

Unified Interference Engineering for Wireless Information Secrecy

Liangzhong Ruan, *Member, IEEE*, Andrea Conti, *Senior member, IEEE*, and Moe Z. Win, *Fellow, IEEE*

Abstract—Wireless communications are highly susceptible to eavesdropping due to their inherent broadcast nature. Recent works have proposed the use of interference for impeding the capabilities of the eavesdropping receivers in wireless networks. To fully unleash the potential of interference for wireless information secrecy, it is necessary to engineer network interference such that it impedes the capability of eavesdropping receivers while having mild effect on legitimate receivers. The task of generating network interference desirable for wireless secrecy is particularly challenging in heterogeneous networks due to their ample set of configurations. This paper proposes a unified interference engineering strategy (IES) for wireless information secrecy in heterogeneous networks. The unified IES combines zero forcing beamforming, artificial noise generation, cooperative jamming, and interference alignment to fully exploit the network's capability in wireless secrecy. The proposed strategy enables multiple nodes with heterogeneous capabilities to achieve mutually beneficial coordination, thereby leading to a new level of wireless information secrecy.

Index Terms—Wireless secrecy, interference engineering, heterogeneous networks, algebraic independence

I. INTRODUCTION

WIRELESS INFORMATION SECRECY is becoming more and more important as the level of networking and connectivity increases in our life [1]. To overcome this challenge, it is essential to account for the contrasting effects of the wireless propagation medium: it makes the secret information from legitimate transmitters (LTs) vulnerable to malicious interception; and at the same time it causes network interference which impedes the eavesdropping receivers (ERs). Therefore, while interference was classically considered as a foe, it now emerges to be a friend in mitigating the eavesdropping capability of ERs [2]–[5]. Several studies have been carried out to characterize network interference, so as to better understand the role of interference in large scale networks [6]–[17].

Wireless networks are evolving toward configurations with diverse topologies and heterogeneous nodes [18]. Compared to conventional cellular networks, the interference issue in such networks is usually more severe due to the complicated network topology and the high node density [19]. On the other hand, from the perspective of wireless secrecy, stronger interference implies greater potential to impede ERs' capability.

Manuscript received September 15, 2017; accepted February 16, 2018. Date of publication ...; date of current version This research was supported, in part, by the National Science Foundation under Grant CCF-1525705 and the Office of Naval Research under Grant N00014-16-1-2141.

L. Ruan and M. Z. Win are with the Laboratory for Information and Decision Systems (LIDS), Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139 USA (e-mail: lruan@mit.edu, moewin@mit.edu). A. Conti is with the University of Ferrara, Ferrara, ITALY (e-mail: a.conti@ieee.org).

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

Digital Object Identifier

Digital Object Identifier: 10.1109/JSAC.2018.2825558

To unleash the potential of network interference for wireless secrecy, it is necessary to coordinate the transmission strategies among nodes with heterogeneous capabilities. This calls for interference engineering strategies (IESs) that can adjust the level of coordination according to both the network topology and the capability of different nodes.

Various IESs have been proposed to protect wireless secrecy by creating interference that is strong at the ERs while it is relatively mild at the legitimate receivers (LRs). These strategies can be classified into different categories including those in the following.

- Artificial noise (AN): these strategies let LTs and legitimate jammers (LJs) send additional dummy signals for creating stronger interference at the ERs [20]–[23].
- Cooperative jamming (CJ): these strategies exploit the full-duplex capabilities [24] of the legitimate nodes so as to better impede the ERs' capability [25]–[27].
- Interference mitigation: zero-forcing beamforming (ZFB) and interference alignment (IA) set the transceivers of legitimate nodes to reduce the effects of interference on the LRs while maintaining those at the ERs [28]–[31].

These IESs have different advantages and limitations. On the one hand, AN and CJ can mitigate the eavesdropping capability of strong ERs, while they may generate a high level of interference at the LRs. On the other hand, ZFB and IA have a problem the other way around. Compared to AN, CJ enables more nodes to generate additional interference, yet it requires legitimate nodes to have the capability of performing in-band full-duplex communications. Compared to ZFB, IA has stronger capability and larger flexibility in mitigating interference, yet it requires coordination among multiple legitimate nodes, which imposes stronger constraints on the minimum level of channel state information (CSI) availability.

We envision that a new level of network secrecy can be achieved by unifying existing IESs. This paper proposes a unified IES that integrates the key ideas of various existing IESs into a coherent framework, so as to go beyond the limits of existing IESs while maintaining their advantages. In particular, the proposed strategy accommodates the different levels of CSI availability and the signal processing capability at various nodes, so as to most effectively generate strong network interference at the ERs while having a mild effect on the LRs. A major challenge in designing such a unified IES is that it requires the joint design of transceivers at multiple legitimate nodes, which involves solving a set of nonlinear equations. Few systematic tools exist to analyze the feasibility conditions or find the solutions of nonlinear equation sets. The authors' prior work [32], [33] addresses a special case of this issue by developing a mathematical

framework tailored to non-linear equations in IA problems for point-to-point interference networks. Enlightened by this prior work, the authors will develop a mathematical framework to address the nonlinear equations in the proposed unified IES for heterogeneous networks. The key contributions of the paper are:

- design of a unified IES which integrates the advantages of AN, CJ, ZFB, and IA to accommodate the diversity of network topology and heterogeneity of wireless nodes;
- development of a dynamic data stream assignment algorithm based on an efficient feasibility test for the proposed unified IES;
- characterization of how the proposed strategy benefits wireless information secrecy.

Organization: Section II describes the network model. Section III formulates the unified IES problem for wireless secrecy. Section IV designs algorithms to solve the unified IES problem. Section V evaluates the performance of the proposed algorithms. Finally, Section VI concludes this paper.

Notations: Random variables are displayed in sans serif, upright fonts; their realizations in serif, italic fonts. Vectors and matrices are denoted by bold lowercase and uppercase letters, respectively. For example, a random variable and its realization are denoted by \mathbf{x} and x ; a random vector and its realization are denoted by \mathbf{x} and \mathbf{x} ; a random matrix and its realization are denoted by \mathbf{X} and \mathbf{X} , respectively. Sets and random sets are denoted by upright sans serif and calligraphic font, respectively. For example, a random set and its realization are denoted by \mathcal{X} and \mathcal{X} , respectively. \mathbb{R} and \mathbb{C} denote the set of real and complex numbers, respectively. The m -by- m identity matrix is denoted by \mathbf{I}_m . $\mathbb{1}_{\mathcal{C}}\{x\}$ is the indicator function, which equals 1 if $x \in \mathcal{C}$ and 0 otherwise. Function $[\cdot]^+ = \max\{\cdot, 0\}$. Notation “ \equiv ” denotes identical equality of two functions. \cdot^T , $\text{Rn}\{\cdot\}$, $\text{tr}\{\cdot\}$, and $\det\{\cdot\}$ denote the transpose, rank, trace, and determinant of a matrix, respectively. $\dim\{\cdot\}$ denotes the dimension of a space. $|\cdot|$ denotes the cardinality of a set. Notation $\mathbf{J}_{\mathbf{x}}(\mathbf{f})$ represents the Jacobian matrix of function \mathbf{f} , and $\mathbf{J}_{\mathbf{x}}(\mathbf{f})|_{\mathbf{x}=\boldsymbol{\alpha}}$ gives the value of this matrix evaluated at point $\boldsymbol{\alpha}$. $\text{span}(\mathbf{A})$ denotes the linear space spanned by the column vectors of \mathbf{A} . $\text{diag}(\mathbf{A}, \dots, \mathbf{X})$ represents a block diagonal matrix with submatrices $\mathbf{A}, \dots, \mathbf{X}$ on its diagonal, and $\text{diag}_m(\mathbf{A}) = \text{diag}(\underbrace{\mathbf{A}, \dots, \mathbf{A}}_{m \text{ times}})$.

II. SYSTEM MODEL

This section describes the network model and defines the information secrecy metric.

A. Model for Heterogeneous Network

Consider wireless networks composed of heterogeneous nodes. For instance, Fig. 1 illustrates a scenario in which long-term-evolution (LTE)-advanced networks co-exist with LTE-machine-type-communication (MTC) networks. The LTE-advanced networks consist of performance-prioritized nodes with comprehensive radio frequency (RF) hardware, whereas the LTE-MTC networks consist of cost-prioritized nodes with

simplified RF hardware. If the two types of networks are designed separately, their co-existence may lead to strong inter-network interference that damages the performance of both. However, if the two types of networks are designed jointly, the multiple categories of nodes may lead to an intractable model. To overcome this challenge, this work proposes a model in which heterogeneous nodes are not represented by their categories, e.g., LTE-advanced basestation (BS), LTE-advanced mobile user (MU), and LTE-MTC MU; instead, the nodes are characterized using a consistent model with a few parameters representing their major properties, such as the role in the network (e.g., transmitter, receiver, and jammer), the communication range, and the signal processing capability. The various combinations of parameters allow the representation of multiple categories of nodes without involving an over-complicated model. This work considers a network of K nodes, in which the k -th node is equipped with N_k antennas, $k \in \mathcal{K}$, where $\mathcal{K} = \{1, 2, \dots, K\}$. The nodes are characterized by three sets of parameters, i.e., nodes’ association, channel connectivity, and coordination level.

1) *Nodes’ association:* A node may be a legitimate user or an eavesdropper. In the first case, it may act as a LT, LJ, or LR. In the second case, it acts as an ER, i.e., only passive attackers are considered in this work. Node t transmits $c_{t,r}$ number of confidential information streams to node r . In the meantime, node e tries to intercept such confidential information. The association of the LT, LR, and ER is denoted by a combination of three numbers (t, r, e) , $t, r \in \mathcal{L} \subseteq \mathcal{K}$, $e \in \mathcal{K} \setminus \mathcal{L}$, where t, r, e are the indexes of the LT, LR and ER, respectively, and \mathcal{L} is the index set of legitimate nodes. If no node is eavesdropping on the transmission, then $e = \text{NULL}$. Denote the set of all node associations as \mathcal{A} . The transceivers for the confidential information streams adopted by node t, r , and e are denoted by $\mathbf{V}_{t,r} \in \mathbb{C}^{N_t \times c_{t,r}}$, $\mathbf{U}_{t,r} \in \mathbb{C}^{N_r \times c_{t,r}}$, and $\mathbf{U}_{t,e} \in \mathbb{C}^{N_e \times c_{t,r}}$, respectively.

In addition to transmitting confidential information streams, some nodes may deliver dummy streams to generate interference for protecting the confidential information. These nodes are called LJ and their index set is \mathcal{J} . Suppose that node j delivers d_j number of dummy streams, then the precoder for these streams is denoted by $\mathbf{V}_j \in \mathbb{C}^{N_j \times d_j}$. Note that the same node index may appear multiple times in \mathcal{A} and \mathcal{J} . For instance, as illustrated in Fig. 1, a node may be a BS, which serves multiple users at the same time; it may have full-duplex capability, and hence it can transmit and receive simultaneously. It is a constraint that if a node is serving as transmitter in multiple links, then its associated LRs are not receiving from other LTs, i.e.,¹ $|\{r : (k, r, *) \in \mathcal{A}\}| + \mathbb{1}_{\mathcal{J}}\{k\}$ and $|\{t : (t, s, *) \in \mathcal{A}\}|$ cannot be greater than 1 simultaneously $\forall (k, s, *) \in \mathcal{A}$.² This constraint excludes network

¹Expression $(t, r, *) \in \mathcal{A}$ means that there exists some e such that $(t, r, e) \in \mathcal{A}$. Similar meanings for expressions such as $(t, *, e) \in \mathcal{A}$ and $(t, *, *) \in \mathcal{A}$.

²In this work, letters t, r, j, e respectively represent indexes of LTs, LRs, LJs, and ERs. The letters k and s can represent indexes of nodes with any identities.

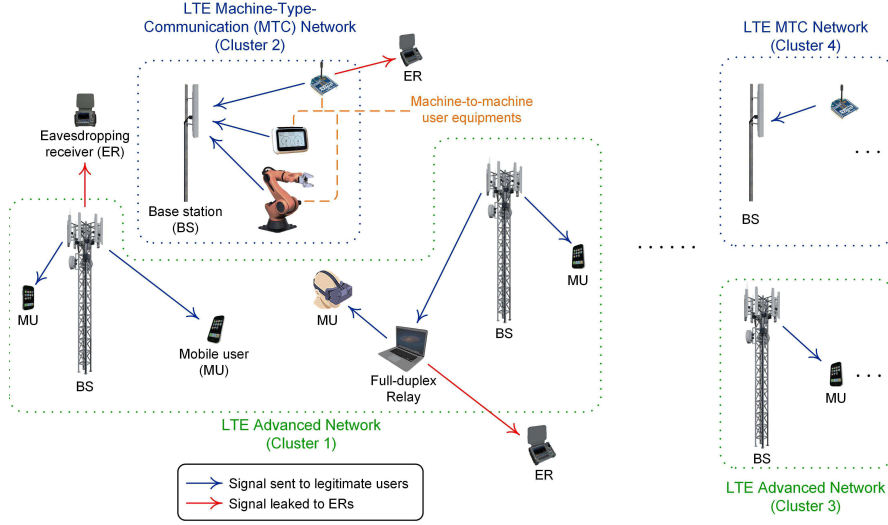


Fig. 1: An example of the configuration of heterogeneous communication networks with ERs.

topologies such as X-channel³, but still includes a variety of topologies, such as point-to-point, one-to-many, many-to-one and full-duplexing.

