}}[i] e^{-j2\pi\frac{ik}{n}}$. Let $\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[k]$ and $\mathsf{C}_{\hat{\underset{\sim}{\mathbf{U}}}}[k]$ denote the covariance matrices of $\hat{\underset{\sim}{\mathbf{W}}}[k]$ and $\hat{\underset{\sim}{\mathbf{U}}}[k]$, respectively. Define $\hat{\mathsf{H}}[k] \triangleq \sum_{\tau=0}^{m} \mathsf{H}[\tau] e^{-j2\pi\frac{\tau k}{n}}$ and $\hat{\mathsf{G}}[k] \triangleq \sum_{\tau=0}^{m} \mathsf{G}[\tau] e^{-j2\pi\frac{\tau k}{n}}$. The secrecy capacity of the n-CGMWTC for a fixed and finite n is stated in the following proposition:

Proposition 2: Let $\hat{\mathcal{C}}_P^n$ denote the collection of n-sets of $n_t \times n_t$ positive semi-definite Hermitian matrices $\left\{\mathsf{C}_{\hat{\mathbf{X}}}[k]\right\}_{k=0}^{n-1}$, which satisfy $\mathsf{C}_{\hat{\mathbf{X}}}[k] = \left(\mathsf{C}_{\hat{\mathbf{X}}}[n-k]\right)^*$ for $\lfloor \frac{n}{2} \rfloor < k < n$, and

$$\sum_{k=0}^{n-1} \mathrm{Tr}\left(\mathsf{C}_{\hat{\mathbf{X}}}[k]\right) \leq n^2 P. \tag{10a}$$

Further define $\hat{\psi}[k]$ as:

$$\hat{\psi}[k] \triangleq \frac{\left|\mathsf{I}_{n_r} + \hat{\mathsf{H}}[k]\mathsf{C}_{\hat{\mathbf{X}}}[k]\left(\hat{\mathsf{H}}[k]\right)^H\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[k]\right)^{-1}\right|}{\left|\mathsf{I}_{n_e} + \hat{\mathsf{G}}[k]\mathsf{C}_{\hat{\mathbf{X}}}[k]\left(\hat{\mathsf{G}}[k]\right)^H\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{U}}}}[k]\right)^{-1}\right|}. \tag{10b}$$

The secrecy capacity of the n-CGMWTC defined in (8)*, for a fixed and finite n, subject to the per-symbol constraint* (3) *is*

$$C_s^{n-CG} = \max_{\{\mathsf{C}_{\hat{\mathbf{X}}}[k]\}_{k=0}^{n-1} \in \hat{\mathcal{C}}_P^n} \frac{1}{2n} \sum_{k=0}^{n-1} \log \hat{\psi}[k]. \tag{10c}$$

Proof: A detailed proof is provided in Appendix B, and in the following we present only the outline of the proof: By applying the multivariate DFT to the channel outputs of the n-CGMWTC, we obtain an equivalent set of n MIMO WTCs in the frequency domain, such that each component WTC has no ISI and has additive Gaussian noise. We then show that the noise components in the equivalent set of n MIMO WTCs at different frequency indexes are mutually independent and that each noise component is a circularly symmetric complex normal random process, i.i.d. across different n-blocks. Next, *relaxing the power constraint to the per n-block power constraint*, it follows that the equivalent set of n parallel MIMO WTCs can be analyzed as a set of independent parallel memoryless MIMO WTCs with additive circularly symmetric complex normal noise, i.i.d. in time (here, we refer to the frequency index as "time"). The secrecy rate of the component MIMO WTCs *for a given power allocation*, has already been established in [6] and [7]. In Prop. 2 we state that the secrecy rate of the equivalent set of n MIMO WTCs subject to a given power allocation for each subchannel can be written as the sum of the secrecy rates of the independent subchannels, divided by the number of subchannels. In order to arrive at this expression, we use an obvious extension of [19, Thm. 1] to the memoryless Gaussian MIMO case. The secrecy capacity for the equivalent set of n parallel MIMO WTCs is obtained by maximizing over all secrecy rates which satisfy the relaxed sum-power constraint, eventually resulting in (10). Lastly, we show that the channel input which achieves the secrecy capacity satisfies the per-symbol average power constraint (3), hence (10) characterizes the secrecy capacity of the n-CGMWTC subject to (3). ∎

C. The Secrecy Capacity of the LGMWTC

In the final step, we first derive the asymptotic expression for C_s^{n-CG} in the limit of $n \to \infty$. Then, we obtain C_s as the limit $\lim_{n\to\infty} C_s^{n-CG}$. The asymptotic expression for $\lim_{n\to\infty} C_s^{n-CG}$ is stated in the following Proposition:

Proposition 3: $\lim_{n\to\infty} C_s^{n-CG}$ *converges to the expression in* (6).

Proof: Similarly to [31, Lemma 5], [33, Sec. V], and [42, Appendix A], we note that (10c) can be expressed as an average over n samples of a Riemann integrable even function over the range $[0, 2\pi)$. Thus, by definition of Riemann integrability [43, Ch. 6], it follows that for $n \to \infty$, (10c) converges to (6c), and that the energy constraint in (10a) asymptotically coincides with the energy constraint in (6a). ∎

From Proposition 1 it follows that $C_s = \lim_{n\to\infty} C_s^{n-CG}$. Therefore, it follows from Proposition 3 that C_s is given by (6), which completes the proof of Thm. 1.

IV. Discussion and Numerical Examples

In the following we discuss the insights obtained from the results derived above. In Subsection IV-A we present a necessary and sufficient condition for non-zero secrecy capacity; Then, in Subsection IV-B we present the application of our result to the characterization of the secrecy capacity of narrowband PLC channels; Lastly, in Subsection IV-C we show that the secrecy capacity of the *scalar* finite-memory LTI Gaussian WTC can be obtained in closed-form, and provide numerical examples.

A. Necessary and Sufficient Condition for $C_s > 0$

The secrecy capacity expression (6c) is the solution to a non-convex optimization problem (see, e.g., [6] for the memoryless case), which makes it hard to directly develop a practical interpretation. To assist with the understanding of Thm. 1 , we now present a necessary and sufficient condition for non-zero secrecy capacity, which follows from Thm. 1.

Proposition 4: Define $\mathsf{H}'_w(\omega) \triangleq \left(\mathsf{C}'_{\mathbf{W}}(\omega)\right)^{-\frac{1}{2}} \mathsf{H}'(\omega)$ *and* $\mathsf{G}'_w(\omega) \triangleq \left(\mathsf{C}'_{\mathbf{U}}(\omega)\right)^{-\frac{1}{2}} \mathsf{G}'(\omega)$. *The secrecy capacity of the LGMWTC is strictly positive if and only if* $\exists \Omega \subset [0, \pi)$ *with a non-zero Lebesgue measure, such that* $\forall \omega \in \Omega$

$$\sup_{\mathbf{v}(\omega)\in\mathbb{C}^{n_t\times 1}} \frac{\left\|\mathsf{H}'_w(\omega)\,\mathbf{v}(\omega)\right\|}{\left\|\mathsf{G}'_w(\omega)\,\mathbf{v}(\omega)\right\|} > 1. \tag{11}$$

Proof: The proof is similar to that of [6, Corollary 2], and is provided in Appendix C. ∎

Note that the vector $\mathbf{v}(\omega)$ can be considered as a beamforming vector. Therefore, Proposition 4 implies that the secrecy capacity is strictly positive only when there exists a continuous set of frequencies for which the sender can beamform the transmitted signal such that the intended receiver observes a higher SNR than the eavesdropper at each frequency in the set of frequencies.

B. Application: The Secrecy Capacity of Narrowband PLC Channels

An important application of our result is the characterization of the secrecy capacity of *scalar* PLC channels in the frequency range of $3 - 500$ kHz, referred to as narrowband (NB) PLC. NB-PLC plays an important role in the realization of smart power grids [44], in which secure communications is a critical issue [44]–[46]. Despite the importance of secure NB-PLC, to date there is no characterization of the secrecy capacity for this channel, which accounts for its unique characteristics [34]: The NB-PLC channel is a linear channel with additive noise , in which the channel impulse response (CIR) is commonly modeled as a real periodically time-varying signal with a finite memory [47], [48], while the additive noise is commonly modeled as a real cyclostationary Gaussian process with a finite correlation length [48], [49]. In the following we fill the knowledge gap of secure communications rates over NB-PLC channels by characterizing the secrecy capacity of the NB-PLC wiretap channel.

Let $W_{\mathrm{PLC}}[i]$ and $U_{\mathrm{PLC}}[i]$ be zero-mean scalar additive cyclostationary Gaussian noises (ACGNs), each with a period of t_{noise} and a temporal correlation which has a finite-duration, whose length is m_{noise}. Let m_{ch} be a non-negative integer representing the length of the memory of the NB-PLC CIR, and let $\{h_{\mathrm{PLC}}[i,\tau]\}_{\tau=0}^{m_{ch}}$ and $\{g_{\mathrm{PLC}}[i,\tau]\}_{\tau=0}^{m_{ch}}$ denote the channel coefficients of the Tx-Rx channel and of the Tx-Ev channel,

respectively, both with period[1] t_{ch}, i.e., $h_{\mathrm{PLC}}[i,\tau]=h_{\mathrm{PLC}}[i+t_{ch},\tau]$ and $g_{\mathrm{PLC}}[i,\tau]=g_{\mathrm{PLC}}[i+t_{ch},\tau]$, $\forall i,\in\mathbb{Z}$, $\forall\tau\in\{0,1,\ldots,m_{ch}-1\}$, and $h_{\mathrm{PLC}}[i,\tau]=g_{\mathrm{PLC}}[i,\tau]=0$, for all integer $\tau<0$ or $\tau>m_{ch}$. Let $m_{\mathrm{PLC}}=\max\{m_{ch},m_{noise}\}$. We use $X[i]$ to denote the transmitted scalar signal, and $Y_{\mathrm{PLC}}[i]$ and $Z_{\mathrm{PLC}}[i]$ to denote the channel outputs at the destination and at the eavesdropper, respectively, all at time i. The input-output relationships of the NB-PLC WTC can be written as

$$Y_{\mathrm{PLC}}[i]=\sum_{\tau=0}^{m_{\mathrm{PLC}}}h_{\mathrm{PLC}}[i,\tau]X[i-\tau]+W_{\mathrm{PLC}}[i] \quad (12a)$$

$$Z_{\mathrm{PLC}}[i]=\sum_{\tau=0}^{m_{\mathrm{PLC}}}g_{\mathrm{PLC}}[i,\tau]X[i-\tau]+U_{\mathrm{PLC}}[i]. \quad (12b)$$

Set n_{PLC} to be the least common multiple of t_{ch} and t_{noise} which satisfies $n_{\mathrm{PLC}}>m_{\mathrm{PLC}}$. We assume that the channel input is subject to an average power constraint

$$\frac{1}{l}\sum_{k=0}^{l-1}\mathbb{E}\left\{\left|X[i]\right|^2\right\}\le P, \quad (13a)$$

for any blocklength l, and we assume that for all $i\ge 0$ it holds that

$$\frac{1}{n_{\mathrm{PLC}}}\sum_{k=0}^{n_{\mathrm{PLC}}-1}\mathbb{E}\left\{\left|X[i\cdot n_{\mathrm{PLC}}+k]\right|^2\right\}\le P, \quad (13b)$$

i.e., over *any block of* n_{PLC} *symbols*, starting from the first transmitted symbol, the average power is upper bound by P. Applying the decimated components decomposition [50, Sec. 17.2] to the cyclostationary processes $W_{\mathrm{PLC}}[i]$ and $U_{\mathrm{PLC}}[i]$, we define the $n_{\mathrm{PLC}}\times 1$ multivariate processes $\mathbf{W}_{\mathrm{PLC}}\left[\tilde{i}\right]$ and $\mathbf{U}_{\mathrm{PLC}}\left[\tilde{i}\right]$, $\tilde{i}\in\mathbb{Z}$, whose elements are given by $\left(\mathbf{W}_{\mathrm{PLC}}\left[\tilde{i}\right]\right)_k=W_{\mathrm{PLC}}\left[\tilde{i}\cdot n_{\mathrm{PLC}}+k\right]$ and $\left(\mathbf{U}_{\mathrm{PLC}}\left[\tilde{i}\right]\right)_k=U_{\mathrm{PLC}}\left[\tilde{i}\cdot n_{\mathrm{PLC}}+k\right]$, respectively, $k\in\{0,1,\ldots,n_{\mathrm{PLC}}-1\}\triangleq\mathcal{N}_{\mathrm{PLC}}$. From [50, Sec. 17.2] it follows that $\mathbf{W}_{\mathrm{PLC}}\left[\tilde{i}\right]$ and $\mathbf{U}_{\mathrm{PLC}}\left[\tilde{i}\right]$ are each a stationary Gaussian process. Let $\mathsf{C}_{\mathbf{W}_{\mathrm{PLC}}}[\tilde{\tau}]$ and $\mathsf{C}_{\mathbf{U}_{\mathrm{PLC}}}[\tilde{\tau}]$ denote the autocorrelation function of $\mathbf{W}_{\mathrm{PLC}}\left[\tilde{i}\right]$ and the autocorrelation function of $\mathbf{U}_{\mathrm{PLC}}\left[\tilde{i}\right]$, respectively. Finally, let $\mathsf{H}_{\mathrm{PLC}}[\tilde{\tau}]$ and $\mathsf{G}_{\mathrm{PLC}}[\tilde{\tau}]$, $\tilde{\tau}\in\{0,1\}$, be $n_{\mathrm{PLC}}\times n_{\mathrm{PLC}}$ matrices whose entries at the k_1-th row and the k_2-th column are given in (14), as shown at the bottom of this page $\forall k_1,k_2\in\mathcal{N}_{\mathrm{PLC}}$.

The secrecy capacity of the NB-PLC WTC is stated in the following corollary:

Corollary 1: Consider the NB-PLC WTC defined in (12)*, subject to the power constraints* (13)*. Define* $\mathsf{C}'_{\mathbf{W}_{\mathrm{PLC}}}(\omega)\triangleq\sum_{\tilde{\tau}=-1}^{1}\mathsf{C}_{\mathbf{W}_{\mathrm{PLC}}}[\tilde{\tau}]e^{-j\omega\tilde{\tau}}$, $\mathsf{C}'_{\mathbf{U}_{\mathrm{PLC}}}(\omega)\triangleq\sum_{\tilde{\tau}=-1}^{1}\mathsf{C}_{\mathbf{U}_{\mathrm{PLC}}}[\tilde{\tau}]e^{-j\omega\tilde{\tau}}$, $\mathsf{H}'_{\mathrm{PLC}}(\omega)\triangleq\sum_{\tilde{\tau}=0}^{1}\mathsf{H}_{\mathrm{PLC}}[\tilde{\tau}]e^{-j\omega\tilde{\tau}}$, *and* $\mathsf{G}'_{\mathrm{PLC}}(\omega)\triangleq\sum_{\tilde{\tau}=0}^{1}\mathsf{G}_{\mathrm{PLC}}[\tilde{\tau}]e^{-j\omega\tilde{\tau}}$.

Let $\mathcal{C}_P^{\mathrm{PLC}}$ *denote the set of* $n_{\mathrm{PLC}}\times n_{\mathrm{PLC}}$ *positive semi-definite Hermitian matrix functions* $\mathsf{C}'_{\mathbf{X}}(\omega)$ *defined over the interval* $\omega\in[0,\pi)$*, which satisfy*

$$\frac{1}{\pi}\int_{\omega=0}^{\pi}\mathrm{Tr}\left(\mathsf{C}'_{\mathbf{X}}(\omega)\right)d\omega\le P\cdot n_{\mathrm{PLC}}, \quad (15a)$$

and define $\psi_{PLC}(\omega)$ *as:*

$$\psi_{\mathrm{PLC}}(\omega)\triangleq\frac{\left|\mathsf{I}_{n_{\mathrm{PLC}}}+\mathsf{H}'_{\mathrm{PLC}}(\omega)\,\mathsf{C}'_{\mathbf{X}}(\omega)\left(\mathsf{H}'_{\mathrm{PLC}}(\omega)\right)^H\left(\mathsf{C}'_{\mathbf{W}_{\mathrm{PLC}}}(\omega)\right)^{-1}\right|}{\left|\mathsf{I}_{n_{\mathrm{PLC}}}+\mathsf{G}'_{\mathrm{PLC}}(\omega)\,\mathsf{C}'_{\mathbf{X}}(\omega)\left(\mathsf{G}'_{\mathrm{PLC}}(\omega)\right)^H\left(\mathsf{C}'_{\mathbf{U}_{\mathrm{PLC}}}(\omega)\right)^{-1}\right|}. \quad (15b)$$

Then, the secrecy capacity of the NB-PLC WTC is given by

$$C_{s,\mathrm{PLC}}=\frac{1}{n_{\mathrm{PLC}}}\max_{\mathsf{C}'_{\mathbf{X}}(\omega)\in\mathcal{C}_P^{PLC}}\frac{1}{2\pi}\int_{\omega=0}^{\pi}\log\psi_{\mathrm{PLC}}(\omega)d\omega. \quad (15c)$$

Proof: The proof follows from the representation of NB-PLC channels as Gaussian MIMO channels with finite memory, see, e.g., [51, Appendix B], and is provided in Appendix D. ∎

[1] In NB-PLC systems, t_{ch} is equal to the mains period and t_{noise} is equal to half the mains period [48]. However, our secrecy capacity result applies also to the more general case in which the periods of the Tx-Rx CIR and of the Tx-Ev CIR are not identical, by setting t_{ch} to be the least common multiple of these periods. The same applies to the noises and t_{noise}, see further explanations in [51, Footnote 1].

$$(\mathsf{H}_{\mathrm{PLC}}[0])_{k_1,k_2}=\begin{cases}h_{\mathrm{PLC}}[k_1,k_1-k_2], & 0\le k_1-k_2\le m_{\mathrm{PLC}}\\ 0, & \text{otherwise},\end{cases} \quad (14a)$$

$$(\mathsf{H}_{\mathrm{PLC}}[1])_{k_1,k_2}=\begin{cases}h_{\mathrm{PLC}}[k_1,n_{\mathrm{PLC}}+k_1-k_2], & 1\le n_{\mathrm{PLC}}+k_1-k_2\le m_{\mathrm{PLC}}\\ 0, & \text{otherwise},\end{cases} \quad (14b)$$

$$(\mathsf{G}_{\mathrm{PLC}}[0])_{k_1,k_2}=\begin{cases}g_{\mathrm{PLC}}[k_1,k_1-k_2], & 0\le k_1-k_2\le m_{\mathrm{PLC}}\\ 0, & \text{otherwise},\end{cases} \quad (14c)$$

$$(\mathsf{G}_{\mathrm{PLC}}[1])_{k_1,k_2}=\begin{cases}g_{\mathrm{PLC}}[k_1,n_{\mathrm{PLC}}+k_1-k_2], & 1\le n_{\mathrm{PLC}}+k_1-k_2\le m_{\mathrm{PLC}}\\ 0, & \text{otherwise}.\end{cases} \quad (14d)$$

C. Scalar Gaussian WTCs With Finite Memory

To analytically evaluate (6c) it is required to search over all possible input correlation matrix functions in $\mathcal{C}_P$. However, for the special case of the scalar linear Gaussian WTC (LGWTC), obtained from the general model by setting $n_t = n_r = n_e = 1$, the secrecy capacity can be obtained explicitly. This result is stated in the following corollary:

Corollary 2: Consider the scalar LGWTC. Define the scalar functions $h'(\omega) \triangleq \mathsf{H}'(\omega)$, $g'(\omega) \triangleq \mathsf{G}'(\omega)$, $c'_W(\omega) \triangleq \mathsf{C}'_{\mathbf{W}}(\omega)$, $c'_U(\omega) \triangleq \mathsf{C}'_{\mathbf{U}}(\omega)$, $\alpha'_r(\omega) \triangleq \frac{|h'(\omega)|^2}{c'_W(\omega)}$, *and* $\alpha'_e(\omega) \triangleq \frac{|g'(\omega)|^2}{c'_U(\omega)}$, *where the domain for all the functions is* $[0,\pi)$. *The secrecy capacity of the scalar LGWTC is given by*

$$C_{s,\text{Scalar}} = \frac{1}{2\pi}\int_{\omega=0}^{\pi} \log\left(\frac{1+\alpha'_r(\omega)\,c'_X(\omega)}{1+\alpha'_e(\omega)\,c'_X(\omega)}\right)d\omega, \quad (16a)$$

where $c'_X(\omega)$, $\omega \in [0,\pi)$, *is obtained as follows: If* $\alpha'_r(\omega) \le \alpha'_e(\omega)$ *then* $c'_X(\omega) = 0$, *otherwise*

$$c'_X(\omega) = \left(\sqrt{\left(\frac{\alpha'_r(\omega)-\alpha'_e(\omega)}{2\alpha'_r(\omega)\,\alpha'_e(\omega)}\right)^2 + \frac{\alpha'_r(\omega)-\alpha'_e(\omega)}{\mu'\cdot\alpha'_r(\omega)\,\alpha'_e(\omega)}} - \frac{\alpha'_r(\omega)+\alpha'_e(\omega)}{2\alpha'_r(\omega)\,\alpha'_e(\omega)}\right)^+, \quad (16b)$$

and $\mu' > 0$ *is selected such that* $\frac{1}{\pi}\int_0^{\pi} c'_X(\omega)\,d\omega = P$.

