On Cooperative and Malicious Behaviors in Multirelay Fading Channels

Meng-Hsi Chen, Shih-Chun Lin, *Member, IEEE*, Y.-W. Peter Hong, *Member, IEEE*, and Xiangyun Zhou, *Member, IEEE*

***Abstract*—Multirelay networks exploit spatial diversity by transmitting user's messages through multiple relay paths. Most works in the literature on cooperative or relay networks assume that all terminals are fully cooperative and neglect the effect of possibly existing malicious relay behaviors. In this work, we consider a multirelay network that consists of both cooperative and malicious relays, and aims to obtain an improved understanding on the optimal behaviors of these two groups of relays via information-theoretic mutual information games. By modeling the set of cooperative relays and the set of malicious relays as two players in a zero-sum game with the maximum achievable rate as the utility, the optimal transmission strategies of both types of relays are derived by identifying the Nash equilibrium of the proposed game. Our main contributions are twofold. First, a generalization to previous works is obtained by allowing malicious relays to either listen or attack in Phase 1 (source-relay transmission phase). This is in contrast to previous works that only allow the malicious relays to listen in Phase 1 and to attack in Phase 2 (relay-destination transmission phase). The latter is shown to be suboptimal in our problem. Second, the impact of CSI knowledge at the destination on the optimal attack strategy that can be adopted by the malicious relays is identified. In particular, for the more practical scenario where the interrelay CSI is unknown at the destination, the constant attack is shown to be optimal as opposed to the commonly considered Gaussian attack.**

***Index Terms*—Cooperative communications, malicious relay, jamming, CSI, game theory, mutual information.**

I. Introduction

COOPERATIVE or relay communications [1]–[5] allow users in a wireless system to transmit their messages through the relaying of multiple cooperative partners or relay stations. The relay paths provide spatial diversity that can be exploited to enhance communication reliability and throughput. In the literature, many relaying strategies [2]–[5], such as decode-and-forward, amplify-and-forward (AF), selective relaying etc., have been proposed to achieve this task. Yet, most of these strategies are proposed based on the assumption that all relays in the network are trustworthy and are fully compliant with the cooperation rules. However, this may not be the case in practice and the existence of malicious relays may significantly degrade the system performance, especially if the cooperative relays are not capable of countering the malicious behaviors. The goal of this work is to investigate the interaction between cooperative and malicious relays and examine its impact on the system performance.

Let us consider a multirelay network that consists of a source, a destination, and multiple relays, including some that are possibly malicious. A two-phase AF relay protocol is employed, where the relays first receive signals from the source in Phase 1 and then forward amplified versions of these signals to the destination in Phase 2 [6]. Here, malicious relays may utilize shared network information to intentionally jam the reception at the receivers or alter the messages that are to be forwarded. Therefore, the source and the cooperative relays must design their transmission strategies to reduce the impact of these malicious behaviors. The main objective of this work is to determine the optimal signaling at the source, the cooperative relays, and the malicious relays. Following the approaches adopted in [6]–[11], we use the two-player zero-sum game [12] to model this fundamental problem. Here, the source and the set of cooperative relays are viewed collectively as one player and the set of malicious relays as the other player. The maximum achievable rate (i.e., the mutual information between source and destination) is chosen as the utility measure. The optimal transmission strategies of different types of relays are derived by identifying the Nash equilibrium (NE) of the proposed game. The strategies are optimal in the sense that no single player can do better by unilaterally altering its own strategy. Compared with [6]–[11], this work provides a better understanding of the optimal signaling of both players in a more general and practical setting. Note that the malicious relays considered in this work are those that purposely disrupt the communication between the source and the destination. Therefore, they are assumed to be rational and seek the best strategy to deteriorate the communication performance. This is different from studies on *faulty* relays [13], where the relay behaviors may be incidental and are often irrational.

The main contributions of this work can be summarized as follows. First, this work considers a more general set of attack strategies where the malicious relays are given the freedom of choosing to either listen to the source in Phase 1 (so that it can

Manuscript received November 08, 2012; revised April 02, 2013; accepted May 01, 2013. Date of publication May 14, 2013; date of current version May 31, 2013. This work was supported in part by the National Science Council, Taiwan, under Grant NSC 100-2628-E-007-025-MY3 and Grant 101-2221-E-011-170-MY3. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wade Trappe.

M.-H. Chen and Y.-W. P. Hong are with the Institute of Communications Engineering and Department of Electrical Engineering, National Tsing Hua University, Hsinchu 30013, Taiwan (e-mail: mhchen@erdos.ee.nthu.edu.tw; ywhong@ee.nthu.edu.tw).

S.-C. Lin is with the Department of Electronic and Computer Engineering, National Taiwan University of Science and Technology, Taipei 10607, Taiwan (e-mail: sclin@mail.ntust.edu.tw).

X. Zhou is with the College of Engineering and Computer Science, The Australian National University, Canberra 0200 ACT, Australia (e-mail: xiangyun.zhou@anu.edu.au).

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/TIFS.2013.2262941

utilize this information to transmit interfering signals in Phase 2) or to directly emit jamming signals (that are independent of the source message) in both phases. This set of attack strategies generalizes that in [7], where malicious relays were only allowed to listen in Phase 1 and attack in Phase 2. Our results show that the optimal strategy taken by the malicious relays should be to jam rather than to listen in Phase 1 and, thus, the malicious attacks considered in [7] were indeed suboptimal. Secondly, the optimal attack strategy taken by the malicious relays are shown to depend on the CSI knowledge at the destination. Specifically, when full CSI is available at the destination (as assumed in [6]–[10]), we show that the optimal attack strategy that can be taken by malicious relays is to emit Gaussian jamming signals in both phases. However, for the more practical scenario where the interrelay CSI (i.e., CSI of the channel between the malicious and the cooperative relays) is assumed to be unknown at the destination, we show that the malicious relays should attack with constant jamming signals in Phase 1 and with Gaussian jamming signals in Phase 2. This result is different from the common wisdom derived under the assumption of full CSI at the destination [6]–[10].

Theoretical studies on jammer or malicious relay behaviors have been considered in [6]–[11], [14], [15]. In [7], an AF relay network with one single-antenna cooperative relay and one single-antenna jammer (i.e., malicious relay) is examined. Our work can be viewed as a generalization of [7] to the case with multiple relays and more general attacking strategy. In [8] and our previous work in [9], the interaction between cooperative and malicious relays is examined for decode-and-forward (DF) networks. For DF networks, the source codebook is revealed to the relays and each relay is assumed to be able to successfully decode the source message. The problem in AF networks, as considered here, differs considerably since one must now take into account the forwarding of noise (and possibly also jamming signals) in Phase 2. The effect of malicious relays or jammers has also been examined in the context of multiple access channels in [6], [10], and in the context of secrecy channels with eavesdroppers in [14]–[17]. Note that, in contrast to the malicious relays (or jammers) considered in our work, the relays and jammers considered in [16] and [17] are friendly and work cooperatively to prevent eavesdropping by unauthorized receivers. More recently, the zero-sum game approach has also been applied to study jamming attacks in parallel slow fading channels in [11] and has also been applied to the study of multimedia security problems in [18]. These works have different considerations and, thus, are less relevant to ours. In the literature, several works on malicious relays have also been conducted using nongame-theoretic approaches, e.g., in [19]–[22]. However, in these works, cooperative relay strategies were derived to counter only limited types of malicious attacks and, thus, may not be effective if the malicious relays decide to alter their attack strategy. Our work considers more general sets of cooperative and malicious relay strategies and the proposed solutions are optimal in the sense that no player can gain by unilaterally altering its own strategy.

The rest of this paper is organized as follows. In Section II, we describe the system model for AF networks with malicious relays. In Section III, we show how our problem can be formulated into a zero-sum game and derive the optimal transmission strategies for the cases with and without interrelay CSI at the destination in Section IVSections and Section V, respectively. Computer simulations are given in Section VI and the paper is concluded in Section VII.

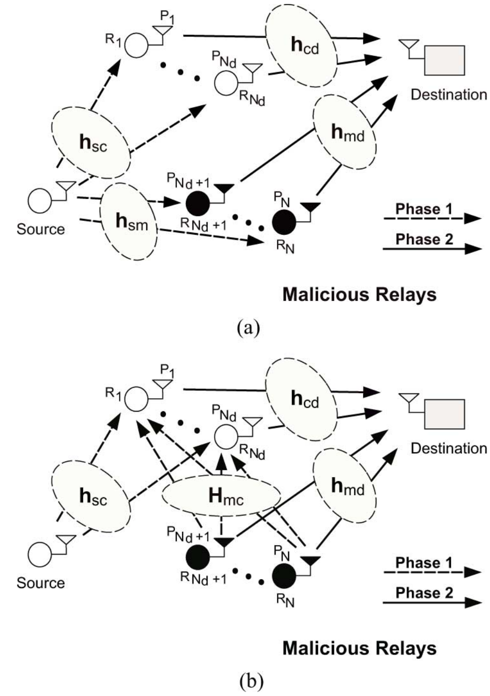


Fig. 1. Cooperative network model with malicious relays. (a) Malicious relays listen in Phase 1 and attack in Phase 2. (b) Malicious relays attack in both Phases 1 and 2.

Notations: $\mathcal{CN}(0,\Sigma)$ denotes the distribution of a complex Gaussian random variable with zero mean and covariance matrix Σ. $\mathrm{Exp}(1/\lambda)$ denotes the distribution of an exponential random variable with mean $1/\lambda$. $\mathbf{E}[\cdot]$ stands for the statistical expectation of a random variable, and $I(\cdot;\cdot)$ stands for the mutual information between two random variables (vectors). A diagonal matrix with elements $x_1,\ldots,x_n$ on its diagonal is denoted by $\mathrm{diag}(x_1,\ldots,x_n)$. Function $C(x)=\log(1+x)$.