Denote the stream assignment at all legitimate nodes as \mathcal{S} , i.e., $\mathcal{S} = \{c_{t,r} : (t, r, *) \in \mathcal{A}\} \cup \{d_j : j \in \mathcal{J}\}$. Let \mathcal{T}_k represent all the transceiver matrices at a legitimate node k , i.e.,

$$\mathcal{T}_k = \{\mathbf{V}_k : k \in \mathcal{J}\} \cup \{\mathbf{V}_{k,r} : (k, r, *) \in \mathcal{A}\} \cup \{\mathbf{U}_{t,k} : (t, k, *) \in \mathcal{A}\}$$

and let \mathcal{T} represent the transceiver matrices of all legitimate nodes, i.e., $\mathcal{T} = \bigcup_{k \in \mathcal{L}} \mathcal{T}_k$.

2) *Channel connectivity*: Denote the CSI from node k to node s as $\mathbf{H}_{k,s} \in \mathbb{C}^{N_s \times N_k}$, $k \neq s$. Given the maximum transmission power of node k , the intensity of signals transmitted by this node can be lower than the noise level at node s due to the deep fading between them. In such case, it is reasonable to treat the link from node k to node s as unconnected and ignore the effect of interference on these links. Denote the set of all connected links as $\mathcal{H} \subseteq \{(k, s) : k, s \in \mathcal{K}, k \neq s\}$. When two nodes k, s are connected, the elements in the CSI matrix $\mathbf{H}_{k,s}$ are independent random variables (RVs) drawn from certain continuous distribution.

Let \mathcal{H}_k be the set of nodes that node k connects to, i.e., $\mathcal{H}_k = \{s : (k, s) \in \mathcal{H}\}$. The set \mathcal{H}_k represents the communication range of node k . For instance, in Fig. 1, though both BSs and MUs may act as LTs, a BS shall connect to more nodes compared to an MU.

3) *Coordination level*: The level of coordination is a main feature of IESSs. In non-coordinated IESSs, a node determines its transceiver according to local CSI. In coordinated IESSs, nodes in a same cluster jointly design their transceivers according to all CSI in the cluster. Larger clusters lead to higher levels of coordination, which significantly enhances the IESS's capability to control interference at a cost of more message overhead and

computation complexity. To accommodate the various levels of coordination in heterogeneous networks, the coordinated cluster sets as well as the non-coordinated sets are introduced into the network model.

The legitimate nodes are partitioned into a number of C coordinated cluster sets, in which the nodes jointly design their transceivers according to all CSI in the cluster. Denote these clusters as $\mathcal{C}_i \subseteq \mathcal{K}$, $i \in \mathcal{C}$, where $\mathcal{C} = \{1, 2, \dots, C\}$. It is required that a pair of associated LT and LR are in the same cluster, i.e., if $(t, r, *) \in \mathcal{A}$, then $t, r \in \mathcal{C}_i$ for some i . The number of nodes in a coordinated cluster set indicates the level of coordination. For instance, in Fig. 1, cluster 2 has more nodes than cluster 1 because the LTE-advanced network consists of nodes with higher communication and computation capabilities and can hence perform coordination on a larger scale.

The non-coordinated sets are introduced to address the inter-cluster interference. No multi-node coordination is involved for the inter-cluster links. Among any two nodes connected by an inter-cluster link, one node adapts to the channel state and the transceivers of the other node to mitigate interference. Denote the non-coordinated set \mathcal{N}_k as the set of nodes in other coordinated cluster sets whose transceivers node k must adapt to. The set \mathcal{N}_k is determined according to the relative capabilities of nodes or according to the network protocol. For instance, in Fig. 1, nodes in LTE-MTC networks shall be in the non-coordinated sets of nodes in LTE-advanced networks due to their relatively low communication and computation capabilities.

All links between legitimate nodes are covered by coordinated cluster sets and non-coordination sets, i.e.,

$$\{(t, r) : t, r \in \mathcal{L}\} = \{(t, r) : t, r \in \mathcal{C}_i, i \in \mathcal{C}\} \cup \{(t, r) : t \in \mathcal{N}_r \text{ or } r \in \mathcal{N}_t\}. \quad (1)$$

Moreover, the two types of sets define the variables that the transceivers at a certain node shall adapt to. Suppose $k \in \mathcal{C}_i$,

³an X-channel is a system with two transmitters, two receivers, where independent messages need to be conveyed from each transmitter to each receiver.

then \mathcal{T}_k is a function of

$$\{\mathbf{H}_{t,r} : t, r \in \mathcal{C}_i\} \cup \{\mathbf{H}_{k,s}, \mathcal{T}_s : s \in \mathcal{N}_k\} \quad (2)$$

To avoid circular definition, loops are not allowed in the non-coordinated sets. For example, for three nodes a , b , and c , if $b \in \mathcal{N}_a$, $c \in \mathcal{N}_b$ and then $a \notin \mathcal{N}_c$.⁴

B. Information Secrecy Metric

Suppose nodes t , r , and e are a set of associated LT, LR, and ER, i.e., $(t, r, e) \in \mathcal{A}$. The received signal $\mathbf{y}_{t,r} \in \mathbb{C}^{c_{t,r} \times 1}$ at node r is given by

$$\mathbf{y}_{t,r} = \mathbf{U}_{t,r}^\dagger \left(\sum_{k:(k,r) \in \mathcal{H}} \sum_{s:(k,s,*) \in \mathcal{A}} \mathbf{H}_{k,r} \mathbf{V}_{k,s} \mathbf{x}_{k,s} + \sum_{\substack{j \in \mathcal{J} \\ (j,r) \in \mathcal{H}}} \mathbf{H}_{j,r} \mathbf{V}_j \mathbf{x}_j + \mathbf{z}_r \right) \quad (3)$$

where $\mathbf{x}_{k,s} \in \mathbb{C}^{c_{k,s} \times 1}$ is the confidential information signal transmitted from node k to node s , $\mathbf{x}_j \in \mathbb{C}^{c_j \times 1}$ is the dummy signal transmitted by node j , and $\mathbf{z}_k \in \mathbb{C}^{N_k}$ represents the additive white Gaussian noise with mean zero and variance one. The received signal $\mathbf{y}_{t,e} \in \mathbb{C}^{c_{t,e} \times 1}$ at node e is given by an equation in the same form of (3), with the index r replaced by index e . The power that node t allocates for transmitting to node r is given by

$$P_{t,r} = \mathbb{E}\{\text{tr}(\mathbf{x}_{t,r}^\dagger \mathbf{V}_{t,r}^\dagger \mathbf{V}_{t,r} \mathbf{x}_{t,r})\}.$$

This work considers information-theoretic secrecy as the performance metric. In particular, under a given transceiver design, the secrecy rate $R_{t,r}$ achievable for legitimate link (t, r) is given by [34], [35]

$$R_{t,r} = \mathbb{E}\{[r_{t,r} - r_{t,e}]^+\} \quad (4)$$

where a realization of $r_{t,r}$ is

$$r_{t,r} = \log_2 \det \{\mathbf{I}_{N_r} + \mathbf{S}_{t,r} \mathbf{N}_{t,r}^{-1}\} \quad (5)$$

in which $\mathbf{S}_{t,r}$, $\mathbf{N}_{t,r}$, are the covariance matrices of desired signal and aggregated interference at node r , respectively. In particular,

$$\mathbf{S}_{t,r} = \mathbf{U}_{t,r}^\dagger \mathbf{H}_{t,r} \mathbf{V}_{t,r} \mathbf{V}_{t,r}^\dagger \mathbf{H}_{t,r}^\dagger \mathbf{U}_{t,r} \quad (6)$$

$$\mathbf{N}_{t,r} = \mathbf{U}_{t,r}^\dagger \left(\sum_{k:(k,r) \in \mathcal{H}} \sum_{s:(k,s,*) \in \mathcal{A}} \mathbf{H}_{k,r} \mathbf{V}_{k,s} \mathbf{V}_{k,s}^\dagger \mathbf{H}_{k,r}^\dagger + \sum_{\substack{j \in \mathcal{J} \\ (j,r) \in \mathcal{H}}} \mathbf{H}_{j,r} \mathbf{V}_j \mathbf{V}_j^\dagger \mathbf{H}_{j,r}^\dagger \right) \mathbf{U}_{t,r} - \mathbf{S}_{t,r} \quad (7)$$

If $e = \text{NULL}$, then $r_{t,e} = 0$; otherwise, the realization of $r_{t,e}$ is defined similarly as $r_{t,r}$, with index r replaced by index e in (5) and (7), with (6) replaced by

$$\mathbf{S}_{t,e} = \mathbf{U}_{t,e}^\dagger \mathbf{H}_{t,e} \mathbf{V}_{t,e} \mathbf{V}_{t,e}^\dagger \mathbf{H}_{t,e}^\dagger \mathbf{U}_{t,e}.$$

It is assumed that the ERs choose their decoders $\mathbf{U}_{t,e}^\dagger$ to maximize $r_{t,e}$, so as to minimize the secrecy rate $R_{t,r}$.

⁴In fact, scenarios such as $b \in \mathcal{N}_a$, $c \in \mathcal{N}_b$, and $a \in \mathcal{N}_c$ imply that the three nodes iteratively update their transceivers, an approach adopted in many coordinated IESSs. Hence, nodes in a loop shall be put into the same coordinated cluster set.

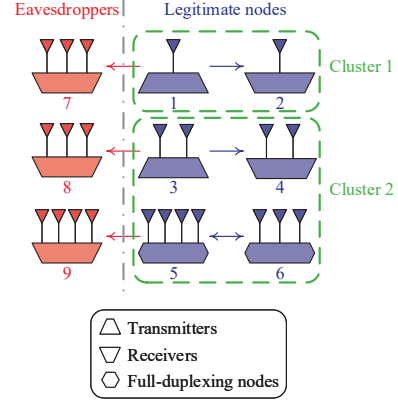


Fig. 2: Configuration of the example network.

When the ratios of transmission power among different links are bounded, i.e., there exists $\theta_l, \theta_u > 0$, and P such that $P_{t,r} \in [\theta_l P, \theta_u P] \forall t, r : (t, r, *) \in \mathcal{A}$, the secure degrees-of-freedom (SDoF) achieved by the legitimate link (t, r) is [28], [29]

$$D_{t,r} = \lim_{P \rightarrow +\infty} \frac{R_{t,r}}{\log_2(P)}.$$

The information-theoretic secrecy is selected to obtain clear insights into how IESSs contribute to wireless secrecy. To achieve this performance metric, the transmitted signals need to be Gaussian-distributed. In fact, the proposed strategy can be performed with no specific assumptions on the distribution of transmitted signals. For instance, signals with finite alphabet set [36], [37] can be adopted to improve the implementability of the proposed strategy.

III. PROBLEM FORMULATION

In this section, the potential of IES for enhancing wireless information secrecy will be demonstrated via a simple case study. Then, an interference engineering problem will be formulated based on the inspirations obtained from the case study.

A. Case Study

Consider a network as illustrated in Fig. 2 consisting of nine nodes, with antenna configuration shown in the figure. The LT-LR-ER association is given by

$$\mathcal{A} = \{(1, 2, 7), (3, 4, 8), (5, 6, 9), (6, 5, 0)\}.$$

The legitimate nodes capable of transmitting are also serving as LJ, i.e., $\mathcal{J} = \{1, 3, 5, 6\}$. All links are connected and the entries of all the channel matrices are independent random variables drawn from Gaussian distribution with mean zero and variance one. As shown in the figure, the legitimate nodes are grouped into two clusters. The transceivers of nodes in cluster 2 adapt to those of nodes in cluster 1 to cancel inter-cluster interference. The transmit signal to noise ratio (SNR) of all transmitters is 20 dB.

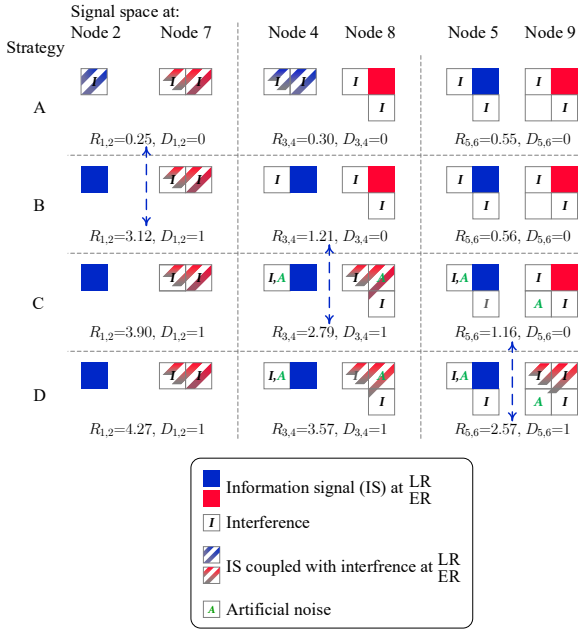


Fig. 3: Signal space at LR and ER under different strategies. Each square block represents a one-dimensional subspace.