Proof: For the scalar n-block memoryless circular Gaussian WTC (n-CGWTC), define the scalar functions $\hat{h}[k] \triangleq \hat{\mathsf{H}}[k]$, $\hat{g}[k] \triangleq \hat{\mathsf{G}}[k]$, $c_{\hat{W}}[k] \triangleq \mathsf{C}_{\hat{\mathbf{W}}}[k]$, $c_{\hat{U}}[k] \triangleq \mathsf{C}_{\hat{\mathbf{U}}}[k]$, $\alpha_r[k] \triangleq \frac{|\hat{h}[k]|^2}{c_{\hat{W}}[k]}$, and $\alpha_e[k] \triangleq \frac{|\hat{g}[k]|^2}{c_{\hat{U}}[k]}$, $k \in \{0,1,\ldots,n-1\}$. The secrecy capacity of the scalar n-CGWTC is given by the solution of the optimization problem in (10) with the matrices replaced by the corresponding scalar quantities. The resulting expression is [21, Thm. 1], [19, Thm. 2]:

$$C^{n-CG}_{s,\text{Scalar}} = \frac{1}{2n}\sum_{k=0}^{n-1}\log\left(\frac{1+\alpha_r[k]c_{\hat{X}}[k]}{1+\alpha_e[k]c_{\hat{X}}[k]}\right), \quad (17a)$$

where $c_{\hat{X}}[k]$, $k \in \{0,1,\ldots,n-1\}$, is obtained as follows: If $\alpha_r[k] \le \alpha_e[k]$ then $c_{\hat{X}}[k] = 0$, otherwise

$$c_{\hat{X}}[k] = \left(\sqrt{\left(\frac{\alpha_r[k]-\alpha_e[k]}{2\alpha_r[k]\alpha_e[k]}\right)^2 + \frac{\alpha_r[k]-\alpha_e[k]}{\mu\cdot\alpha_r[k]\alpha_e[k]}} - \frac{\alpha_r[k]+\alpha_e[k]}{2\alpha_r[k]\alpha_e[k]}\right)^+, \quad (17b)$$

and $\mu > 0$ is selected such that $\sum_{k=0}^{n-1} c_{\hat{X}}[k] = n^2 P$.

Now, it follows from Proposition 1 that $C_{s,\text{Scalar}} = \lim_{n\to\infty} C^{n-CG}_{s,\text{Scalar}}$, thus, the corollary is proved by first showing that in the limit of $n \to \infty$ the power constraint on $c_{\hat{X}}[k]$ (17b) converges to the power constraint on $c'_X(\omega)$ in (16b), and then showing that (17a) can be expressed as an average over n samples of a Riemann integrable even function[2] over the range $[0, 2\pi)$. Therefore, from [43, Ch. 6], it follows for $n \to \infty$, (17a) coincides with (16a). As these steps are essentially the same as the steps in the proof of Proposition 3, they are not repeated here. ■

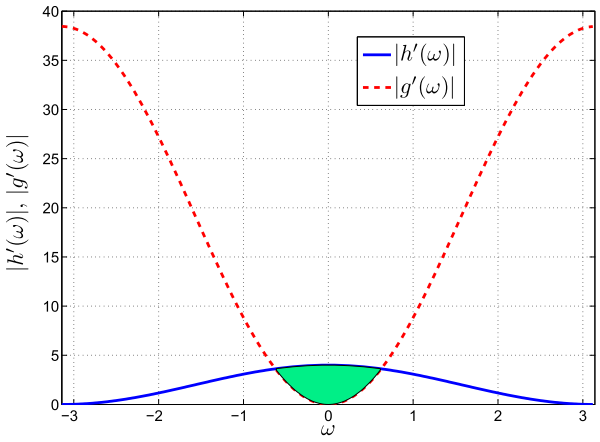

Fig. 1. The magnitudes of $h'(\omega)$ and $g'(\omega)$. The shadowed region corresponds to frequencies in which $|h'(\omega)| \ge |g'(\omega)|$.

While Corollary 2 applies only to scalar Gaussian WTCs with finite memory, it facilitates a deeper understanding of the main result stated in Thm. 1: Recall that for scalar Gaussian WTCs *without memory*, i.e., without ISI and with AWGN, the secrecy capacity is zero if the signal-to-noise ratio (SNR) at the intended receiver (SNR_r) is less than or equal to the SNR at the eavesdropper (SNR_e) [4]. In contrast, Corollary 2 and Proposition 4 imply that for scalar Gaussian WTCs *with finite memory*, the secrecy capacity is zero if and only if $\alpha'_r(\omega) \le \alpha'_e(\omega)$ for all sets $\Omega \subset [0,\pi)$ of positive Lebesgue measure. This implies that $C_{s,\text{Scalar}}$ is zero if and only if the "SNR density" at the intended receiver, i.e., $\frac{|h'(\omega)|^2}{c'_W(\omega)}$, is less than that at the eavesdropper, i.e., $\frac{|g'(\omega)|^2}{c'_U(\omega)}$, *over the entire frequency range*. It thus follows that the finite memory of the channel introduces additional degrees-of-freedom for concealing the information from the eavesdropper. To demonstrate this, consider the following two-tap channels to the receiver and to the eavesdropper, respectively: $h'(\omega) = 1 + e^{-j\omega}$ and $g'(\omega) = 3.1 - 3.1e^{-j\omega}$. Let the noises in both channels be AWGN with unit variance, thus, $\text{SNR}_r \approx 3$[dB] while $\text{SNR}_e \approx 13$[dB]. The magnitude of the frequency response for these two channels is depicted in Fig. 1. From the above discussion it follows that the shaded region in which $|h'(\omega)| \ge |g'(\omega)|$ facilitates a positive secrecy capacity, and this is achieved by waterfilling over this region according to (16b). Therefore, although SNR_e is 10[dB] higher than SNR_r, the secrecy capacity of this channel, derived via (16), is 0.21 bits per channel use.

V. Conclusions

In this work we characterized for the first time the secrecy capacity of finite-memory MIMO Gaussian WTCs.

[2]The function is even in the sense that for $1 \le k \le \lfloor \frac{n}{2} \rfloor$, then $\xi[k] \triangleq \log\left(\frac{1+\alpha_r[k]c_{\hat{X}}[k]}{1+\alpha_e[k]c_{\hat{X}}[k]}\right)$ satisfies $\xi[k] = \xi[n-k]$.

The secrecy capacity is derived via the analysis of an equivalent multivariate block-memoryless channel model, and the result is stated as a maximization over the input covariance matrices in the frequency domain. Based on the capacity characterization we were able to characterize a necessary and sufficient condition for non-zero secrecy capacity. We also derived the secrecy capacity of narrowband PLC channels, as a special case of the main result, thereby resolving one of the major open problems for this communications channel. For the scalar case, we explicitly demonstrated that the frequency selectivity of the channel can be utilized to facilitate secure communications over scenarios in which the SNR at the intended receiver is less than the SNR at the eavesdropper.

APPENDIX A
PROOF OF PROPOSITION 1

In order to prove that C_s is obtained from C_s^{n-CG} by taking $n \to \infty$, we begin by characterizing the secrecy capacity of the n-MGMWTC, which was defined in the proof outline in Subsection III-A. This capacity is characterized in Subsection A-A. Then, in Subsection A-B we show that C_s can be obtained from the secrecy capacity of the n-MGMWTC by taking $n \to \infty$. Lastly, in Subsection A-C we show that for $n \to \infty$, the secrecy capacity of the n-MGMWTC is equal to the secrecy capacity of the n-CGMWTC. Combining these results we obtain (9).

Define

$$C_s^{n-MG} \triangleq \frac{1}{n} \sup_{\substack{p\left(\mathbf{V}^{n-1},\mathbf{X}^{n-1}\right):\\ \mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\}\le P,\ \forall 0\le i<n}} \left\{ I\left(\mathbf{V}^{n-1};\mathbf{Y}_m^{n-1}\right) - I\left(\mathbf{V}^{n-1};\mathbf{Z}_m^{n-1}\right)\right\}. \quad \text{(A.1)}$$

A. Characterizing the Secrecy Capacity of the n-MGMWTC

The secrecy capacity of the n-MGMWTC is stated in the following proposition:

Proposition A.1: The secrecy capacity of the n-MGMWTC defined in Subsection III-A is given by C_s^{n-MG}.

Proof: In order to obtain the secrecy capacity of the n-MGMWTC defined in Subsection III-A, we first show that C_s^{n-MG} is the maximum achievable secrecy rate for the n-MGMWTC when considering *only codes whose blocklength is an integer multiple of* n, i.e, $[R, b\cdot n]$ codes, where $b \in \mathbb{N}$. Then, we show that any secrecy rate achievable for the n-MGMWTC can be achieved by considering only codes whose blocklength is an integer multiple of n.

Let us consider the n-MGMWTC constrained to using only codes whose blocklength is an integer multiple of n. In this case, we can represent the channel as an equivalent $n\cdot n_t \times (n-m)\cdot n_r \times (n-m)\cdot n_e$ MIMO WTC (without loss of information), via the following assignments: Define the input of the transformed channel at time $i \in \mathbb{N}$ by the $n\cdot n_t \times 1$ vector $\mathbf{X}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{X}_{\tilde{i}\cdot n}^{\left(\tilde{i}+1\right)\cdot n-1}$, $\tilde{i}\ge 0$, the output at the intended receiver at time $i \in \mathbb{N}$ by the $(n-m)\cdot n_r \times 1$ vector $\mathbf{Y}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{Y}_{\tilde{i}\cdot n+m}^{\left(\tilde{i}+1\right)\cdot n-1}$, and the output at the eavesdropper at time $\tilde{i} \in \mathbb{N}$ by the $(n-m)\cdot n_e \times 1$ vector $\mathbf{Z}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{Z}_{\tilde{i}\cdot n+m}^{\left(\tilde{i}+1\right)\cdot n-1}$. The transformation is clearly bijective, and thus, the secrecy capacity of the equivalent channel is equal to the secrecy capacity of the original n-MGMWTC. Since the n-MGMWTC is n-block memoryless, it follows from Def. 6 that the *equivalent transformed MIMO channel obtained above is memoryless*, with the transmitter having n times more antennas than in the n-MGMWTC, and both the intended receiver and the eavesdropper having $(n-m)$ times more antennas than in the n-MGMWTC. The signals received at the intended receiver and at the eavesdropper are corrupted by the additive noise vectors $\mathbf{W}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{W}_{\tilde{i}\cdot n+m}^{\left(\tilde{i}+1\right)\cdot n-1}$ and $\mathbf{U}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{U}_{\tilde{i}\cdot n+m}^{\left(\tilde{i}+1\right)\cdot n-1}$, respectively. From the noise characterization in Subsection II-B and the definition of the n-MGMWTC, it follows that both $\mathbf{W}_{eq}\left[\tilde{i}\right]$ and $\mathbf{U}_{eq}\left[\tilde{i}\right]$ are zero-mean Gaussian with positive-definite covariance matrices (since the elements of the random vectors are not linearly dependent, see [57, Ch. 8.1]), and each process $\mathbf{W}_{eq}\left[\tilde{i}\right]$ and $\mathbf{U}_{eq}\left[\tilde{i}\right]$ is i.i.d. in time (here we refer to the index $\tilde{i}$ as "time"). The secrecy capacity of the transformed channel, denoted Q_n^{eq}, can be expressed in the form of the result of Csiszár and Körner [2, Eq. (11)][3]

$$\begin{aligned} Q_n^{eq} &= \sup_{p\left(\mathbf{V}_{eq},\mathbf{X}_{eq}\right)} \left\{ I\left(\mathbf{V}_{eq};\mathbf{Y}_{eq}\right) - I\left(\mathbf{V}_{eq};\mathbf{Z}_{eq}\right)\right\} \\ &\overset{(a)}{=} \sup_{\substack{p\left(\mathbf{V}^{n-1},\mathbf{X}^{n-1}\right):\\ \mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\}\le P,\ \forall 0\le i<n}} \left\{ I\left(\mathbf{V}^{n-1};\mathbf{Y}_m^{n-1}\right) - I\left(\mathbf{V}^{n-1};\mathbf{Z}_m^{n-1}\right)\right\}, \end{aligned} \quad \text{(A.2)}$$

where (a) follows from the definition of the quantities used in the equivalent channel, and $\mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\} \le P,\ \forall 0 \le i < n$ corresponds to the *per-symbol* power constraint of the n-MGMWTC. As every channel use in the transformed MIMO channel corresponds to n channel uses in the n-MGMWTC, it follows from (A.2) that the maximal achievable secrecy rate of the n-MGMWTC in bits per channel use, subject to the restriction that only codes whose blocklength is an integer multiple of n are allowed, is $\frac{1}{n}Q_n^{eq} = C_s^{n-MG}$.

Next, we show that any secrecy rate achievable for the n-MGMWTC can be achieved by considering only codes whose blocklength is an integer multiple of n: Consider a secrecy rate R_s achievable for the n-MGMWTC and fix $\epsilon_1 > 0, \epsilon_2 > 0, \epsilon_3 > 0$. From Def. 4 it follows that $\exists l_0 > 0$ such that $\forall l > l_0$ there exists an $[R, l]$ code which satisfies (4a)-(4c). Thus, by setting b_0 as the smallest integer for which $b_0\cdot n \ge l_0$, it follows that for all integer $b > b_0$ there exists an $[R, b\cdot n]$ code which satisfies (4a)-(4c). Therefore, the secrecy rate R_s is also achievable when considering only

[3]While [2] considered discrete alphabets, it is noted that the result can be extended to incorporate continuous-valued power-constrained inputs as considered in this paper, see [2, Sec. VI], [3, Ch. 5.1], [6, Sec. IV.A], and [8, Sec. I].

codes whose blocklength is an integer multiple of n. We thus conclude that C_s^{n-MG} is the maximum achievable secrecy rate for the n-MGMWTC. ∎

B. Proving That $C_s = \lim_{n\to\infty} C_s^{n-MG}$

Next, we prove that the secrecy capacity of the LGMWTC, C_s, coincides with C_s^{n-MG} in the limit of $n \to \infty$. We begin by defining

$$C_n(\mathbf{s}_0) \triangleq \frac{1}{n} \sup_{\substack{p(\mathbf{V}^{n-1},\mathbf{X}^{n-1}):\\ \mathbb{E}\{\|\mathbf{X}[i]\|^2\}\le P,\ \forall 0\le i<n}} \left\{ I\left(\mathbf{V}^{n-1}; \mathbf{Y}^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) - I\left(\mathbf{V}^{n-1}; \mathbf{Z}^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) \right\}. \quad \text{(A.3)}$$

The outline of the proof is as follows:

- First, we show in Lemma A.1 and Lemma A.2 that for the LGMWTC (2), the mutual information between the channel inputs and any m channel outputs can be upper bounded by a fixed and finite number.
- Next, in Lemma A.3, we prove that $C_s \le \inf_{\mathbf{s}_0\in\mathcal{S}_0} \left(\liminf_{n\to\infty} C_n(\mathbf{s}_0)\right)$.
- Then, in Lemma A.4, we show that $\inf_{\mathbf{s}_0\in\mathcal{S}_0} \left(\liminf_{n\to\infty} C_n(\mathbf{s}_0)\right) \le \liminf_{n\to\infty} C_s^{n-MG}$.
- Lastly, in Lemma A.5, we prove that $\limsup_{n\to\infty} C_s^{n-MG} \le C_s$.

By combining these lemmas, we conclude in Proposition A.2 that the secrecy capacity of the LGMWTC is equal to $\lim_{n\to\infty} C_s^{n-MG}$ and that the limit exists.

Lemma A.1: There exists a finite and fixed $\eta > 0$, such that for all positive integers a, b, n, l, satisfying $b > l$, $n > 2m$, and $n + m > a \ge m$, it holds that

$$I\left(\mathbf{X}^{b\cdot n+a-1}; \mathbf{Z}_a^{a+m-1} \middle| \mathbf{Z}_{a+m}^{n+a-1}, \mathbf{Z}_{n+a+m}^{2n+a-1}, \ldots, \mathbf{Z}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1}, \mathbf{U}_{a-m}^{a-1}\right) \le \eta, \quad \text{(A.4a)}$$

and

$$I\left(\mathbf{X}^{b\cdot n+a-1}; \mathbf{Z}_{l\cdot n+a}^{l\cdot n+a+m-1} \middle| \mathbf{Z}_{a+m}^{n+a-1}, \mathbf{Z}_{n+a+m}^{2n+a-1}, \ldots, \mathbf{Z}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1}, \mathbf{Z}_a^{a+m-1}, \mathbf{Z}_{n+a}^{n+a+m-1}, \ldots, \mathbf{Z}_{(l-1)\cdot n+a}^{(l-1)\cdot n+a+m-1}, \mathbf{U}_{a-m}^{a-1}\right) \le \eta. \quad \text{(A.4b)}$$

Proof: We now provide a sketch of the proof of the lemma; The detailed proof appears in [64]. From the input-output relationship of the LGMWTC (2) it follows that any sequence of $k > 0$ consecutive channel outputs corresponding to indexes $i_0, i_0+1, \ldots, i_0+k-1$, *when their subsequent and preceding channel outputs are given*, depends on the channel inputs at indexes $i_0 - m, i_0 - m + 1, \ldots, i_0 + k - 1$, due to the finite length of the channel impulse response, and the dependence extends also to the channel inputs at indexes $\{i_0 - 2m, i_0 - 2m+1, \ldots, i_0-m-1\} \cup \{i_0+k, i_0+k+1 \ldots, i_0+k+m-1\}$, due to the temporal span of the noise correlation. The latter follows as, given the corresponding channel outputs, these inputs are statistically dependent on the noise at these indexes. Therefore, similarly to the derivation in [53, Eq. (63)-(65)], we obtain that each of the two conditional mutual information expressions in (A.4) is upper-bounded by the mean of a quadratic function of at most $4m$ channel inputs. Since the channel input $\mathbf{X}[i]$ is subject to a per-symbol power constraint, the lemma follows. ∎

Lemma A.2: There exists a finite and fixed $\tilde{\eta} > 0$, such that for any positive integer $n > 2m$, and for all initial states $\mathbf{s}_0 \in \mathcal{S}_0$, it holds that

$$I\left(\mathbf{X}^{n-1}; \mathbf{Y}^{m-1} \middle| \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) \le \tilde{\eta}. \quad \text{(A.5)}$$

Proof: Note that

$$\begin{aligned} &I\left(\mathbf{X}^{n-1}; \mathbf{Y}^{m-1} \middle| \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) \\ &= h\left(\mathbf{Y}^{m-1} \middle| \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) - h\left(\mathbf{Y}^{m-1} \middle| \mathbf{X}^{n-1}, \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) \\ &\overset{(a)}{\le} h\left(\mathbf{Y}^{m-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) - h\left(\mathbf{Y}^{m-1} \middle| \mathbf{X}^{n-1}, \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right), \end{aligned} \quad \text{(A.6)}$$

where (a) follows since conditioning reduces entropy [52, Ch. 8.6]. From the input-output relationship of the LGMWTC it follows that $\exists \mathsf{H}_1, \mathsf{H}_0 \in \mathbb{R}^{(n_r\cdot m)\times(n_t\cdot m)}$ such that $\mathbf{Y}^{m-1} = \mathsf{H}_1\mathbf{X}^{m-1} + \mathsf{H}_0\mathbf{X}_{-m}^{-1} + \mathbf{W}^{m-1}$ and $\exists \underline{\mathsf{H}} \in \mathbb{R}^{(n_r\cdot(n-m))\times(n_t\cdot n)}$ such that $\mathbf{Y}_m^{n-1} = \underline{\mathsf{H}}\mathbf{X}^{n-1} + \mathbf{W}_m^{n-1}$. Therefore,

$$\begin{aligned} &h\left(\mathbf{Y}^{m-1} \middle| \mathbf{X}^{n-1}, \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) \\ &= h\left(\mathsf{H}_1\mathbf{X}^{m-1} + \mathsf{H}_0\mathbf{X}_{-m}^{-1} + \mathbf{W}^{m-1} \middle| \mathbf{X}^{n-1}, \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) \\ &\overset{(a)}{=} h\left(\mathbf{W}^{m-1} \middle| \mathbf{X}^{n-1}, \mathbf{W}_m^{n-1}, \mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}\right) \\ &\overset{(b)}{=} h\left(\mathbf{W}^{m-1} \middle| \mathbf{W}_m^{n-1}, \mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}\right) \\ &\overset{(c)}{=} h\left(\mathbf{W}^{m-1} \middle| \mathbf{W}_m^{2m-1}, \mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}\right) \\ &= \int_{\mathbf{w}_m^{2m-1}\in\mathbb{R}^{n_r\cdot m}} h\left(\mathbf{W}^{m-1} \middle| \mathbf{W}_m^{2m-1} = \mathbf{w}_m^{2m-1}, \mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}\right) \times p_{\mathbf{W}_m^{2m-1}}\left(\mathbf{w}_m^{2m-1}\right) d\mathbf{w}_m^{2m-1}, \end{aligned} \quad \text{(A.7)}$$

where (a) follows as $\mathbf{S}_0 = \left[\left(\mathbf{X}_{-m}^{-1}\right)^T, \left(\mathbf{W}_{-m}^{-1}\right)^T, \left(\mathbf{U}_{-m}^{-1}\right)^T\right]^T$; (b) follows since the noise $\mathbf{W}[i]$ is independent of the channel input $\mathbf{X}[i]$; (c) follows since the temporal correlation of the multivariate Gaussian process $\mathbf{W}[i]$ is finite and shorter than $m+1$, and therefore $\mathbf{W}^{m-1}$ is independent of $\mathbf{W}_{2m}^{n-1}$. Since $\mathbf{W}^{m-1}$ and $\left[\left(\mathbf{W}_m^{2m-1}\right)^T, \left(\mathbf{W}_{-m}^{-1}\right)^T\right]^T$ are jointly Gaussian, the conditional distribution $\mathbf{W}^{m-1} \middle| \mathbf{W}_m^{2m-1} = \mathbf{w}_m^{2m-1}, \mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}$ is a multivariate Gaussian distribution [59, Proposition 3.13], with covariance matrix