II. System Model

Consider an AF multirelay network with a source, a destination, and N relays (among which N_c are cooperative and $N-N_c$ are malicious), as shown in Fig. 1. The cooperative relays are denoted by $R_1,\ldots,R_{N_c}$ and the malicious relays are denoted by $R_{N_c+1},\ldots,R_N$. Each node is equipped with a single antenna and are assumed to be half-duplex. The relays are subject to individual power constraints given by $P_1,\ldots,P_N$, where P_i is the power constraint at relay R_i. A two-phase AF transmission protocol is considered where the (cooperative) relays first receive signals from the source in Phase 1 and forward amplified versions of the received signal to the destination in Phase 2. The malicious relays, on the other hand, may choose to either listen to the source in Phase 1 and utilize this information to emit interfering signals in Phase 2 (as shown in Fig. 1(a)) or emit jamming signals in both phases (as shown in Fig. 1(b)). Our scenario is based on the setting where the cooperative relay selection process has been done and all relays, which agree to be cooperative, can be trusted by the source. In this case, the source and the cooperative relays have a common objective to increase the system throughput. The malicious relays, on the other hand, are adversaries that aim to disrupt the communication between the source and the destination. This setting is consistent with the line of works given in [6]–[10] as well as related works on physical-layer security given in [23], [24].

Let r_i be the signal received by relay R_i in Phase 1. The signal received by the N_c cooperative relays are denoted by the vector $\mathbf{r}_c = [r_1, \ldots, r_{N_c}]^T$ and that by the malicious relays are denoted by $\mathbf{r}_m = [r_{N_c-1}, \ldots, r_N]^T$. These signals depend on the transmission strategy that the malicious relays choose to employ. If the malicious relays choose to *listen* in Phase 1, the received signals can be expressed as

$$\mathbf{r}_c = \mathbf{h}_{sc} s + \mathbf{z}_c, \tag{1}$$

$$\mathbf{r}_m = \mathbf{h}_{sm} s + \mathbf{z}_m, \tag{2}$$

where s with variance $\sigma_s^2 = \mathbf{E}[|s|^2] \leq P_s$ is the signal transmitted by the source and $\mathbf{z}_c \sim \mathcal{CN}(0, \sigma_{\mathbf{z}_c}^2 \mathbf{I})$ and $\mathbf{z}_m \sim \mathcal{CN}(0, \sigma_{\mathbf{z}_m}^2 \mathbf{I})$ are the Gaussian noise vectors at the cooperative and the malicious relays, respectively. Here, $\mathbf{h}_{sc} = [h_{s,1}, \ldots, h_{s,N_c}]^T$ is the channel vector from the source to the cooperative relays and $\mathbf{h}_{sm} = [h_{s,N_c+1}, \ldots, h_{s,N}]$ is that from the source to the malicious relays, where $h_{s,i}$ is the channel between the source and relay R_i. On the other hand, if the malicious relays decide to *attack* in Phase 1, the signals received at the cooperative relays become

$$\mathbf{r}_c = \mathbf{h}_{sc} s + \mathbf{H}_{mc} \mathbf{x}_m^{(1)} + \mathbf{z}_c, \tag{3}$$

where $\mathbf{H}_{mc}$ is the $N_c \times (N - N_c)$ channel matrix between the cooperative and the malicious relays with $\{\mathbf{H}_{mc}\}_{ij} = h_{N_c+j,i}$ being the channel from R_j to R_i, and $\mathbf{x}_m^{(1)} = [x_{N_c+1}^{(1)}, \ldots, x_N^{(1)}]^T$ is the vector of jamming signals emitted by the malicious relays in Phase 1. In this case, we set $\mathbf{r}_m = 0$ since, under the half-duplex constraint, the malicious relays cannot receive when it is transmitting.

In Phase 2, the cooperative and the malicious relays will simultaneously transmit signals $\mathbf{x}_c = [x_1, \ldots, x_{N_c}]^T$ and $\mathbf{x}_m^{(2)} = [x_{N_c+1}^{(2)}, \ldots, x_N^{(2)}]^T$, respectively, to the destination, where x_i is the signal transmitted by cooperative relay R_i and $x_j^{(2)}$ is the signal transmitted by malicious relay R_j in Phase 2. The received signal at the destination is

$$y_d = \mathbf{h}_{cd}^\dagger \mathbf{x}_c + \mathbf{h}_{md}^\dagger \mathbf{x}_m^{(2)} + z_d, \tag{4}$$

where $\mathbf{h}_{cd} = [h_{1,d}, \ldots, h_{N_c,d}]^T$ is the channel vector from the cooperative relays to the destination, $\mathbf{h}_{md} = [h_{N_c+1,d}, \ldots, h_{N,d}]^T$ is the channel vector from the malicious relays to the destination, and $z_d \sim \mathcal{CN}(0, \sigma_{z_d}^2)$ is the Gaussian noise at the destination. Here, $h_{i,d}$ is the channel between relay R_i and the destination.

By employing the AF relaying strategy [25], [26], the signal transmitted by the cooperative relays can be expressed as

$$\mathbf{x}_c = \mathbf{\Gamma}_c \mathbf{r}_c, \tag{5}$$

where $\mathbf{\Gamma}_c = \mathrm{diag}(\gamma_1, \ldots, \gamma_{N_c})$ with γ_i being the amplifying gain at relay R_i. To satisfy the power constraints at each relay, the amplifying gain at cooperative relay R_i, for $i \in \{1, \ldots, N_c\}$, must be chosen such that

$$\gamma_i = \frac{\ell_i}{\sqrt{\mathbf{E}[|r_i|^2]}} = \frac{\ell_i}{\sqrt{\sigma_{sc}^2 \sigma_s^2 + \sigma_{\mathbf{z}_c}^2 + \sigma_{mc}^2 \sum_{j=N_c+1}^{N} \mathbf{E}[|x_j^{(1)}|^2]}} \tag{6}$$

with ℓ_i satisfying the constraint $|\ell_i|^2 \leq P_i$. Here, ℓ_i is referred to as the *normalized amplifying gain*. In this case, the AF matrix can be expressed as

$$\mathbf{\Gamma}_c = \mathbf{L}_c \mathbf{D}_c, \tag{7}$$

where $\mathbf{L}_c = \mathrm{diag}(\ell_1, \ldots, \ell_{N_c})$ and $\mathbf{D}_c = \mathrm{diag}(\mathbf{E}[|r_1|^2]^{-1/2}, \ldots, \mathbf{E}[|r_{N_c}|^2]^{-1/2})$. On the other hand, the signals transmitted by the malicious relays, i.e., $\mathbf{x}_m^{(1)}$ and $\mathbf{x}_m^{(2)}$, can be chosen arbitrarily. However, if the malicious relays choose to listen in Phase 1 instead of attacking, the signal $\mathbf{x}_m^{(2)}$ may in general depend on the realization of $\mathbf{r}_m$. The signals transmitted by malicious relay R_i (i.e., for $i \in \{N_c + 1, \ldots, N\}$) in Phases 1 and 2 must satisfy the power constraints $\mathbf{E}[|x_i^{(1)}|^2] \leq \alpha_i P_i$ and $\mathbf{E}[|x_i^{(2)}|^2] \leq (1 - \alpha_i) P_i$, respectively, where α_i and $1 - \alpha_i$ are the fractions of power that relay R_i allocates to its transmission in Phases 1 and 2, respectively.

All channels are assumed to be fast Rayleigh faded with the entries of each vector (or matrix) $\mathbf{h}_{cd}$, $\mathbf{h}_{md}$, $\mathbf{h}_{sc}$, $\mathbf{h}_{sm}$, and $\mathbf{H}_{mc}$ being independent and identically distributed (i.i.d.) circularly-symmetric complex Gaussian random variables with zero mean and variances σ_{cd}^2, σ_{md}^2, σ_{sc}^2, σ_{sm}^2, and σ_{mc}^2, respectively. The optimal transmission strategies are derived under two scenarios: the scenario where full CSI (including the interrelay channel matrix $\mathbf{H}_{mc}$) is available at the destination and the more practical scenario where only the source-to-relay and the relay-to-destination channels, i.e., $\mathbf{h}_{sc}$, $\mathbf{h}_{sm}$, $\mathbf{h}_{cd}$, and $\mathbf{h}_{md}$, are known at the destination. Note that in practice, the transmitter-side CSI is usually obtained using feedback from the destination. When the wireless channel undergoes fast fading, it is very difficult or sometimes impossible for the transmitters (i.e., the source for the source-relay link, or the relay for the relay-destination link, etc.) to obtain accurate CSI due to the delay in the CSI feedback. Thus for both scenarios considered in this paper (destination knows $\mathbf{H}_{mc}$ or not), the source and all relays are assumed to know only the distributions of the channels.

III. Game-Theoretic Formulation

In this section, the interaction between cooperative and malicious relays is modeled as a two-player zero-sum game, where the goal of the two players are opposite of one another.

Specifically, let us consider a two-player game

$$G_{AF} = ((\mathcal{A}_1, \mathcal{A}_2), (u_1, u_2)), \tag{8}$$

where $\mathcal{A}_1$ and $\mathcal{A}_2$ are the action sets (or the strategy spaces) for Players 1 and 2, and u_1 and u_2 are their corresponding utility functions. Here, u_1 and u_2 are functions of the so-called *action profile* $\mathbf{a} = (a_1, a_2)$, where $a_1 \in \mathcal{A}_1$ and $a_2 \in \mathcal{A}_2$. The cooperative relays and the source are together viewed as Player 1 and the malicious relays are together viewed as Player 2. In this game, both players are aware of each others' action sets and choose actions simultaneously from their respective sets. The destination utilizes all CSI available to decode the source's message. The goal of Player 1 is to maximize the mutual information between the signal transmitted by the source and that received at the destination whereas that of Player 2 is opposite.[1] Specifically, when full CSI is available at the destination, the utility functions u_1 and u_2 in (8) are given by

$$u_1 = -u_2 = I(s; y_d|\mathcal{H}), \tag{9}$$

where $\mathcal{H} \triangleq \{\mathbf{h}_{cd}, \mathbf{h}_{md}, \mathbf{h}_{sc}, \mathbf{h}_{sm}, \mathbf{H}_{mc}\}$. When only the source-to-relay and the relay-to-destination channels are known at the destination, the utility functions are given by

$$u_1 = -u_2 = I(s; y_d|\mathcal{H}'), \tag{10}$$

where $\mathcal{H}' \triangleq \{\mathbf{h}_{cd}, \mathbf{h}_{md}, \mathbf{h}_{sc}, \mathbf{h}_{sm}\}$. With the above choice of utility functions, G_{AF} becomes a zero-sum game [12] in both cases since $u_1 + u_2 = 0$.