To understand the effects of IESs on wireless information secrecy, four strategies are described and compared in the following.

- Strategy A (No interference engineering): Node 1, 3, 5 each transmit one confidential information stream with random precoder. Node 6 does not transmit.
- Strategy B (ZFB): The legitimate nodes adopt the same stream assignment as in Strategy A, and use ZFB to cancel interference. Specifically, set $\mathbf{v}_{3,4}$, $\mathbf{u}_{3,4}$, $\mathbf{v}_{5,6}$, and $\mathbf{u}_{5,6}$ to be orthogonal to $\text{span}(\mathbf{h}_{3,2}^\dagger)$, $\text{span}(\mathbf{h}_{1,4}^\dagger)$, $\text{span}([\mathbf{h}_{5,2}^\dagger \ \mathbf{H}_{5,4}^\dagger])$, and $\text{span}([\mathbf{h}_{1,6}^\dagger \ (\mathbf{H}_{3,6}\mathbf{v}_{3,4})^\dagger])$, respectively.
- Strategy C (Strategy B + AN + IA): The legitimate nodes adopt Strategy B. In addition, node 5 transmits a dummy data stream to generate AN, and then cancels its interference at the LRs by using IA. Specifically, set \mathbf{v}_5 to be orthogonal to $\text{span}([\mathbf{h}_{3,2}^\dagger \ \mathbf{H}_{5,4}^\dagger \mathbf{u}_{3,4} \ \mathbf{H}_{5,6}^\dagger \mathbf{u}_{5,6}])$.
- Strategy D (Strategy C + CJ): The agents adopt Strategy C. In addition, node 6 transmits one information stream to node 5 to perform CJ, and aligns its interference at the LRs using IA. Specifically, set $\mathbf{v}_{6,5}$ to be orthogonal to $\text{span}([\mathbf{h}_{6,2}^\dagger \ \mathbf{H}_{6,4}^\dagger \mathbf{u}_{3,4}])$.

Fig. 3 illustrates the signal space at the receivers as well as the secrecy rate and SDoFs of the legitimate users under the above four strategies. Compared to Strategy A, Strategy B improves the secrecy rate by reducing the interference at the LRs. However, the interference generated by the confidential information streams does not have sufficient dimension to prevent capable ERs, i.e., node 8 and 9, from decoupling information streams from interference. To generate additional interference, in Strategy C node 5 exploits its additional antennas to transmit an additional dummy stream so that the

dimensions of interference at the ERs increase while those at the LRs do not. This approach creates sufficient dimension of interference at node 8. To further protect their secrecy, nodes 5 and 6 exploit their full-duplexing capability to deliver more streams in Strategy D, and finally prevent node 9 from decoupling the confidential information from the interference. From this case study, two inspirations can be obtained as in the following.

- Necessity of unifying various IESs: Strategy D achieves good secrecy performance at all nodes. This is due to the fact that it fully exploits the capability of “strong” nodes, such as nodes 5 and 6 (multiple antennas, full-duplexing), while accommodating the “weak” nodes, such as nodes 1 and 2 (single antenna, half-duplex). This capability of simultaneously engineering the interference for multiple heterogeneous nodes is enabled by jointly exploiting ZFB, AN, IA, and CJ.
- Sufficient dimensions of interference at the ERs: As highlighted by the three blue double arrows in Fig. 3, the information secrecy performance of the legitimate nodes is greatly improved when the legitimate users have generated sufficient dimensions of interference such that the ERs cannot decouple the information signal from the interference. Hence, the criterion of “generating sufficient dimension of interference at the ERs” provides a simple objective that has major impact on system performance.

B. Unified IES for Wireless Secrecy

The case study described in the previous section demonstrates the benefit of employing a unified IES for information secrecy and highlights a simple design criterion which has a major impact on system performance. To utilize such inspirations in networks with generic topology, the following problem is formulated:

Problem 1 (Unified IES for information secrecy): Given a network as defined in Section II-A, optimize the stream assignment \mathcal{S} and transceiver design \mathcal{T} to maximize the number of confidential data streams, subject to generating interference that occupies all dimensions of the signal space at the ERs while causing no interference at the LRs, i.e.,

$$\mathcal{P}_1: \max_{\mathcal{S}, \mathcal{T}} \sum_{t \in \mathcal{L}} \sum_{r: (t, r, *) \in \mathcal{A}} c_{t,r} \quad (8a)$$

$$\text{s.t. } \text{Rn}\{\mathbf{N}_e\} = N_e, \forall (*, *, e) \in \mathcal{A} \quad (8b)$$

$$\text{Rn}\{\mathbf{S}_{t,r}\} = c_{t,r}, \forall (t, r, *) \in \mathcal{A} \quad (8c)$$

$$\text{Rn}\{\mathbf{V}_j\} = d_j, \forall j \in \mathcal{J} \quad (8d)$$

$$\mathbf{N}_{t,r} = \mathbf{0}, \forall (t, r, *) \in \mathcal{A} \quad (8e)$$

where

$$\begin{aligned} \mathbf{N}_e &= \sum_{\substack{t \in \mathcal{L} \\ (t, e) \in \mathcal{H}}} \sum_{\substack{r: (t, r, *) \in \mathcal{A} \\ (t, r, e) \notin \mathcal{A}}} \mathbf{H}_{t,e} \mathbf{V}_{t,r} \mathbf{V}_{t,r}^\dagger \mathbf{H}_{t,e}^\dagger \\ &+ \sum_{\substack{j \in \mathcal{J} \\ (j, e) \in \mathcal{H}}} \mathbf{H}_{j,e} \mathbf{V}_j \mathbf{V}_j^\dagger \mathbf{H}_{j,e}^\dagger \end{aligned} \quad (9)$$

is the aggregated interference at node e , and $\mathbf{S}_{t,r}$ and $\mathbf{N}_{t,r}$ are defined in (6) and (7), respectively. \square

Problem 2 (Transformed unified IES problem):

$$\mathcal{P}_2 : \max_{\mathcal{S}, \tilde{\mathcal{T}}} \sum_{t \in \mathcal{L}} \sum_{r: (t, r, *) \in \mathcal{A}} c_{t, r} \quad (10a)$$

$$\text{s.t.} \quad \sum_{t \in \mathcal{L}} \sum_{r: (t, r, *) \in \mathcal{A}, (t, r, e) \notin \mathcal{A}} \mathbb{1}_{\mathcal{H}}\{(t, e)\} c_{t, r} + \sum_{j \in \mathcal{J}} \mathbb{1}_{\mathcal{H}}\{(j, e)\} d_j \geq N_e, \quad \forall (*, *, e) \in \mathcal{A} \quad (10b)$$

$$\text{Rn}\{\check{\mathbf{V}}_t\} = \sum_{s: (t, s, *) \in \mathcal{A}} c_{t, s} + \mathbb{1}_{\mathcal{J}}\{t\} d_t + \sum_{s \in \mathcal{N}_t} \sum_{k: (k, s, *) \in \mathcal{A}} c_{k, s}, \quad \forall (t, *, *) \in \mathcal{A} \quad (10c)$$

$$\text{Rn}\{\check{\mathbf{U}}_r\} = \sum_{k: (k, r, *) \in \mathcal{A}} c_{k, r} + \sum_{k \in \mathcal{N}_r} \left(\sum_{s: (k, s, *) \in \mathcal{A}} c_{k, s} + \mathbb{1}_{\mathcal{J}}\{k\} d_k \right), \quad \forall (*, r, *) \in \mathcal{A} \quad (10d)$$

$$\check{\mathbf{U}}_r^\dagger \mathbf{H}_{t, r} \check{\mathbf{V}}_t = \mathbf{0}, \quad \forall t, r \in \mathcal{C}_i, i \in \{1, 2, \dots, C\}, (t, r) \in \mathcal{H}, (t, r, *) \notin \mathcal{A} \quad (10e)$$

where $\tilde{\mathcal{T}}$ is the set of transformed transceivers $\check{\mathbf{U}}_k, \check{\mathbf{V}}_k$. The transformed transceivers are functions of CSI in the coordinated cluster set that node k belongs to, i.e., $\check{\mathbf{U}}_k, \check{\mathbf{V}}_k$ are functions of $\{\mathbf{H}_{t, r}, \text{ with } t, r \in \mathcal{C}_i\}$ in which i is chosen such that $k \in \mathcal{C}_i$.

IV. ALGORITHM DESIGN FOR THE UNIFIED IES

In this section, algorithms are designed for the unified IES problem.

A. Problem Transformation

In Problem 1, the constraints (8c) and (8e) require that LRs have sufficient dimensions of signal spaces for the desired signal, which is exempt from interference. While looking similar to those in IA problems, the constraints in Problem 1 are more complicated due to the generic system model defined in Section II-A. In particular:

- typical IA considers networks consisting of point-to-point communication links. Here, the user association set \mathcal{A} accommodates networks consisting of broadcast, multiple access, and full-duplexing communications;
- typical IA considers networks with full connectivity. Here, the connectivity set \mathcal{H} allows the consideration of networks with partial connectivity; and
- typical IA considers networks with global CSI. Here, the coordinated cluster sets \mathcal{C}_i and non-coordinated sets \mathcal{N}_k restrict the availability of CSI.

The following theorem converts Problem 1 into an equivalent one with simplified constraints.

Theorem 4.1 (Equivalent form of Problem 1): Consider the randomness of channel states as defined in Section II-A2. The maximum objective value in Problem 1 is the same of that in Problem 2 almost surely (i.e., with probability 1). Moreover, a transceiver design $\tilde{\mathcal{T}}$ that satisfies all constraints of Problem 2 can be converted to a transceiver design \mathcal{T} that satisfies all constraints of Problem 1 almost surely via Alg. 1.

Proof: Please refer to Appendix II for the proof. \square

In Problem 2, the objective (10a) and the first constraint (10b) are only associated with stream assignment \mathcal{S} . Hence, for a given \mathcal{S} , Problem 2 is reduced to a transceiver design problem of keeping the rank of transceivers at each node, i.e., (10c) and (10d), while mitigating the interference over intra-cluster links, i.e., (10e). Moreover, the transceivers are functions of CSI within the coordinated cluster set. Therefore, for a given \mathcal{S} , the design of $\tilde{\mathcal{T}}$ in each coordinated cluster is similar to a generalized interference alignment (GIA) problem

Algorithm 1 Conversion of transceivers

Each node k first checks its non-coordinated set \mathcal{N}_k , and waits until all nodes in \mathcal{N}_k complete their conversion, then performs the following operations to convert the transceivers.

- (i) Node k cancels inter-cluster interference to/from nodes in the non-coordinated set, i.e.,

$$\begin{aligned} \hat{\mathbf{V}}_k &= f\left(\check{\mathbf{V}}_k, \sum_{r \in \mathcal{N}_k} \mathbf{H}_{k, r}^\dagger \left(\sum_{t: (t, r, *) \in \mathcal{A}} \mathbf{U}_{t, r} \mathbf{U}_{t, r}^\dagger \right) \mathbf{H}_{k, r}\right) \\ \hat{\mathbf{U}}_k &= f\left(\check{\mathbf{U}}_k, \sum_{t \in \mathcal{N}_k} \mathbf{H}_{t, k} \left(\sum_{r: (t, r, *) \in \mathcal{A}} \mathbf{V}_{t, r} \mathbf{V}_{t, r}^\dagger \right. \right. \\ &\quad \left. \left. + \mathbb{1}_{\mathcal{J}}\{t\} \mathbf{V}_t \mathbf{V}_t^\dagger \right) \mathbf{H}_{t, k}^\dagger\right). \end{aligned} \quad (11)$$

where function f is defined in Appendix I.

- (ii) Node k cancels intra-cluster interference that is not addressed by (10e), i.e.,

- *Precoders for dummy signals:*

$$\mathbf{V}_k = f\left(\hat{\mathbf{V}}_k, \sum_{s: (k, s, *) \in \mathcal{A}} \mathbf{H}_{k, s}^\dagger \hat{\mathbf{U}}_s \hat{\mathbf{U}}_s^\dagger \mathbf{H}_{k, s}\right) \quad (12)$$

- *Precoders for information signals:*

$$\begin{aligned} \mathbf{V}_{k, r} &= f\left(\hat{\mathbf{V}}_k, \sum_{\substack{s: (k, s, *) \in \mathcal{A}, \\ s \neq r}} \mathbf{H}_{k, s}^\dagger \hat{\mathbf{U}}_s \hat{\mathbf{U}}_s^\dagger \mathbf{H}_{k, s} + \mathbf{V}_k^\dagger \mathbf{V}_k\right) \\ \forall r \text{ with } (k, r, *) &\in \mathcal{A} \end{aligned} \quad (13)$$

- *Decoders for information signals:*

$$\begin{aligned} \mathbf{U}_{t, k} &= f\left(\check{\mathbf{U}}_k, \sum_{\substack{s: (s, k, *) \in \mathcal{A}, \\ s \neq t}} \mathbf{H}_{s, k} \hat{\mathbf{V}}_s \hat{\mathbf{V}}_s^\dagger \mathbf{H}_{k, s}^\dagger\right) \\ \forall t \text{ with } (t, k, *) &\in \mathcal{A} \end{aligned} \quad (14)$$

that has been addressed in [33]. Hence, by adopting the problem transformation proposed in Theorem 4.1, the challenges induced by the generic system model proposed in Section II-A are addressed.