$\tilde{\mathsf{Q}} \in \mathbb{R}^{(n_r m)\times(n_r m)}$ given by

$$\begin{aligned}\tilde{\mathsf{Q}} \triangleq\ & \mathbb{E}\left\{\mathbf{W}^{m-1}\left(\mathbf{W}^{m-1}\right)^T\right\} \\ & - \mathbb{E}\left\{\mathbf{W}^{m-1}\left[\left(\mathbf{W}_m^{2m-1}\right)^T, \left(\mathbf{W}_{-m}^{-1}\right)^T\right]\right\} \\ & \times\Bigg(\mathbb{E}\Bigg\{\left[\left(\mathbf{W}_m^{2m-1}\right)^T, \left(\mathbf{W}_{-m}^{-1}\right)^T\right]^T \\ & \quad\times\left[\left(\mathbf{W}_m^{2m-1}\right)^T, \left(\mathbf{W}_{-m}^{-1}\right)^T\right]\Bigg\}\Bigg)^{-1} \\ & \times\mathbb{E}\left\{\left[\left(\mathbf{W}_m^{2m-1}\right)^T, \left(\mathbf{W}_{-m}^{-1}\right)^T\right]^T\left(\mathbf{W}^{m-1}\right)^T\right\}. \quad \text{(A.8)}\end{aligned}$$

We note that as the noise samples are not linearly dependent,[4] it follows that $\left|\tilde{\mathsf{Q}}\right| > 0$ [57, Ch. 8.1]. Then, from the differential entropy of a multivariate Gaussian RV [52, Thm. 8.4.1] we conclude that (A.7) can be written as

$$h\left(\mathbf{Y}^{m-1}\middle|\mathbf{X}^{n-1}, \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) = \frac{1}{2}\log\left((2\pi e)^{n_r m}\left|\tilde{\mathsf{Q}}\right|\right), \quad \text{(A.9)}$$

where $\left|\tilde{\mathsf{Q}}\right|$ is positive, finite, and independent of n. Next, note that

$$\begin{aligned}& h\left(\mathbf{Y}^{m-1}\middle|\mathbf{S}_0 = \mathbf{s}_0\right) \\ & \quad = h\left(\mathsf{H}_1\mathbf{X}^{m-1} + \mathsf{H}_0\mathbf{X}_{-m}^{-1} + \mathbf{W}^{m-1}\middle|\mathbf{S}_0 = \mathbf{s}_0\right) \\ & \quad = h\left(\mathsf{H}_1\mathbf{X}^{m-1} + \mathbf{W}^{m-1}\middle|\mathbf{X}_{-m}^{-1} = \mathbf{x}_{-m}^{-1}, \mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}\right). \quad \text{(A.10)}\end{aligned}$$

Let $\mathsf{K}_{\mathbf{Y}}$ be the covariance matrix of the conditional distribution $\mathsf{H}_1\mathbf{X}^{m-1} + \mathbf{W}^{m-1}\big|\mathbf{X}_{-m}^{-1} = \mathbf{x}_{-m}^{-1}, \mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}$, $\mathsf{K}_{\mathbf{X}}$ be the covariance matrix of $\mathbf{X}^{m-1}$, and $\mathsf{K}_{\mathbf{W}}$ be the covariance matrix of the conditional distribution $\mathbf{W}^{m-1}\big|\mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}$. Since the channel input $\mathbf{X}[i]$ is subject to a per-symbol power constraint P for $i \geq 0$, it follows that the entries of $\mathsf{K}_{\mathbf{X}}$ are all not larger than P for any initial state $\mathbf{x}_{-m}^{-1}$. As $\mathbf{W}^{m-1}$ and $\mathbf{W}_{-m}^{-1}$ are jointly Gaussian, it follows from [59, Proposition 3.13] that $\mathsf{K}_{\mathbf{W}}$ is independent of the realization of $\mathbf{W}_{-m}^{-1}$, $\mathbf{w}_{-m}^{-1}$. Since $\mathbf{X}[i]\big|\mathbf{X}_{-m}^{-1}, \mathbf{W}_{-m}^{-1} \overset{d}{=} \mathbf{X}[i]\big|\mathbf{X}_{-m}^{-1}$ and $\mathbf{W}[i]\big|\mathbf{X}_{-m}^{-1}, \mathbf{W}_{-m}^{-1} \overset{d}{=} \mathbf{W}[i]\big|\mathbf{W}_{-m}^{-1}$ are mutually independent, and the encoder is independent of the initial channel state, it follows that $\mathsf{K}_{\mathbf{Y}} = \mathsf{H}_1\mathsf{K}_{\mathbf{X}}\mathsf{H}_1^T + \mathsf{K}_{\mathbf{W}}$. As the noise samples are not linearly dependent, we obtain $|\mathsf{K}_{\mathbf{Y}}| > 0$ [57, Ch. 8.1]. Defining γ_k as $\gamma_k \triangleq \sum_{k_1=0}^{m\cdot n_t-1}\sum_{k_2=0}^{m\cdot n_t-1}\left|(\mathsf{H}_1)_{k,k_2}(\mathsf{H}_1)_{k,k_1}\right|$, it follows from Hadamard's inequality [52, Thm. 17.9.2] that

$$\begin{aligned}|\mathsf{K}_{\mathbf{Y}}| &\leq \prod_{k=0}^{m\cdot n_r-1}(\mathsf{K}_{\mathbf{Y}})_{k,k} \\ &= \prod_{k=0}^{m\cdot n_r-1}\left(\left(\mathsf{H}_1\mathsf{K}_{\mathbf{X}}\mathsf{H}_1^T\right)_{k,k} + (\mathsf{K}_{\mathbf{W}})_{k,k}\right) \\ &= \prod_{k=0}^{m\cdot n_r-1}\Bigg(\sum_{k_1=0}^{m\cdot n_t-1}\sum_{k_2=0}^{m\cdot n_t-1}(\mathsf{H}_1)_{k,k_2}(\mathsf{K}_{\mathbf{X}})_{k_2,k_1}(\mathsf{H}_1)_{k,k_1} \\ &\qquad + (\mathsf{K}_{\mathbf{W}})_{k,k}\Bigg) \\ &\leq \prod_{k=0}^{m\cdot n_r-1}\left(\gamma_k P + (\mathsf{K}_{\mathbf{W}})_{k,k}\right).\end{aligned}$$

It follows that $|\mathsf{K}_{\mathbf{Y}}|$ is positive, finite, and independent of n. Plugging (A.9) and (A.10) into (A.6) leads to

$$\begin{aligned}& I\left(\mathbf{X}^{n-1}; \mathbf{Y}^{m-1}\middle|\mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) \\ & \quad \leq h\left(\mathsf{H}_1\mathbf{X}^{m-1} + \mathbf{W}^{m-1}\middle|\mathbf{X}_{-m}^{-1} = \mathbf{x}_{-m}^{-1}, \mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}\right) \\ & \qquad - \frac{1}{2}\log\left((2\pi e)^{n_r m}\left|\tilde{\mathsf{Q}}\right|\right) \\ & \quad \overset{(a)}{\leq} \frac{1}{2}\log\left((2\pi e)^{n_r m}|\mathsf{K}_{\mathbf{Y}}|\right) - \frac{1}{2}\log\left((2\pi e)^{n_r m}\left|\tilde{\mathsf{Q}}\right|\right), \quad \text{(A.11)}\end{aligned}$$

where (a) follows since $h\left(\mathsf{H}_1\mathbf{X}^{m-1} + \mathbf{W}^{m-1}\big|\mathbf{X}_{-m}^{-1} = \mathbf{x}_{-m}^{-1}, \mathbf{W}_{-m}^{-1} = \mathbf{w}_{-m}^{-1}\right)$ is upper-bounded by the differential entropy of an $n_r \cdot m \times 1$ multivariate Gaussian RV with the same covariance matrix [52, Thm. 8.6.5]. It therefore follows from (A.11) that $\exists\tilde{\eta}$ independent of n such that $I\left(\mathbf{X}^{n-1}; \mathbf{Y}^{m-1}\middle|\mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) \leq \tilde{\eta}$. ∎

Comment A.1: Note that the per-symbol power constraint (3) *is required in the proofs of Lemmas A.1 and A.2 in order to upper bound the mutual information between a transmitted block of $b \cdot n + a$ channel inputs (for Lemma A.1) or n channel inputs (for Lemma A.2) and a received block of m channel outputs, by a finite quantity independent of n. Consequently, the per-symbol constraint is essential for proving the asymptotic secrecy capacity equivalence stated in Proposition 1.*

Lemma A.3: The secrecy capacity of the LGMWTC satisfies $C_s \leq \inf_{\mathbf{s}_0\in\mathcal{S}_0}\left(\liminf_{n\to\infty} C_n(\mathbf{s}_0)\right)$.

Proof: We prove the lemma by showing that every secrecy rate R_s achievable for the LGMWTC satisfies $R_s \leq \liminf_{n\to\infty} C_n(\mathbf{s}_0)$ for any initial state $\mathbf{s}_0$. By definition, if R_s is achievable for the LGMWTC, then for every non-negative triplet $\epsilon_1, \epsilon_2, \epsilon_3 > 0$ and for all sufficiently large n there exists an $[R, n]$ code, such that (4a)-(4c) are satisfied. Fix $\mathbf{S}_0 = \tilde{\mathbf{s}}_0$, and recall that from Fano's inequality [52, Sec. 2.10] it follows that

$$\begin{aligned}H\left(M\middle|\mathbf{Y}^{n-1}, \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) &\leq 1 + \Pr\left(M \neq \hat{M}\middle|\mathbf{S}_0 = \tilde{\mathbf{s}}_0\right)\cdot nR \\ &\overset{(a)}{\leq} 1 + \epsilon_1 \cdot nR, \quad \text{(A.12)}\end{aligned}$$

[4]Note that for any pair of jointly-Gaussian real-valued random vectors $\mathbf{A}$ and $\mathbf{B}$, such that the entries of $\left[\mathbf{A}^T, \mathbf{B}^T\right]^T$ are not linearly dependent, it follows from [58, Ch. 3.5] that the entries of $\mathbf{A}$ conditioned on $\mathbf{B} = \mathbf{b}$ are also not linearly dependent.

where (a) follows from (4a) since $\Pr\left(M \neq \hat{M} \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) \leq \sup_{\mathbf{s}_0 \in \mathcal{S}_0} \Pr\left(M \neq \hat{M} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) \leq \epsilon_1$. Therefore,

$$\begin{aligned} & I\left(M; \mathbf{Y}^{n-1} \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) - I\left(M; \mathbf{Z}^{n-1} \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) \\ & = H\left(M \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) - H\left(M \middle| \mathbf{Y}^{n-1}, \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) \\ & \qquad - I\left(M; \mathbf{Z}^{n-1} \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) \\ & \overset{(a)}{\geq} H\left(M \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) - 1 - \epsilon_1 \cdot nR - \epsilon_2 \cdot n \\ & \overset{(b)}{=} nR - 1 - \epsilon_1 \cdot nR - \epsilon_2 \cdot n, \end{aligned} \tag{A.13}$$

where (a) follows from (A.12) and from (4b), as $I\left(M; \mathbf{Z}^{n-1} \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) \leq \sup_{\mathbf{s}_0 \in \mathcal{S}_0} I\left(M; \mathbf{Z}^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) < \epsilon_2 \cdot n$; and (b) follows since M is uniformly distributed and is independent of $\mathbf{S}_0$. Combining (4c) and (A.13) leads to

$$\begin{aligned} & (1-\epsilon_1)(R_s - \epsilon_3) - \frac{1}{n} - \epsilon_2 \\ & \leq \frac{1}{n}\left(I\left(M; \mathbf{Y}^{n-1} \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) - I\left(M; \mathbf{Z}^{n-1} \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right)\right) \\ & \overset{(a)}{\leq} \frac{1}{n} \sup_{\substack{p(\mathbf{V}^{n-1}, \mathbf{X}^{n-1}): \\ \mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\} \leq P, \ \forall 0 \leq i < n}} \left\{ I\left(\mathbf{V}^{n-1}; \mathbf{Y}^{n-1} \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) \right. \\ & \qquad \left. - I\left(\mathbf{V}^{n-1}; \mathbf{Z}^{n-1} \middle| \mathbf{S}_0 = \tilde{\mathbf{s}}_0\right) \right\} \\ & \equiv C_n\left(\tilde{\mathbf{s}}_0\right), \end{aligned} \tag{A.14}$$

where (a) follows since we can define a pair $\left(\mathbf{V}^{n-1}, \mathbf{X}^{n-1}\right)$ such that $\mathbf{V}^{n-1}$ is a random variable representing the uniformly distributed message M and $p\left(\mathbf{X}^{n-1} | \mathbf{V}^{n-1}\right)$ is defined by the encoder of the $[R, n]$ code (either deterministic or stochastic), as done in the proof of [29, Lemma 4]. Since (A.14) holds for all sufficiently large n, it follows from [43, Thm. 3.19] that $\liminf_{n\to\infty}\left((1-\epsilon_1)(R_s-\epsilon_3) - \frac{1}{n} - \epsilon_2\right) \leq \liminf_{n\to\infty} C_n\left(\tilde{\mathbf{s}}_0\right)$, thus

$$(1-\epsilon_1)(R_s - \epsilon_3) - \epsilon_2 \leq \liminf_{n\to\infty} C_n\left(\tilde{\mathbf{s}}_0\right). \tag{A.15}$$

Since ϵ_1, ϵ_2, and ϵ_3 can also be made arbitrarily small, (A.15) implies that

$$R_s \leq \liminf_{n\to\infty} C_n\left(\tilde{\mathbf{s}}_0\right), \tag{A.16}$$

and as (A.16) is true for any achievable secrecy rate R_s, we conclude that for all $\tilde{\mathbf{s}}_0 \in \mathcal{S}_0$, $C_s \leq \liminf_{n\to\infty} C_n\left(\tilde{\mathbf{s}}_0\right)$,[5] thus $C_s \leq \inf_{\mathbf{s}_0 \in \mathcal{S}_0}\left(\liminf_{n\to\infty} C_n\left(\mathbf{s}_0\right)\right)$. ∎

Lemma A.4: C_s^{n-MG}, defined in (A.1)*, satisfies* $\inf_{\mathbf{s}_0 \in \mathcal{S}_0}\left(\liminf_{n\to\infty} C_n\left(\mathbf{s}_0\right)\right) \leq \liminf_{n\to\infty} C_s^{n-MG}$.

Proof: First, we show that for all $\mathbf{s}_0 \in \mathcal{S}_0$, $C_n\left(\mathbf{s}_0\right) \leq C_s^{n-MG} + \frac{\tilde{\eta}}{n}$. Note that

$$\begin{aligned} & I\left(\mathbf{V}^{n-1}; \mathbf{Y}^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) \\ & \overset{(a)}{=} I\left(\mathbf{V}^{n-1}; \mathbf{Y}_m^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) \\ & \qquad + I\left(\mathbf{V}^{n-1}; \mathbf{Y}^{m-1} \middle| \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) \\ & \overset{(b)}{\leq} I\left(\mathbf{V}^{n-1}; \mathbf{Y}_m^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) \\ & \qquad + I\left(\mathbf{X}^{n-1}; \mathbf{Y}^{m-1} \middle| \mathbf{Y}_m^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) \\ & \overset{(c)}{\leq} I\left(\mathbf{V}^{n-1}; \mathbf{Y}_m^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) + \tilde{\eta} \\ & \overset{(d)}{=} I\left(\mathbf{V}^{n-1}; \mathbf{Y}_m^{n-1}\right) + \tilde{\eta}, \end{aligned} \tag{A.17}$$

where (a) follows from the mutual information chain rule [52, Sec. 2.5]; (b) follows from the data processing inequality and the Markov chain[6] $\mathbf{V}^{n-1}|\mathbf{S}_0 \to \mathbf{X}^{n-1}|\mathbf{S}_0 \to \mathbf{Y}^{n-1}|\mathbf{S}_0$; (c) follows from Lemma A.2; and (d) follows since $\mathbf{Y}[i]$ is independent of the initial state $\forall i \geq m$. Using (A.17) in the definition of $C_n\left(\mathbf{s}_0\right)$ in (A.3) we obtain

$$\begin{aligned} C_n\left(\mathbf{s}_0\right) & \overset{(a)}{\leq} \frac{1}{n} \sup_{\substack{p(\mathbf{V}^{n-1}, \mathbf{X}^{n-1}): \\ \mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\} \leq P, \ \forall 0 \leq i < n}} \left\{ I\left(\mathbf{V}^{n-1}; \mathbf{Y}_m^{n-1}\right) + \tilde{\eta} \right. \\ & \qquad \left. - I\left(\mathbf{V}^{n-1}; \mathbf{Z}^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) \right\} \\ & \overset{(b)}{\leq} \frac{1}{n} \sup_{\substack{p(\mathbf{V}^{n-1}, \mathbf{X}^{n-1}): \\ \mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\} \leq P, \ \forall 0 \leq i < n}} \left\{ I\left(\mathbf{V}^{n-1}; \mathbf{Y}_m^{n-1}\right) \right. \\ & \qquad \left. - I\left(\mathbf{V}^{n-1}; \mathbf{Z}_m^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) \right\} + \frac{1}{n}\tilde{\eta} \\ & \overset{(c)}{=} \frac{1}{n} \sup_{\substack{p(\mathbf{V}^{n-1}, \mathbf{X}^{n-1}): \\ \mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\} \leq P, \ \forall 0 \leq i < n}} \left\{ I\left(\mathbf{V}^{n-1}; \mathbf{Y}_m^{n-1}\right) \right. \\ & \qquad \left. - I\left(\mathbf{V}^{n-1}; \mathbf{Z}_m^{n-1}\right) \right\} + \frac{1}{n}\tilde{\eta} \\ & \equiv C_s^{n-MG} + \frac{\tilde{\eta}}{n}, \end{aligned}$$

where (a) follows from (A.17); (b) follows from the non-negativity of the mutual information which implies that $I\left(\mathbf{V}^{n-1}; \mathbf{Z}_m^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) \leq I\left(\mathbf{V}^{n-1}; \mathbf{Z}^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right)$; and (c) follows since $\mathbf{Z}[i]$ is independent of the initial state $\forall i \geq m$.

Now, since for all $\mathbf{s}_0 \in \mathcal{S}_0$, $C_n\left(\mathbf{s}_0\right) \leq C_s^{n-MG} + \frac{\tilde{\eta}}{n}$, then $\liminf_{n\to\infty} C_n\left(\mathbf{s}_0\right) \leq \liminf_{n\to\infty} C_s^{n-MG}$, therefore,

$$\inf_{\mathbf{s}_0 \in \mathcal{S}_0}\left(\liminf_{n\to\infty} C_n\left(\mathbf{s}_0\right)\right) \leq \liminf_{n\to\infty} C_s^{n-MG}.$$

This proves the lemma. ∎

[5] As the supremum is defined as the least upper bound [43, Def. 1.8], it follows that if every achievable secrecy rate R_s is not larger than a given real number $\gamma \in \mathbb{R}$, then the supremum of all achievable secrecy rates, C_s, is also not larger than γ.

[6] The Markov chain $\mathbf{V}^{n-1}|\mathbf{S}_0 \to \mathbf{X}^{n-1}|\mathbf{S}_0 \to \mathbf{Y}^{n-1}|\mathbf{S}_0$ is a short notation for the relationship $p\left(\mathbf{V}^{n-1}, \mathbf{X}^{n-1}, \mathbf{Y}^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) = p\left(\mathbf{V}^{n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) p\left(\mathbf{X}^{n-1} \middle| \mathbf{V}^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right) p\left(\mathbf{Y}^{n-1} \middle| \mathbf{X}^{n-1}, \mathbf{S}_0 = \mathbf{s}_0\right)$, for all $\mathbf{s}_0 \in \mathcal{S}_0$, see, e.g., [65].

Lemma A.5: C_s^{n-MG}, *defined in* (A.1), *satisfies* $\limsup_{n\to\infty} C_s^{n-MG} \leq C_s$.