Each element in the action set of Player 1, i.e., $\mathcal{A}_1$, is a pair $(f_s, \mathbf{L}_c)$, where f_s is a probability density function (PDF) of the source signal s with $\mathbf{E}[|s|^2] \leq P_s$ and $\mathbf{L}_c$ is a diagonal matrix of normalized amplifying gains with $|\ell_i|^2 \leq P_i$, for $i = 1, \ldots, N_c$.

On the other hand, the action set of Player 2, i.e., the malicious relays, is the union of two action subsets $\mathcal{A}_{2a}$ and $\mathcal{A}_{2l}$, i.e., $\mathcal{A}_2 = \mathcal{A}_{2a} \bigcup \mathcal{A}_{2l}$.

The subset $\mathcal{A}_{2a}$ consists of actions where the malicious relays *attack* by emitting independent jamming signals in both phases. Since the malicious relays do not listen to the source in this case, the jamming signals emitted by the malicious relays in both phases will be independent of the source signal s. When malicious relay R_i allocates α_i fraction of power to the transmission in Phase 1 (and $1 - \alpha_i$ to Phase 2), the action taken by Player 2 can be represented by a pair of PDFs $(f_{\mathbf{x}_m^{(1)}}, f_{\mathbf{x}_m^{(2)}})$ that satisfies the power constraints

$$\int |x|^2 f_{x_i^{(1)}}(x)dx \leq \alpha_i P_i \text{ and } \int |x|^2 f_{x_i^{(2)}}(x)dx \leq (1 - \alpha_i)P_i. \tag{11}$$

The subset of actions that satisfies the above power constraints are denoted by $\mathcal{A}_{2a}^{(\boldsymbol{\alpha})}$, where $\boldsymbol{\alpha} = [\alpha_{N_c+1}, \ldots, \alpha_N]^T$. The action subset $\mathcal{A}_{2a}$ is then defined as the union of $\mathcal{A}_{2a}^{(\boldsymbol{\alpha})}$ over all possible power allocations $\boldsymbol{\alpha}$, i.e., $\mathcal{A}_{2a} = \cup_{\boldsymbol{\alpha}} \mathcal{A}_{2a}^{(\boldsymbol{\alpha})}$.

Moreover, the subset $\mathcal{A}_{2l}$ consists of actions where the malicious relays first *listen* to the source in Phase 1 and then emits jamming signals only in Phase 2. In this case, the signal transmitted by each malicious relay in Phase 2 may possibly depend on its local received signal, i.e., r_i for relay R_i. Therefore, each action in $\mathcal{A}_{2l}$ can be described by a PDF $f_{\mathbf{x}_m^{(2)}}$, where the Markov relation $x_j^{(2)} \leftrightarrow r_j \leftrightarrow s \leftrightarrow r_i \leftrightarrow x_i^{(2)}$ holds for all $i \neq j \in \{N_c + 1, \ldots, N\}$ and

$$\int |x|^2 f_{x_i^{(2)}}(x)dx \leq P_i, \tag{12}$$

for $i = N_c + 1, \ldots, N$. Please note that, in [7], the malicious relays are assumed to always listen in Phase 1 and, thus, only the action subset $\mathcal{A}_{2l}$ was considered for Player 2.

Definition 1 ([12]): The action profile $\mathbf{a}^* = (a_1^*, a_2^*)$ is a Nash Equilibrium (NE) if $u_1(a_1^*, a_2^*) \geq u_1(a_1, a_2^*)$, for any $a_1 \in \mathcal{A}_1$, and $u_2(a_1^*, a_2^*) \geq u_2(a_1^*, a_2)$, for any $a_2 \in \mathcal{A}_2$.

An action profile $\mathbf{a} = (a_1, a_2)$ is a pair of transmission strategies employed by the two players. Definition 1 implies that, by employing strategies corresponding to the NE $\mathbf{a}^*$, no player can increase his/her utility by unilaterally changing his/her own strategy. In fact, the optimality of the NE solution is even stronger in the case of zero-sum games, as given in [12] and stated below.

Theorem 1 ([12]): An action profile $\mathbf{a}^* = (a_1^*, a_2^*)$ is the NE of a zero-sum game if and only if

$$\begin{aligned} \max_{a_1 \in \mathcal{A}_1} \min_{a_2 \in \mathcal{A}_2} u_1(a_1, a_2) &= u_1(a_1^*, a_2^*) \\ &= -u_2(a_1^*, a_2^*) = \min_{a_2 \in \mathcal{A}_2} \max_{a_1 \in \mathcal{A}_1} u_1(a_1, a_2). \end{aligned}$$

The above theorem indicates that the NE of a zero-sum game achieves the max–min solution for both players [12]. Hence, the strategies obtained from the NE are optimal in the sense that they are able to maximize the worst case utility of both players. In general, the NE of a game may not be unique. However, since all NEs achieve the max–min utility for both players, that is, for any two NEs $\mathbf{a}^* = (a_1^*, a_2^*)$ and $\mathbf{b}^* = (b_1^*, b_2^*)$, we have $u_1(a_1^*, a_2^*) = u_1(b_1^*, b_2^*)$ (cf. [12, Proposition 22.2b]), all NEs are equally optimal. In the following sections, the NEs (and, thus, the optimal transmission strategies) are derived for cases with and without interrelay CSI.

Remark 1: In this work, the players are assumed to know only the utility functions and the action sets (i.e., the sets of possible actions). The specific actions taken by the players and the channel state information (CSI) are both unknown. Specifically, as in [7]–[10], the utility function is chosen as the mutual information between the source and destination, which is related to the achievable transmission rate between the source and the destination, and is a common objective adopted in many communication systems. Also as in [7]–[10], our action sets are defined as the set of all possible PDFs of transmit signals that satisfy the individual power constraints. These action sets include all possible transmission schemes (or codebooks) [27, p. 184, eq. (7.1)] and, thus, no specific information must be obtained by the players (other than their power constraints) in order to infer knowledge of these action sets. If the power constraints are not completely known, each player can assume larger action sets for the other player by considering upper bounds on their power constraints.

IV. Optimal Transmission Strategies for the Case With Full CSI at the Destination

In this section, we derive the optimal transmission strategies for the case where full CSI is available at the destination. Since Player 2's action set $\mathcal{A}_2$ is the union of two action subsets $\mathcal{A}_{2a}$ and $\mathcal{A}_{2l}$, the optimal transmission strategy for malicious relays is first derived within each action subset and then compared among each other to determine the globally optimal strategy. The following lemmas are first proved and are utilized to find the NE in Theorem 2.

[1]The mutual information between the signal transmitted by the source and that received at the destination is the maximum code rate the source can transmit to ensure successful decoding at the destination. This is a common measure of performance in communication systems and, thus, is adopted as the utility of Player 1 (i.e., the source and the cooperative relays). Player 2 (i.e., the malicious relays) is the adversary that aims to disrupt the communication between the source and the destination and, thus, its utility is opposite, namely, minus the utility of Player 1. Our game formulation falls into the class of mutual information games as studied in [7]–[10], [27] and references within.

Lemma 1: Let $\mathbf{h} = [h_1, \ldots, h_M]^T$ be an $M \times 1$ random vector with independent zero-mean Gaussian entries and let

$$\mathcal{J}(\mathbf{K}) = \mathbf{E}_{\mathbf{h}}\left[C\left(\frac{u}{v + \mathbf{h}^\dagger \mathbf{K}\mathbf{h}}\right)\right] \tag{13}$$

be an objective function with u and v being nonnegative constants, and $\mathbf{K}$ be a positive semidefinite Hermitian matrix.

(a) If the diagonal entries of $\mathbf{K}$ are subject to the constraints $\{\mathbf{K}\}_{ii} = p_i$, for $i = 1, \ldots, M$, then the objective function $\mathcal{J}(\mathbf{K})$ is minimized by choosing $\mathbf{K}$ to be the diagonal matrix $\mathbf{K} = \mathrm{diag}(p_1, \ldots, p_M)$.

(b) If the diagonal entries are subject to the constraints $\{\mathbf{K}\}_{ii} \leq P_i$, for $i = 1, \ldots, M$, the objective function $\mathcal{J}(\mathbf{K})$ is further minimized by choosing $\mathbf{K} = \mathrm{diag}(P_1, \ldots, P_M)$.

The proof of Lemma 1 is given in Appendix A. In the following lemma, we first determine the optimal strategy for Player 2 among the action subset $\mathcal{A}_{2a}^{(\boldsymbol{\alpha})}$ (which includes strategies where malicious relays attack in both phases with power allocation $\boldsymbol{\alpha}$) when Player 1 employs the strategy $(f_s, \mathbf{L}_c)$ with $f_s \sim \mathcal{CN}(0, \sigma_s^2)$ and arbitrary choice of $\mathbf{L}_c$.

Lemma 2: Suppose that the instantaneous CSI $\mathcal{H} = \{\mathbf{h}_{cd}, \mathbf{h}_{md}, \mathbf{h}_{sc}, \mathbf{h}_{sm}, \mathbf{H}_{mc}\}$ is available at the destination and that Player 1 employs the strategy $(f_s, \mathbf{L}_c)$, where $s \sim \mathcal{CN}(0, \sigma_s^2)$ and $\mathbf{L}_c$ is an arbitrary amplifying matrix. The optimal strategy for Player 2 among the action subset $\mathcal{A}_{2a}^{(\boldsymbol{\alpha})}$ is given by $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})})$, where $f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})} \sim \mathcal{CN}(\mathbf{0}, \Sigma_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})})$ with $\Sigma_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})} = \mathrm{diag}(\alpha_{N_c+1}P_{N_c+1}, \ldots, \alpha_N P_N)$ and $f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})} \sim \mathcal{CN}(\mathbf{0}, \Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})})$ with $\Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})} = \mathrm{diag}((1-\alpha_{N_c+1})P_{N_c+1}, \ldots, (1-\alpha_N)P_N)$.