Remark 1 (Message overhead of Alg. 1): Alg. 1 does not involve iterative process. Moreover, from (11)–(14), each node

only need to know local CSI, e.g., node k only needs to know CSI in the set $\{\mathbf{H}_{k,r}, \mathbf{H}_{t,k}, t, r \in \mathcal{L}\}$. Therefore, the message overhead induced by Alg. 1 is mild. \square

Remark 2 (Unified IES enables adjustable coordination): In Problem 2, the design of transformed transceivers $\tilde{\mathcal{T}}$ in each coordinated cluster set is independent of that in other clusters. Hence, the requirement of global CSI or iterative message exchanges induced by coordination is limited within each coordination cluster set $\mathcal{C}_i, i \in \mathcal{C}$. The smaller the coordination cluster \mathcal{C}_i is, the fewer message exchanges are required for coordination. Therefore, with the unified IES, the message overhead induced by coordination can be brought down by reducing the sizes of coordination cluster sets.

On the other hand, in the rank constraints of transformed transceivers, i.e., (10c) and (10d), the last terms on the right hand side represent the additional rank needed for handling interference to or from nodes in non-coordinated sets $\mathcal{N}_k, k \in \mathcal{L}$. The smaller the non-coordinated set \mathcal{N}_k is, the lower the rank of $\tilde{\mathbf{V}}_k, \tilde{\mathbf{U}}_k$ need to be. Lower rank constraints enlarge the feasible set of Problem 2 and hence improve the secrecy performance of the network. Therefore, with the unified IES, the network's performance can be increased by reducing the sizes of non-coordination sets.

The joint constraint for the sizes of the coordination cluster sets and the non-coordination sets is given in (1). With this constraint, the unified IES enables a new framework for adjustable coordination, in which the coordination level can be tuned to achieve a balance between the volume of message overhead and the network's performance. Moreover, since the size of each set can be adjusted separately, the unified IES can adapt to the heterogeneous coordination capabilities of different nodes. This offers a great advantage for implementation. \square

B. Transceiver Design

As discussed in the previous section, for a given \mathcal{S} , the design of transceivers $\tilde{\mathcal{T}}$ in Problem 2 can be equivalently transformed to a set of nonlinear polynomial equations, for which few systematic tools exist to perform feasibility analysis and algorithm design. In the authors' prior work [32], [33], by exploiting algebraic geometry, a mathematical framework has been constructed to address this challenge for GIA problems. Inspired by this approach, the following analysis focuses on two objectives:

- establish a framework that applies to generic polynomials for problems beyond GIA.
- propose a sufficient feasibility condition that applies to networks with generic stream assignment \mathcal{S} for facilitating the optimization of stream assignment \mathcal{S} .

The proposed mathematical framework addresses the following category of problems:

Problem 3 (Polynomial equation sets): Let \mathcal{F} be an algebraically-closed field. Variables $t_p \in \mathcal{F}, p \in \mathcal{P}$, where $\mathcal{P} = \{1, 2, \dots, P\}$, are realizations of independent RVs drawn from continuous distributions. Find $x_q \in \mathcal{F}, q \in \mathcal{Q}$, where $\mathcal{Q} = \{1, 2, \dots, Q\}$, such that polynomial functions $f_p \in \mathcal{F}(x_1, x_2, \dots, x_Q)$ satisfy $f_p = t_p, p \in \mathcal{P}$. \square

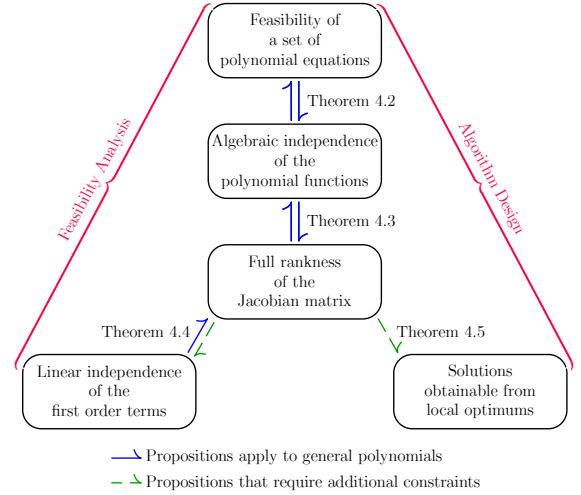


Fig. 4: Outline of the algebraic framework for polynomial equation sets.

Denote $\mathbf{x} = (x_1, x_2, \dots, x_Q)$ and $\mathbf{f} = (f_1, f_2, \dots, f_P)$. As outlined in Fig. 4, the proposed framework for polynomial equation sets consists of Theorems 4.2–4.5.

Theorem 4.2 (Feasibility and algebraic independence): Problem 3 has solutions almost surely if and only if polynomials $f_p, p \in \mathcal{P}$ are algebraically independent.

Proof: The proof is given in [33, Appendix A]. \square

Theorem 4.3 (Algebraic independence and the rank of Jacobian matrix): Polynomials $f_p, p \in \mathcal{P}$ are algebraically independent if and only if matrix $\mathbf{J}_{\mathbf{x}}(\mathbf{f})$ is full row-rank. Moreover, if there exists a point $\boldsymbol{\alpha} \in \mathcal{F}^S$ such that $\mathbf{J}_{\mathbf{x}}(\mathbf{f})|_{\mathbf{x}=\boldsymbol{\alpha}}$ is full row-rank, $\mathbf{J}_{\mathbf{x}}(\mathbf{f})$ is full row-rank. Conversely, if $\mathbf{J}_{\mathbf{x}}(\mathbf{f})$ is full row-rank, $\mathbf{J}_{\mathbf{x}}(\mathbf{f})|_{\mathbf{x}=\boldsymbol{\alpha}}$ is full row-rank on a dense open subset of \mathcal{F}^S .

Proof: The proof is given in Appendix III. \square

Denote \tilde{f}_p as functions that contain all the linear terms in $f_p, p \in \mathcal{P}$. The following definition describes a scenario in which the independence of \tilde{f}_p “represent” that of f_p .

Definition 1 (Independence representable by linear terms): Denote the coefficient of the linear term of x_q in f_p as $b_{p,q}$, and denote $g_{p,q}(\mathbf{x}) = \frac{\partial f_p(\mathbf{x})}{\partial x_q}$. The independence of polynomials $\{f_p\}$ is representable by linear terms if partial derivatives $g_{p,q}(\mathbf{x})$ are the same when the corresponding linear coefficients $b_{p,q}$ are the same, and are zero functions when $b_{p,q} = 0$, i.e.,

$$g_{p,q}(\mathbf{x}) \equiv \begin{cases} g_{\tilde{p},\tilde{q}}(\mathbf{x}) & \text{if } b_{p,q} = b_{\tilde{p},\tilde{q}}, \\ 0 & \text{if } b_{p,q} = 0. \end{cases} \quad (15)$$

Theorem 4.4 (Rank of Jacobian matrix and linear independence): If $\{\tilde{f}_p\}$ are linearly independent, $\mathbf{J}_{\mathbf{x}}(\mathbf{f})$ is full row-rank. The reverse statement is true almost surely if $\{\tilde{f}_p\}$ satisfy Definition 1 and linear coefficients $\{b_{p,q}\}$ are either selected from a set of independent RVs drawn from continuous distribution (allow repetitive selection) or 0.

Proof: The proof is given in Appendix IV. \square

Remark 3 (Feasibility analysis based on linear independence): By combining Theorem 4.2–4.4, the linear indepen-

$$\mathbf{H}_i = \left[\begin{array}{cccccc} \mathbf{H}_{k_2, k_1}^U & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{H}_{k_2, k_1}^V & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{H}_{k_3, k_1}^U & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{k_3, k_1}^V & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{k_L, k_1}^U & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{H}_{k_L, k_1}^V \\ \mathbf{0} & \mathbf{H}_{k_1, k_2}^U & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{H}_{k_1, k_2}^V & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_{k_3, k_2}^U & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{H}_{k_3, k_2}^V & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{H}_{k_L, k_2}^U & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{H}_{k_L, k_2}^V \\ \mathbf{0} & \mathbf{0} & \mathbf{H}_{k_1, k_3}^U & \cdots & \mathbf{0} & \mathbf{H}_{k_1, k_3}^V & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{H}_{k_L, k_L}^U & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{H}_{k_L, k_L}^V \end{array} \right] \left. \begin{array}{l} (k_l, k_1) \in \mathcal{H} \\ (k_l, k_1, *) \notin \mathcal{A} \\ \vdots \\ (k_l, k_2) \in \mathcal{H} \\ (k_l, k_2, *) \notin \mathcal{A} \\ \vdots \\ (k_l, k_L) \in \mathcal{H} \\ (k_l, k_L, *) \notin \mathcal{A} \end{array} \right\} \quad (16a)$$

$$\mathbf{H}_{t,r}^U = \text{diag}_{d_r^U} \left(\begin{array}{cccc} h_{t,r}(d_r^U + 1, 1), & h_{t,r}(d_r^U + 2, 1), & \cdots, & h_{t,r}(N_k, 1) \\ h_{t,r}(d_r^U + 1, 2), & h_{t,r}(d_r^U + 2, 2), & \cdots, & h_{t,r}(N_k, 2) \\ \vdots & \vdots & \ddots & \vdots \\ h_{t,r}(d_r^U + 1, d_t^V), & h_{t,r}(d_r^U + 2, d_t^V), & \cdots, & h_{t,r}(N_k, d_t^V) \end{array} \right) \quad (16b)$$

$$\mathbf{H}_{t,r}^V = \left[\begin{array}{l} \text{diag}_{d_t^V} (h_{t,r}(1, d_t^V + 1), h_{t,r}(1, d_t^V + 2), \cdots, h_{t,r}(1, M_j)) \\ \text{diag}_{d_t^V} (h_{t,r}(2, d_t^V + 1), h_{t,r}(2, d_t^V + 2), \cdots, h_{t,r}(2, M_j)) \\ \vdots \\ \text{diag}_{d_t^V} (h_{t,r}(d_r^U, d_t^V + 1), h_{t,r}(d_r^U, d_t^V + 2), \cdots, h_{t,r}(d_r^U, M_j)) \end{array} \right] \quad (16c)$$

dence of the first-order terms is a sufficient condition for a set of polynomial equations to be feasible. With additional constraints on the structure of the polynomials, this condition is also necessary. Since linear independence is in general more analytically tractable compared to algebraic independence, Theorem 4.2–4.4 enable analysis on the feasibility of a set of polynomials. \square

Theorem 4.5 (Rank of Jacobian matrix and local optimum): Consider a function $g(y_1, y_2, \dots, y_P)$ that is nonnegative, convex, with continuous second-order differentiation. The value of this function is equal to 0 only at point $\mathbf{t} = (t_1, t_2, \dots, t_P)$. Then if $f_p, p \in \mathcal{P}$ are second-order polynomials and $\mathbf{J}_x(\mathbf{f})$ is full row-rank, a local optimum of Problem 4 is a solution of Problem 3 almost surely.

Problem 4 (Optimization form of polynomial equations):

$$\mathcal{P}_4: \max_{\mathbf{x}} g(\mathbf{f}(\mathbf{x}))$$

Proof: The proof is similar to that of [33, Thm 4.5]. \square

Remark 4 (Algorithm design for solving second-order polynomials): By combining Theorem 4.2, 4.3, and 4.5, it can be seen that when the polynomials are of second order, a polynomial equation set can be transformed to an optimization problem whose global optimum can be found via local search algorithms. This provides a systematic tool to design algorithms that solve second-order polynomial equation sets, e.g., the design of $\tilde{\mathcal{T}}$ in Problem 2. \square

The developed mathematical framework enables the determination of the feasibility condition of Problem 2.

Theorem 4.6 (Feasibility conditions of Problem 2): Given a stream assignment \mathcal{S} , Problem 2 has solutions almost surely if and only if matrices \mathbf{H}_i defined in (16a) are full row-rank for all coordinated cluster sets $\mathcal{C}_i = \{k_1, k_2, \dots, k_L\}$.

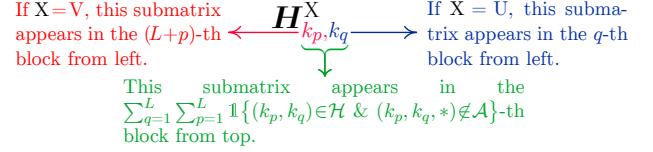


Fig. 5: The positions of the sub-matrices in \mathbf{H}_i .