Proof: In order to prove the lemma we show that every non-negative $R_s < \limsup_{n\to\infty} C_s^{n-MG}$ is an achievable secrecy rate for the LGMWTC[7] To that aim, consider such $R_s < \limsup_{n\to\infty} C_s^{n-MG}$: From [60, Thm. 5.5] it follows that if $R_s < \limsup_{n\to\infty} C_s^{n-MG}$, then *there are infinitely many values of* $n \in \mathbb{N}$ *such that* $R_s \leq C_s^{n-MG}$, hence, R_s is an achievable secrecy rate for the n-MGMWTC for these values of n. Consequently, it follows that for a given real number $\eta > 0$ and for any arbitrarily fixed non-negative triplet $\epsilon_1, \epsilon_2, \epsilon_3 > 0$, $\exists n > n_1 \triangleq \left\lceil \frac{2\eta}{\epsilon_2} \right\rceil$ such that R_s is an achievable secrecy rate for the n-MGMWTC. Note that since $n > n_1$ it follows that $\epsilon_2 - \frac{2\eta}{n} > 0$. By Def. 4, the achievability of R_s implies that we can find a sufficiently large $b_0 \in \mathbb{N}$, such that for all integer $b > b_0$ there exists an $[R_1, b \cdot n]$ code for the n-MGMWTC which satisfies

$$\sup_{\mathbf{s}_0 \in \mathcal{S}_0} P_e^{b\cdot n}(\mathbf{s}_0) \overset{(a)}{=} P_e^{b\cdot n} \leq \epsilon_1, \tag{A.18a}$$

$$\begin{aligned}\sup_{\mathbf{s}_0 \in \mathcal{S}_0} \frac{1}{b\cdot n} I\left(M; \mathbf{Z}_m^{n-1}, \mathbf{Z}_{n+m}^{2n-1}, \ldots, \mathbf{Z}_{(b-1)\cdot n+m}^{b\cdot n-1} \middle| \mathbf{S}_0 = \mathbf{s}_0\right) \\ \overset{(b)}{=} \frac{1}{b\cdot n} I\left(M; \mathbf{Z}_m^{n-1}, \mathbf{Z}_{n+m}^{2n-1}, \ldots, \mathbf{Z}_{(b-1)\cdot n+m}^{b\cdot n-1}\right) \\ \leq \epsilon_2 - \frac{2\eta}{n},\end{aligned} \tag{A.18b}$$

and

$$R_1 \geq R_s - \frac{\epsilon_3}{2}, \tag{A.18c}$$

where (a) and (b) follow since the n-MGMWTC is n-block memoryless, hence, the channel outputs and the probability of error are independent of the initial state, when the length of the codeword is an integer multiple of n. Denote this code by $\mathcal{C}_{b\cdot n}^{MG}$, and recall that from the definition of the n-MGMWTC, it follows that the decoders at the intended receiver and at the eavesdropper use only the last $n-m$ channel outputs out of each block of n consecutive channel outputs of the LGMWTC. Let $\mathbf{X}_{MG}^{b\cdot n-1}$ denote the codeword of length $b\cdot n$ used for transmitting a message $\zeta \in \mathcal{M}$ via the code $\mathcal{C}_{b\cdot n}^{MG}$ for the n-MGMWTC.

Next, based on the code $\mathcal{C}_{b\cdot n}^{MG}$, we construct a code for the LGMWTC with codeword length $l = b\cdot n + a$, where a can be selected arbitrarily from $a \in \{m, m+1, \ldots, n+m-1\}$. We denote this code by $\mathcal{C}_l^{LG}$, and in the following we analyze the performance of $\mathcal{C}_l^{LG}$. In the analysis we use $\bar{\mathbf{Y}}[i]$ and $\bar{\mathbf{Z}}[i]$ to denote the channel outputs of the LGMWTC at the intended receiver and at the eavesdropper, respectively, when the code $\mathcal{C}_l^{LG}$ is employed. The encoder of the $\mathcal{C}_l^{LG}$ code encodes the message $\zeta \in \mathcal{M}$ into the codeword $\mathbf{X}_{LG}^{l-1}$ by setting $\mathbf{X}_{LG}^{a-1} = \mathsf{0}_{a\cdot n_t \times 1}$ and setting $\mathbf{X}_{LG,a}^{l-1}$ to be equal to the codeword used for transmitting ζ using the $\mathcal{C}_{b\cdot n}^{MG}$ code, i.e., $\mathbf{X}_{LG,a}^{l-1} = \mathbf{X}_{MG}^{b\cdot n-1}$ for the same message ζ. The decoder of the $\mathcal{C}_l^{LG}$ code discards the first a channel outputs of the codeword, and then discards the first m channel outputs of each block of n channel outputs. The remaining channel outputs, namely $\bar{\mathbf{Y}}_{LG} \triangleq \left(\bar{\mathbf{Y}}_{a+m}^{n+a-1}, \bar{\mathbf{Y}}_{n+a+m}^{2n+a-1}, \ldots, \bar{\mathbf{Y}}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1}\right)$, are then used for decoding the message using the decoder for the $\mathcal{C}_{b\cdot n}^{MG}$ code.

Define

$$\mathbf{Y}_{MG} \triangleq \left(\mathbf{Y}_m^{n-1}, \mathbf{Y}_{n+m}^{2n-1}, \ldots, \mathbf{Y}_{(b-1)\cdot n+m}^{b\cdot n-1}\right),$$

and

$$\mathbf{W}_a \triangleq \left(\mathbf{W}_{a+m}^{n+a-1}, \mathbf{W}_{n+a+m}^{2n+a-1}, \ldots, \mathbf{W}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1}\right).$$

It follows from the definition of the LGMWTC that $\exists \bar{\mathsf{H}} \in \mathbb{R}^{n_r\cdot b\cdot (n-m)\times n_t\cdot b\cdot n}$ such that $\bar{\mathbf{Y}}_{LG} = \bar{\mathsf{H}}\mathbf{X}_{LG,a}^{l-1} + \mathbf{W}_a$ and also $\mathbf{Y}_{MG} = \bar{\mathsf{H}}\mathbf{X}_{MG}^{b\cdot n-1} + \mathbf{W}_0$. It now follows from the stationarity of $\mathbf{W}[i]$ and the relationship between $\mathcal{C}_l^{LG}$ and $\mathcal{C}_{b\cdot n}^{MG}$ that the decoder for the $\mathcal{C}_l^{LG}$ code operates on channel outputs which have the same statistical characterization as the channel outputs $\mathbf{Y}_{MG}$, which result from transmitting codewords using the $\mathcal{C}_{b\cdot n}^{MG}$ code. *Hence, the probability of error for the code* $\mathcal{C}_l^{LG}$ *is identical to that for the code* $\mathcal{C}_{b\cdot n}^{MG}$. Similarly, by defining $\bar{\mathbf{Z}}_{LG} \triangleq \left(\bar{\mathbf{Z}}_{a+m}^{n+a-1}, \bar{\mathbf{Z}}_{n+a+m}^{2n+a-1}, \ldots, \bar{\mathbf{Z}}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1}\right)$, $\mathbf{Z}_{MG} \triangleq \left(\mathbf{Z}_m^{n-1}, \mathbf{Z}_{n+m}^{2n-1}, \ldots, \mathbf{Z}_{(b-1)\cdot n+m}^{b\cdot n-1}\right)$ and $\mathbf{U}_a \triangleq \left(\mathbf{U}_{a+m}^{n+a-1}, \mathbf{U}_{n+a+m}^{2n+a-1}, \ldots, \mathbf{U}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1}\right)$, it follows that $\exists \bar{\mathsf{G}} \in \mathbb{R}^{n_e\cdot b\cdot (n-m)\times n_t\cdot b\cdot n}$ such that $\bar{\mathbf{Z}}_{LG} = \bar{\mathsf{G}}\mathbf{X}_{LG,a}^{l-1} + \mathbf{U}_a$ and also $\mathbf{Z}_{MG} = \bar{\mathsf{G}}\mathbf{X}_{MG}^{b\cdot n-1} + \mathbf{U}_0$, which implies that $\bar{\mathbf{Z}}_{LG}$ and $\mathbf{Z}_{MG}$ both have the same statistical characterization. Consequently,

$$\begin{aligned} I(M; \mathbf{Z}_{MG}) &\overset{(a)}{=} I\left(M, \mathbf{X}_{MG}^{b\cdot n-1}; \mathbf{Z}_{MG}\right) - I\left(\mathbf{X}_{MG}^{b\cdot n-1}; \mathbf{Z}_{MG} \middle| M\right) \\ &\overset{(b)}{=} I\left(\mathbf{X}_{MG}^{b\cdot n-1}; \mathbf{Z}_{MG}\right) - I\left(\mathbf{X}_{MG}^{b\cdot n-1}; \mathbf{Z}_{MG} \middle| M\right) \\ &\overset{(c)}{=} I\left(\mathbf{X}_{LG,a}^{l-1}; \bar{\mathbf{Z}}_{LG}\right) - I\left(\mathbf{X}_{LG,a}^{l-1}; \bar{\mathbf{Z}}_{LG} \middle| M\right) \\ &\overset{(d)}{=} I\left(M; \bar{\mathbf{Z}}_{LG}\right), \end{aligned} \tag{A.19}$$

where (a) follows from the chain rule for mutual information [52, Ch. 2.5]; (b) follows since $M \to \mathbf{X}_{MG}^{b\cdot n-1} \to \mathbf{Z}_{MG}$ form a Markov chain; (c) follows from the combination of the following three properties: (1) the stationarity of $\mathbf{U}[i]$; (2) the definition of the encoder of the $\mathcal{C}_l^{LG}$ code; (3) the fact that the channel matrix $\bar{\mathsf{G}}$ is identical for both the LGMWTC and the n-MGMWTC, which imply that the joint distribution of $\left(\mathbf{X}_{MG}^{b\cdot n-1}, \mathbf{Z}_{MG}\right)$ is identical to the joint distribution of $\left(\mathbf{X}_{LG,a}^{l-1}, \bar{\mathbf{Z}}_{LG}\right)$, and also implies that the joint distribution of $\left(\mathbf{X}_{MG}^{b\cdot n-1}, \mathbf{Z}_{MG}\right)$ given M is identical to the joint distribution of $\left(\mathbf{X}_{LG,a}^{l-1}, \bar{\mathbf{Z}}_{LG}\right)$ given M; and (d) follows from the

[7]Note that if every non-negative $R_s < \limsup_{n\to\infty} C_s^{n-MG}$ satisfies $R_s \leq C_s$, then necessarily, $\limsup_{n\to\infty} C_s^{n-MG} \leq C_s$. This follows since if $\limsup_{n\to\infty} C_s^{n-MG} > C_s$ then $\exists \tilde{R}_s$, such that $C_s < \tilde{R}_s < \limsup_{n\to\infty} C_s^{n-MG}$, i.e., $\tilde{R}_s$ does not satisfy out initial assumption.

construction of the $\mathcal{C}_l^{LG}$ code, which sets $\mathbf{X}_{LG}^{a-1}$ to be the all zero vector, and by applying the reverse of the transition from (a) to (b).

Next, let $\bar{\mathbf{Z}}^{l-1}$ denote the entire set of l vector channel outputs obtained when transmitting using the code $\mathcal{C}_l^{LG}$. When this transmission is applied, the information leakage rate for the LGMWTC satisfies

$$\begin{aligned}
&\sup_{\mathbf{s}_0\in\mathcal{S}_0}\frac{1}{l}I\left(M;\bar{\mathbf{Z}}^{l-1}\middle|\mathbf{S}_0=\mathbf{s}_0\right)\\
&\quad=\sup_{\mathbf{s}_0\in\mathcal{S}_0}\frac{1}{b\cdot n+a}I\left(M;\bar{\mathbf{Z}}^{b\cdot n+a-1}\middle|\mathbf{S}_0=\mathbf{s}_0\right)\\
&\quad\overset{(a)}{=}\sup_{\mathbf{s}_0\in\mathcal{S}_0}\frac{1}{b\cdot n+a}\Bigg(I\left(M;\bar{\mathbf{Z}}^{a-1}\middle|\mathbf{S}_0=\mathbf{s}_0\right)\\
&\qquad\qquad+I\left(M;\bar{\mathbf{Z}}_a^{b\cdot n+a-1}\middle|\bar{\mathbf{Z}}^{a-1},\mathbf{S}_0=\mathbf{s}_0\right)\Bigg)\\
&\quad\overset{(b)}{=}\sup_{\mathbf{s}_0\in\mathcal{S}_0}\frac{1}{b\cdot n+a}I\left(M;\bar{\mathbf{Z}}_a^{b\cdot n+a-1}\middle|\bar{\mathbf{Z}}^{a-1},\mathbf{S}_0=\mathbf{s}_0\right)\\
&\quad\overset{(c)}{=}\sup_{\mathbf{s}_0\in\mathcal{S}_0}\frac{1}{b\cdot n+a}I\left(M;\bar{\mathbf{Z}}_a^{b\cdot n+a-1}\middle|\mathbf{U}^{a-1},\mathbf{S}_0=\mathbf{s}_0\right)\\
&\quad\overset{(d)}{=}\frac{1}{b\cdot n+a}I\left(M;\bar{\mathbf{Z}}_a^{b\cdot n+a-1}\middle|\mathbf{U}_{a-m}^{a-1}\right),
\end{aligned}\tag{A.20}$$

where (a) follows from the chain rule for mutual information [52, Ch. 2.5]; (b) follows since when using the code $\mathcal{C}_l^{LG}$, the first a channel outputs depend only on the initial state and the noise, hence, M and $\bar{\mathbf{Z}}^{a-1}$ are mutually independent; (c) follows since $\mathbf{X}_{LG}^{a-1}$ is all zeros, thus $\exists\check{\mathbf{G}}\in\mathbb{R}^{n_e\cdot a\times n_t\cdot m}$ such that $\bar{\mathbf{Z}}^{a-1}=\check{\mathbf{G}}\mathbf{X}_{-m}^{-1}+\mathbf{U}^{a-1}$; (d) follows since the finite memory of the channel implies that $\bar{\mathbf{Z}}_a^{b\cdot n+a-1}$ is independent of the initial state and of $\mathbf{U}^{a-m-1}$, regardless of the code. This can be shown by noting that we can define a matrix $\check{\check{\mathbf{G}}}\in\mathbb{R}^{n_e\cdot b\cdot n\times n_t(b\cdot n+m)}$ such that $\bar{\mathbf{Z}}_a^{b\cdot n+a-1}=\check{\check{\mathbf{G}}}\mathbf{X}_{LG,a-m}^{b\cdot n+a-1}+\mathbf{U}_a^{b\cdot n+a-1}$, and noting that $\mathbf{X}_{LG}[i]$ is independent of both $\mathbf{U}^{a-m-1}$ and $\mathbf{S}_0$ for all $a\le i\le b\cdot n+a-1$, and that, due to the finite memory of the noise, then for all $i\ge a\ge m$ $\mathbf{U}[i]$ is independent of both $\mathbf{S}_0$ as well as $\mathbf{U}^{a-m-1}$. Next, we note that $\frac{1}{b\cdot n}I\left(M;\bar{\mathbf{Z}}_a^{b\cdot n+a-1}\middle|\mathbf{U}_{a-m}^{a-1}\right)$ can be upper bounded as stated in (A.21) as shown at the top of next page, where (a) follows from the chain rule for mutual information [52, Ch. 2.5]; (b) follows from the data-processing inequality [52, Ch. 2.8]; (c) follows from Lemma A.1, and from the finite memory of the channel which implies that for $i\ge a+m$ $\bar{\mathbf{Z}}[i]$ is independent of $\mathbf{U}_{a-m}^{a-1}$; (d) follows from (A.19); (e) follows from (A.18b). Plugging (A.21) into (A.20) yields

$$\sup_{\mathbf{s}_0\in\mathcal{S}_0}\frac{1}{l}I\left(M;\bar{\mathbf{Z}}^{l-1}\middle|\mathbf{S}_0=\mathbf{s}_0\right)\le\frac{b\cdot n}{b\cdot n+a}\left(\epsilon_2-\frac{\eta}{n}\right)\le\epsilon_2.$$

The code rate for $\mathcal{C}_l^{LG}$ is obtained from

$$\begin{aligned}
R_{LG}&=R_1\cdot\frac{b\cdot n}{b\cdot n+a}\\
&\overset{(a)}{\ge}\left(R_s-\frac{\epsilon_3}{2}\right)\frac{b\cdot n}{b\cdot n+a},
\end{aligned}$$

where (a) follows from (A.18c). Thus, for sufficiently large b, namely, $b>\frac{2a(R_s-\epsilon_3)}{n\cdot\epsilon_3}$, it follows that $R_{LG}\ge R_s-\epsilon_3$. It therefore follows that for all sufficiently large b and $a\in\{m,m+1,\ldots,n+m-1\}$, there exists a code for the LGMWTC with blocklength $l=b\cdot n+a$ which satisfies (4a)-(4c). Consequently, for any secrecy rate $R_s\le\limsup_{n\to\infty}C_s^{n-MG}$, $\exists l_0\in\mathbb{N}$ large enough such that reliable secure communications is achievable for the LGMWTC at any rate arbitrarily close to R_s, for all blocklengths larger than l_0. Thus, $R_s\le C_s$, from which it follows that $\limsup_{n\to\infty}C_s^{n-MG}\le C_s$. ■

Comment A.2: Note that without an eavesdropper, the n-MGMWTC becomes an instance to the n-block memoryless Gaussian multiterminal channel (n-MGMC), defined in [33, Appendix A], and the LGMWTC becomes an instance to the linear Gaussian multiterminal channel (LGMC), defined in [33, Appendix A]. In [33, Lemma 2] it is shown that the capacity of the n-MGMC is not greater than the capacity of the LGMC for all $n>2m$. However, when the eavesdropper is present, the secrecy capacity of the n-MGMWTC can be shown to be upper-bounded by that of the LGMWTC only for $n\to\infty$, as the information leakage due to the first m channel outputs of each n-block received at the eavesdropper, which are not accounted for in the leakage model of the n-MGMWTC, is negligible only for asymptotic blocklengths with $n\to\infty$.

Proposition A.2: The secrecy capacity of the LGMWTC defined in (2) *subject to the power constraint in* (3) *satisfies*

$$C_s=\lim_{n\to\infty}C_s^{n-MG},$$

where C_s^{n-MG} is the secrecy capacity of the n-MGMWTC, which is stated in (A.1)*, and the limit exists.*

Proof: By combining the above lemmas it follows that

$$\begin{aligned}
\limsup_{n\to\infty}C_s^{n-MG}&\overset{(a)}{\le}C_s\\
&\overset{(b)}{\le}\inf_{\mathbf{s}_0\in\mathcal{S}_0}\left(\liminf_{n\to\infty}C_n\left(\mathbf{s}_0\right)\right)\\
&\overset{(c)}{\le}\liminf_{n\to\infty}C_s^{n-MG},
\end{aligned}$$

where (a) follows from Lemma A.5, (b) follows from Lemma A.3, and (c) follows from Lemma A.4. Since $\liminf_{n\to\infty}C_s^{n-MG}\le\limsup_{n\to\infty}C_s^{n-MG}$, it follows from [43, Sec. 3.18] that

$$C_s=\lim_{n\to\infty}C_s^{n-MG},$$

and the limit exists. This proves the proposition. ■

C. Proving That $\lim_{n\to\infty}C_s^{n-MG}$ is Equal to $\lim_{n\to\infty}C_s^{n-CG}$

We next prove that in the limit of $n\to\infty$, the n-CGMWTC and the n-MGMWTC have the same secrecy capacity. This is done in the following steps:

- First, we obtain in Lemma A.6 an expression for the secrecy capacity of the n-CGMWTC, C_s^{n-CG}, by proving that it can be transformed into an equivalent memoryless MIMO WTC.
- Next, in Lemma A.7 we prove that for a single n-block, the mutual information between the channel input and

$$
\begin{aligned}
&\frac{1}{b\cdot n} I\left(M; \bar{\mathbf{Z}}_a^{b\cdot n+a-1} \middle| \mathbf{U}_{a-m}^{a-1}\right)\\
&\overset{(a)}{=} \frac{1}{b\cdot n} I\left(M; \bar{\mathbf{Z}}_{a+m}^{n+a-1}, \bar{\mathbf{Z}}_{n+a+m}^{2n+a-1}, \ldots, \bar{\mathbf{Z}}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1} \middle| \mathbf{U}_{a-m}^{a-1}\right)\\
&\quad + \frac{1}{b\cdot n}\Bigg(I\Big(M; \bar{\mathbf{Z}}_a^{a+m-1} \Big| \bar{\mathbf{Z}}_{a+m}^{n+a-1}, \bar{\mathbf{Z}}_{n+a+m}^{2n+a-1}, \ldots, \bar{\mathbf{Z}}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1}, \mathbf{U}_{a-m}^{a-1}\Big)\\
&\qquad + \sum_{k=1}^{b-1} I\Big(M; \bar{\mathbf{Z}}_{k\cdot n+a}^{k\cdot n+a+m-1} \Big| \bar{\mathbf{Z}}_{a+m}^{n+a-1}, \bar{\mathbf{Z}}_{n+a+m}^{2n+a-1}, \ldots, \bar{\mathbf{Z}}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1},\\
&\qquad\qquad \bar{\mathbf{Z}}_a^{a+m-1}, \bar{\mathbf{Z}}_{n+a}^{n+a+m-1}, \ldots, \bar{\mathbf{Z}}_{(k-1)\cdot n+a}^{(k-1)\cdot n+a+m-1}, \mathbf{U}_{a-m}^{a-1}\Big)\Bigg)\\
&\overset{(b)}{\leq} \frac{1}{b\cdot n} I\left(M; \bar{\mathbf{Z}}_{a+m}^{n+a-1}, \bar{\mathbf{Z}}_{n+a+m}^{2n+a-1}, \ldots, \bar{\mathbf{Z}}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1} \middle| \mathbf{U}_{a-m}^{a-1}\right)\\
&\quad + \frac{1}{b\cdot n}\Bigg(I\Big(\mathbf{X}_{LG}^{b\cdot n+a-1}; \bar{\mathbf{Z}}_a^{a+m-1} \Big| \bar{\mathbf{Z}}_{a+m}^{n+a-1}, \bar{\mathbf{Z}}_{n+a+m}^{2n+a-1}, \ldots, \bar{\mathbf{Z}}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1}, \mathbf{U}_{a-m}^{a-1}\Big)\\
&\qquad + \sum_{k=1}^{b-1} I\Big(\mathbf{X}_{LG}^{b\cdot n+a-1}; \bar{\mathbf{Z}}_{k\cdot n+a}^{k\cdot n+a+m-1} \Big| \bar{\mathbf{Z}}_{a+m}^{n+a-1}, \bar{\mathbf{Z}}_{n+a+m}^{2n+a-1}, \ldots, \bar{\mathbf{Z}}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1},\\
&\qquad\qquad \bar{\mathbf{Z}}_a^{a+m-1}, \bar{\mathbf{Z}}_{n+a}^{n+a+m-1}, \ldots, \bar{\mathbf{Z}}_{(k-1)\cdot n+a}^{(k-1)\cdot n+a+m-1}, \mathbf{U}_{a-m}^{a-1}\Big)\Bigg)\\
&\overset{(c)}{\leq} \frac{1}{b\cdot n} I\left(M; \bar{\mathbf{Z}}_{a+m}^{n+a-1}, \bar{\mathbf{Z}}_{n+a+m}^{2n+a-1}, \ldots, \bar{\mathbf{Z}}_{(b-1)\cdot n+a+m}^{b\cdot n+a-1}\right) + \frac{\eta}{n}\\
&\overset{(d)}{=} \frac{1}{b\cdot n} I\left(M; \mathbf{Z}_m^{n-1}, \mathbf{Z}_{n+m}^{2n-1}, \ldots, \mathbf{Z}_{(b-1)\cdot n+m}^{b\cdot n-1}\right) + \frac{\eta}{n}\\
&\overset{(e)}{\leq} \epsilon_2 - \frac{\eta}{n},
\end{aligned}
\tag{A.21}
$$

the last $n-m$ channel outputs is the same for both the n-CGMWTC and the n-MGMWTC.