Proof: First, we prove the optimality of choosing both $\mathbf{x}_m^{(1)}$ and $\mathbf{x}_m^{(2)}$ to be Gaussian. Recall from (10) that the utility function u_2 of Player 2 is $-I(s; y_d|\mathcal{H}) = -h(s|\mathcal{H}) + h(s|y_d, \mathcal{H})$. By substituting (3) and (5) into (4), the received signal at the destination can be written as

$$y_d = \mathbf{h}_{cd}^\dagger \boldsymbol{\Gamma}_c \mathbf{h}_{sc} s + \mathbf{h}_{cd}^\dagger \boldsymbol{\Gamma}_c \mathbf{H}_{mc}\mathbf{x}_m^{(1)} + \mathbf{h}_{md}^\dagger \mathbf{x}_m^{(2)} + \mathbf{h}_{cd}^\dagger \boldsymbol{\Gamma}_c \mathbf{z}_c + z_d, \tag{14}$$

where $\boldsymbol{\Gamma}_c = \mathbf{L}_c\mathbf{D}_c$. Recall that $\mathbf{L}_c = \mathrm{diag}(\ell_1, \ldots, \ell_{N_c})$ and $\mathbf{D}_c = \mathrm{diag}(\mathbf{E}[|r_1|^2]^{-1/2}, \ldots, \mathbf{E}[|r_{N_c}|^2]^{-1/2})$, where $\mathbf{E}[|r_i|^2] = \sigma_{sc}^2\sigma_s^2 + \sigma_{\mathbf{z}_c}^2 + \sigma_{mc}^2 \sum_{j=N_c+1}^{N} \mathbf{E}[|x_j^{(1)}|^2]$. Given the strategy of Player 1, only the second term $h(s|y_d, \mathcal{H})$ in the utility of Player 2 is affected by the choice of Player 2's action. To maximize this term, notice that $h(s|y_d, \mathcal{H}) = h(s - ay_d|y_d, \mathcal{H}) \leq h(s - ay_d|\mathcal{H}) \leq \mathbf{E}_{\mathcal{H}}[\log(2\pi e\sigma_e^2)]$, where σ_e^2 is the variance of $s - ay_d$ given $\mathcal{H}$. The two inequalities hold with equality by choosing $a = \mathbf{E}[sy_d^\dagger]/\mathbf{E}[|y_d|^2]$ and by having both $s - ay_d$ and y_d be Gaussian when conditioned on $\mathcal{H}$[27], [28]. From (14), we can see that the latter condition is satisfied by choosing both $\mathbf{x}_m^{(1)}$ and $\mathbf{x}_m^{(2)}$ to be independent zero-mean Gaussian random vector with covariance matrices given by $\Sigma_{\mathbf{x}_m^{(1)}}$ and $\Sigma_{\mathbf{x}_m^{(2)}}$, respectively.

In this case, the utility $-I(s; y_d|\mathcal{H})$ of Player 2 is given by

$$-\mathbf{E}_{\mathcal{H}}\left[C\left(\frac{\sigma_s^2|\mathbf{h}_{cd}^\dagger \mathbf{L}_c\mathbf{D}_c\mathbf{h}_{sc}|^2}{\mathbf{h}_{cd}^\dagger \mathbf{L}_c\mathbf{D}_c\boldsymbol{\Lambda}\mathbf{D}_c^\dagger\mathbf{L}_c^\dagger\mathbf{h}_{cd} + \mathbf{h}_{md}^\dagger\Sigma_{\mathbf{x}_m^{(2)}}\mathbf{h}_{md} + \sigma_{z_d}^2}\right)\right],$$

where $\boldsymbol{\Lambda} = \sigma_{\mathbf{z}_c}^2\mathbf{I} + \mathbf{H}_{mc}\Sigma_{\mathbf{x}_m^{(1)}}\mathbf{H}_{mc}^\dagger$. Let us first compute the optimal covariance matrix of the signal in Phase 2, i.e., $\Sigma_{\mathbf{x}_m^{(2)}}$, for any given covariance matrix in Phase 1, i.e., $\Sigma_{\mathbf{x}_m^{(1)}}$. To do this, we first examine the conditional expectation over $\mathbf{h}_{md}$ given $\mathbf{h}_{cd}$, $\mathbf{h}_{sc}$, and $\mathbf{H}_{mc}$, i.e.,

$$\mathbf{E}_{\mathbf{h}_{md}|\mathbf{h}_{cd},\mathbf{h}_{sc},\mathbf{H}_{mc}}\left[C\left(\frac{u}{v + \mathbf{h}_{md}^\dagger\Sigma_{\mathbf{x}_m^{(2)}}\mathbf{h}_{md}}\right)\right], \tag{15}$$

where $u = \sigma_s^2|\mathbf{h}_{cd}^\dagger\mathbf{L}_c\mathbf{D}_c\mathbf{h}_{sc}|^2 \geq 0$ and $v = \mathbf{h}_{cd}^\dagger\mathbf{L}_c\mathbf{D}_c\boldsymbol{\Lambda}\mathbf{D}_c^\dagger\mathbf{L}_c^\dagger\mathbf{h}_{cd} + \sigma_{z_d}^2 \geq 0$. Notice that u and v can be viewed as constants when given $\mathbf{h}_{cd}$, $\mathbf{h}_{sc}$, $\mathbf{H}_{mc}$ and $\Sigma_{\mathbf{x}_m^{(1)}}$. Therefore, by Lemma 1(b), the optimal choice of $\Sigma_{\mathbf{x}_m^{(2)}}$ under the power constraints in (11) is given by $\Sigma_{\mathbf{x}_m^{(2)}}^* = \mathrm{diag}((1-\alpha_{N_c+1})P_{N_c+1}, \ldots, (1-\alpha_N)P_N)$. Since $\Sigma_{\mathbf{x}_m^{(2)}}^*$ does not depend on $\mathbf{h}_{cd}$, $\mathbf{h}_{sc}$, and $\mathbf{H}_{mc}$, it is also the solution that maximizes the overall utility function of Player 2.

Now, given $\Sigma_{\mathbf{x}_m^{(2)}} = \Sigma_{\mathbf{x}_m^{(2)}}^*$, we can find the optimal value of $\Sigma_{\mathbf{x}_m^{(1)}}$. First, suppose that the diagonal entries of $\Sigma_{\mathbf{x}_m^{(1)}}$ are fixed and are given by $\{\Sigma_{\mathbf{x}_m^{(1)}}\}_{ii} = p_{N_c+i}$, for $i = 1, \ldots, N - N_c$. Notice that, when conditioned on $\mathbf{h}_{md}$, $\mathbf{h}_{cd}$, and $\mathbf{h}_{sc}$, the expectation over $\mathbf{H}_{mc}$ can be written as

$$\mathbf{E}_{\mathbf{H}_{mc}|\mathbf{h}_{md},\mathbf{h}_{cd},\mathbf{h}_{sc}} \times \left[C\left(\frac{u'}{\mathbf{h}_{cd}^\dagger\mathbf{L}_c\mathbf{D}_c\mathbf{H}_{mc}\Sigma_{\mathbf{x}_m^{(1)}}\mathbf{H}_{mc}^\dagger\mathbf{D}_c^\dagger\mathbf{L}_c^\dagger\mathbf{h}_{cd} + v'}\right)\right], \tag{16}$$

where $u' = \sigma_s^2|\mathbf{h}_{cd}^\dagger\mathbf{L}_c\mathbf{D}_c\mathbf{h}_{sc}|^2 \geq 0$ and $v' = \sigma_{\mathbf{z}_c}^2|\mathbf{D}_c^\dagger\mathbf{L}_c^\dagger\mathbf{h}_{cd}|^2 + \mathbf{h}_{md}^\dagger\Sigma_{\mathbf{x}_m^{(2)}}^*\mathbf{h}_{md} + \sigma_{z_d}^2 \geq 0$. Notice that u' and v' can be viewed as constants when given $\mathbf{h}_{md}$, $\mathbf{h}_{cd}$, $\mathbf{h}_{sc}$, $\Sigma_{\mathbf{x}_m^{(2)}}^*$, and the diagonal elements of $\Sigma_{\mathbf{x}_m^{(1)}}$ (since $\mathbf{D}_c$ depends only on the trace of $\Sigma_{\mathbf{x}_m^{(1)}}$). Moreover, in this case, each entry in the vector $\mathbf{H}_{mc}^\dagger\mathbf{D}_c^\dagger\mathbf{L}_c^\dagger\mathbf{h}_{cd}$ is equal to a linear combination of the random variables in the corresponding row of $\mathbf{H}_{mc}^\dagger$. Therefore, the entries will again be independent zero-mean Gaussian random variables. By Lemma 1(a), the optimal choice of $\Sigma_{\mathbf{x}_m^{(1)}}$ will then be diagonal with the i-th diagonal entry being p_{N_c+i}, i.e., $\Sigma_{\mathbf{x}_m^{(1)}} = \mathrm{diag}(p_{N_c+1}, \ldots, p_N)$. By substituting this choice of $\Sigma_{\mathbf{x}_m^{(1)}}$ into the utility function of Player 2, we have

$$\begin{aligned}-I(s; y_d|\mathcal{H}) &= -\mathbf{E}_{\mathcal{H}_d}\left[\mathbf{E}_{\mathcal{H}_c|\mathcal{H}_d}\left[C\left(\frac{\sigma_s^2|\mathbf{h}_{cd}^\dagger\boldsymbol{\Gamma}_c\mathbf{h}_{sc}|^2}{\mathbf{h}_{cd}^\dagger\boldsymbol{\Gamma}_c\boldsymbol{\Lambda}\boldsymbol{\Gamma}_c^\dagger\mathbf{h}_{cd} + \beta}\right)\right]\right]\\ &= -\mathbf{E}_{\mathcal{H}_d}\left[\mathbf{E}_{\mathcal{H}_c|\mathcal{H}_d}\left[C\left(\frac{\sigma_s^2|Z|^2}{\sigma_{\mathbf{z}_c}^2\sum_{i=1}^{N_c}|h_{id}|^2|\gamma_i|^2 + \sum_{k=N_c+1}^{N}p_k|Y_k|^2 + \beta}\right)\right]\right]\end{aligned} \tag{17}$$