The sub-matrices in \mathbf{H}_i are defined in (16b) and (16c), with their position in \mathbf{H}_i described in Fig. 5. In (16b) and (16c), $h_{t,r}(p, q)$ denotes the element in the p -th row and q -th column of $\mathbf{H}_{t,r}$,

$$\begin{aligned} d_r^U &\triangleq \sum_{k:(k,r,*) \in \mathcal{A}} c_{k,r} + \sum_{k \in \mathcal{N}_r} \left(\sum_{s:(k,s,*) \in \mathcal{A}} c_{k,s} + \mathbb{1}_{\mathcal{J}}\{k\} d_k \right) \\ d_t^V &\triangleq \sum_{s:(t,s,*) \in \mathcal{A}} c_{t,s} + \mathbb{1}_{\mathcal{J}}\{t\} d_t + \sum_{s \in \mathcal{N}_t} \sum_{k:(k,s,*) \in \mathcal{A}} c_{k,s}. \end{aligned}$$

Proof: First convert Problem 2 to a set of polynomial equations by adopting the approach used in [33, Thm 4.1]. Then the theorem can be proved by adopting Theorem 4.2, Theorem 4.3, and Theorem 4.4 sequentially. \square

In Theorem 4.6, verifying the full-rankness of matrices \mathbf{H}_i can be computationally costly for large coordinated cluster sets, making it difficult to optimize stream assignment \mathcal{S} in Problem 2. The following corollary proposes sufficient feasibility conditions for Problem 2 that only involve scalar inequalities.

Corollary 4.1 (Sufficient feasibility conditions of Problem 2): Given stream assignment \mathcal{S} , Problem 2 has solutions almost surely if there exists a set of binary variables $\{c_{t,r,p,q}^T, c_{t,r,p,q}^R \in \{0, 1\}\}$, where $t, r \in \mathcal{C}_i$, $(t, r) \in \mathcal{H}$,

$(t, r, *) \notin \mathcal{A}$, $p \in \{1, 2, \dots, d_r^U\}$, and $q \in \{1, 2, \dots, d_t^V\}$ for every coordinated cluster set \mathcal{C}_i that satisfy the following constraints.

$$c_{t,r,p,q}^T + c_{t,r,p,q}^R = 1, \quad \forall t, r, p, q \quad (17a)$$

$$c_{t,r,1,q}^T = c_{t,r,2,q}^T = \dots = c_{t,r,d_r^U,q}^T, \quad \forall t, r, q \quad (17b)$$

$$\sum_{\substack{t:t \in \mathcal{C}_i, (t,r) \in \mathcal{H} \\ (t,r,*) \notin \mathcal{A}}} \sum_{q=1}^{d_t^V} c_{t,r,p,q}^R \leq N_r - d_r^U, \quad \forall r \quad (17c)$$

$$\sum_{\substack{r:r \in \mathcal{C}_i, (t,r) \in \mathcal{H} \\ (t,r,*) \notin \mathcal{A}}} d_r^U c_{t,r,p,q}^T \leq N_t - d_t^V, \quad \forall t, q. \quad (17d)$$

Proof: The proof is similar to that of [32, Lem. 3.7], with Theorem 4.6 replacing the role of [32, Thm. 3.2]. \square

Remark 5 (Metric for the tightness of feasibility): The binary variables $\{c_{t,r,p,q}^T, c_{t,r,p,q}^R\}$ were introduced in the authors' prior work [32] to represent a *constraint allocation policy* that is used for characterizing the IA feasibility conditions. Specifically, inequalities (17c) and (17d) ensure that the number of constraints assigned to a node is no greater than the number of variables in its transceiver design. The difference between the right hand side and the left hand side of (17c) and (17d) represents the number of additional variables after assignment of constraints. Therefore, define

$$R_t^V \triangleq \min_{q \in \{1, 2, \dots, d_t^V\}} \left\{ N_t - d_t^V - \sum_{\substack{r:r \in \mathcal{C}_i, (t,r) \in \mathcal{H} \\ (t,r,*) \notin \mathcal{A}}} d_r^U c_{t,r,p,q}^T \right\} \quad (18a)$$

$$R_r^U \triangleq N_r - d_r^U - \sum_{\substack{t:t \in \mathcal{C}_i, (t,r) \in \mathcal{H} \\ (t,r,*) \notin \mathcal{A}}} \sum_{q=1}^{d_t^V} c_{t,r,p,q}^R. \quad (18b)$$

Then these metrics represent the tightness of unified IES constraints. They will be used to facilitate the optimization of stream assignment \mathcal{S} in the next section. \square

When it is determined that Problem 2 has solutions almost surely, one can first calculate the desired transformed transceivers \check{U}_r, \check{V}_t via GIA algorithms, e.g. [33, Alg. 1], then generate desired transceivers $U_{t,r}, V_{t,r}$, and V_j via Alg. 1.

C. Stream Assignment Design

In this section, the stream assignment \mathcal{S} will be designed. The design of \mathcal{S} is a combinatorial problem whose optimal solution often involves exhaustive search with exponential complexity with respect to (w.r.t.) the number of nodes in the networks. For low complexity consideration, we propose an iterative search algorithm, i.e. Alg. 2.

Note that Alg. 2 always converges. This is because the objective of Problem 2, i.e., (10a) is upper bounded, and non-decreasing in the iteration between Step (ii) and (iii).

Remark 6 (Message overhead of Alg. 2): From (18)–(21), in Alg. 2, the stream assignment \mathcal{S} is determined by the antenna configuration $\{N_k\}$, level of coordination $\{\mathcal{C}_i, \mathcal{N}_k\}$, and channel connectivity \mathcal{H} . Since these parameters are either constants or changes on macroscopic time scale, Alg. 2 only needs to be recurrently performed on macroscopic time scale. This property assures that the message overhead induced by Alg. 2 will not be significant for the network. \square

Algorithm 2 Stream assignment

- Initialize \mathcal{S} : $c_{t,r} = 0, d_j = 0, \forall (t, r, *) \in \mathcal{A}, j \in \mathcal{J}$.
 (i) Add dummy streams to most efficiently increase the dimension of interference at ERs. Specifically, the node with index given by (19) increases d_{j^*} by 1.

$$j^* = \arg \max_{j \in \mathcal{J}} \sum_{\substack{e=1 \\ e \notin \mathcal{L}}}^K \mathbb{1}_{\mathcal{E}}\{e\} \mathbb{1}_{\mathcal{H}}\{(j, e)\} \quad (19)$$

where $\mathcal{E} = \{e : I_e < N_e\}$ is the set of ERs for which (10b) does not hold,

$$I_e = \sum_{t \in \mathcal{L}} \sum_{\substack{r:(t,r,*) \in \mathcal{A} \\ (t,r,e) \notin \mathcal{A}}} \mathbb{1}_{\mathcal{H}}\{(t, e)\} c_{t,r} + \sum_{j \in \mathcal{J}} \mathbb{1}_{\mathcal{H}}\{(j, e)\} d_j.$$

Repeat this step until the dimensions of interference at the ERs, i.e., $\min\{I_e, N_e\}$ can no longer be increased by increasing the number of dummy streams d_j .

- (ii) Add information streams to the link with the most relaxed feasibility constraints. Specifically, the link with index given by (20) increases d_{t^*, r^*} by 1.

$$(t^*, r^*) = \begin{cases} \arg \max_{\substack{(t,r,*) \in \mathcal{A} \\ \mathcal{E}_t \neq \emptyset}} \min \left\{ R_t^V, R_r^U, \min_{k:r \in \mathcal{N}_k} \{R_k^V\}, \right. \\ \quad \left. \min_{s:t \in \mathcal{N}_s} \{R_s^U\} \right\}, & \text{if } \mathcal{E} \neq \emptyset \\ \arg \max_{(t,r,*) \in \mathcal{A}} \min \left\{ R_t^V, R_r^U, \min_{k:r \in \mathcal{N}_k} \{R_k^V\}, \right. \\ \quad \left. \min_{s:t \in \mathcal{N}_s} \{R_s^U\} \right\}, & \text{otherwise} \end{cases} \quad (20)$$

where $\mathcal{E}_t = \{e : e \in \mathcal{E}, (t, e) \in \mathcal{H}\}$, while R_t^V and R_r^U are defined in (18). Then use [32, Alg. 2] to update the constraint allocation policy $\{c_{t,r,p,q}^T, c_{t,r,p,q}^R\}$ and determine the feasibility of Problem 2. Repeat this step as long as the problem is feasible. Otherwise, go to Step (iii) with the last stream assignment policy \mathcal{S} that makes Problem 2 feasible.

- (iii) Reduce the number of dummy streams without affecting the dimensions of aggregated interference at the ERs. Specifically, the node with index given by (21) decreases d_{j^*} by 1.

$$j^* = \arg \min_{j \in \check{\mathcal{J}}} \sum_{\substack{e=1 \\ e \notin \mathcal{L}}}^K \mathbb{1}_{\mathcal{H}}\{(j, e)\} \quad (21)$$

where $\check{\mathcal{J}} = \{j : I_e > N_e, \forall e \text{ with } (j, e) \in \mathcal{H}\}$ is the set of LJ whose number of dummy streams can be reduced without affecting the dimensions of aggregated interference at the ERs. Repeat this step until no dummy stream can be removed, i.e., $\check{\mathcal{J}} = \emptyset$. If some dummy streams have been removed in Step (iii), go back to Step (ii). Otherwise, exit the algorithm.

With the algorithms proposed in Section IV, we have overcome the technical challenges brought by the generic system model and come up with an efficient method to design and optimize the unified IES for information secrecy.

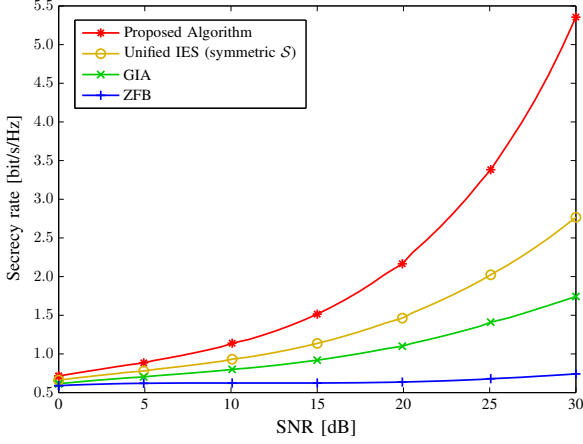


Fig. 6: Secrecy rate per LR as a function of transmit SNR under various IESs. In this test, $\alpha = 3$, $\rho^{(s)} = 0.04$, $\rho^{(a)} = 0.08$, $\rho^{(e)} = 0.1$, $N^{(e)} = 20$.

V. PERFORMANCE EVALUATION

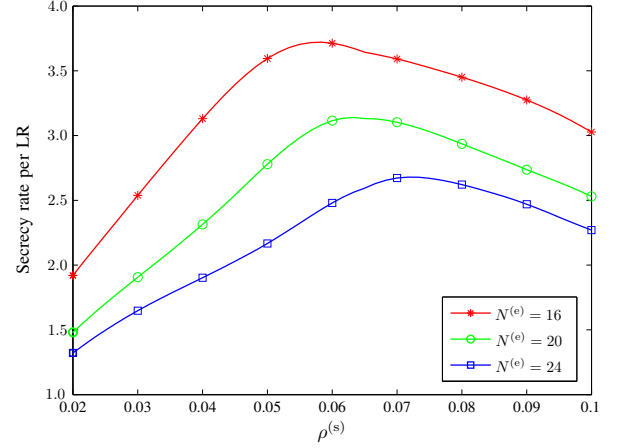
In this section, two network settings are considered to evaluate the performance of the proposed algorithms. The network consists of three types of nodes, i.e., simple legitimate nodes, advanced legitimate nodes, and ERs. A simple node has two antennas, and can only perform half-duplex communication. An advanced node has eight antennas, and can perform full-duplex communication. The simple nodes are in the non-coordinated sets of advanced nodes. An ERs has $N^{(e)}$ number of antennas. The three types of nodes are uniformly distributed in a square, with density $\rho^{(s)}$, $\rho^{(a)}$, $\rho^{(e)}$ respectively. The nodes associate with each other according to their distance. For instance, the nearest pair of simple nodes associate with each other, and then the second nearest pair associate with each other, and so on. Each ER associates with the nearest LT that has not been eavesdropped on by other ERs.

The channel state between two nodes positioned at $\mathbf{a}, \mathbf{b} \in \mathbb{R}^2$ is given by $\mathbf{H} = \sqrt{L_{\mathbf{a},\mathbf{b}}} \tilde{\mathbf{H}}$, where the elements in $\tilde{\mathbf{H}}$ are independent random variables following complex Gaussian distribution with mean zero and variance one and the pathloss $L_{\mathbf{a},\mathbf{b}} = \|\mathbf{a} - \mathbf{b}\|^{-\alpha}$, in which the pathloss exponent $\alpha \in [2, 5]$.

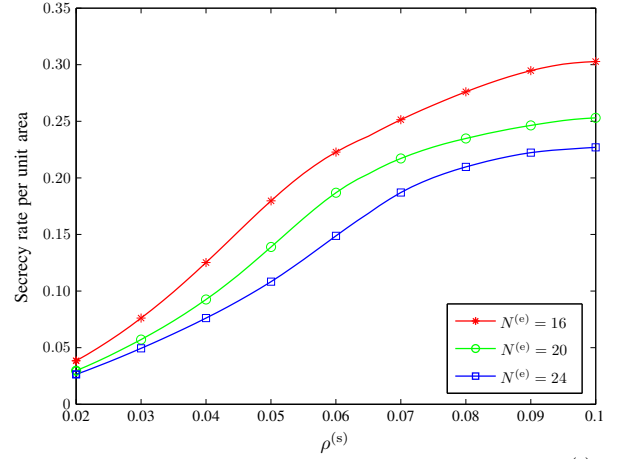
Fig. 6 shows the average secrecy rate per LR as a function of transmit SNR for various IESs. Here, the transmit SNR is defined by $10 \log(P)$, where P is the transmission power of each LT. The proposed algorithm is compared with three baselines defined in the following.