- Then, we show in Lemma A.8 that the mutual information between the channel inputs and any m channel outputs of the n-CGMWTC can be upper bounded by a fixed and finite number.
- Lastly, in Proposition A.3 we use Lemma A.6, Lemma A.7, and Lemma A.8 to prove that there exists a finite η, such that $\forall n > 2m$, $C_s^{n-MG} - \frac{\eta}{n} \leq C_s^{n-CG} \leq C_s^{n-MG} + \frac{\eta}{n}$, thus in the limit of $n \to \infty$, C_s^{n-MG} is equal to C_s^{n-CG}.

Lemma A.6: The secrecy capacity of the n-CGMWTC subject to the power constraint in (3) *is given by*

$$
C_s^{n-CG} = \frac{1}{n} \sup_{\substack{p(\mathbf{V}^{n-1},\mathbf{X}^{n-1}):\\ \mathbb{E}\{\|\mathbf{X}[i]\|^2\}\leq P,\ \forall 0\leq i<n}} \left\{ I\left(\mathbf{V}^{n-1}; \underset{\sim}{\mathbf{Y}}^{n-1}\right) - I\left(\mathbf{V}^{n-1}; \underset{\sim}{\mathbf{Z}}^{n-1}\right) \right\}. \tag{A.22}
$$

Proof: The proof of this lemma follows the same outline as in the proof of Proposition A.1. We first show that (A.22) characterizes the maximum achievable secrecy rate when considering only codes whose blocklength is an integer multiple of n, i.e, $[R, b\cdot n]$ codes where b is a positive integer. This is proved by transforming the n-CGMWTC into an equivalent memoryless MIMO WTC using a bijective transformation, and then characterizing the capacity of the transformed channel. Then, we show that every secrecy rate achievable for the n-CGMWTC can be achieved by considering only codes whose blocklength is an integer multiple of n.

Let us consider the n-CGMWTC subject to the constraint that only codes with blocklengths that are integer multiples of n are allowed. In this case we can transform the channel into an equivalent $n\cdot n_t \times n\cdot n_r \times n\cdot n_e$ memoryless MIMO wiretap channel without loss of information, via the following assignment: Define the input of the transformed channel by the $n\cdot n_t \times 1$ vector $\mathbf{X}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{X}_{\tilde{i}\cdot n}^{\left(\tilde{i}+1\right)\cdot n-1}$, $\tilde{i} \geq 0$, the output at the intended receiver by the $n\cdot n_r \times 1$ vector $\mathbf{Y}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{Y}_{\tilde{i}\cdot n}^{\left(\tilde{i}+1\right)\cdot n-1}$, and the output at the eavesdropper by the $n\cdot n_e \times 1$ vector $\mathbf{Z}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{Z}_{\tilde{i}\cdot n}^{\left(\tilde{i}+1\right)\cdot n-1}$. The transformation is clearly bijective thus, the secrecy capacity of the transformed channel is equal to the secrecy capacity of the original channel. Since the n-CGMWTC is n-block memoryless, it follows from Def. 6 and Def. 7 that the transformed MIMO channel is memoryless. The outputs at the intended receiver and at the eavesdropper are corrupted by the additive noise vectors $\mathbf{W}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{W}_{\tilde{i}\cdot n}^{\left(\tilde{i}+1\right)\cdot n-1}$ and $\mathbf{U}_{eq}\left[\tilde{i}\right] \triangleq \mathbf{U}_{\tilde{i}\cdot n}^{\left(\tilde{i}+1\right)\cdot n-1}$, respectively. From the definition of $\mathbf{W}[i]$ and $\mathbf{U}[i]$ in Section III it follows that both $\mathbf{W}_{eq}\left[\tilde{i}\right]$ and $\mathbf{U}_{eq}\left[\tilde{i}\right]$ are zero-mean real Gaussian vectors with positive-definite covariance matrices (this follows since the elements of the random vectors are not linearly dependent, see [57, Ch. 8.1]).

From the construction of the transformed equivalent channel, the definition of the noises for the n-CGMWTC in the proof outline of Thm. 1, and of block-memorylessness in Def. 7, it follows that both $\underset{\sim}{\mathbf{W}}_{eq}\left[\tilde{i}\right]$ and $\underset{\sim}{\mathbf{U}}_{eq}\left[\tilde{i}\right]$ are i.i.d. and mutually independent. The secrecy capacity of the transformed channel, denoted C_n^{eq}, can be written in the form of the result of Csiszár and Körner [2, Eq. (11)]:

$$C_n^{eq} = \sup_{\substack{p(\mathbf{V}^{n-1},\mathbf{X}^{n-1}):\\ \mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\}\leq P,\ \forall 0\leq i<n}} \left\{ I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}^{n-1}\right) - I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}^{n-1}\right)\right\},$$

where the constraint $\mathbb{E}\left\{\|\mathbf{X}[i]\|^2\right\} \leq P,\ \forall 0 \leq i < n$ follows from the *per-symbol* power constraint of the n-CGMWTC. As each MIMO channel use corresponds to n channel uses in the original channel, it follows that the achievable secrecy rate of the n-CGMWTC, subject to the constraint that only codes with blocklengths that are integer multiples of n are allowed, in bits per channel use, is $\frac{1}{n}C_n^{eq}$, which coincides with (A.22).

Next, we show that any secrecy rate achievable for the n-CGMWTC can be achieved by considering only codes with blocklengths that are integer multiples of n: Consider a secrecy rate R_s achievable for the n-CGMWTC and fix ϵ_1, ϵ_2, and ϵ_3 to arbitrary positive real numbers. From Def. 4 it follows that $\exists n_0 > 0$ such that $\forall l > n_0$ there exists an $[R, l]$ code which satisfies (4a)-(4c). Thus, by setting b_0 as the smallest integer such that $b_0 \cdot n \geq n_0$ it follows that for all integer $b > b_0$ there exists a $[R, b \cdot n]$ code which satisfies (4a)-(4c). Therefore, the secrecy rate R_s is also achievable when considering only codes whose blocklength is an integer multiple of n. We therefore conclude that (A.22) denotes the maximum achievable secrecy rate for the n-CGMWTC, which completes the proof of the lemma. ∎

Lemma A.7: For any joint distribution $p\left(\mathbf{V}^{n-1},\mathbf{X}^{n-1}\right)$ *such that* $\mathbf{V}^{n-1} \to \mathbf{X}^{n-1} \to \mathbf{Y}_m^{n-1}, \mathbf{Z}_m^{n-1}$ *and* $\mathbf{V}^{n-1} \to \mathbf{X}^{n-1} \to \underset{\sim}{\mathbf{Y}}_m^{n-1}, \underset{\sim}{\mathbf{Z}}_m^{n-1}$ *form a Markov chain, the channel outputs of the n-MGMWTC and of the n-CGMWTC satisfy*

$$I\left(\mathbf{V}^{n-1};\mathbf{Y}_m^{n-1}\right) = I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right), \tag{A.23a}$$

and

$$I\left(\mathbf{V}^{n-1};\mathbf{Z}_m^{n-1}\right) = I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}_m^{n-1}\right). \tag{A.23b}$$

Proof: It follows from (2) and (8) that $\exists \underset{\sim}{\mathsf{H}} \in \mathbb{R}^{(n_r\cdot(n-m))\times(n_t\cdot n)}$ such that $\mathbf{Y}_m^{n-1} = \underset{\sim}{\mathsf{H}}\mathbf{X}^{n-1} + \mathbf{W}_m^{n-1}$ and $\underset{\sim}{\mathbf{Y}}_m^{n-1} = \underset{\sim}{\mathsf{H}}\mathbf{X}^{n-1} + \underset{\sim}{\mathbf{W}}_m^{n-1}$. Hence, as the channel input $\mathbf{X}^{n-1}$ is independent of the noise in both channels it follows that

$$\begin{aligned} p_{\mathbf{Y}_m^{n-1}\left|\mathbf{X}^{n-1}\right.}\left(\mathbf{y}_m^{n-1}\middle|\mathbf{x}^{n-1}\right) &= p_{\mathbf{W}_m^{n-1}}\left(\mathbf{y}_m^{n-1}-\underset{\sim}{\mathsf{H}}\mathbf{x}^{n-1}\right) \\ &\overset{(a)}{=} p_{\underset{\sim}{\mathbf{W}}_m^{n-1}}\left(\mathbf{y}_m^{n-1}-\underset{\sim}{\mathsf{H}}\mathbf{x}^{n-1}\right) \\ &= p_{\underset{\sim}{\mathbf{Y}}_m^{n-1}\left|\mathbf{X}^{n-1}\right.}\left(\mathbf{y}_m^{n-1}\middle|\mathbf{x}^{n-1}\right), \end{aligned} \tag{A.24}$$

where (a) follows as, by definition, the random vectors $\mathbf{W}_m^{n-1}$ and $\underset{\sim}{\mathbf{W}}_m^{n-1}$ are identically distributed, as both are zero-mean real Gaussian random vectors with the same correlation matrix: To see this, the $\forall i_1, i_2 \in \{m, m+1, \ldots, n-1\}$ we write

$$\begin{aligned} \mathbb{E}\left\{\underset{\sim}{\mathbf{W}}[i_1]\underset{\sim}{\mathbf{W}}^H[i_2]\right\} &= \mathsf{C}_{\underset{\sim}{\mathbf{W}}}[i_1-i_2] \\ &= \mathsf{C}_{\mathbf{W}}[i_1-i_2] + \mathsf{C}_{\mathbf{W}}[i_1-i_2+n] + \mathsf{C}_{\mathbf{W}}[i_1-i_2-n] \\ &\overset{(b)}{=} \mathsf{C}_{\mathbf{W}}[i_1-i_2] \\ &= \mathbb{E}\left\{\mathbf{W}[i_1]\mathbf{W}^H[i_2]\right\}, \end{aligned}$$

where (b) follows from (7a) as $|i_1 - i_2| < n - m$. It therefore follows that

$$\begin{aligned} &p_{\mathbf{V}^{n-1},\mathbf{Y}_m^{n-1}}\left(\mathbf{v}^{n-1},\mathbf{y}_m^{n-1}\right) \\ &= \int_{\mathbf{x}^{n-1}\in\mathbb{R}^{n_t\cdot n}} p_{\mathbf{V}^{n-1},\mathbf{X}^{n-1},\mathbf{Y}_m^{n-1}}\left(\mathbf{v}^{n-1},\mathbf{x}^{n-1},\mathbf{y}_m^{n-1}\right)d\mathbf{x}^{n-1} \\ &\overset{(a)}{=} \int_{\mathbf{x}^{n-1}\in\mathbb{R}^{n_t\cdot n}} p_{\mathbf{Y}_m^{n-1}\left|\mathbf{X}^{n-1}\right.}\left(\mathbf{y}_m^{n-1}\middle|\mathbf{x}^{n-1}\right) \\ &\qquad\times p_{\mathbf{V}^{n-1},\mathbf{X}^{n-1}}\left(\mathbf{v}^{n-1},\mathbf{x}^{n-1}\right)d\mathbf{x}^{n-1} \\ &\overset{(b)}{=} \int_{\mathbf{x}^{n-1}\in\mathbb{R}^{n_t\cdot n}} p_{\underset{\sim}{\mathbf{Y}}_m^{n-1}\left|\mathbf{X}^{n-1}\right.}\left(\mathbf{y}_m^{n-1}\middle|\mathbf{x}^{n-1}\right) \\ &\qquad\times p_{\mathbf{V}^{n-1},\mathbf{X}^{n-1}}\left(\mathbf{v}^{n-1},\mathbf{x}^{n-1}\right)d\mathbf{x}^{n-1} \\ &\overset{(c)}{=} \int_{\mathbf{x}^{n-1}\in\mathbb{R}^{n_t\cdot n}} p_{\mathbf{V}^{n-1},\mathbf{X}^{n-1},\underset{\sim}{\mathbf{Y}}_m^{n-1}}\left(\mathbf{v}^{n-1},\mathbf{x}^{n-1},\mathbf{y}_m^{n-1}\right)d\mathbf{x}^{n-1} \\ &= p_{\mathbf{V}^{n-1},\underset{\sim}{\mathbf{Y}}_m^{n-1}}\left(\mathbf{v}^{n-1},\mathbf{y}_m^{n-1}\right), \end{aligned} \tag{A.25}$$

where (a) follows since $\mathbf{V}^{n-1} \to \mathbf{X}^{n-1} \to \mathbf{Y}_m^{n-1}$ form a Markov chain; (b) follows from (A.24); and (c) follows since $\mathbf{V}^{n-1} \to \mathbf{X}^{n-1} \to \underset{\sim}{\mathbf{Y}}_m^{n-1}$ form a Markov chain. Equality (A.25) directly leads to (A.23a). The proof of (A.23b) is obtained using similar steps with the letters Y and W in the derivations of (A.24) and (A.25) replaced by Z and U, respectively. This completes the proof of the lemma. ∎

Lemma A.8: There exists a finite and fixed $\eta > 0$*, such that the channel outputs of the n-CGMWTC satisfy*

$$I\left(\mathbf{X}^{n-1};\underset{\sim}{\mathbf{Y}}^{m-1}\middle|\underset{\sim}{\mathbf{Y}}_m^{n-1}\right) \leq \underset{\sim}{\eta}, \tag{A.26a}$$

and

$$I\left(\mathbf{X}^{n-1};\underset{\sim}{\mathbf{Z}}^{m-1}\middle|\underset{\sim}{\mathbf{Z}}_m^{n-1}\right) \leq \underset{\sim}{\eta}. \tag{A.26b}$$

Proof: The proof follows similar steps as the proof of Lemma A.2 and will not be repeated here. ∎

Proposition A.3: The secrecy capacity of the n-MGMWTC and the secrecy capacity of the n-CGMWTC satisfy

$$\lim_{n\to\infty} C_s^{n-MG} = \lim_{n\to\infty} C_s^{n-CG}, \tag{A.27}$$

and the limits exist.

Proof: It follows from the mutual information chain rule [52, Sec. 2.5] that

$$\begin{aligned} &I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}^{n-1}\right)\\ &\quad= I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)+I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}^{m-1}\Big|\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)\\ &\quad\overset{(a)}{\leq} I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)+I\left(\mathbf{X}^{n-1};\underset{\sim}{\mathbf{Y}}^{m-1}\Big|\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)\\ &\quad\overset{(b)}{\leq} I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)+\underset{\sim}{\eta}, \end{aligned} \tag{A.28a}$$

where (a) follows from the data processing inequality [52, Thm. 2.8.1] and the Markov chain $\mathbf{V}^{n-1}\rightarrow\mathbf{X}^{n-1}\rightarrow\underset{\sim}{\mathbf{Y}}^{n-1},\underset{\sim}{\mathbf{Z}}^{n-1}$, and (b) follows from Lemma A.8. Similarly,

$$I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}^{n-1}\right)\leq I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}_m^{n-1}\right)+\underset{\sim}{\eta}. \tag{A.28b}$$

Now, for any given joint distribution $p\left(\mathbf{V}^{n-1},\mathbf{X}^{n-1}\right)$, it follows from (A.28a) that

$$\begin{aligned} &I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}^{n-1}\right)-I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}^{n-1}\right)\\ &\quad\leq I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)+\underset{\sim}{\eta}-I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}^{n-1}\right)\\ &\quad\overset{(a)}{\leq} I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)-I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}_m^{n-1}\right)+\underset{\sim}{\eta}\\ &\quad\overset{(b)}{=} I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)-I\left(\mathbf{V}^{n-1};\mathbf{Z}_m^{n-1}\right)+\underset{\sim}{\eta}, \end{aligned} \tag{A.29}$$

where (a) follows from the chain rule for mutual information [52, Sec. 2.5] and the fact that mutual information is non-negative; (b) follows from Lemma A.7. From Lemma A.6 it follows that

$$\begin{aligned} C_s^{n-CG}&=\frac{1}{n}\sup_{\substack{p(\mathbf{V}^{n-1},\mathbf{X}^{n-1}):\\ \mathbb{E}\{\|\mathbf{X}[i]\|^2\}\leq P,\ \forall 0\leq i<n}}\left\{I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}^{n-1}\right)\right.\\ &\qquad\left.-I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}^{n-1}\right)\right\}\\ &\overset{(a)}{\leq}\frac{1}{n}\sup_{\substack{p(\mathbf{V}^{n-1},\mathbf{X}^{n-1}):\\ \mathbb{E}\{\|\mathbf{X}[i]\|^2\}\leq P,\ \forall 0\leq i<n}}\left\{I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)\right.\\ &\qquad\left.-I\left(\mathbf{V}^{n-1};\mathbf{Z}_m^{n-1}\right)\right\}+\frac{\underset{\sim}{\eta}}{n}\\ &=C_s^{n-MG}+\frac{\underset{\sim}{\eta}}{n}, \end{aligned} \tag{A.30}$$

where (a) follows from (A.29).

Next, for any given $p\left(\mathbf{V}^{n-1},\mathbf{X}^{n-1}\right)$, we also have the following relationship

$$\begin{aligned} &I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)-I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}_m^{n-1}\right)\\ &\quad\overset{(a)}{=} I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)-I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}_m^{n-1}\right)\\ &\quad\overset{(b)}{\leq} I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)-I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}^{n-1}\right)+\underset{\sim}{\eta}\\ &\quad\overset{(c)}{\leq} I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}^{n-1}\right)-I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}^{n-1}\right)+\underset{\sim}{\eta}, \end{aligned} \tag{A.31}$$

where (a) follows from Lemma A.7; (b) follows from (A.28b); (c) follows from the chain rule for mutual information [52, Sec. 2.5] and as mutual information is non-negative which implies that $I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}^{n-1}\right)\geq I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)$. From the definition of C_s^{n-MG} in (A.1) it follows that

$$\begin{aligned} C_s^{n-MG}&=\frac{1}{n}\sup_{\substack{p(\mathbf{V}^{n-1},\mathbf{X}^{n-1}):\\ \mathbb{E}\{\|\mathbf{X}[i]\|^2\}\leq P,\ \forall 0\leq i<n}}\left\{I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}_m^{n-1}\right)\right.\\ &\qquad\left.-I\left(\mathbf{V}^{n-1};\mathbf{Z}_m^{n-1}\right)\right\}\\ &\overset{(a)}{\leq}\frac{1}{n}\sup_{\substack{p(\mathbf{V}^{n-1},\mathbf{X}^{n-1}):\\ \mathbb{E}\{\|\mathbf{X}[i]\|^2\}\leq P,\ \forall 0\leq i<n}}\left\{I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Y}}^{n-1}\right)\right.\\ &\qquad\left.-I\left(\mathbf{V}^{n-1};\underset{\sim}{\mathbf{Z}}^{n-1}\right)\right\}+\frac{\underset{\sim}{\eta}}{n}\\ &=C_s^{n-CG}+\frac{\underset{\sim}{\eta}}{n}, \end{aligned} \tag{A.32}$$

where (a) follows from (A.31). Combining (A.30) and (A.32) yields

$$C_s^{n-MG}-\frac{\underset{\sim}{\eta}}{n}\leq C_s^{n-CG}\leq C_s^{n-MG}+\frac{\underset{\sim}{\eta}}{n}. \tag{A.33}$$

Since $\lim_{n\rightarrow\infty}\frac{\underset{\sim}{\eta}}{n}=0$, and since $\lim_{n\rightarrow\infty}C_s^{n-MG}=C_s$ exists, letting $n\rightarrow\infty$ in (A.33) proves the proposition. ∎

Combining Propositions A.2 and A.3 proves Proposition 1.