where $\mathcal{H}_c = \{\mathbf{h}_{sc}, \mathbf{H}_{mc}\}$, $\mathcal{H}_d = \{\mathbf{h}_{cd}, \mathbf{h}_{md}\}$, $\boldsymbol{\Gamma}_c = \mathbf{L}_c\mathbf{D}_c$, $\beta = \mathbf{h}_{md}^\dagger\Sigma_{\mathbf{x}_m^{(2)}}\mathbf{h}_{md} + \sigma_{z_d}^2$, $Z \triangleq \sum_{i=1}^{N_c} h_{id}^*\gamma_i h_{si}$, and $Y_k \triangleq \sum_{i=1}^{N_c}\gamma_i^* h_{id}h_{ki}$, for $k = N_c+1, \ldots, N$. Notice that, given $\mathbf{h}_{cd}$ and $\mathbf{h}_{md}$, the terms Z and Y_k, for $k = N_c+1, \ldots, N$, are independent zero-mean complex Gaussian random variables with variances $\sigma_Z^2 = \sigma_{sc}^2 \sum_{i=1}^{N_c} |h_{id}|^2|\gamma_i|^2 = \sum_{i=1}^{N_c}(\sigma_{sc}^2|h_{id}|^2|\ell_i|^2)/(\sigma_{sc}^2\sigma_s^2 + \sigma_{\mathbf{z}_c}^2 + \sigma_{mc}^2\sum_{j=N_c+1}^{N} p_j)$ and $\sigma_{Y_k}^2 = \sigma_{mc}^2 \sum_{i=1}^{N_c} |\gamma_i|^2|h_{id}|^2 = \sum_{i=1}^{N_c}(\sigma_{mc}^2|h_{id}|^2|\ell_i|^2)/(\sigma_{sc}^2\sigma_s^2 + \sigma_{\mathbf{z}_c}^2 + \sigma_{mc}^2\sum_{j=N_c+1}^{N} p_j)$, for $k = N_c+1,\ldots,N$. Therefore, the conditional expectation inside (17) can be computed as in (18), shown at the bottom of the page, where $\tilde{Z}$ and $\tilde{Y}_k$, for $k = N_c+1,\ldots,N$, are i.i.d. random variables with distribution $\mathcal{CN}(0,1)$. Note that, for any realization of $\tilde{Z}$ and $\{\tilde{Y}_k\}_{k=N_c+1}^{N}$, the conditional expectation decreases monotonically with each p_i. Hence, under the power constraints $p_i \le \alpha_i P_i$, for $i = N_c+1,\ldots,N$, the optimal choice of $\Sigma_{\mathbf{x}_m^{(1)}}$ that minimizes the conditional expectation above (and, thus, maximizes the utility function in (17)) is given by $\Sigma^*_{\mathbf{x}_m^{(1)}} = \mathrm{diag}(\alpha_{N_c+1}P_{N_c+1},\ldots,\alpha_N P_N)$. ■

The above lemma shows that, given $f_s \sim \mathcal{CN}(0,P_s)$ and arbitrary amplifying matrix $\mathbf{L}_c$, the optimal strategy for Player 2 among the set $\mathcal{A}_{2a}^{(\boldsymbol{\alpha})}$ is to emit Gaussian jamming signals in both phases. This is true for any choice of power allocation $\boldsymbol{\alpha}$. In the following, we further show that the strategy for Player 1 in the form given above is indeed optimal when Player 2 employs the strategy given in Lemma 2. Note that, in the following Lemma, the phase ϕ_i of the ith cooperative relay's transmission signal can be chosen arbitrarily. The intuition behind this result is that since the cooperative relays do not have knowledge of the channel realizations, they cannot adjust the phases of their signals to make them coherently received at the destination.

Lemma 3: Suppose that $\mathcal{H}$ is known at the destination and that Player 2 employs the strategy $(f^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(1)}}, f^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(2)}})$, where $f^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(1)}} \sim \mathcal{CN}(\mathbf{0},\Sigma^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(1)}})$ with $\Sigma^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(1)}} = \mathrm{diag}(\alpha_{N_c+1}P_{N_c+1},\ldots,\alpha_N P_N)$ and $f^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(2)}} \sim \mathcal{CN}(\mathbf{0},\Sigma^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(2)}})$ with $\Sigma^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(2)}} = \mathrm{diag}((1-\alpha_{N_c+1})P_{N_c+1},\ldots,(1-\alpha_N)P_N)$. The optimal strategy for Player 1 is given by $(f_s^*,\mathbf{L}_c^*)$, where $f_s^* \sim \mathcal{CN}(0,P_s)$ and $\mathbf{L}_c^* = \mathrm{diag}\left(\sqrt{P_1}e^{j\phi_1},\ldots,\sqrt{P_{N_c}}e^{j\phi_{N_c}}\right)$ with ϕ_i, for $i = 1,\ldots,N_c$, chosen arbitrarily.

Proof: First, we prove the optimality of choosing $\mathbf{s} \sim \mathcal{CN}(0,P_s)$ when Player 2 employs the strategy $(f^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(1)}}, f^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(2)}})$. Recall from (10) that the utility function u_1 of Player 1 is $I(s;y_d|\mathcal{H}) = h(y_d|\mathcal{H}) - h(y_d|s,\mathcal{H})$, where y_d is given as in (14).

Here, $h(y_d|s,\mathcal{H}) = h(y_d - \mathbf{h}_{cd}^\dagger\boldsymbol{\Gamma}_c\mathbf{h}_{sc}s|s,\mathcal{H}) = h(\mathbf{h}_{cd}^\dagger\boldsymbol{\Gamma}_c\mathbf{H}_{mc}\mathbf{x}_m^{(1)} + \mathbf{h}_{md}^\dagger\mathbf{x}_m^{(2)} + \mathbf{h}_{cd}^\dagger\boldsymbol{\Gamma}_c\mathbf{z}_c + z_d|\mathcal{H})$ is independent of the distribution of s since $\mathbf{x}_m^{(1)}$ and $\mathbf{x}_m^{(2)}$ are independent of s. Therefore, the utility of Player 1 is maximized by maximizing the term $h(y_d|\mathcal{H})$. The optimal choice in this case is $s \sim \mathcal{CN}(0,P_s)$, where P_s is the maximum source power, since all the other terms in (14) are Gaussian when given $\mathcal{H}$ and since $h(y_d|\mathcal{H})$ is monotonically increasing with respect to the variance of s.

Given $\mathbf{x}_m^{(1)} \sim \mathcal{CN}(0,\Sigma^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(1)}})$ and $\mathbf{x}_m^{(2)} \sim \mathcal{CN}(0,\Sigma^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(2)}})$, the utility of Player 1 can be written as

$$I(s;y_d|\mathcal{H}) = \mathbf{E}_{\mathcal{H}_d}\left[\mathbf{E}_{\mathcal{H}_c|\mathcal{H}_d}\left[C\left(\frac{P_s|\mathbf{h}_{cd}^\dagger\boldsymbol{\Gamma}_c\mathbf{h}_{sc}|^2}{\mathbf{h}_{cd}^\dagger\boldsymbol{\Gamma}_c\boldsymbol{\Lambda}\boldsymbol{\Gamma}_c^\dagger\mathbf{h}_{cd}+\beta}\right)\right]\right], \tag{19}$$

where $\mathcal{H}_c = \{\mathbf{h}_{sc},\mathbf{H}_{mc}\}$, $\mathcal{H}_d = \{\mathbf{h}_{cd},\mathbf{h}_{md}\}$, $\boldsymbol{\Lambda} = \sigma_{\mathbf{z}_c}^2\mathbf{I} + \mathbf{H}_{mc}\Sigma^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(1)}}\mathbf{H}_{mc}^\dagger$ and $\beta = \mathbf{h}_{md}^\dagger\Sigma^{(\boldsymbol{\alpha})}_{\mathbf{x}_m^{(2)}}\mathbf{h}_{md} + \sigma_{z_d}^2$. Following similar arguments as in the proof of Lemma 2, the conditional expectation inside (19) can be written as the second equation at the bottom of the page, where $\tilde{Z}$ and $\tilde{Y}_k$, for $k = N_c+1,\ldots,N$, are i.i.d. random variables with distribution $\mathcal{CN}(0,1)$ and $\beta' = \beta\left(\sigma_{sc}^2P_s + \sigma_{\mathbf{z}_c}^2 + \sigma_{mc}^2\sum_{j=N_c+1}^{N}\alpha_jP_j\right)$. Notice that, for any realization of $\tilde{Z}$ and $\{\tilde{Y}_k\}_{N_c+1}^{N}$, the conditional expectation in-

$$\begin{aligned}
&\mathbf{E}_{\tilde{Z},\tilde{Y}_k|\mathcal{H}_d}\left[C\left(\frac{\frac{\sigma_s^2\sigma_{sc}^2\sum_{i=1}^{N_c}|h_{id}|^2|\ell_i|^2}{\sigma_{sc}^2\sigma_s^2+\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum_{j=N_c+1}^{N}p_j}|\tilde{Z}|^2}{\frac{\sigma_{\mathbf{z}_c}^2\sum_{i=1}^{N_c}|h_{id}|^2|\ell_i|^2}{\sigma_{sc}^2\sigma_s^2+\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum_{j=N_c+1}^{N}p_j} + \frac{\sigma_{mc}^2\sum_{i=1}^{N_c}|h_{id}|^2|\ell_i|^2\left(\sum_{k=N_c+1}^{N}p_k|\tilde{Y}_k|^2\right)}{\sigma_{sc}^2\sigma_s^2+\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum_{j=N_c+1}^{N}p_j}+\beta}\right)\right]\\
&= \mathbf{E}_{\tilde{Z},\tilde{Y}_k|\mathcal{H}_d}\left[C\left(\frac{\sigma_s^2\sigma_{sc}^2\sum_{i=1}^{N_c}|h_{id}|^2|\ell_i|^2|\tilde{Z}|^2}{\sum_{i=1}^{N_c}|h_{id}|^2|\ell_i|^2\left(\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum_{k=N_c+1}^{N}p_k|\tilde{Y}_k|^2\right)+\beta\left(\sigma_{sc}^2\sigma_s^2+\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum_{j=N_c+1}^{N}p_j\right)}\right)\right],
\end{aligned} \tag{18}$$

$$\begin{aligned}
&\mathbf{E}_{\mathcal{H}_c|\mathcal{H}_d}\left[C\left(\frac{P_s|\mathbf{h}_{cd}^\dagger\mathbf{L}_c\mathbf{h}_{sc}|^2}{\mathbf{h}_{cd}^\dagger\mathbf{L}_c\boldsymbol{\Lambda}\mathbf{L}_c^\dagger\mathbf{h}_{cd}+\beta}\right)\right]\\
&= \mathbf{E}_{\tilde{Z},\tilde{Y}_k|\mathcal{H}_d}\left[C\left(\frac{P_s\sigma_{sc}^2\sum\limits_{i=1}^{N_c}|h_{id}|^2|\ell_i|^2|\tilde{Z}|^2}{\sum\limits_{i=1}^{N_c}|h_{id}|^2|\ell_i|^2\left(\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum\limits_{k=N_c+1}^{N}\alpha_kP_k|\tilde{Y}_k|^2\right)+\beta'}\right)\right]
\end{aligned}$$

creases monotonically with $|\ell_i|$, for all $i = 1, \dots, N_c$. Hence, under the power constraints $|\ell_i|^2 \leq P_i$, for $i = 1, \dots, N_c$, the amplifying matrix $\mathbf{L}_c^*$ given in the lemma statement maximizes the conditional mean inside (19). The choice of their phases, i.e., $\{\phi_i\}_{i=1}^{N_c}$, are arbitrary. Since $\mathbf{L}_c^*$ does not depend on $\mathbf{h}_{cd}$ and $\mathbf{h}_{md}$, it also maximizes the utility of Player 1 (which further takes the average over $\mathbf{h}_{cd}$ and $\mathbf{h}_{md}$). ■