- **Unified IES with symmetric \mathcal{S} :** The legitimate nodes adopt a symmetric stream assignment \mathcal{S} and then use the approach proposed in Section IV-B to design transceivers.
- **GIA:** The legitimate nodes adopt the GIA algorithm proposed in [38] (full-duplexing capability of advanced nodes is not exploited).
- **ZFB:** The legitimate nodes adopt ZFB to cancel interference (without involving coordinated cluster among multiple transmitters).

The comparison of the performance achieved by various IESs decomposes the performance gain of the proposed algorithm. The performance of GIA compared to that of ZFB



(a) Secrecy rate per LR as a function of $\rho^{(s)}$.



(b) Secrecy rate per per unit area as a function of $\rho^{(s)}$.

Fig. 7: Secrecy rate achieved by the proposed algorithm as a function of legitimate node density $\rho^{(s)}$. The secrecy rate per LR and per unit area are plotted in subfigure (a) and (b), respectively. In this test, $\alpha = 3$, $\rho^{(a)} = 2\rho^{(s)}$, $\rho^{(e)} = 0.1$, SNR is at 20 dB.

shows the benefit of coordination among multiple nodes. The performance of unified IES with symmetric \mathcal{S} compared to that of GIA shows the benefit of exploiting the full-duplexing capability of advanced nodes. Finally, the performance of the proposed algorithm compared to that of unified IES with symmetric \mathcal{S} illustrates the performance gain due to dynamically adjusting data stream assignment \mathcal{S} to adapt to network topology. The performance gain of the proposed highlights the benefit of unifying various IESs into a coherent framework.

Fig. 7 illustrates the secrecy rate achieved by the proposed algorithm as a function of legitimate node density for different ER antenna number. When the density of legitimate nodes increases, there are two contesting effects that change the secrecy rate. On the one hand, higher density enables neighboring legitimate nodes to help each other more effectively in protecting secrecy via interference. On the other hand, higher density also means more legitimate nodes are sharing the limited channel resources. In low density region, the first effect dominates over the second one, leading to an increase in secrecy rate per LR, and vice versa in the high

Algorithm 3 Stream assignment

- If \mathbf{W} is an empty matrix, let $\hat{\mathbf{V}} = \mathbf{V}$. Otherwise, do the following:
- (i) Perform singular value decomposition (SVD) on $\mathbf{V}^\dagger \mathbf{W} \mathbf{V}$, i.e., $\mathbf{R} \mathbf{D} \mathbf{R}^\dagger = \mathbf{V}^\dagger \mathbf{W} \mathbf{V}$ where \mathbf{R} is a unitary matrix, \mathbf{D} is a diagonal matrix with d number of non-zero diagonal elements on the top left of the matrix.
 - (ii) Let $\mathbf{R} = [\hat{\mathbf{R}} \quad \hat{\mathbf{R}}]$, where $\hat{\mathbf{R}}$ has $c - d$ columns.
 - (iii) Set $\hat{\mathbf{V}} = \mathbf{V} \hat{\mathbf{R}}$.

density region. However, even in the high density region, the proposed unified IES dynamically adjusts the generation of interference, so that the secrecy rate per unit area remains an increasing function of legitimate node density. This is an advantage over existing IESs for wireless secrecy, which may generate network interference that is inefficient or even harmful for wireless secrecy in scenarios with excessively high node density [2]–[4].

VI. CONCLUSION

This work proposed a unified IES to enhance wireless information secrecy in heterogeneous networks with different levels of CSI availability and signal processing capability at various nodes. A transceiver conversion algorithm was proposed to overcome the challenges brought by the generic topology of heterogeneous networks, then the transceiver design issue of the unified IES was addressed by a mathematical framework using tools from algebraic geometry. Finally, a low-complexity stream assignment algorithm was designed for the unified IES. By integrating key ideas from various existing IESs, the proposed strategy enables a new framework for adjustable coordination, which accommodates nodes with heterogeneous coordination capabilities to achieve high level of wireless secrecy with low message overhead. Numerical evaluation of the unified IES showed that the proposed strategy can significantly improve the wireless information secrecy in heterogeneous networks.

APPENDIX I

INTERFERENCE CANCELLATION IN A LINEAR SUBSPACE

Given a matrix \mathbf{V} and a positive semi-definitive matrix \mathbf{W} , with $\text{Rn}\{\mathbf{V}\} = c$ and $\text{Rn}\{\mathbf{V}^\dagger \mathbf{W} \mathbf{V}\} = d$, Alg. 3 generates a matrix $\hat{\mathbf{V}}$ that satisfies

$$\begin{aligned} \text{Rn}\{\hat{\mathbf{V}}\} &= c - d, \quad \text{span}(\hat{\mathbf{V}}) \subseteq \text{span}(\mathbf{V}), \\ \text{and } \hat{\mathbf{V}}^\dagger \mathbf{W} \hat{\mathbf{V}} &= \mathbf{0}. \end{aligned} \quad (22)$$

Denote the input-output mapping of Alg. 3 as $\hat{\mathbf{V}} = f(\mathbf{V}, \mathbf{W})$. The function f will be used in Alg. 1.

APPENDIX II

PROOF OF THEOREM 4.1

Note that the objective functions of the two problems, i.e., (8a) and (10a) are the same function of \mathcal{S} . Therefore, to prove the theorem, it is sufficient to show that:

- (i) if a stream assignment \mathcal{S} is feasible in Problem 1, then it is feasible in Problem 2 almost surely;
- (ii) if a stream assignment \mathcal{S} is feasible in Problem 2, then it is feasible in Problem 1 almost surely; and
- (iii) if a stream assignment \mathcal{S} is feasible in Problem 2, then the transceivers \mathcal{T} generated by Alg. 1 satisfy all constraints of Problem 1 almost surely.

First prove statement (i). Since $\mathbf{V}_{t,r} \in \mathbb{C}^{N_t \times c_{t,r}}$, $\mathbf{V}_j \in \mathbb{C}^{N_t \times d_j}$, we have $\text{Rn}\{\mathbf{V}_{t,r}\} \leq c_{t,r}$, $\text{Rn}\{\mathbf{V}_j\} \leq d_j$. Therefore, from (8b) and (9),

$$\begin{aligned} & \sum_{t \in \mathcal{L}} \sum_{\substack{r: (t,r,*) \in \mathcal{A}, \\ (t,r,e) \notin \mathcal{A}}} \mathbb{1}_{\mathcal{H}}\{(t,e)\} c_{t,r} + \sum_{j \in \mathcal{J}} \mathbb{1}_{\mathcal{H}}\{(j,e)\} d_j \\ & \geq \sum_{t \in \mathcal{L}} \sum_{\substack{r: (t,r,*) \in \mathcal{A}, \\ (t,r,e) \notin \mathcal{A}}} \mathbb{1}_{\mathcal{H}}\{(t,e)\} \text{Rn}\{\mathbf{V}_{t,r}\} + \sum_{j \in \mathcal{J}} \mathbb{1}_{\mathcal{H}}\{(j,e)\} \text{Rn}\{\mathbf{V}_j\} \\ & \geq \text{Rn}\left\{ \sum_{\substack{t \in \mathcal{L} \\ (t,e) \in \mathcal{H}}} \sum_{\substack{r: (t,r,*) \in \mathcal{A}, \\ (t,r,e) \notin \mathcal{A}}} \mathbf{H}_{t,e} \mathbf{V}_{t,r} \mathbf{V}_{t,r}^\dagger \mathbf{H}_{t,e}^\dagger + \sum_{\substack{j \in \mathcal{J} \\ (j,e) \in \mathcal{H}}} \mathbf{H}_{j,e} \mathbf{V}_j \mathbf{V}_j^\dagger \mathbf{H}_{j,e}^\dagger \right\} \\ & = N_e \end{aligned}$$

Hence, (10b) holds.

Define $\hat{\mathbf{V}}_t$ as the matrix aggregated by the precoders at node t . For example, if $(t, 1, *) \in \mathcal{A}$, $(t, 2, *) \in \mathcal{A}$, $t \in \mathcal{J}$ then $\hat{\mathbf{V}}_t = [\mathbf{V}_{t,1}, \mathbf{V}_{t,1}, \mathbf{V}_t]$. From (8c), (8d), and (8e),

$$\text{Rn}\{\hat{\mathbf{V}}_t\} = \sum_{r: (t,r,*) \in \mathcal{A}} c_{t,r} + \mathbb{1}_{\mathcal{J}}\{t\} d_t \quad (23)$$

Similarly, define $\hat{\mathbf{U}}_r$ as the matrix aggregated by the decoders at node r , then

$$\text{Rn}\{\hat{\mathbf{U}}_r\} = \sum_{t: (t,r,*) \in \mathcal{A}} c_{t,r} \quad (24)$$

From (8e),

$$\hat{\mathbf{U}}_r^\dagger \mathbf{H}_{t,r} \hat{\mathbf{V}}_t = \mathbf{0}, \quad \forall t \neq r, (t, r, *) \notin \mathcal{A}. \quad (25)$$

Now, consider the impact of the limited CSI availability described by (2). Suppose nodes t, r are in the same coordinated cluster set \mathcal{C}_i , and $(t, r, *) \notin \mathcal{A}$. At node r , denote the signal space occupied by inter- and intra-cluster interference as

$$\mathcal{I}_r^{\text{inter}} = \text{span}\left(\sum_{k \in \mathcal{N}_r} \mathbf{H}_{k,r} \hat{\mathbf{V}}_k\right), \quad (26a)$$

$$\mathcal{I}_r^{\text{intra}} = \text{span}\left(\sum_{\substack{k \in \mathcal{C}_i, (k,r) \in \mathcal{H} \\ (k,r,*) \notin \mathcal{A}}} \mathbf{H}_{k,r} \hat{\mathbf{V}}_k\right). \quad (26b)$$

Since $\hat{\mathbf{V}}_k$ does not adapt to $\mathbf{H}_{k,r}$, $k \in \mathcal{N}_r$, from (23),

$$\dim\{\mathcal{I}_r^{\text{inter}}\} = \sum_{k \in \mathcal{N}_r} \left(\sum_{k: (k,s,*) \in \mathcal{A}} c_{k,s} + \mathbb{1}_{\mathcal{J}}\{k\} d_k \right) \quad (27)$$

almost surely.

According to (2), within the coordinated cluster set \mathcal{C}_i , the channel state $\mathbf{H}_{k,r}$, $k \in \mathcal{N}_r$ only affects $\hat{\mathbf{U}}_r$ and $\hat{\mathbf{V}}_r$. Since both $\hat{\mathbf{U}}_r$ and $\hat{\mathbf{V}}_r$ do not appear in (26b), $\mathcal{I}_r^{\text{intra}}$ is independent of $\mathcal{I}_r^{\text{inter}}$, which means that

$$\mathcal{I}_r^{\text{inter}} \cap \mathcal{I}_r^{\text{intra}} = \{0\} \quad (28)$$

almost surely. Moreover, from (25), the space spanned by the columns of $\hat{\mathbf{U}}_r$ is orthogonal to $\mathcal{I}_r^{\text{inter}}$ and $\mathcal{I}_r^{\text{intra}}$, i.e.,

$$\text{span}(\hat{\mathbf{U}}_r) \perp \mathcal{I}_r^{\text{intra}}, \text{ and } \text{span}(\hat{\mathbf{U}}_r) \perp \mathcal{I}_r^{\text{inter}}. \quad (29)$$

From (28) and (29)

$$\begin{aligned} \dim\{\text{span}(\hat{\mathbf{U}}_r)\} + \dim\{\mathcal{I}_r^{\text{inter}}\} + \dim\{\mathcal{I}_r^{\text{intra}}\} \\ = \dim\{\text{span}(\hat{\mathbf{U}}_r) + \mathcal{I}_r^{\text{inter}} + \mathcal{I}_r^{\text{intra}}\} \leq N_r \end{aligned} \quad (30)$$

From (24), (27), and (30)

$$\begin{aligned} \dim\{\mathcal{I}_r^{\text{intra}}\} \leq N_r - \sum_{k:(k,r,*) \in \mathcal{A}} c_{k,r} \\ - \sum_{k \in \mathcal{N}_r} \left(\sum_{s:(k,s,*) \in \mathcal{A}} c_{k,s} + \mathbb{1}_{\mathcal{J}}\{k\} d_k \right) \end{aligned}$$

Therefore, there exists a linear subspace $\check{\mathcal{U}}_r$ that satisfies

$$\check{\mathcal{U}}_r \perp \mathcal{I}_r^{\text{intra}} \quad (31a)$$

$$\begin{aligned} \dim\{\check{\mathcal{U}}_r\} = \sum_{k:(k,r,*) \in \mathcal{A}} c_{k,r} \\ + \sum_{k \in \mathcal{N}_r} \left(\sum_{s:(k,s,*) \in \mathcal{A}} c_{k,s} + \mathbb{1}_{\mathcal{J}}\{k\} d_k \right) \end{aligned} \quad (31b)$$

and $\text{span}(\hat{\mathbf{U}}_r)$ can now be expressed as

$$\text{span}(\hat{\mathbf{U}}_r) = \{\mathbf{u} : \mathbf{u} \in \check{\mathcal{U}}_r, \mathbf{u} \perp \mathcal{I}_r^{\text{inter}}\}. \quad (32)$$

From (2) and (31a), $\check{\mathcal{U}}_r$ is independent of $\mathcal{I}_r^{\text{inter}}$.