Appendix B
Proof of Proposition 2

Recall that the secrecy capacity of the n-CGMWTC subject to the *per-symbol* power constraint (3), is denoted by C_s^{n-CG}. In order to derive the expression in (10) for C_s^{n-CG}, we first derive the secrecy capacity of the n-CGMWTC subject to the *time-averaged* power constraint [6, Sec. II], [31, Eq. (7)], [33, Eq. (7)]:

$$\mathbb{E}\left\{\frac{1}{l}\sum_{i=0}^{l-1}\|\mathbf{X}[i]\|^2\right\}\leq P, \tag{B.1a}$$

for all blocklengths l, and specifically, *for each n-block of the n-CGMWTC* we require,

$$\mathbb{E}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\|\mathbf{X}[i]\|^2\right\}\leq P. \tag{B.1b}$$

We denote the secrecy capacity of the n-CGMWTC subject to (B.1) with $C_{s,TA}^{n-CG}$. The derivation consists of the following steps:

- First, in Lemma B.1 we show that applying the DFT transforms the n-CGMWTC into a set of independent parallel MIMO WTCs. We then explain that any achievable rate for the n-CGMWTC can be obtained by considering only codewords whose length is an integer multiple of n.
- Next, in Lemma B.2 we derive the maximal achievable secrecy rate given a fixed power allocation, when the blocklength is an integer multiple of n, by a simple extension of the results of [19, Thm. 1]. We conclude that $C_{s,TA}^{n-CG}$ can be written as a maximization of the sum of the per-subchannel secrecy capacities over all power allocations satisfying a specified sum-power constraint.

- Then, in Lemma B.3 we characterize symmetry conditions on the maximal achievable secrecy rate expression and on the optimal input distribution for the n-CGMWTC, subject to (B.1). This results in an explicit expression for $C_{s,TA}^{n-CG}$ stated in (B.14).
- Lastly, in Corollary B.1 we prove that $C_s^{n-CG} = C_{s,TA}^{n-CG}$.

The approach of characterizing the capacity of a channel subject to a per-symbol power constraint by considering a time-averaged power constraint was also used in [31] for the point-to-point LTI channel (without an eavesdropper).

We begin with some preliminary properties of the multivariate DFT defined in (1). Recall that in (1), each entry $l \in \{0, 1, \ldots, n_q - 1\}$ of the multivariate DFT $\left\{\hat{\mathbf{q}}[k]\right\}_{k=0}^{n-1}$ is obtained as the scalar DFT of the l-th entries of the sequence of vectors $\{\mathbf{q}[i]\}_{i=0}^{n-1}$. Consequently, the following properties of the multivariate DFT of real-valued multivariate sequences can be obtained as straightforward extensions of the corresponding properties of scalar DFTs, see, e.g., [56, Ch. 8.5-8.6]:

P1 The multivariate DFT defined in (1) is invertible, and the l-th entry of the inverse DFT is obtained as the scalar inverse DFT of the set of the l-th entries of the sequence of vectors $\left\{\hat{\mathbf{q}}[k]\right\}_{k=0}^{n-1}$. Hence, we can write

$$\mathbf{q}[i] = \frac{1}{n}\sum_{k=0}^{n-1} \hat{\mathbf{q}}[k] e^{j2\pi \frac{ik}{n}}. \tag{B.2}$$

P2 Since $\mathbf{q}[i]$ is real, then $\hat{\mathbf{q}}[k] = \left(\hat{\mathbf{q}}[n-k]\right)^*$ for all $1 \leq k \leq n-1$. Consequently, $\left\{\hat{\mathbf{q}}[k]\right\}_{k=0}^{n-1}$ can be obtained from $\left\{\hat{\mathbf{q}}[k]\right\}_{k=0}^{\lfloor \frac{n}{2} \rfloor}$. Note that $\hat{\mathbf{q}}[0]$ is real for any n and that $\hat{\mathbf{q}}\left[\lfloor \frac{n}{2} \rfloor\right]$ is real for even n.

P3 Parseval's relationship for the multivariate DFT is given by $\sum_{i=0}^{n-1} \|\mathbf{q}[i]\|^2 = \frac{1}{n}\sum_{k=0}^{n-1} \left\|\hat{\mathbf{q}}[k]\right\|^2$.

P4 The DFT of a multivariate circular convolution is the product of the corresponding DFT sequences: Let $n_{q_1}, n_{q_2} \in \mathbb{N}$, and consider the pair of sequences of length n, $\mathbf{p}[i] \in \mathbb{R}^{n_{q_1}}$ and $\mathsf{R}[i] \in \mathbb{R}^{n_{q_2} \times n_{q_1}}$, $i \in \mathcal{N}$. Let $\left\{\hat{\mathbf{p}}[k]\right\}_{k=0}^{n-1}$ be the n-point DFT of $\{\mathbf{p}[i]\}_{i=0}^{n-1}$, and define $\hat{\mathsf{R}}[k] \triangleq \sum_{i=0}^{n-1} \mathsf{R}[i] e^{-j2\pi \frac{ik}{n}}$, $k \in \mathcal{N}$. Consider the sequence $\{\mathbf{q}[i]\}_{i=0}^{n-1}$ given by $\mathbf{q}[i] = \sum_{\tau=0}^{n-1} \mathsf{R}[\tau]\mathbf{p}\left[((i-\tau))_n\right]$. The n-point DFT of $\{\mathbf{q}[i]\}_{i=0}^{n-1}$ is given by $\hat{\mathbf{q}}[k] = \hat{\mathsf{R}}[k]\hat{\mathbf{p}}[k]$, $k \in \mathcal{N}$.

A. Step 1: Transforming the n-CGMWTC Into a Set of Independent Parallel MIMO WTCs

Focusing on the n-CGMWTC, consider the input sequence transmitted during one n-block, $\mathbf{X}^{n-1}$, and the corresponding channel outputs observed at the intended receiver and at the eavesdropper, denoted $\underset{\sim}{\mathbf{Y}}^{n-1}$ and $\underset{\sim}{\mathbf{Z}}^{n-1}$, respectively. Recall that by definition of the n-CGMWTC, the outputs are independent of the initial channel state $\mathbf{S}_0$. For $\tau \in \mathcal{N}$ define the zero-padded extensions of the Tx–Rx and of the Tx–Ev channel impulse responses by $\underset{\sim}{\mathsf{H}}[\tau]$ and $\underset{\sim}{\mathsf{G}}[\tau]$, respectively, where $\underset{\sim}{\mathsf{H}}[\tau] = \mathsf{H}[\tau]$ and $\underset{\sim}{\mathsf{G}}[\tau] = \mathsf{G}[\tau]$ for $0 \leq \tau \leq m$, while $\underset{\sim}{\mathsf{H}}[\tau] = \mathsf{0}_{n_r \times n_t}$ and $\underset{\sim}{\mathsf{G}}[\tau] = \mathsf{0}_{n_e \times n_t}$ for $m < \tau < n$. Using these definitions, Eqn. (8) can be written as

$$\underset{\sim}{\mathbf{Y}}[i] = \sum_{\tau=0}^{n-1} \underset{\sim}{\mathsf{H}}[\tau]\mathbf{X}\left[((i-\tau))_n\right] + \underset{\sim}{\mathbf{W}}[i] \tag{B.3a}$$

$$\underset{\sim}{\mathbf{Z}}[i] = \sum_{\tau=0}^{n-1} \underset{\sim}{\mathsf{G}}[\tau]\mathbf{X}\left[((i-\tau))_n\right] + \underset{\sim}{\mathbf{U}}[i], \tag{B.3b}$$

$i \in \mathcal{N}$. Let $\left\{\hat{\mathbf{X}}[k]\right\}_{k=0}^{n-1}$, $\left\{\hat{\underset{\sim}{\mathbf{Y}}}[k]\right\}_{k=0}^{n-1}$, and $\left\{\hat{\underset{\sim}{\mathbf{Z}}}[k]\right\}_{k=0}^{n-1}$ be the n-point DFTs of $\left\{\mathbf{X}[i]\right\}_{i=0}^{n-1}$, $\left\{\underset{\sim}{\mathbf{Y}}[i]\right\}_{i=0}^{n-1}$, and $\left\{\underset{\sim}{\mathbf{Z}}[i]\right\}_{i=0}^{n-1}$, respectively. Note that $\hat{\mathsf{H}}[k]$ and $\hat{\mathsf{G}}[k]$, defined in Section III-B in terms of $\{\mathsf{H}[\tau]\}_{\tau=0}^{m}$ and $\{\mathsf{G}[\tau]\}_{\tau=0}^{m}$, can be equivalently stated in terms of $\left\{\underset{\sim}{\mathsf{H}}[\tau]\right\}_{\tau=0}^{n-1}$ and $\left\{\underset{\sim}{\mathsf{G}}[\tau]\right\}_{\tau=0}^{n-1}$ via $\hat{\mathsf{H}}[k] = \sum_{\tau=0}^{n-1} \underset{\sim}{\mathsf{H}}[\tau] e^{-j2\pi \frac{\tau k}{n}}$ and $\hat{\mathsf{G}}[k] = \sum_{\tau=0}^{n-1} \underset{\sim}{\mathsf{G}}[\tau] e^{-j2\pi \frac{\tau k}{n}}$. Using the sequences $\left\{\hat{\underset{\sim}{\mathbf{W}}}[k]\right\}_{k=0}^{n-1}$ and $\left\{\hat{\underset{\sim}{\mathbf{U}}}[k]\right\}_{k=0}^{n-1}$, which correspond to the DFTs of $\{\underset{\sim}{\mathbf{W}}[i]\}_{i=0}^{n-1}$ and $\{\underset{\sim}{\mathbf{U}}[i]\}_{i=0}^{n-1}$, respectively (see Subsection III-B) and property *P4* for the DFT of a multivariate circular convolution, we obtain the following relationships:

$$\hat{\underset{\sim}{\mathbf{Y}}}[k] = \hat{\mathsf{H}}[k]\hat{\mathbf{X}}[k] + \hat{\underset{\sim}{\mathbf{W}}}[k] \tag{B.4a}$$

$$\hat{\underset{\sim}{\mathbf{Z}}}[k] = \hat{\mathsf{G}}[k]\hat{\mathbf{X}}[k] + \hat{\underset{\sim}{\mathbf{U}}}[k], \tag{B.4b}$$

$k \in \mathcal{N}$. Since the DFT is an invertible transformation and the channel outputs are real, it follows that the channel outputs $\{\underset{\sim}{\mathbf{Y}}[i]\}_{i\in\mathcal{N}}$ and $\{\underset{\sim}{\mathbf{Z}}[i]\}_{i\in\mathcal{N}}$ can be obtained from (B.4) for $k \in \{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor\} \triangleq \mathcal{L}_{CG}$. Therefore, it is sufficient to consider $\left\{\hat{\underset{\sim}{\mathbf{Y}}}[k]\right\}_{k\in\mathcal{L}_{CG}}$ and $\left\{\hat{\underset{\sim}{\mathbf{Z}}}[k]\right\}_{k\in\mathcal{L}_{CG}}$ for deriving the secrecy capacity of the n-CGMWTC. Define next

$$P_k \triangleq \mathbb{E}\left\{\left\|\hat{\mathbf{X}}[k]\right\|^2\right\}. \tag{B.5}$$

The average power constraint (B.1) yields a per n-block power constraint

$$\begin{aligned} n^2 P &\geq n\mathbb{E}\left\{\sum_{i=0}^{n-1} \|\mathbf{X}[i]\|^2\right\} \\ &\overset{(a)}{=} \mathbb{E}\left\{\sum_{k=0}^{n-1} \left\|\hat{\mathbf{X}}[k]\right\|^2\right\} \\ &= \sum_{k=0}^{n-1} P_k, \end{aligned} \tag{B.6}$$

where (a) follows from Parseval's relationship (property *P3*). As $\hat{\mathbf{X}}[k] = \left(\hat{\mathbf{X}}[n-k]\right)^*$, it follows that $P_{n-k} = P_k$ must hold. In conclusion, when the codeword length is an integer multiple of n, then the secrecy capacity of the n-CGMWTC (8) subject to the time-averaged power constraint (B.1) is equal to the secrecy capacity of the memoryless WTC (B.4) subject to the power constraint (B.6).

Finally, as explained in the last paragraph in the proof of Lemma A.6, the capacity of the n-CGMWTC can be completely characterized by considering only codewords whose length is an integer multiple of n.

Lemma B.1: For $k \in \mathcal{L}_{CG}$, $\hat{\underset{\sim}{W}}[k]$ and $\hat{\underset{\sim}{U}}[k]$ are zero mean Gaussian random vectors statistically independent over k, i.e., for all $k_1 \neq k_2$, $\hat{\underset{\sim}{W}}[k_1]$ and $\hat{\underset{\sim}{W}}[k_2]$ are independent, and $\hat{\underset{\sim}{U}}[k_1]$ and $\hat{\underset{\sim}{U}}[k_2]$ are independent. For $1 \leq k < \frac{n}{2}$, $\hat{\underset{\sim}{W}}[k]$ and $\hat{\underset{\sim}{U}}[k]$ are circularly symmetric complex random vectors, and for $k = 0$, and also for $k = \frac{n}{2}$ when n is even, $\hat{\underset{\sim}{W}}[k]$ and $\hat{\underset{\sim}{U}}[k]$ are zero-mean real Gaussian random vectors. The covariance matrices are given by

$$\mathsf{C}_{\hat{\underset{\sim}{W}}}[k] \triangleq \mathbb{E}\left\{\hat{\underset{\sim}{W}}[k]\left(\hat{\underset{\sim}{W}}[k]\right)^H\right\} = n\sum_{\tau=-m}^{m}\mathsf{C}_{\mathbf{W}}[\tau]\, e^{-j2\pi\frac{k\tau}{n}} \tag{B.7a}$$

and

$$\mathsf{C}_{\hat{\underset{\sim}{U}}}[k] \triangleq \mathbb{E}\left\{\hat{\underset{\sim}{U}}[k]\left(\hat{\underset{\sim}{U}}[k]\right)^H\right\} = n\sum_{\tau=-m}^{m}\mathsf{C}_{\mathbf{U}}[\tau]\, e^{-j2\pi\frac{k\tau}{n}}. \tag{B.7b}$$

Furthermore, for each fixed k_1, $\hat{\underset{\sim}{W}}[k_1]$ obtained from different n-blocks are i.i.d., and also $\hat{\underset{\sim}{U}}[k_1]$ obtained from different n-blocks are i.i.d. Finally, $\hat{\underset{\sim}{W}}[k_1]$ and $\hat{\underset{\sim}{U}}[k_2]$ are mutually independent for any $(k_1, k_2) \in \mathcal{L}_{CG} \times \mathcal{L}_{CG}$

Proof: The proof follows similar arguments to those used in the proof in [33, Appendix B] for scalar noises and is thus omitted here. Please refer to [64] for the detailed proof. ∎

Since the noises $\left\{\hat{\underset{\sim}{W}}[k]\right\}_{k\in\mathcal{L}_{CG}}$, $\left\{\hat{\underset{\sim}{U}}[k]\right\}_{k\in\mathcal{L}_{CG}}$ are mutually independent it follows that the channels (B.4) are *parallel* Gaussian channels.

B. Step 2: The Maximal Achievable Secrecy Rate $C_{s,TA}^{n-CG}$

Define for $k \in \mathcal{L}_{CG}$

$$R_n^k(P_k) \triangleq \sup_{\substack{p\left(\mathbf{V}[k],\hat{\mathbf{X}}[k]\right),\\ \mathbb{E}\left\{\left\|\hat{\mathbf{X}}[k]\right\|^2\right\}\leq P_k}} \left\{I\left(\mathbf{V}[k];\hat{\underset{\sim}{\mathbf{Y}}}[k]\right) - I\left(\mathbf{V}[k];\hat{\underset{\sim}{\mathbf{Z}}}[k]\right)\right\}. \tag{B.8}$$

Note that $R_n^k(P_k)$ represents the secrecy capacity of an $n_t \times n_r \times n_e$ *memoryless* MIMO WTC with additive Gaussian noise i.i.d. in time, subject to input power constraint P_k [6, Corollary 1]. Let $R_n'\left(\{P_k\}_{k=0}^{\lfloor\frac{n}{2}\rfloor}\right)$ denote the maximal achievable secrecy rate for the WTC (B.4) subject to a given a set of per-channel power constraints $\left\{\mathbb{E}\left\{\left\|\hat{\mathbf{X}}[k]\right\|^2\right\} \leq P_k\right\}_{k=0}^{\lfloor\frac{n}{2}\rfloor}$.

Lemma B.2: When the codeword length is restricted to be an integer multiple of n, $R_n'\left(\{P_k\}_{k=0}^{\lfloor\frac{n}{2}\rfloor}\right)$ satisfies:

$$R_n'\left(\{P_k\}_{k=0}^{\lfloor\frac{n}{2}\rfloor}\right) = \sum_{k=0}^{\lfloor\frac{n}{2}\rfloor} R_n^k(P_k). \tag{B.9}$$

Proof: From Lemma B.1 we have that the noises at each subchannel k are each i.i.d. over different n-blocks, and that the noises at subchannel k are independent of the noises at all other subchannels. It thus follows that (B.4) can be considered as $\lfloor\frac{n}{2}\rfloor + 1$ *parallel memoryless MIMO WTCs* (e.g., by extending the definition in [19, Sec. 1.3] for scalar channels to the MIMO case). In [19, Thm. 1] it was shown that the secrecy capacity of independent memoryless parallel *scalar* WTCs is given by the sum of the secrecy capacities of each subchannel. Although differently from [19, Sec. 1.3], which considered the secrecy capacity of parallel scalar WTCs, in the current analysis we consider the maximization of the achievable secrecy rate of parallel *MIMO* WTCs *subject to a fixed per-subchannel power allocation*, the proof for our case follows identical steps to the proof of [19, Thm. 1], and thus it is not repeated here. ∎

Note that (B.9) is the *maximum* achievable secrecy rate for the WTC (B.4) *for a given assignment of* $\{P_k\}_{k=0}^{\lfloor\frac{n}{2}\rfloor}$ when the codeword length is an integer multiple of n; The secrecy capacity of the n-CGMWTC subject to the power constraint (B.1) is therefore obtained by finding the assignment of $\{P_k\}_{k=0}^{\lfloor\frac{n}{2}\rfloor}$ which maximizes (B.9) subject to (B.6) while the set $\{P_k\}_{k=0}^{n-1}$ is constrained to satisfy $P_{n-k} = P_k$ for every $1 \leq k < \frac{n}{2}$. As each of the $\lfloor\frac{n}{2}\rfloor$ channel uses - one for each subchannel in the set of $\lfloor\frac{n}{2}\rfloor$ parallel subchannels, corresponds to n channel uses of the n-CGMWTC, we can summarize the above discussion in the following result

$$\begin{aligned} C_{s,TA}^{n-CG} &= \frac{1}{n}\max_{\substack{\{P_k\}_{k=0}^{\lfloor\frac{n}{2}\rfloor}:\\ \sum_{k=0}^{n-1}P_k\leq n^2P,\, P_{n-k}=P_k>0}} R_n'\left(\{P_k\}_{k=0}^{\lfloor\frac{n}{2}\rfloor}\right) \\ &= \max_{\substack{\{P_k\}_{k=0}^{\lfloor\frac{n}{2}\rfloor}:\\ \sum_{k=0}^{n-1}P_k\leq n^2P,\, P_{n-k}=P_k>0}} \frac{1}{n}\sum_{k=0}^{\lfloor\frac{n}{2}\rfloor} R_n^k(P_k). \end{aligned} \tag{B.10}$$

C. Step 3: Deriving an Explicit Expression for the Maximization (B.10)

Define $\tilde{\mathcal{L}}^n$ as $\tilde{\mathcal{L}}^n = \{0\}$ for n odd and $\tilde{\mathcal{L}}^n = \left\{0, \frac{n}{2}\right\}$ for n even. From Lemma B.1, it follows that for $1 \leq k < \frac{n}{2}$, the k-th subchannel is a *complex* memoryless MIMO WTC with circularly symmetric complex normal additive white Gaussian noise. For the remaining values of k, i.e., for $k \in \tilde{\mathcal{L}}^n$, it follows from Lemma B.1 that the k-th subchannel is a *real* memoryless Gaussian MIMO WTC. For a fixed $\rho \geq 0$, let $\mathcal{Q}_\rho$ be the set of $n_t \times n_t$ Hermitian positive semi-definite matrices Q such that $\mathrm{Tr}(\mathsf{Q}) \leq \rho$. We define[8] for $k \in \mathcal{N}$,

$$\tilde{R}_n^k(\rho) \triangleq \max_{\mathsf{Q}\in\mathcal{Q}_\rho}\frac{1}{2}\log\frac{\left|\mathsf{I}_{n_r} + \hat{\mathsf{H}}[k]\mathsf{Q}\left(\hat{\mathsf{H}}[k]\right)^H\left(\mathsf{C}_{\hat{\underset{\sim}{W}}}[k]\right)^{-1}\right|}{\left|\mathsf{I}_{n_e} + \hat{\mathsf{G}}[k]\mathsf{Q}\left(\hat{\mathsf{G}}[k]\right)^H\left(\mathsf{C}_{\hat{\underset{\sim}{U}}}[k]\right)^{-1}\right|}. \tag{B.11}$$

Lemma B.3: For $\lfloor\frac{n}{2}\rfloor < k < n$, $\tilde{R}_n^k(\rho) = \tilde{R}_n^{n-k}(\rho)$. When $\tilde{R}_n^k(\rho)$ is obtained with Q_{opt}, then $\tilde{R}_n^{n-k}(\rho)$ is obtained with Q_{opt}^*.