Now, we focus on the action subset $\mathcal{A}_{2l}$, where the malicious relays listen to the source in Phase 1 and emits jamming signals only in Phase 2. In the following, we determine the optimal transmission strategy for Player 2 among $\mathcal{A}_{2l}$ when Player 1 employs the strategy $(f_s, \mathbf{L}_c)$, where $f_s \sim \mathcal{CN}(0, P_s)$ and $\mathbf{L}_c$ is chosen arbitrarily.

Lemma 4: Suppose that the instantaneous CSI $\mathcal{H}$ is available at the destination and that Player 1 employs the strategy $(f_s, \mathbf{L}_c)$, where $f_s \sim \mathcal{CN}(0, \sigma_s^2)$ and $\mathbf{L}_c$ is an arbitrary amplifying matrix. The optimal strategy for Player 2 among the action subset $\mathcal{A}_{2l}$ is given by $f_{\mathbf{x}_m^{(2)}} \sim \mathcal{CN}(0, \Sigma_{\mathbf{n}_m}^*)$ with covariance matrix $\Sigma_{\mathbf{n}_m}^* = \mathrm{diag}(P_{N_c+1}, \dots, P_N)$.

Proof: From (4),(5) and(1), we can see that the received signal at the destination in Phase 2 can be written as

$$y_d = \mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc} s + \mathbf{h}_{md}^\dagger \mathbf{x}_m^{(2)} + \mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{z}_c + z_d, \quad (20)$$

where $\mathbf{\Gamma}_c = \mathbf{L}_c \mathbf{D}_c$ with $\mathbf{L}_c = \mathrm{diag}(\ell_1, \dots, \ell_{N_c})$ and $\mathbf{D}_c = \mathrm{diag}(\mathbf{E}[|r_1|^2]^{-1/2}, \dots, \mathbf{E}[|r_{N_c}|^2]^{-1/2})$. Since the malicious relays do not emit signals in Phase 1, the received signal power at cooperative relay R_i is equal to $\mathbf{E}[|r_i|^2] = \sigma_{sc}^2 \sigma_s^2 + \sigma_{\mathbf{z}_c}^2$.

Let us first assume that the malicious relays have perfect knowledge of the source symbol s. In this case, the action subset for Player 2 now contains all PDFs $f_{\mathbf{x}_m^{(2)}}$ such that the Markov relation $x_i^{(2)} \leftrightarrow s \leftrightarrow x_j^{(2)}$ holds for all $i \neq j \in \{N_c+1, \dots, N\}$ and $\mathbf{E}[|x_i^{(2)}|^2] \leq P_i$, for all $i \in \{N_c+1, \dots, N\}$. Notice that this set, which we denote by $\mathcal{A}'_{2l}$, includes the original action set $\mathcal{A}_{2l}$ as a subset. In the following, we first find the optimal strategy for Player 2 among actions in $\mathcal{A}'_{2l}$ and then conclude our proof by showing this strategy also belongs to the original action subset $\mathcal{A}_{2l}$.

Following arguments similar to that in the proof of Lemma 3, it can be shown that the utility function of Player 2, i.e., $-I(s; y_d|\mathcal{H})$, is maximized by choosing $\mathbf{x}_m^{(2)}$ to be Gaussian. In this case, the utility of Player 2 is given by

$$\begin{aligned} -I(s; y_d|\mathcal{H}) &= -h(s|\mathcal{H}) + h(s|y_d, \mathcal{H}) \\ &= -h(s|\mathcal{H}) + \mathbf{E}_{\mathcal{H}}[\log(2\pi e \sigma_e^2)], \end{aligned} \quad (21)$$

where σ_e^2 is the variance of $s - a y_d$ with $a = \mathbf{E}[s y_d^\dagger]/\mathbf{E}[|y_d|^2]$, i.e., $\sigma_e^2 = \sigma_s^2 - |\mathbf{E}[s y_d^\dagger]|^2/\mathbf{E}[|y_d|^2]$. Notice that, to maximize the utility in (21), it is sufficient to choose

$$\mathbf{x}_m^{(2)} = \boldsymbol{\gamma}_m s + \mathbf{n}_m, \quad (22)$$

where $\boldsymbol{\gamma}_m = [\gamma_{N_c+1}, \dots, \gamma_N]^T$ and $\mathbf{n}_m \sim \mathcal{CN}(0, \Sigma_{\mathbf{n}_m})$ is a $N_c \times 1$ Gaussian jamming vector independent of s. In fact, for any choice of Gaussian attack $\tilde{\mathbf{x}}_m^{(2)}$, there exists $\mathbf{x}_m^{(2)}$ of the form in (22) that achieves the same utility. In particular, by taking $\boldsymbol{\gamma}_m = \mathbf{E}[\tilde{\mathbf{x}}_m^{(2)} s^\dagger]/\sigma_s^2$ and $\Sigma_{\mathbf{n}_m} = \Sigma_{\tilde{\mathbf{x}}_m^{(2)}} - \boldsymbol{\gamma}_m \boldsymbol{\gamma}_m^\dagger \sigma_s^2$, we have $\mathbf{E}[s \tilde{\mathbf{x}}_m^{(2)\dagger}] = \mathbf{E}[s \mathbf{x}_m^{(2)\dagger}]$ and $\Sigma_{\tilde{\mathbf{x}}_m^{(2)}} = \Sigma_{\mathbf{x}_m^{(2)}}$. Since $\mathbf{E}[s y_d^\dagger]$ and $\mathbf{E}[|y_d|^2]$ depend only on the values of $\mathbf{E}[s \tilde{\mathbf{x}}_m^{(2)\dagger}]$ and $\Sigma_{\tilde{\mathbf{x}}_m^{(2)}}$, the linear attack $\mathbf{x}_m^{(2)}$ is able to achieve the same utility as $\tilde{\mathbf{x}}_m^{(2)}$.

With $\mathbf{x}_m^{(2)}$ given as in (22), the received signal in(20) becomes

$$y_d = (\mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc} + \mathbf{h}_{md}^\dagger \boldsymbol{\gamma}_m) s + \mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{z}_c + \mathbf{h}_{md}^\dagger \mathbf{n}_m + z_d. \quad (23)$$

In this case, the utility $-I(s; y_d|\mathcal{H})$ of Player 2 is

$$-\mathbf{E}_{\mathcal{H}'_d}\left[\mathbf{E}_{\mathbf{h}_{sc}|\mathcal{H}'_d}\left[C\left(\frac{\sigma_s^2 |\mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc} + \mathbf{h}_{md}^\dagger \boldsymbol{\gamma}_m|^2}{\sigma_{\mathbf{z}_c}^2 \mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{\Gamma}_c^\dagger \mathbf{h}_{cd} + \mathbf{h}_{md}^\dagger \Sigma_{\mathbf{n}_m} \mathbf{h}_{md} + \sigma_{z_d}^2}\right)\right]\right],$$

where $\mathcal{H}'_d = \{\mathbf{h}_{md}, \mathbf{h}_{cd}, \mathbf{h}_{sm}\}$.

Let us first consider the conditional expectation inside the utility above. Suppose that $\Sigma_{\mathbf{x}_m^{(2)}}$ is given and let $\mathbf{h}_{md}^\dagger \boldsymbol{\gamma}_m = |\mathbf{h}_{md}^\dagger \boldsymbol{\gamma}_m| e^{j\theta}$. In this case, we have

$$\begin{aligned} &\mathbf{E}_{\mathbf{h}_{sc}|\mathcal{H}'_d}\left[C\left(\frac{\sigma_s^2 |\mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc} + \mathbf{h}_{md}^\dagger \boldsymbol{\gamma}_m|^2}{\sigma_{\mathbf{z}_c}^2 \mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{\Gamma}_c^\dagger \mathbf{h}_{cd} + \mathbf{h}_{md}^\dagger \Sigma_{\mathbf{n}_m} \mathbf{h}_{md} + \sigma_{z_d}^2}\right)\right] \\ &\overset{(a)}{=} \mathbf{E}_{\mathbf{h}_{sc}|\mathcal{H}'_d}\left[C\left(\frac{\sigma_s^2 |\mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc} e^{-j\theta} + |\mathbf{h}_{md}^\dagger \boldsymbol{\gamma}_m||^2}{\sigma_{\mathbf{z}_c}^2 \mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{\Gamma}_c^\dagger \mathbf{h}_{cd} + \mathbf{h}_{md}^\dagger \Sigma_{\mathbf{n}_m} \mathbf{h}_{md} + \sigma_{z_d}^2}\right)\right] \\ &\overset{(b)}{\geq} \mathbf{E}_{\mathbf{h}_{sc}|\mathcal{H}'_d}\left[C\left(\frac{\sigma_s^2 |\mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc}|^2}{\sigma_{\mathbf{z}_c}^2 \mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{\Gamma}_c^\dagger \mathbf{h}_{cd} + \mathbf{h}_{md}^\dagger \Sigma_{\mathbf{n}_m} \mathbf{h}_{md} + \sigma_{z_d}^2}\right)\right] \\ &\overset{(c)}{\geq} \mathbf{E}_{\mathbf{h}_{sc}|\mathcal{H}'_d}\left[C\left(\frac{\sigma_s^2 |\mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc}|^2}{\sigma_{\mathbf{z}_c}^2 \mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{\Gamma}_c^\dagger \mathbf{h}_{cd} + \mathbf{h}_{md}^\dagger \Sigma_{\mathbf{x}_m^{(2)}} \mathbf{h}_{md} + \sigma_{z_d}^2}\right)\right], \end{aligned}$$