By repeating the analysis from (26a) to (32) on node t , it can be obtained that there exists a linear subspace $\check{\mathcal{V}}_t$ that has dimension

$$\dim\{\check{\mathcal{V}}_t\} = \sum_{s:(t,s,*) \in \mathcal{A}} c_{t,s} + \mathbb{1}_{\mathcal{J}}\{t\} d_t + \sum_{s \in \mathcal{N}_t} \sum_{k:(k,s,*) \in \mathcal{A}} c_{k,s} \quad (33)$$

and is independent of $\bar{\mathcal{I}}_{t_inter}$, where

$$\bar{\mathcal{I}}_{t_inter} = \text{span}\left(\sum_{s \in \mathcal{N}_t} \mathbf{H}_{t,s}^\dagger \hat{\mathbf{U}}_s\right).$$

The subspace $\text{span}(\hat{\mathbf{V}}_t)$ can now be expressed as

$$\text{span}(\hat{\mathbf{V}}_t) = \{\mathbf{v} : \mathbf{v} \in \check{\mathcal{V}}_t, \mathbf{v} \perp \bar{\mathcal{I}}_{t_inter}\}.$$

Construct $\check{\mathbf{U}}_r$ and $\check{\mathbf{V}}_r$ such that their columns form a basis of $\check{\mathcal{U}}_r$ and $\check{\mathcal{V}}_t$, respectively. Define $\check{\mathcal{U}}_r^{\text{sub}} \subseteq \check{\mathcal{U}}_r$ as the subspace on which interference is cancelled, i.e.,

$$\check{\mathcal{U}}_r^{\text{sub}} = \{\mathbf{u}_r : \mathbf{u}_r^\dagger \mathbf{H}_{t,r} \check{\mathbf{V}}_t = 0, \mathbf{u}_r \in \check{\mathcal{U}}_r\}.$$

If

$$\check{\mathbf{U}}_r^\dagger \mathbf{H}_{t,r} \check{\mathbf{V}}_t \neq \mathbf{0} \quad (34)$$

then $\dim(\check{\mathcal{U}}_r^{\text{sub}}) < \dim(\check{\mathcal{U}}_r)$. Moreover, since $\check{\mathcal{U}}_r$ and $\mathbf{H}_{t,r}$ are independent of $\mathcal{I}_r^{\text{inter}}$, so is $\check{\mathcal{U}}_r^{\text{sub}}$. Therefore, from (32), $\text{span}(\hat{\mathbf{U}}_r) \not\subseteq \check{\mathcal{U}}_r^{\text{sub}}$ almost surely. This means that

$$\hat{\mathbf{U}}_r^\dagger \mathbf{H}_{t,r} \check{\mathbf{V}}_t \neq \mathbf{0} \quad (35)$$

almost surely. Similarly, define

$$\check{\mathcal{V}}_t^{\text{sub}} = \{\mathbf{v}_t : \hat{\mathbf{U}}_r^\dagger \mathbf{H}_{t,r} \mathbf{v}_t = 0, \mathbf{v}_t \in \check{\mathcal{V}}_t\},$$

and repeat the analysis from (34) to (35), then it can be obtained that $\hat{\mathbf{U}}_r^\dagger \mathbf{H}_{t,r} \check{\mathbf{V}}_t \neq \mathbf{0}$ almost surely, which is in contradiction with (25). Therefore, (34) shall not hold, i.e.,

$$\check{\mathbf{U}}_r^\dagger \mathbf{H}_{t,r} \check{\mathbf{V}}_t = \mathbf{0} \quad (36)$$

From (31b), (33), and (36), we have that (10c), (10d), and (10e) hold. This completes the proof of statement (i).

Now turn to the proof of statements (ii) and (iii). Noticing that statement (ii) is true as long as statement (iii) holds, the following analysis focuses on proving statement (iii). According to the properties of function f , i.e., (22) and the properties of $\check{\mathbf{V}}_k$ and $\check{\mathbf{U}}_k$, i.e., (10c)–(10e), after inter-cluster interference mitigation, i.e., (11), $\check{\mathbf{V}}_k$ satisfies

$$\begin{aligned} \text{Rn}\{\hat{\mathbf{V}}_k\} &= \text{Rn}\{\check{\mathbf{V}}_k\} - \\ &\quad \text{Rn}\left\{\sum_{r \in \mathcal{N}_k} \mathbf{H}_{k,r}^\dagger \left(\sum_{t:(t,r,*) \in \mathcal{A}} \mathbf{U}_{t,r} \mathbf{U}_{t,r}^\dagger\right) \mathbf{H}_{k,r}\right\} \\ &= \sum_{r:(k,r,*) \in \mathcal{A}} c_{k,r} + \mathbb{1}_{\mathcal{J}}\{k\} d_k \end{aligned} \quad (37a)$$

$$\mathbf{U}_{t,r}^\dagger \mathbf{H}_{k,r} \hat{\mathbf{V}}_k = \mathbf{0}, \quad \forall r \in \mathcal{N}_k, (t, r, *) \in \mathcal{A} \quad (37b)$$

$$\check{\mathbf{U}}_r^\dagger \mathbf{H}_{k,r} \hat{\mathbf{V}}_k = \mathbf{0}, \quad \forall r \in \mathcal{C}_i, (k, r, *) \notin \mathcal{A} \quad (37c)$$

and $\hat{\mathbf{U}}_k$ satisfies

$$\begin{aligned} \text{Rn}\{\hat{\mathbf{U}}_k\} &= \text{Rn}\{\check{\mathbf{U}}_k\} - \text{Rn}\left\{\sum_{t \in \mathcal{N}_k} \mathbf{H}_{t,k} \left(\sum_{r:(t,r,*) \in \mathcal{A}} \mathbf{V}_{t,r} \mathbf{V}_{t,r}^\dagger\right) \mathbf{H}_{t,k}^\dagger\right\} \\ &\quad + \mathbb{1}_{\mathcal{J}}\{k\} \mathbf{V}_k \mathbf{V}_k^\dagger \mathbf{H}_{t,k}^\dagger \\ &= \sum_{t:(t,k,*) \in \mathcal{A}} c_{t,k} \end{aligned} \quad (38a)$$

$$\hat{\mathbf{U}}_k^\dagger \mathbf{H}_{t,k} \mathbf{V}_{t,r} = \mathbf{0} \quad \forall t \in \mathcal{N}_k, (t, r, *) \in \mathcal{A} \quad (38b)$$

$$\hat{\mathbf{U}}_k^\dagger \mathbf{H}_{t,k} \check{\mathbf{V}}_t = \mathbf{0} \quad \forall t \in \mathcal{C}_i, (t, k, *) \notin \mathcal{A}. \quad (38c)$$

According to the properties of function f in (22) and the properties of $\hat{\mathbf{V}}_k$, $\check{\mathbf{U}}_k$, $k \in \mathcal{C}_i$ in (37a)–(38c), we obtained, after all clusters performed intra-cluster interference mitigation in (12), (13), and (14), that

$$\text{Rn}\{\mathbf{V}_k\} = d_k \quad \forall k \in \mathcal{J} \quad (39a)$$

$$\text{Rn}\{\mathbf{V}_{k,r}\} = c_{k,r} \quad \forall (k, r, *) \in \mathcal{A} \quad (39b)$$

$$\text{Rn}\{\mathbf{U}_{t,k}\} = c_{t,k} \quad \forall (t, k, *) \in \mathcal{A} \quad (39c)$$

$$\begin{aligned} \mathbf{U}_{k,r}^\dagger \mathbf{H}_{t,r} \mathbf{V}_{t,s} = \mathbf{0} \quad &\forall (k, r, *), (t, s, *) \in \mathcal{A}, (k, r) \neq (t, s) \\ &(t, r) \in \mathcal{H} \end{aligned} \quad (39d)$$

$$\mathbf{U}_{k,r}^\dagger \mathbf{H}_{j,r} \mathbf{V}_j = \mathbf{0} \quad \forall (k, r, *) \in \mathcal{A}, j \in \mathcal{J}, (j, r) \in \mathcal{H}. \quad (39e)$$

From (10e) and (11)–(14), the transceivers \mathbf{V}_k , $\mathbf{V}_{k,r}$, and $\mathbf{U}_{t,k}$ are independent of the CSI associated with ERs, i.e., $\{\mathbf{H}_{t,e}, (t, *, e) \in \mathcal{A}\}$. Moreover, when $(t, r, *) \in \mathcal{A}$, $\mathbf{V}_{t,r}$ and $\mathbf{U}_{t,r}$ are independent of $\mathbf{H}_{t,r}$. Therefore, from (39a), (39b), and (39c), it can be obtained that

$$\begin{aligned} \text{Rn}\{\mathbf{N}_e\} &= \min\left\{N_e, \sum_{t \in \mathcal{L}} \sum_{\substack{r:(t,r,*) \in \mathcal{A}, \\ (t,r,e) \notin \mathcal{A}}} \mathbb{1}_{\mathcal{H}}\{(t, e)\} c_{t,r}\right. \\ &\quad \left. + \sum_{j \in \mathcal{J}} \mathbb{1}_{\mathcal{H}}\{(j, e)\} d_j\right\} \end{aligned} \quad (40a)$$

$$\text{Rn}\{\mathbf{U}_{t,r} \mathbf{H}_{t,r} \mathbf{V}_{t,r}\} = c_{t,r} \quad (40b)$$

almost surely. From (10b) and (40a), (8b) holds. From (40b), (8c) holds. From (39a), (8d) holds. From (39d) and (39e), (8e) holds. This completes the proof of statement (iii).

APPENDIX III PROOF OF THEOREM 4.3

The first statement of the theorem can be directly obtained from [39, Thm. 2.3], i.e., f_p , $p \in \mathcal{P}$ are algebraically dependent if and only if $\text{Rn}\{\mathbf{J}_x(\mathbf{f})\} < L$. When $\mathbf{J}_x(\mathbf{f})$ is rank deficient, there exists a vector $\mathbf{c} \in \mathcal{F}^{1 \times L} \neq \mathbf{0}$ such that

$$\mathbf{c}\mathbf{J}_x(\mathbf{f}) \equiv \mathbf{0}. \quad (41)$$

The second statement of the theorem is equivalent to: if f_p , $p \in \mathcal{P}$ are dependent, $\mathbf{J}_x(\mathbf{f})|_{\mathbf{x}=\boldsymbol{\alpha}}$ is rank-deficient for all $\boldsymbol{\alpha} \in \mathcal{F}^S$. This is a direct consequence of (41).

Now turn to the third statement of the theorem. Denote the $L \times L$ sub-matrices of $\mathbf{J}_x(\mathbf{f})$ as $\tilde{\mathbf{J}}_i$, $i \in \{1, 2, \dots, M\}$, where M is the binomial coefficient of S -choose- L . Denote $p_i(\mathbf{x}) = \det\{\tilde{\mathbf{J}}_i\}$. From the Leibniz formula [40, Section 6.1.1], p_i are polynomials in variables \mathbf{x} . Then the set of $\boldsymbol{\alpha}$ on which $\mathbf{J}_x(\mathbf{f})|_{\mathbf{x}=\boldsymbol{\alpha}}$ is full row-rank is given by

$$\begin{aligned} \mathcal{M} &= \{\boldsymbol{\alpha} : \text{Rn}\{\mathbf{J}_x(\mathbf{f})|_{\mathbf{x}=\boldsymbol{\alpha}}\} = P\} \\ &= \cup_{i=1}^M \{\boldsymbol{\alpha} : p_i(\boldsymbol{\alpha}) \neq 0\}. \end{aligned} \quad (42)$$

When $\text{Rn}\{\mathbf{J}_x(\mathbf{f})\} = P$, there exists at least one p_i such that $p_i(\mathbf{x}) \neq 0$. Denote $\mathcal{I} = \{i : p_i(\mathbf{x}) \neq 0\}$. Then (42) can be written as $\mathcal{M} = \cup_{i \in \mathcal{I}} \{\boldsymbol{\alpha} : p_i(\boldsymbol{\alpha}) \neq 0\}$.

If $\boldsymbol{\alpha} \notin \mathcal{M}$, then $p_i(\boldsymbol{\alpha}) = 0$, $\forall i \in \mathcal{I}$. Without loss of generality, assume that $1 \in \mathcal{I}$. Since $p_1 \neq 0$, there exists $\check{\boldsymbol{\alpha}}$ such that $p_1(\check{\boldsymbol{\alpha}}) \neq 0$. Define $\check{p}_1(t) = p_1(\boldsymbol{\alpha} - t(\boldsymbol{\alpha} - \check{\boldsymbol{\alpha}}))$, then $\check{p}_1(t)$ is a non-constant polynomial of t . From the Fundamental Theorem of Algebra [41], $\check{p}_1(t) = 0$ has only a finite number of solutions in \mathcal{F} . Hence, one can easily construct a sequence t_n such that $\lim_{n \rightarrow \infty} t_n = 0$ and $\check{p}_1(t_n) \neq 0$. Denote $\boldsymbol{\alpha}_n = \boldsymbol{\alpha} - t_n(\boldsymbol{\alpha} - \check{\boldsymbol{\alpha}})$. Then $\boldsymbol{\alpha} \in \mathcal{S}$ and $\lim_{n \rightarrow \infty} \boldsymbol{\alpha}_n = \boldsymbol{\alpha}$. This shows that \mathcal{M} is dense.