Proof: Define

$$\mathsf{F}_r^k(\mathsf{Q}) \triangleq \mathsf{I}_{n_r} + \left(\mathsf{C}_{\hat{\underset{\sim}{W}}}[k]\right)^{-\frac{1}{2}}\hat{\mathsf{H}}[k]\mathsf{Q}\left(\hat{\mathsf{H}}[k]\right)^H\left(\mathsf{C}_{\hat{\underset{\sim}{W}}}[k]\right)^{-\frac{1}{2}},$$

[8]Following [6, (20)] and [7, Thm. 1], $\tilde{R}_n^k(\rho)$ can be written as a maximization over $\mathcal{Q}_\rho$, instead of a supremum.

and

$$\mathsf{F}_e^k(\mathsf{Q}) \triangleq \mathsf{I}_{n_e} + \left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{U}}}}[k]\right)^{-\frac{1}{2}} \hat{\mathsf{G}}[k]\mathsf{Q}\left(\hat{\mathsf{G}}[k]\right)^H \left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{U}}}}[k]\right)^{-\frac{1}{2}}.$$

Since $\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[k]$ and $\mathsf{C}_{\hat{\underset{\sim}{\mathbf{U}}}}[k]$ are positive-definite Hermitian matrices $\forall k \in \mathcal{N}$, it follows from [62, Thm. 7.2.6] that $\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[k]\right)^{-\frac{1}{2}}$ and $\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{U}}}}[k]\right)^{-\frac{1}{2}}$ are also positive-definite Hermitian matrices. Thus, $\forall \mathsf{Q} \in \mathcal{Q}_\rho$, $\mathsf{F}_r^k(\mathsf{Q})$ and $\mathsf{F}_e^k(\mathsf{Q})$ are Hermitian matrices.

As $\mathsf{H}[\tau]$ and $\mathsf{G}[\tau]$ are real matrices, it follows that $\hat{\mathsf{H}}[n-k] = \left(\hat{\mathsf{H}}[k]\right)^*$ and $\hat{\mathsf{G}}[n-k] = \left(\hat{\mathsf{G}}[k]\right)^*$. Note that due to Hermitian and positive definiteness of the covariance matrices of the noises we have that $\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[n-k]\right)^{-\frac{1}{2}} = \left(\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[k]\right)^{-\frac{1}{2}}\right)^*$ and $\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{U}}}}[n-k]\right)^{-\frac{1}{2}} = \left(\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{U}}}}[k]\right)^{-\frac{1}{2}}\right)^*$. It therefore follows that

$$\begin{aligned}
&\left(\mathsf{F}_r^k(\mathsf{Q})\right)^* \\
&= \left(\mathsf{I}_{n_r} + \left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[k]\right)^{-\frac{1}{2}} \hat{\mathsf{H}}[k]\mathsf{Q}\left(\hat{\mathsf{H}}[k]\right)^H \left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[k]\right)^{-\frac{1}{2}}\right)^* \\
&\overset{(a)}{=} \mathsf{I}_{n_r} + \left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[n-k]\right)^{-\frac{1}{2}} \hat{\mathsf{H}}[n-k]\mathsf{Q}^*\left(\hat{\mathsf{H}}[n-k]\right)^H \\
&\qquad\qquad \times \left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[n-k]\right)^{-\frac{1}{2}} \\
&= \mathsf{F}_r^{n-k}\left(\mathsf{Q}^*\right), \qquad \text{(B.12)}
\end{aligned}$$

where (a) follows from [61, Ch. 3.6], and from plugging $\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[n-k]\right)^{-\frac{1}{2}} = \left(\left(\mathsf{C}_{\hat{\underset{\sim}{\mathbf{W}}}}[k]\right)^{-\frac{1}{2}}\right)^*$ and $\hat{\mathsf{H}}[n-k] = \left(\hat{\mathsf{H}}[k]\right)^*$. Similarly, $\mathsf{F}_e^k(\mathsf{Q}) = \left(\mathsf{F}_e^{n-k}(\mathsf{Q}^*)\right)^*$. Therefore

$$\begin{aligned}
\tilde{R}_n^{n-k}(\rho) &\overset{(a)}{=} \max_{\mathsf{Q}\in\mathcal{Q}_\rho} \frac{1}{2}\log\frac{\left|\mathsf{F}_r^{n-k}(\mathsf{Q})\right|}{\left|\mathsf{F}_e^{n-k}(\mathsf{Q})\right|} \\
&\overset{(b)}{=} \max_{\mathsf{Q}\in\mathcal{Q}_\rho} \frac{1}{2}\log\frac{\left|\mathsf{F}_r^{k}(\mathsf{Q}^*)\right|}{\left|\mathsf{F}_e^{k}(\mathsf{Q}^*)\right|} \\
&\overset{(c)}{=} \max_{\mathsf{Q}\in\mathcal{Q}_\rho} \frac{1}{2}\log\frac{\left|\mathsf{F}_r^{k}(\mathsf{Q})\right|}{\left|\mathsf{F}_e^{k}(\mathsf{Q})\right|} \\
&= \tilde{R}_n^k(\rho),
\end{aligned}$$

where (a) follows from applying Sylvester's determinant theorem [61, Ch. 6.2] to (B.11); (b) follows since the determinant of a Hermitian matrix is the same as the determinant of its conjugate [61, Ch. 7.5], thus $\left|\mathsf{F}_r^{n-k}(\mathsf{Q})\right| = \left|\left(\mathsf{F}_r^{n-k}(\mathsf{Q})\right)^*\right| = \left|\left(\mathsf{F}_r^{k}(\mathsf{Q}^*)\right)\right|$ and $\left|\mathsf{F}_e^{n-k}(\mathsf{Q})\right| = \left|\left(\mathsf{F}_e^{n-k}(\mathsf{Q})\right)^*\right| = \left|\left(\mathsf{F}_e^{k}(\mathsf{Q}^*)\right)\right|$; (c) follows since the definition of $\mathcal{Q}_\rho$ implies that if $\mathsf{Q} \in \mathcal{Q}_\rho$ then also $\mathsf{Q}^* \in \mathcal{Q}_\rho$. Let $\mathsf{Q}_{opt} \triangleq \arg\max_{\mathsf{Q}\in\mathcal{Q}_\rho} \frac{1}{2}\log\frac{\left|\mathsf{F}_r^k(\mathsf{Q})\right|}{\left|\mathsf{F}_e^k(\mathsf{Q})\right|}$. Since $\frac{1}{2}\log\frac{\left|\mathsf{F}_r^k(\mathsf{Q}_{opt})\right|}{\left|\mathsf{F}_e^k(\mathsf{Q}_{opt})\right|} = \frac{1}{2}\log\frac{\left|\mathsf{F}_r^{n-k}\left(\mathsf{Q}_{opt}^*\right)\right|}{\left|\mathsf{F}_e^{n-k}\left(\mathsf{Q}_{opt}^*\right)\right|}$, it follows that Q_{opt}^* maximizes $\frac{1}{2}\log\frac{\left|\mathsf{F}_r^{n-k}(\mathsf{Q})\right|}{\left|\mathsf{F}_e^{n-k}(\mathsf{Q})\right|}$. This proves the lemma. ∎

It follows from [6, Thm. 1], [7, Thm. 1], and [8, Corollary 1] that $R_n^k(P_k)$ defined in (B.8) is given by

$$R_n^k(P_k) = \begin{cases} 2\tilde{R}_n^k(P_k) & 1 \le k < \frac{n}{2} \\ \tilde{R}_n^k(P_k) & k \in \tilde{\mathcal{L}}^n \end{cases}, \qquad \text{(B.13)}$$

and that the maximizing channel input for the k-th subchannel, $\hat{\mathbf{X}}[k]$, is circularly symmetric complex normal for $1 \le k < \frac{n}{2}$ and zero-mean normal for $k \in \tilde{\mathcal{L}}^n$, with the covariance matrix of $\hat{\mathbf{X}}[k]$, denoted $\mathsf{C}_{\hat{\mathbf{X}}}[k]$, satisfying $\mathrm{Tr}\left(\mathsf{C}_{\hat{\mathbf{X}}}[k]\right) \le P_k$. Let $\mathcal{B}_P^n$ be the set of containing all sets of non-negative scalars $\{P_k\}_{k=0}^{n-1}$ such that $\sum_{k=0}^{n-1} P_k \le n^2 P$ and $P_k = P_{n-k}$. Plugging (B.13) into (B.10) yields

$$\begin{aligned}
C_{s,TA}^{n-CG} &= \max_{\{P_k\}_{k=0}^{n-1}\in\mathcal{B}_P^n} \frac{1}{n}\left(\sum_{k=0}^{\lfloor\frac{n}{2}\rfloor} \tilde{R}_n^k(P_k) + \sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor} \tilde{R}_n^k(P_k)\right) \\
&= \max_{\{P_k\}_{k=0}^{n-1}\in\mathcal{B}_P^n} \frac{1}{n}\left(\sum_{k=0}^{\lfloor\frac{n}{2}\rfloor} \tilde{R}_n^k(P_k) + \sum_{k=\lfloor\frac{n}{2}\rfloor+1}^{n-1} \tilde{R}_n^k(P_k)\right) \\
&\overset{(a)}{=} \max_{\{P_k\}_{k=0}^{n-1}\in\mathcal{B}_P^n} \frac{1}{n}\sum_{k=0}^{n-1} \tilde{R}_n^k(P_k) \\
&\overset{(b)}{=} \max_{\{\mathsf{C}_{\hat{\mathbf{X}}}[k]\}_{k=0}^{n-1}\in\hat{\mathcal{C}}_P^n} \frac{1}{2n}\sum_{k=0}^{n-1} \log\hat{\psi}[k], \qquad \text{(B.14)}
\end{aligned}$$

where (a) follows since for $\lfloor\frac{n}{2}\rfloor < k < n$ we conclude from Lemma B.3 that $\tilde{R}_n^k(P_k) = \tilde{R}_n^k(P_{n-k}) = \tilde{R}_n^{n-k}(P_{n-k})$; and (b) follows from plugging the definition of $\tilde{R}_n^k(P_k)$ from (B.11), from Lemma B.3 which restrict the sets of matrices to $\hat{\mathcal{C}}_P^n$, and from the definition of $\hat{\psi}[k]$ in (10b). Note that (B.14) coincides with (10).

D. Step 4: Proving That $C_s^{n-CG} = C_{s,TA}^{n-CG}$

So far we have derived $C_{s,TA}^{n-CG}$, the secrecy capacity of the n-CGMWTC subject to the *time-averaged* power constraint (B.1) when the blocklength is an integer multiple of n. However, we are interested in C_s^{n-CG}, the secrecy capacity of the n-CGMWTC subject to the *per-symbol* power constraint (3). As the per-symbol constraint (3) is more restrictive than the time-averaged constraint (B.1), it follows that $C_s^{n-CG} \le C_{s,TA}^{n-CG}$. In this subsection we prove that the secrecy capacities are equal. Let $\left\{\mathsf{C}_{\hat{\mathbf{X}},opt}[k]\right\}_{k=0}^{n-1}$ be the set of n matrices which maximize (B.14). From the derivation of the secrecy capacity of the n-CGMWTC subject to a *time-averaged* power constraint (B.1) derived in subsections B-A - B-C we note the following characteristics of the optimal channel input:

- As $\mathbf{X}[i]$ is a real multivariate sequence it follows from the properties of the DFT that for $\lfloor\frac{n}{2}\rfloor < k < n$, $\hat{\mathbf{X}}[k]$ is obtained from $\hat{\mathbf{X}}[k] = \left(\hat{\mathbf{X}}[n-k]\right)^*$.

- From the secrecy capacity for real-valued memoryless Gaussian MIMO WTCs [11, Corollary 1][9] it follows that for $k \in \tilde{\mathcal{L}}^n$, $\hat{\mathbf{X}}[k]$ is a zero-mean real-valued Gaussian random vector with covariance matrix $\mathsf{C}_{\hat{\mathbf{X}},opt}[k]$.
- From the secrecy capacity for complex memoryless Gaussian MIMO WTCs with circularly symmetric complex normal noise [6, Thm. 1][10] it follows that for $1 \leq k < \frac{n}{2}$, $\hat{\mathbf{X}}[k]$ is a circularly symmetric complex normal RV with covariance matrix $\mathsf{C}_{\hat{\mathbf{X}},opt}[k]$.
- As the subchannels are independent, the optimal input which achieves (B.14) satisfies $p\left(\hat{\mathbf{X}}^{\lfloor \frac{n}{2} \rfloor}\right) = \prod_{k=0}^{\lfloor \frac{n}{2} \rfloor} p\left(\hat{\mathbf{X}}[k]\right)$, i.e., $\left\{\hat{\mathbf{X}}[k]\right\}_{k=0}^{\lfloor \frac{n}{2} \rfloor}$ are mutually independent RVs.

The above characteristics give rise to the following corollary:

Corollary B.1: The secrecy capacity of the n-CGMWTC with a time-averaged power constraint, $C_{s,TA}^{n-CG}$, is obtained with an equal per-symbol power allocation.

Proof: Let $\mathcal{L}_{-}^{n}$ be set of indexes $k \in \mathcal{N}$ such that $k \notin \tilde{\mathcal{L}}^n$. Note that for $k \in \tilde{\mathcal{L}}_{-}^{n}$, $\hat{\mathbf{X}}[k] = \left(\hat{\mathbf{X}}[n-k]\right)^*$. We consider the autocorrelation of the time-domain optimal channel input which obtains $C_{s,TA}^{n-CG}$. As the time-domain channel input of the n-CGMWTC is real-valued we can write:

$$\begin{aligned}
&\mathbb{E}\left\{\mathbf{X}[i_1]\left(\mathbf{X}[i_2]\right)^T\right\} \\
&= \mathbb{E}\left\{\mathbf{X}[i_1]\left(\mathbf{X}[i_2]\right)^H\right\} \\
&\overset{(a)}{=} \frac{1}{n^2}\sum_{k_1=0}^{n-1}\sum_{k_2=0}^{n-1}\mathbb{E}\left\{\hat{\mathbf{X}}[k_1]\left(\hat{\mathbf{X}}[k_2]\right)^H\right\}e^{j2\pi\frac{i_1k_1-i_2k_2}{n}} \\
&\overset{(b)}{=} \frac{1}{n^2}\Bigg(\sum_{k_1=0}^{n-1}\mathbb{E}\left\{\hat{\mathbf{X}}[k_1]\left(\hat{\mathbf{X}}[k_1]\right)^H\right\}e^{j2\pi k_1\frac{i_1-i_2}{n}} \\
&\qquad + \sum_{k_1\in\mathcal{L}_{-}^{n}}\mathbb{E}\left\{\hat{\mathbf{X}}[k_1]\left(\hat{\mathbf{X}}[k_1]\right)^H\right\}e^{j2\pi k_1\frac{i_1+i_2}{n}}\Bigg) \\
&\overset{(c)}{=} \frac{1}{n^2}\sum_{k_1=0}^{n-1}\mathbb{E}\left\{\hat{\mathbf{X}}[k_1]\left(\hat{\mathbf{X}}[k_1]\right)^H\right\}e^{j2\pi k_1\frac{i_1-i_2}{n}}, \qquad \text{(B.15)}
\end{aligned}$$

where (a) follows by plugging the inverse DFT (B.2); (b) follows since $\left\{\hat{\mathbf{X}}[k]\right\}_{k=0}^{\lfloor \frac{n}{2} \rfloor}$ are zero-mean and mutually independent, thus $\mathbb{E}\left\{\hat{\mathbf{X}}[k_1]\left(\hat{\mathbf{X}}[k_2]\right)^H\right\}$ is non zero only when $k_2 = k_1$ and when $k_2 = n-k_1$, and since $\hat{\mathbf{X}}[k] = \left(\hat{\mathbf{X}}[n-k]\right)^*$; (c) follows since for $k \in \mathcal{L}_{-}^{n}$, the optimal $\hat{\mathbf{X}}[k]$ is circularly symmetric complex normal, thus $\mathbb{E}\left\{\hat{\mathbf{X}}[k]\left(\hat{\mathbf{X}}[k]\right)^T[k]\right\} = \mathsf{0}_{n_t\times n_t}$ [54, Sec. III-A.]. It follows from (B.15) that $\mathbb{E}\left\{\mathbf{X}[i]\left(\mathbf{X}[i]\right)^T\right\} = \frac{1}{n^2}\sum_{k_1=0}^{n-1}\mathbb{E}\left\{\hat{\mathbf{X}}[k_1]\left(\hat{\mathbf{X}}[k_1]\right)^H\right\}$, thus, the covariance matrix of the time-domain optimal channel input $\mathbf{X}[i]$ which achieves $C_{s,TA}^{n-CG}$ is independent of the time index $i \in \mathcal{N}$. As the constraint is the same for all n-blocks we conclude that $C_{s,TA}^{n-CG}$ is obtained with an equal per-symbol power allocation, namely satisfies (3) with equality. ∎

Since $C_s^{n-CG} \leq C_{s,TA}^{n-CG}$, then Corollary B.1 implies that $C_s^{n-CG} = C_{s,TA}^{n-CG}$. Combining this with (B.14), and noting that it is enough to consider blocklengths which are integer multiples of n to characterize the secrecy capacity of the n-CGMWTC, proves that C_s^{n-CG} is obtained by (10).

Appendix C
Proof of Proposition 4

In order to prove Proposition 4, we first show that if (11) is satisfied, then the secrecy capacity of the LGMWTC, C_s, is strictly positive; then, we prove that if C_s is strictly positive, it follows that (11) must be satisfied. The proof follows a similar outline to that of [6, Corollary 2]. Before we begin, we note that defining $\mathsf{H}'_w(\omega) = \left(\mathsf{C}'_{\mathbf{W}}(\omega)\right)^{-\frac{1}{2}}\mathsf{H}'(\omega)$ and $\mathsf{G}'_w(\omega) = \left(\mathsf{C}'_{\mathbf{U}}(\omega)\right)^{-\frac{1}{2}}\mathsf{G}'(\omega)$, and using Sylvester's determinant theorem [61, Ch. 6.2] (6c) can be written as

$$C_s = \max_{\mathsf{C}'_{\mathbf{X}}(\omega)\in\mathcal{C}_P}\frac{1}{2\pi}\int_{\omega=0}^{\pi}\log\frac{\left|\mathsf{I}_{n_r}+\mathsf{H}'_w(\omega)\,\mathsf{C}'_{\mathbf{X}}(\omega)\left(\mathsf{H}'_w(\omega)\right)^H\right|}{\left|\mathsf{I}_{n_e}+\mathsf{G}'_w(\omega)\,\mathsf{C}'_{\mathbf{X}}(\omega)\left(\mathsf{G}'_w(\omega)\right)^H\right|}d\omega. \qquad \text{(C.1)}$$

Assume that (11) is satisfied, then, $\forall\omega\in\Omega$, there exists a vector $\mathbf{v}(\omega)$ such that

$$\left\|\mathsf{G}'_w(\omega)\,\mathbf{v}(\omega)\right\| < \left\|\mathsf{H}'_w(\omega)\,\mathbf{v}(\omega)\right\|. \qquad \text{(C.2)}$$

Note that if $\mathbf{v}(\omega)$ satisfies (C.2) then $\frac{\mathbf{v}(\omega)}{\|\mathbf{v}(\omega)\|}$ also satisfies (C.2), hence we can consider only vectors $\mathbf{v}(\omega)$ such that $\|\mathbf{v}(\omega)\| = 1$. Now, let $|\Omega|$ denote the Lebesgue measure of Ω and set $\mathsf{C}'_{\mathbf{X}}(\omega) = \mathsf{0}_{n_t\times n_t}$ for $\omega\notin\Omega$ and $\mathsf{C}'_{\mathbf{X}}(\omega) = \frac{\pi\cdot P}{|\Omega|}\mathbf{v}(\omega)\left(\mathbf{v}(\omega)\right)^H$ for $\omega\in\Omega$. Note that $\mathsf{C}'_{\mathbf{X}}(\omega)$ is a positive definite Hermitian matrix which satisfies (6a), hence $\mathsf{C}'_{\mathbf{X}}(\omega)\in\mathcal{C}_P$. It follows that

$$\begin{aligned}
&C_s \\
&\overset{(a)}{\geq} \frac{1}{2\pi}\int_{\omega\in\Omega}\log\frac{\left|\mathbf{I}_{n_r}+\frac{\pi\cdot P}{|\Omega|}\mathsf{H}'_w(\omega)\,\mathbf{v}(\omega)\left(\mathbf{v}(\omega)\right)^H\left(\mathsf{H}'_w(\omega)\right)^H\right|}{\left|\mathbf{I}_{n_e}+\frac{\pi\cdot P}{|\Omega|}\mathsf{G}'_w(\omega)\,\mathbf{v}(\omega)\left(\mathbf{v}(\omega)\right)^H\left(\mathsf{G}'_w(\omega)\right)^H\right|}d\omega \\
&\overset{(b)}{=} \frac{1}{2\pi}\int_{\omega\in\Omega}\Bigg(\log\left(1+\frac{\pi\cdot P}{|\Omega|}\cdot\left\|\mathsf{H}'_w(\omega)\,\mathbf{v}(\omega)\right\|^2\right) \\
&\qquad - \log\left(1+\frac{\pi\cdot P}{|\Omega|}\cdot\left\|\mathsf{G}'_w(\omega)\,\mathbf{v}(\omega)\right\|^2\right)\Bigg)d\omega, \qquad \text{(C.3)}
\end{aligned}$$

where (a) follows from plugging $\mathsf{C}'_{\mathbf{X}}(\omega)$ defined above into (C.1), and (b) follows from Sylvester's

[9] Note that the real-valued memoryless Gaussian MIMO WTC is a special case of the real-valued memoryless Gaussian MIMO BC with common and confidential messages studied in [11], when there is no common message and only a single confidential message.