where (a) follows by the fact that $\mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc} + \mathbf{h}_{md}^\dagger \boldsymbol{\gamma}_m = (\mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc} e^{-j\theta} + |\mathbf{h}_{md}^\dagger \boldsymbol{\gamma}_m|) e^{j\theta}$ and (b) follows from [8, Lemma 1] and [29], which states that

$$\mathbf{E}_h\left[\frac{k_1 + |h + k_2|^2}{k_1}\right] \geq \mathbf{E}_h\left[\frac{k_1 + |h|^2}{k_1}\right], \quad (24)$$

for h that is a complex Gaussian random variable and $k_1 > 0$ and $k_2 \geq 0$ that are real constants. Given $\mathbf{h}_{md}$, $\mathbf{h}_{sm}$, and $\mathbf{h}_{cd}$, the latter result is applied by setting $k_1 = (\sigma_{\mathbf{z}_c}^2 \mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{\Gamma}_c^\dagger \mathbf{h}_{cd} + \mathbf{h}_{md}^\dagger \Sigma_{\mathbf{n}_m} \mathbf{h}_{md} + \sigma_{z_d}^2)/\sigma_s^2$ and $k_2 = |\mathbf{h}_{md}^\dagger \boldsymbol{\gamma}_m|$, and by identifying that $\mathbf{h}_{cd}^\dagger \mathbf{\Gamma}_c \mathbf{h}_{sc} e^{-j\theta}$ is a complex Gaussian random variable. Furthermore, (c) follows from the fact that

$$\mathbf{h}_{md}^\dagger \Sigma_{\mathbf{x}_m^{(2)}} \mathbf{h}_{md} = \sigma_s^2 |\boldsymbol{\gamma}_m^\dagger \mathbf{h}_{md}|^2 + \mathbf{h}_{md}^\dagger \Sigma_{\mathbf{n}_m} \mathbf{h}_{md} \geq \mathbf{h}_{md}^\dagger \Sigma_{\mathbf{n}_m} \mathbf{h}_{md}.$$

Note that the lower bound is achieved by setting $\boldsymbol{\gamma}_m = \mathbf{0}$. In this case, $\mathbf{x}_m^{(2)} = \mathbf{n}_m$ and $\Sigma_{\mathbf{x}_m^{(2)}} = \Sigma_{\mathbf{n}_m}$. Finally, by Lemma 1(b), the conditional expectation is further minimized under the power constraints in (12) by taking $\Sigma_{\mathbf{n}_m}$ equal to $\Sigma_{\mathbf{n}_m}^* \triangleq \mathrm{diag}(P_{N_c+1}, \dots, P_N)$. Since the optimal choices of $\boldsymbol{\gamma}_m$ and $\Sigma_{\mathbf{n}_m}$ do not depend on $\mathbf{h}_{md}$, $\mathbf{h}_{sm}$, and $\mathbf{h}_{cd}$, they also are the solutions that maximize the overall utility function. Notice that, with $\mathbf{x}_m^{(2)} = \mathbf{n}_m \sim \mathcal{CN}(\mathbf{0}, \Sigma_{\mathbf{n}_m}^*)$, the signals $x_i^{(2)}$ and $x_j^{(2)}$ are independent and, thus, also satisfy the Markov relation $x_i^{(2)} \leftrightarrow r_i \leftrightarrow s \leftrightarrow r_j \leftrightarrow x_j^{(2)}$ for all $i \neq j$. Hence, this choice of action also belongs to the original action subset $\mathcal{A}_{2l}$ and, thus, is the solution to the original problem. ∎

Note that the optimal jamming signal given in Lemma 4 does not depend on the signal received in Phase 1. This indicates that no advantage can be gained by having malicious relays listen to the source in Phase 1. Similar results were observed in [7] and [8] under different system setups. Indeed, without knowledge of other relays' channels, it is difficult for the malicious relays to coordinate a destructive attack based on their received signals. The strategy given in Lemma 4 is a special case of that given in Lemma 3 with $\alpha_i = 0, \forall i$ and, therefore, can also be viewed as a strategy in the action subset $\mathcal{A}_{2a}$ (or, more specifically, in the subset $\mathcal{A}_{2a}^{(\mathbf{0})}$). Therefore, the best strategy chosen from $\mathcal{A}_{2a}$ is the best overall strategy. The NE of the proposed game can then be found as given in the following theorem.

Theorem 2: When the instantaneous CSI $\mathcal{H}$ is available at the destination, a Nash equilibrium of the zero-sum game G_{AF} is given by $(f_s^*, \mathbf{L}_c^*)$ for Player 1 and $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)})$ for Player 2, where $\boldsymbol{\alpha}^*$ is the optimal power allocation between Phases 1 and 2 at the malicious relays, $f_s^* \sim \mathcal{CN}(0, P_s)$, $\mathbf{L}_c^* = \operatorname{diag}(\sqrt{P_1}e^{j\phi_1}, \ldots, \sqrt{P_{N_c}}e^{j\phi_{N_c}})$ with $\{\phi_i\}_{i=1}^{N_c}$ chosen arbitrarily, $f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)} \sim \mathcal{CN}(\mathbf{0}, \Sigma_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)})$ with $\Sigma_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)} = \operatorname{diag}(\alpha_{N_c+1}^* P_{N_c+1}, \ldots, \alpha_N^* P_N)$, and $f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)} \sim \mathcal{CN}(\mathbf{0}, \Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)})$ with $\Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)} = \operatorname{diag}((1 - \alpha_{N_c+1}^*)P_{N_c+1}, \ldots, (1 - \alpha_N^*)P_N)$. The optimal power allocation is in (25) at the bottom of the page, where $\mathbf{D}^{(\boldsymbol{\alpha})}$ is $\operatorname{diag}(\mathbf{E}[|r_1|^2]^{-1/2}, \ldots, \mathbf{E}[|r_{N_c}|^2]^{-1/2})$ with $\mathbf{E}[|r_i|^2] = \sigma_{sc}^2\sigma_s^2 + \sigma_{\mathbf{z}_c}^2 + \sigma_{mc}^2 \sum_{j=N_c+1}^{N} \alpha_j P_j$.

Proof: Suppose that Player 1 employs the strategy $(f_s^*, \mathbf{L}_c^*)$. To show that $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)})$ is optimal for Player 2 in this case, we need to show that no other strategies in $\mathcal{A}_{2a}^{(\boldsymbol{\alpha}^*)}$, in $\mathcal{A}_{2a}^{(\boldsymbol{\alpha})}$ for some other $\boldsymbol{\alpha}$, and in $\mathcal{A}_{2l}$ can achieve a higher utility for Player 2. Specifically, by Lemma 2, we know that the strategy $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)})$ achieves the maximum utility among all strategies in $\mathcal{A}_{2a}^{(\alpha^*)}$. That is, Player 2 cannot gain by opting for another strategy in $\mathcal{A}_{2a}^{(\alpha^*)}$. If Player 2 searches among subset $\mathcal{A}_{2a}^{(\boldsymbol{\alpha})}$, for some $\boldsymbol{\alpha} \neq \boldsymbol{\alpha}^*$, then the optimal strategy is given by $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})})$. In this case, the utility of Player 2 is equal to $-u(\boldsymbol{\alpha})$ in (25), which is smaller than that achieved by $\boldsymbol{\alpha}^*$. Moreover, since the optimal strategy for Player 2 in $\mathcal{A}_{2l}$ also belongs to $\mathcal{A}_{2a}^{(\mathbf{0})}$, a strategy in $\mathcal{A}_{2l}$ will not be able to achieve a higher utility either. Hence, Player 2 cannot gain by altering its strategy from $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)})$.

On the other hand, given that Player 2 employs the strategy $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)})$, then we know by Lemma 3 that the optimal strategy for Player 1 is given by $(f_s^*, \mathbf{L}_c^*)$. Therefore, Player 1 also will not be able to gain by unilaterally altering its strategy. Hence, $(f_s^*, \mathbf{L}_c^*)$ for Player 1 and $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)})$ for Player 2 together form a Nash equilibrium for the zero-sum game G_{AF}. ∎

This theorem indicates that the optimal strategy for Player 1 is to employ Gaussian signalling at the source and to have the cooperative relays amplify-and-forward with maximum power; and the optimal strategy for Player 2 is to emit Gaussian jamming signals in both phases.

V. Optimal Transmission Strategies for the Case Without Interrelay CSI at the Destination

In this section, we consider the more practical case where the interrelay CSI $\mathbf{H}_{mc}$ is not known at the destination. Note that knowledge of $\mathbf{H}_{mc}$ at the destination matters because it affects the utility that can be achieved (cf. equation(9) and (10)). In particular, knowledge of $\mathbf{H}_{mc}$ affects the distribution of the equivalent noise term $\mathbf{h}_{cd}^\dagger \boldsymbol{\Gamma}_c \mathbf{H}_{mc} \mathbf{x}_m^{(1)}$ in (14) (depending on whether the distribution is conditioned on $\mathbf{H}_{mc}$ or not) when the destination decodes the source message and, thus, affects the mutual information. The optimal transmission strategies are first derived within each of the action subsets $\mathcal{A}_{2a}$ and $\mathcal{A}_{2l}$ and then compared to obtain the overall best strategy. The following lemmas are first proved and are then used to find the NE in Theorem 3.