If $\boldsymbol{\alpha} \in \mathcal{M}$, then there exists i such that $p_i(\boldsymbol{\alpha}) \neq 0$. Since p_i is continuous, there exists some $\epsilon > 0$ such that $p_i(\check{\boldsymbol{\alpha}}) \neq 0$, $\forall |\check{\boldsymbol{\alpha}} - \boldsymbol{\alpha}| < \epsilon$. This shows that \mathcal{M} is open, and this completes the proof.

APPENDIX IV PROOF OF THEOREM 4.4

We first prove that $\mathbf{J}_x(\mathbf{f})$ is full row-rank if $\{\check{f}_p\}$ are linearly independent. Denote

$$\begin{aligned} \check{\mathbf{f}} &= (\check{f}_1, \check{f}_2, \dots, \check{f}_P) \\ \mathbf{b}_p &= [b_{p,1} \quad b_{p,2} \quad \dots \quad b_{p,q}]^T \text{ and} \\ \mathbf{B} &= [\mathbf{b}_1 \quad \mathbf{b}_2 \quad \dots \quad \mathbf{b}_P]^T. \end{aligned}$$

When $\{\check{f}_p\}$ are linearly independent, so are $\{\mathbf{b}_p\}$, $p \in \mathcal{P}$, i.e., $\text{Rn}\{\mathbf{B}\} = P$. On the other hand, noting that $\frac{\partial \check{f}_p}{\partial x_q} = \frac{\partial f_p}{\partial x_q}$ when $x_q = 0$, $\forall p, q$, we have $\text{Rn}\{\mathbf{J}_x(\mathbf{f})|_{\mathbf{x}=\mathbf{0}}\} = \text{Rn}\{\mathbf{B}\} = P$. From this equation and Theorem 4.3, $\mathbf{J}_x(\mathbf{f})$ is full row-rank.

We then prove the second statement of the theorem. First consider the case with $S = P$. Since $\frac{\partial \check{f}_p(\mathbf{x})}{\partial x_q} = b_{p,q}$, from the

Leibniz formula [40, 6.1.1], the determinant of $\mathbf{J}_x(\check{\mathbf{f}})$ can be written as a polynomial function of $\{b_{p,q}\}$, i.e.,

$$\det\{\mathbf{J}_x(\check{\mathbf{f}})\} = p(b_{1,1}, b_{1,2}, \dots, b_{Q,Q}). \quad (43)$$

Similarly, $\det\{\mathbf{J}_x(\mathbf{f})\} = p(g_{1,1}(\mathbf{x}), g_{1,2}(\mathbf{x}), \dots, g_{Q,Q}(\mathbf{x}))$. When $\{f_p\}$ are algebraically independent, $\det\{\mathbf{J}_x(\mathbf{f})\}$ must not be vanishing, i.e., $p(g_{1,1}(\mathbf{x}), g_{1,2}(\mathbf{x}), \dots, g_{Q,Q}(\mathbf{x})) \neq 0$ [39, Thm. 2.2]. Therefore, p must be a non-zero polynomial after removing terms with $g_{p,q}(\mathbf{x}) \equiv 0$ and combining terms with $g_{p,q}(\mathbf{x}) \equiv g_{\check{p},\check{q}}(\mathbf{x})$. Hence, when (15) holds, p is also a non-zero polynomial after removing terms with $b_{p,q} = 0$ and combining terms with $b_{p,q} = b_{\check{p},\check{q}}$. By substituting this result in (43), we obtain that with the randomness of $\{b_{p,q}\}$, $\det\{\mathbf{J}_x(\check{\mathbf{f}})\} \neq 0$ almost surely. This shows that $\{\check{f}_p(\mathbf{x})\}$ are linearly independent almost surely. When $S > L$, one can prove the second statement by repeating the above analysis for each $L \times L$ sub-matrix of $\mathbf{J}_x(\check{\mathbf{f}})$ and $\mathbf{J}_x(\mathbf{f})$.

REFERENCES

- [1] 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, 2008.
- [2] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.
- [3] A. Rabbachin, A. Conti, and M. Z. Win, "Wireless network intrinsic secrecy," *IEEE/ACM Trans. Netw.*, vol. 23, no. 1, pp. 56 – 69, Feb. 2015.
- [4] M. Z. Win, L. Ruan, A. Rabbachin, Y. Shen, and A. Conti, "Multi-tier network secrecy in the ether," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 28–32, Jun. 2015.
- [5] L. Wang, K. K. Wong, M. ElKashlan, A. Nallanathan, and S. Lambotharan, "Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: A new look at interference," *IEEE J. Sel. Areas Commun.*, vol. 10, no. 8, pp. 1375–1389, Dec. 2016.
- [6] R. J. McEliece and W. E. Stark, "Channels with block interference," *IEEE Trans. Inf. Theory*, vol. IT-30, pp. 44–53, Jan. 1984.
- [7] M. Chiani, A. Conti, and O. Andrisano, "Outage evaluation for slow frequency-hopping mobile radio systems," *IEEE Trans. Commun.*, vol. 47, no. 12, pp. 1865–1874, Dec. 1999.
- [8] M. Z. Win, P. C. Pinto, A. Giorgetti, M. Chiani, and L. A. Shepp, "Error performance of ultrawideband systems in a Poisson field of narrowband interferers," in *Proc. IEEE Int. Symp. on Spread Spectrum Tech. & Applicat.*, Manaus, Brazil, Aug. 2006, pp. 410–416.
- [9] M. Z. Win, "A mathematical model for network interference," *IEEE Communication Theory Workshop*, Sedona, AZ, May 2007.
- [10] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its applications," *Proc. IEEE*, vol. 97, no. 2, pp. 205–230, Feb. 2009, special issue on *Ultra-Wide Bandwidth (UWB) Technology & Emerging Applications*.
- [11] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless network," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.
- [12] K. S. Ali, H. ElSawy, M. Haenggi, and M. S. Alouini, "The effect of spatial interference correlation and jamming on secrecy in cellular networks," *IEEE Wireless Communications Letters*, vol. 6, no. 4, pp. 530–533, Aug 2017.
- [13] H. ElSawy, A. Sultan-Salem, M.-S. Alouini, and M. Z. Win, "Modeling and analysis of cellular networks using stochastic geometry: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 167–203, First Quarter 2017.
- [14] A. Conti, B. M. Masini, F. Zabini, and O. Andrisano, "On the down-link performance of multi-carrier CDMA systems with partial equalization," *IEEE Trans. Wireless Commun.*, vol. 6, no. 1, pp. 230–239, Jan. 2007.
- [15] L. H. Afify, H. ElSawy, T. Y. Al-Naffouri, and M. S. Alouini, "A unified stochastic geometry model for MIMO cellular networks with retransmissions," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8595–8609, Dec 2016.

- [16] A. Rabbachin, T. Q. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 480–493, Feb. 2011.
- [17] A. Conti, D. Dardari, G. Pasolini, and O. Andrisano, "Bluetooth and IEEE 802.11b coexistence: Analytical performance evaluation in fading channels," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 2, pp. 259–269, Feb. 2003.
- [18] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Fourth Quarter 2015.
- [19] H. Dhillon, R. Ganti, F. Baccelli, and J. Andrews, "Modeling and analysis of K-Tier downlink heterogeneous cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 550–560, April 2012.
- [20] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [21] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3085–3096, Apr. 2016.
- [22] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.
- [23] H. M. Wang, C. Wang, D. W. K. Ng, M. H. Lee, and J. Xiao, "Artificial noise assisted secure transmission for distributed antenna systems," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4050–4064, Aug. 2016.
- [24] D. W. K. Ng, Y. Wu, and R. Schober, "Power efficient resource allocation for full-duplex radio distributed antenna networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2896–2911, April 2016.
- [25] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
- [26] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [27] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
- [28] O. Koyluoglu, H. El Gamal, L. Lai, and H. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.
- [29] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, Mar. 2012.
- [30] D. Ng, E. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.
- [31] S. H. Lee, W. Zhao, and A. Khisti, "Secure degrees of freedom of the Gaussian diamond-wiretap channel," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 496–508, Jan. 2017.
- [32] L. Ruan, V. K. Lau, and M. Z. Win, "The feasibility conditions for interference alignment in MIMO networks," *IEEE Trans. Signal Process.*, vol. 61, no. 8, pp. 2066–2077, Apr. 2013.
- [33] —, "Generalized interference alignment – Part I: Theoretical framework," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2675–2687, May 2016.
- [34] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
- [35] 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.
- [36] W. Zeng, C. Xiao, J. Lu, and K. B. Letaief, "Globally optimal precoder design with finite-alphabet inputs for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1861–1874, November 2012.
- [37] Y. Wu, C. Xiao, X. Gao, J. D. Matyjas, and Z. Ding, "Linear precoder design for MIMO interference channels with finite-alphabet signaling," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3766–3780, September 2013.
- [38] L. Ruan, V. K. Lau, and M. Z. Win, "Generalized interference alignment – Part II: Application to wireless secrecy," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2688–2701, May 2016.
- [39] R. Ehrenborg and G.-C. Rota, "Apolarity and canonical forms for homogeneous polynomials," *European Journal of Combinatorics*, vol. 14, no. 3, pp. 157–181, May 1993.
- [40] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*, 1st ed. SIAM, 2000.
- [41] B. Fine and G. Rosenberger, *The Fundamental Theorem of Algebra*. New York, NY, USA: Springer, 1997.



Liangzhong Ruan (S'10-M'14) received the Ph.D. degree in electrical engineering and computer science from the Hong Kong University of Science and Technology (HKUST), Clear Water Bay, in 2013, and the B.Eng. degree in electrical engineering from Tsinghua University, Beijing, China, in 2007.

From 2012 to 2013, he was with the Laboratory for Information & Decision Systems (LIDS), Massachusetts Institute of Technology (MIT), Cambridge, USA, as a visiting graduate student. He is currently a postdoctoral associate at the Wireless Information and Network Sciences Laboratory, MIT. His research interests include interference management, intrinsic wireless secrecy, and quantum entanglement distillation.

Dr. Ruan has served as an area chair for EUSIPCO'16, a session chair for IEEE Globecom'11, and TPC members for IEEE Globecom'15 and VTC'15. He also serves as reviewers for multiple transactions, including IEEE Journal on Selected Areas in Communications, IEEE Transactions on Signal Processing, and IEEE Transactions on Wireless Communications.



Andrea Conti (S'99-M'01-SM'11) received the Laurea (*summa cum laude*) in telecommunications engineering and the Ph.D. in electronic engineering and computer science from the University of Bologna, Italy, in 1997 and 2001, respectively.

He is an Associate Professor at the University of Ferrara, Italy. His research interests involve theory and experimentation of wireless systems and networks including network localization, distributed sensing, adaptive diversity communications, and network secrecy. He is recipient of the HTE Puskás

Tivadar Medal and co-recipient of the IEEE Communications Society's Stephen O. Rice Prize in the field of Communications Theory and of the IEEE Communications Society's Fred W. Ellersick Prize.

Dr. Conti has served as editor for IEEE journals, as well as chaired international conferences. He has been elected Chair of the IEEE Communications Society's Radio Communications Technical Committee. He is a co-founder and elected Secretary of the IEEE Quantum Communications & Information Technology Emerging Technical Subcommittee. He is an elected Fellow of the IET and has been selected as an IEEE Distinguished Lecturer.



Moe Z. Win (S'85-M'87-SM'97-F'04) is a professor at the Massachusetts Institute of Technology (MIT) and the founding director of the Wireless Information and Network Sciences Laboratory. Prior to joining MIT, he was with AT&T Research Laboratories and NASA Jet Propulsion Laboratory.

His research encompasses fundamental theories, algorithm design, and network experimentation for a broad range of real-world problems. His current research topics include network localization and navigation, network interference exploitation, and quantum information science. He has served the IEEE Communications Society as an elected Member-at-Large on the Board of Governors, as elected Chair of the Radio Communications Committee, and as an IEEE Distinguished Lecturer. Over the last two decades, he held various Editorial posts for IEEE journals and organized numerous international conferences. Currently, he is serving on the SIAM Diversity Advisory Committee.

Dr. Win is an elected Fellow of the AAAS, the IEEE, and the IET. He was honored with two IEEE Technical Field Awards: the IEEE Kiyo Tomiyasu Award (2011) and the IEEE Eric E. Sumner Award (2006, jointly with R. A. Scholtz). Other recognitions include the IEEE Communications Society Edwin H. Armstrong Achievement Award (2016), the International Prize for Communications Cristoforo Colombo (2013), the Copernicus Fellowship (2011) and the *Laurea Honoris Causa* (2008) from the University of Ferrara, and the U.S. Presidential Early Career Award for Scientists and Engineers (2004). He is an ISI Highly Cited Researcher.