[10] Note that [6] showed that circularly symmetric complex normal inputs are optimal for complex memoryless Gaussian MIMO WTCs with additive circularly-symmetric complex normal (ACSCN) noise, subject to the more general time-averaged power constraint, which subsumes the per-symbol power constraint. It directly follows from [6] and [63, Lemma 1] that the optimal codeword that achieves the secrecy capacity in [6] also satisfies the per-symbol power constraint. Thus, we conclude that circularly symmetric complex normal input are also optimal for complex memoryless Gaussian MIMO WTCs with ACSCN noise subject to the per-symbol power constraint.

determinant theorem [61, Ch. 6.2]. Note that $\forall \omega \in \mathbf{\Omega}$, $\log\left(1+\frac{\pi\cdot P}{|\mathbf{\Omega}|}\cdot\left\|\mathsf{H}'_w(\omega)\,\mathbf{v}\,(\omega)\right\|^2\right) > \log\left(1+\frac{\pi\cdot P}{|\mathbf{\Omega}|}\cdot\left\|\mathsf{G}'_w(\omega)\,\mathbf{v}\,(\omega)\right\|^2\right)$. As the Lebesgue measure of $\mathbf{\Omega}$ is non-zero, it follows that (C.3) is strictly positive, thus C_s is strictly positive, i.e., (11) is a sufficient condition for a strictly positive secrecy capacity.

Next, we show that if (11) is not satisfied, then $C_s = 0$. Let $\mathsf{C}'_{\mathbf{X},opt}(\omega) \in \mathcal{C}_P$ be the maximizing covariance matrix for (C.1). Thus, we have

$$C_s = \frac{1}{2\pi}\int\limits_{\omega=0}^{\pi}\log\frac{\left|\mathsf{I}_{n_r}+\mathsf{H}'_w(\omega)\,\mathsf{C}'_{\mathbf{X},opt}(\omega)\left(\mathsf{H}'_w(\omega)\right)^H\right|}{\left|\mathsf{I}_{n_e}+\mathsf{G}'_w(\omega)\,\mathsf{C}'_{\mathbf{X},opt}(\omega)\left(\mathsf{G}'_w(\omega)\right)^H\right|}d\omega. \tag{C.4}$$

Since $\mathsf{C}'_{\mathbf{X},opt}(\omega) \in \mathcal{C}_P$, it follows that $\forall\omega \in [0,\pi)$, $\mathsf{C}'_{\mathbf{X},opt}(\omega)$ is a positive semi-definite Hermitian matrix, thus, from [61, Ch. 7.5-7.6] it can be written as $\mathsf{C}'_{\mathbf{X},opt}(\omega) = \mathsf{L}(\omega)\left(\mathsf{L}(\omega)\right)^H$. Plugging this decomposition into (C.4) we write

$$\begin{aligned}C_s &= \frac{1}{2\pi}\int\limits_{\omega=0}^{\pi}\log\frac{\left|\mathsf{I}_{n_r}+\mathsf{H}'_w(\omega)\,\mathsf{L}(\omega)\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{H}'_w(\omega)\right)^H\right|}{\left|\mathsf{I}_{n_e}+\mathsf{G}'_w(\omega)\,\mathsf{L}(\omega)\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{G}'_w(\omega)\right)^H\right|}d\omega\\ &\overset{(a)}{=}\frac{1}{2\pi}\int\limits_{\omega=0}^{\pi}\log\frac{\left|\mathsf{I}_{n_t}+\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{H}'_w(\omega)\right)^H\mathsf{H}'_w(\omega)\,\mathsf{L}(\omega)\right|}{\left|\mathsf{I}_{n_t}+\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{G}'_w(\omega)\right)^H\mathsf{G}'_w(\omega)\,\mathsf{L}(\omega)\right|}d\omega,\end{aligned} \tag{C.5}$$

where (a) follows from Sylvester's determinant theorem [61, Ch. 6.2]. Now, define

$$\begin{aligned}\mathsf{B}(\omega) \triangleq{}& \left(\mathsf{L}(\omega)\right)^H\left(\mathsf{G}'_w(\omega)\right)^H\mathsf{G}'_w(\omega)\,\mathsf{L}(\omega)\\ &-\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{H}'_w(\omega)\right)^H\mathsf{H}'_w(\omega)\,\mathsf{L}(\omega).\end{aligned}$$

$\mathsf{B}(\omega)$ is clearly Hermitian. If (11) is not satisfied, then for all $\omega \in [0,\pi)$, possibly except for a zero-measure subset of $[0,\pi)$, $\mathsf{B}(\omega)$ is positive semi-definite, since $\forall \mathbf{a} \in \mathbb{C}^{n_t}$

$$\begin{aligned}\mathbf{a}^H\mathsf{B}(\omega)\,\mathbf{a} &= \left\|\mathsf{G}'_w(\omega)\,\mathsf{L}(\omega)\,\mathbf{a}\right\|^2-\left\|\mathsf{H}'_w(\omega)\,\mathsf{L}(\omega)\,\mathbf{a}\right\|^2\\ &\overset{(a)}{=}\left\|\mathsf{G}'_w(\omega)\,\tilde{\mathbf{a}}\right\|^2-\left\|\mathsf{H}'_w(\omega)\,\tilde{\mathbf{a}}\right\|^2\\ &\overset{(b)}{\geq}0,\end{aligned}$$

where (a) follows by setting $\tilde{\mathbf{a}} \triangleq \mathsf{L}(\omega)\,\mathbf{a}$, and (b) follows since

$$\frac{\left\|\mathsf{H}'_w(\omega)\,\tilde{\mathbf{a}}\right\|}{\left\|\mathsf{G}'_w(\omega)\,\tilde{\mathbf{a}}\right\|} \leq \sup_{\mathbf{v}\in\mathbb{C}^{\mathbf{n_t}}}\frac{\left\|\mathsf{H}'_w(\omega)\,\mathbf{v}\right\|}{\left\|\mathsf{G}'_w(\omega)\,\mathbf{v}\right\|} \leq 1.$$

Let $\lambda_{\mathsf{G},k}(\omega)$ and $\lambda_{\mathsf{H},k}(\omega)$ be the k-th largest eigenvalue of $\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{G}'_w(\omega)\right)^H\mathsf{G}'_w(\omega)\,\mathsf{L}(\omega)$ and the k-th largest eigenvalue of $\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{H}'_w(\omega)\right)^H\mathsf{H}'_w(\omega)\,\mathsf{L}(\omega)$, respectively, $k \in \{1,2,\ldots,n_t\}$. As $\mathsf{B}(\omega)$ is a positive semi-definite Hermitian matrix, it follows from the min-max theorem [61, Ch. 7.5] [62, Ch. 7.7] that $\forall k \in \{1,2,\ldots,n_t\}$,

$$\lambda_{\mathsf{G},k}(\omega) \geq \lambda_{\mathsf{H},k}(\omega) \geq 0, \tag{C.6}$$

where the non-negativity of the eigenvalues $\lambda_{\mathsf{G},k}(\omega)$ and $\lambda_{\mathsf{H},k}(\omega)$ follows since $\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{G}'_w(\omega)\right)^H\mathsf{G}'_w(\omega)\,\mathsf{L}(\omega)$ and $\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{H}'_w(\omega)\right)^H\mathsf{H}'_w(\omega)\,\mathsf{L}(\omega)$ are positive semi-definite. Therefore, for all $\omega \in [0,\pi)$, except for maybe a zero-measure subset of $[0,\pi)$, it follows that

$$\begin{aligned}&\left|\mathsf{I}_{n_t}+\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{G}'_w(\omega)\right)^H\mathsf{G}'_w(\omega)\,\mathsf{L}(\omega)\right|\\ &\quad\overset{(a)}{=}\prod_{k=1}^{n_t}\left(1+\lambda_{\mathsf{G},k}(\omega)\right)\\ &\quad\overset{(b)}{\geq}\prod_{k=1}^{n_t}\left(1+\lambda_{\mathsf{H},k}(\omega)\right)\\ &\quad\overset{(c)}{=}\left|\mathsf{I}_{n_t}+\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{H}'_w(\omega)\right)^H\mathsf{H}'_w(\omega)\,\mathsf{L}(\omega)\right|,\end{aligned} \tag{C.7}$$

where (a) and (c) follow from [61, Ch. 7.5] since $\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{G}'_w(\omega)\right)^H\mathsf{G}'_w(\omega)\,\mathsf{L}(\omega)$ and $\left(\mathsf{L}(\omega)\right)^H\left(\mathsf{H}'_w(\omega)\right)^H\mathsf{H}'_w(\omega)\,\mathsf{L}(\omega)$ are Hermitian; (b) follows from (C.6). Applying the relationship (C.7) to (C.5) yields $C_s \leq 0$, therefore (11) is a necessary condition for a strictly positive secrecy capacity. This completes our proof.

Appendix D
Proof of Corollary 1

We first consider only blocklengths which are an integer multiple of n_{PLC}. Define the $n_{\mathrm{PLC}} \times 1$ multivariate processes $\mathbf{X}_{\mathrm{PLC}}\left[\tilde{i}\right]$, $\mathbf{Y}_{\mathrm{PLC}}\left[\tilde{i}\right]$, and $\mathbf{Z}_{\mathrm{PLC}}\left[\tilde{i}\right]$, using the following assignments: $\left(\mathbf{X}_{\mathrm{PLC}}\left[\tilde{i}\right]\right)_k = X\left[\tilde{i}\cdot n_{\mathrm{PLC}}+k\right]$, $\left(\mathbf{Y}_{\mathrm{PLC}}\left[\tilde{i}\right]\right)_k = Y_{\mathrm{PLC}}\left[\tilde{i}\cdot n_{\mathrm{PLC}}+k\right]$, and $\left(\mathbf{Z}_{\mathrm{PLC}}\left[\tilde{i}\right]\right)_k = Z_{\mathrm{PLC}}\left[\tilde{i}\cdot n_{\mathrm{PLC}}+k\right]$, respectively, $k \in \mathcal{N}_{\mathrm{PLC}}$. It follows from (13b) that

$$\begin{aligned}\mathbb{E}\left\{\left\|\mathbf{X}_{\mathrm{PLC}}\left[\tilde{i}\right]\right\|^2\right\} &= \sum_{k=0}^{n_{\mathrm{PLC}}-1}\mathbb{E}\left\{\left|X\left[\tilde{i}\cdot n_{\mathrm{PLC}}+k\right]\right|^2\right\}\\ &\leq P\cdot n_{\mathrm{PLC}},\end{aligned} \tag{D.1}$$

thus, $\mathbf{X}_{\mathrm{PLC}}\left[\tilde{i}\right]$ is subject to a per-symbol power constraint $P\cdot n_{\mathrm{PLC}}$. From [51, Appendix B], it follows that the *scalar* NB-PLC WTC (12) can be transformed into the following equivalent MIMO Gaussian channel with finite memory $m=1$:

$$\mathbf{Y}_{\mathrm{PLC}}\left[\tilde{i}\right] = \sum_{\tilde{\tau}=0}^{1}\mathsf{H}_{\mathrm{PLC}}\left[\tilde{\tau}\right]\mathbf{X}_{\mathrm{PLC}}\left[\tilde{i}-\tilde{\tau}\right]+\mathbf{W}_{\mathrm{PLC}}\left[\tilde{i}\right] \tag{D.2a}$$

$$\mathbf{Z}_{\mathrm{PLC}}\left[\tilde{i}\right] = \sum_{\tilde{\tau}=0}^{1}\mathsf{G}_{\mathrm{PLC}}\left[\tilde{\tau}\right]\mathbf{X}_{\mathrm{PLC}}\left[\tilde{i}-\tilde{\tau}\right]+\mathbf{U}_{\mathrm{PLC}}\left[\tilde{i}\right], \tag{D.2b}$$

where the transformation is bijective as we consider only codes with blocklength which is an integer multiple of n_{PLC}. It follows from Thm. 1 that the secrecy capacity of the equivalent MIMO WTC (D.2) is given by $n_{\mathrm{PLC}}\cdot C_{s,PLC}$, where $C_{s,PLC}$ is given by (15c), subject to (15a). Since each channel input in the equivalent MIMO channel corresponds

to n_{PLC} channel inputs in the original NB-PLC WTC, the corollary follows for codes whose blocklength which is an integer multiple of n_{PLC}. Lastly, we note that as n_{PLC} is fixed and finite, then any achievable secrecy rate can be achieved using codes whose blocklength is an integer multiple of n_{PLC}, where the proof is similar to that of Proposition A.1 and of Lemma A.6.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

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

[5] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[8] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[9] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[10] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[11] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.

[12] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

[13] S. A. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, May 2015.

[14] S. Loyka and C. D. Charalambous, "Rank-Deficient solutions for optimal signaling over secure MIMO channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Honolulu, HI, USA, Jun. 2014, pp. 201–205.

[15] H. Fujita, "Secrecy capacity of wiretap channels with additive colored Gaussian noise," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Kyoto, Japan, Mar. 2012, pp. 1877–1880.

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

[17] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[18] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[19] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Securing Wireless Communications at the Physical Layer*. New York, NY, USA: Springer, 2010, pp. 1–18.

[20] A. Khisti and T. Liu, "Private broadcasting over independent parallel channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5173–5187, Sep. 2014.

[21] E. A. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," in *Proc. Int. Conf. Telecommun.*, St. Petersburg, Russia, Jun. 2008, pp. 1–6.

[22] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

[23] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[24] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[25] L. Lai and H. El Gamal, "Cooperative secrecy: The relay-eavesdropper channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, Jun. 2007, pp. 931–935.

[26] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[27] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[28] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[29] M. Bloch and J. N. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *Proc. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2008, pp. 818–825.

[30] M. Kobayashi, M. Debbah, and S. Shamai (Shitz), "Secured communication over frequency-selective fading channels: A practical Vandermonde precoding," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 386547-1–386547-19, Jun. 2009.

[31] W. Hirt and J. L. Massey, "Capacity of the discrete-time Gaussian channel with intersymbol interference," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 380–388, May 1988.

[32] S. Verdú, "Multiple-access channels with memory with and without frame synchronism," *IEEE Trans. Inf. Theory*, vol. 35, no. 3, pp. 605–619, May 1989.

[33] A. J. Goldsmith and M. Effros, "The capacity region of broadcast channels with intersymbol interference and colored Gaussian noise," *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 219–240, Jan. 2001.

[34] A. Pittolo and A. M. Tonello, "Physical layer security in power line communication networks: An emerging scenario, other than wireless," *IET Commun.*, vol. 8, no. 8, pp. 1239–1247, May 2014.

[35] S. C. Cripps, *RF Power Amplifiers for Wireless Communications*. Norwood, MA, USA: Artech House, 2006.

[36] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3037–3063, Sep. 2005.

[37] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.

[38] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: Wiley, 1968.

[39] R. Dabora and A. J. Goldsmith, "The capacity region of the degraded finite-state broadcast channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1828–1851, Apr. 2010.

[40] Y.-H. Kim, "A coding theorem for a class of stationary channels with feedback," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1488–1499, Apr. 2008.

[41] Y. Murin, R. Dabora, and D. Gündüz, "Source-channel coding theorems for the multiple-access relay channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5446–5465, Sep. 2013.

[42] R. S. Cheng and S. Verdú, "Gaussian multiaccess channels with ISI: Capacity region and multiuser water-filling," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 773–785, May 1993.

[43] W. Rudin, *Principles of Mathematical Analysis*. New York, NY, USA: McGraw-Hill, 1976.

[44] S. Galli, A. Scaglione, and Z. Wang, "For the grid and through the grid: The role of power line communications in the smart grid," *Proc. IEEE*, vol. 99, no. 6, pp. 998–1027, Jun. 2011.

[45] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan. 2010.

[46] V. C. Gungor *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[47] F. J. C. Corripio, J. A. C. Arrabal, L. D. del Rio, and J. T. E. Munoz, "Analysis of the cyclic short-term variation of indoor power line channels," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 7, pp. 1327–1338, Jul. 2006.
[48] M. Nassar, J. Lin, Y. Mortazavi, A. Dabak, I. H. Kim, and B. L. Evans, "Local utility power line communications in the 3–500 kHz band: Channel impairments, noise, and standards," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 116–127, Sep. 2012.
[49] M. Katayama, T. Yamazato, and H. Okada, "A mathematical model of noise in narrowband power line communication systems," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 7, pp. 1267–1276, Jul. 2006.
[50] G. B. Giannakis, "Cyclostationary signal analysis," in *The Digital Signal Processing Handbook*. Boca Raton, FL, USA: CRC Press, 1998, pp. 17.1–17.31.
[51] N. Shlezinger and R. Dabora, "On the capacity of narrowband PLC channels," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1191–1201, Apr. 2015.
[52] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.
[53] D. Guo, S. Shamai (Shitz), and S. Verdú, "Mutual information and minimum mean-square error in Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1261–1282, Apr. 2005.
[54] F. D. Neeser and J. L. Massey, "Proper complex random processes with applications to information theory," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1293–1302, Jul. 1993.
[55] R. G. Gallager. (2008). *Circularly-Symmetric Gaussian Random Vectors*. [Online]. Available: http://www.rle.mit.edu/rgallager/documents/CircSymGauss.pdf
[56] A. V. Oppenheim, R. W. Schafer, and J. R. Buck, *Discrete-Time Signal Processing*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1989.
[57] A. Papoulis, *Probability, Random Variables and Stochastic Processes*, 3rd ed. New York, NY, USA: McGraw-Hill, 1991.
[58] R. G. Gallager, *Stochastic Processes: Theory for Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2013.
[59] M. L. Eaton, *Multivariate Statistics: A Vector Space Approach*. Beachwood, OH, USA: Institute of Mathematical Statistics, 2007.
[60] H. Amann and J. Escher, *Analysis I*. Basel, Switzerland: Birkhauser Verlag, 2005.
[61] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*. Philadelphia, PA, USA: SIAM, 2000.
[62] R. A. Horn and C. A. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1990.
[63] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[64] N. Shlezinger, D. Zahavi, Y. Murin, and R. Dabora. (2017). "The secrecy capacity of MIMO Gaussian channels with finite memory—Full version," [Online]. Available: http://arxiv.org/abs/1701.02882
[65] R. Dabora and A. J. Goldsmith, "Capacity theorems for discrete, finite-state broadcast channels with feedback and unidirectional receiver cooperation," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 5958–5983, Dec. 2010.

Nir Shlezinger (S'14) received his B.Sc. and M.Sc. degrees in 2011 and 2013, respectively, from Ben-Gurion University, Israel, all in Electrical and Computer Engineering. He is currently pursuing a Ph.D. degree in Electrical Engineering at Ben-Gurion University. From 2009 to 2013 he worked as an engineer at Yitran Communications. His research interests include information theory and signal processing for communications.

Daniel Zahavi (S'14) received the B.Sc. degree in 2009 from Technion, Israel Institute of Technology, Israel, and the M.Sc. degree in 2012 from Ben-Gurion University of the Negev, Israel, both in Electrical Engineering. From 2010 to 2014 he worked as a communications research engineer with Signal Corps of Israel Defense Forces. He is now pursuing the Ph.D. degree in electrical engineering at Ben-Gurion University of the Negev, Israel.

Yonathan Murin (M'15) received his B.Sc. degree in Electrical Engineering and Computer Science from Tel-Aviv University, Israel, in 2004, and his M.Sc. and Ph.D. degrees in 2011 and 2015, respectively, from Ben-Gurion University of the Negev, Israel, both in Electrical Engineering. He is currently a postdoctoral scholar in the Wireless Systems Lab at Stanford University. From 2004 to 2010, he worked as a DSP and algorithms engineer, and as a team leader at Comsys Communication and Signal Processing. His research interests include network information theory and wireless communications, coding theory, molecular communications, and signal processing for neuroscience.

Ron Dabora (M'07–SM'14) received his B.Sc. and M.Sc. degrees in 1994 and 2000, respectively, from Tel-Aviv University, and his Ph.D. degree in 2007 from Cornell University, all in Electrical Engineering. From 1994 to 2000, he worked as an engineer at the Ministry of Defense of Israel, and from 2000 to 2003, he was with the Algorithms Group at Millimetrix Broadband Networks, Israel. From 2007 to 2009, he was a postdoctoral researcher at the Department of Electrical Engineering, Stanford University. Since 2009, he is an assistant professor at the Department of Electrical and Computer Engineering, Ben- Gurion University, Israel. His research interests include network information theory, wireless communications, and power line communications. Dr. Dabora served as a TPC member in a number of international conferences including WCNC, PIMRC, and ICC. From 2012 to 2014, he served as an associate editor for the IEEE SIGNAL PROCESSING LETTERS, and he currently serves as a senior area editor for the IEEE SIGNAL PROCESSING LETTERS.