Lemma 5: Suppose that the instantaneous CSI $\mathcal{H}' \triangleq \{\mathbf{h}_{cd}, \mathbf{h}_{md}, \mathbf{h}_{sc}, \mathbf{h}_{sm}\}$ is available at the destination and that Player 1 employs the strategy $(f_s, \mathbf{L}_c)$, where $f_s \sim \mathcal{CN}(0, \sigma_s^2)$ and $\mathbf{L}_c$ is an arbitrary amplifying matrix. The optimal strategy for Player 2 among the action subset $\mathcal{A}_{2a}^{(\boldsymbol{\alpha})}$ is given by $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})})$, where $f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})}$ is the density of a constant random vector $\mathbf{x}_m^{(1)} = \mathbf{U}\mathbf{p}^{(\boldsymbol{\alpha})}$ with $\mathbf{U}$ being an arbitrary unitary matrix and $\mathbf{p}^{(\boldsymbol{\alpha})} = [\sqrt{\alpha_{N_c+1}P_{N_c+1}}, \ldots, \sqrt{\alpha_N P_N}]^T$, and $f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})} \sim \mathcal{CN}(0, \Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})})$ with $\Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})} = \operatorname{diag}((1 - \alpha_{N_c+1})P_{N_c+1}, \ldots, (1 - \alpha_N)P_N)$. That is, the malicious relays transmit constant jamming signals in Phase 1 and Gaussian jamming signals in Phase 2.

Proof: First, we prove the optimality of choosing $\mathbf{x}_m^{(1)}$ to be a constant random vector and $\mathbf{x}_m^{(2)}$ to be Gaussian distributed. Recall that the received signal is

$$y_d = \mathbf{h}_{cd}^\dagger \boldsymbol{\Gamma}_c \mathbf{h}_{sc} s + \mathbf{h}_{cd}^\dagger \boldsymbol{\Gamma}_c \mathbf{H}_{mc} \mathbf{x}_m^{(1)} + \mathbf{h}_{md}^\dagger \mathbf{x}_m^{(2)} + \mathbf{h}_{cd}^\dagger \boldsymbol{\Gamma}_c \mathbf{z}_c + z_d,$$

$$\boldsymbol{\alpha}^* = \arg\min_{\boldsymbol{\alpha} \in [0,1]^{N-N_c}} u(\boldsymbol{\alpha}), \text{ where } u(\boldsymbol{\alpha})$$
$$= \mathbf{E}_{\mathcal{H}}\left[C\left(\frac{P_s |\mathbf{h}_{cd}^\dagger \mathbf{L}_c^* \mathbf{D}_c^{(\boldsymbol{\alpha})} \mathbf{h}_{sc}|^2}{\mathbf{h}_{cd}^\dagger \mathbf{L}_c^* \mathbf{D}_c^{(\boldsymbol{\alpha})} \left(\sigma_{\mathbf{z}_c}^2 \mathbf{I} + \mathbf{H}_{mc} \Sigma_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})} \mathbf{H}_{mc}^\dagger \right) (\mathbf{D}_c^{(\boldsymbol{\alpha})})^\dagger (\mathbf{L}_c^*)^\dagger \mathbf{h}_{cd} + \mathbf{h}_{md}^\dagger \Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})} \mathbf{h}_{md} + \sigma_{z_d}^2} \right) \right], \tag{25}$$

where $\mathbf{\Gamma}_c = \mathbf{L}_c\mathbf{D}_c$, and the utility function u_2 of Player 2 is $-I(s; y_d|\mathcal{H}') = -h(s|\mathcal{H}') + h(s|y_d, \mathcal{H}')$. Following the arguments given in Lemma 2, the term $h(s|y_d, \mathcal{H}')$ (and, thus, the utility of Player 2) is maximized by allowing y_d to be Gaussian when conditioned on $\mathcal{H}'$. This is achieved by choosing $\mathbf{x}_m^{(1)}$ to be a constant vector and $\mathbf{x}_m^{(2)}$ to be a Gaussian vector with distribution $\mathcal{CN}(0, \Sigma_{\mathbf{x}_m^{(2)}})$, which is independent of $\mathbf{x}_m^{(1)}$. Notice that, in this case, $\mathbf{H}_{mc}\mathbf{x}_m^{(1)}$ is Gaussian with distribution $\mathcal{CN}(0, \sigma_{mc}^2|\mathbf{x}_m^{(1)}|^2\mathbf{I})$.

With the choice of distributions for $\mathbf{x}_m^{(1)}$ and $\mathbf{x}_m^{(2)}$, the utility $-I(s; y_d|\mathcal{H}')$ of Player 2 becomes

$$-\mathbf{E}_{\mathcal{H}_c'}\left[\mathbf{E}_{\mathbf{h}_{md}|\mathcal{H}_c'}\left[C\left(\frac{\sigma_s^2|\mathbf{h}_{cd}^\dagger\mathbf{\Gamma}_c\mathbf{h}_{sc}|^2}{\lambda\mathbf{h}_{cd}^\dagger\mathbf{\Gamma}_c\mathbf{\Gamma}_c^\dagger\mathbf{h}_{cd}+\mathbf{h}_{md}^\dagger\Sigma_{\mathbf{x}_m^{(2)}}\mathbf{h}_{md}+\sigma_{z_d}^2}\right)\right]\right],$$

where $\mathcal{H}_c' = \{\mathbf{h}_{cd}, \mathbf{h}_{sc}\}$ and $\lambda \triangleq \sigma_{\mathbf{z}_c}^2 + \sigma_{mc}^2\left\|\mathbf{x}_m^{(1)}\right\|^2$. For any given $\mathbf{x}_m^{(1)}$, we can see from Lemma 1(b) that the conditional expectation inside the utility expression above is minimized under the power constraints in (11) by choosing

$$\Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})} = \mathrm{diag}((1-\alpha_{N_c+1})P_{N_c+1}, \ldots, (1-\alpha_N)P_N). \quad (26)$$

Since $\Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})}$ does not depend on the realization of $\mathbf{h}_{cd}$ and $\mathbf{h}_{sc}$, it is also the solution that maximizes the utility function of Player 2.

Moreover, given $\Sigma_{\mathbf{x}_m^{(2)}} = \Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})}$, we can write the utility function $-I(s; y_d|\mathcal{H}')$ as shown in (27) at the bottom of the page, where $\mathcal{H}_d = \{\mathbf{h}_{cd}, \mathbf{h}_{md}\}$, $\beta = \mathbf{h}_{md}^\dagger\Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})}\mathbf{h}_{md} + \sigma_{z_d}^2$. Notice that, given $\mathcal{H}_d$, the term $Z \triangleq \sum_{i=1}^{N_c} h_{id}^*\gamma_i h_{si}$ is equivalently a zero-mean complex Gaussian random variable with variance

$$\sigma_Z^2 = \sigma_{sc}^2\sum_{i=1}^{N_c}|h_{id}|^2|\gamma_i|^2 = \sum_{i=1}^{N_c}\frac{\sigma_{sc}^2|h_{id}|^2|\ell_i|^2}{\sigma_{sc}^2\sigma_s^2+\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum\limits_{j=N_c+1}^{N}|x_j^{(1)}|^2}.$$

Therefore, the conditional expectation inside (27) can be computed as in (28), shown at the bottom of the page, with $\tilde{Z} \sim \mathcal{CN}(0,1)$. From the above, we can see that the conditional expectation is minimized (and, thus, the utility is maximized) by choosing $\mathbf{x}_m^{(1)}$ such that $|x_i^{(1)}|^2$ is maximized for each i. Under the power constraints given in (11), the solution is given by $\mathbf{x}_m^{(1)} = \mathbf{U}\mathbf{p}^{(\boldsymbol{\alpha})}$, where $\mathbf{p}^{(\boldsymbol{\alpha})} = [\sqrt{\alpha_{N_c+1}P_{N_c+1}}, \ldots, \sqrt{\alpha_N P_N}]^T$ and $\mathbf{U}$ is an arbitrary unitary matrix. ■

The above lemma shows that, given $s \sim \mathcal{CN}(0, \sigma_s^2)$ and arbitrary $\mathbf{L}_c$, the optimal strategy for Player 2 among the set $\mathcal{A}_{2a}$ is to emit a constant jamming signal in Phase 1 and a Gaussian jamming signal in Phase 2. This differs from the previous case where Gaussian jamming signals are used in both phases. In the following lemma, we show that the choice of f_s and $\mathbf{L}_c$ in the premise of Lemma 5 is indeed optimal when Gaussian jamming signals are employed by the malicious relays. The proof is similar to that of Lemma 6 and, therefore, is omitted.

Lemma 6: Suppose that the instantaneous CSI $\mathcal{H}'$ is available at the destination and that Player 2 employs the strategy $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})})$, where $f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha})}$ is the density of a constant random vector $\mathbf{x}_m^{(1)} = \mathbf{U}\mathbf{p}^{(\boldsymbol{\alpha})}$ with $\mathbf{U}$ being an arbitrary unitary matrix and $\mathbf{p}^{(\boldsymbol{\alpha})} = [\sqrt{\alpha_{N_c+1}P_{N_c+1}}, \ldots, \sqrt{\alpha_N P_N}]^T$, and $f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})} \sim \mathcal{CN}(0, \Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})})$ with $\Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})} = \mathrm{diag}((1-\alpha_{N_c+1})P_{N_c+1}, \ldots, (1-\alpha_N)P_N)$. The optimal strategy for Player 1 is given by $(f_s^*, \mathbf{L}_c^*)$, where $f_s^* \sim \mathcal{CN}(0, P_s)$ and $\mathbf{L}_c^* = \mathrm{diag}\left(\sqrt{P_1}e^{j\phi_1}, \ldots, \sqrt{P_{N_c}}e^{j\phi_{N_c}}\right)$ with ϕ_i, for $i = 1, \ldots, N_c$, chosen arbitrarily.

Next, we also need to determine the optimal transmission strategy among the action subset $\mathcal{A}_{2l}$. Notice that, when the malicious relays listen in Phase 1, the interrelay CSI $\mathbf{H}_{mc}$ has no affect on the utility of both players. Therefore, Lemma 4 holds regardless of whether $\mathbf{H}_{mc}$ is available at the destination. This implies that the optimal strategy for Player 2 among the set $\mathcal{A}_{2l}$, as described Lemma 4, is a special case of that in Lemma 5 with $\alpha_i = 0$, for $i = N_c + 1, \ldots, N$. Hence, the best strategy chosen among the set $\mathcal{A}_{2a}$ should be the best strategy overall. The NE of the case with full CSI can then be established as follows.

Theorem 3: When the instantaneous CSI $\mathcal{H}'$ is available at the destination, a Nash equilibrium of the zero-sum game

$$-\mathbf{E}_{\mathcal{H}_d}\left[\mathbf{E}_{\mathbf{h}_{sc}|\mathcal{H}_d}\left[C\left(\frac{\sigma_s^2\left|\sum\limits_{i=1}^{N_c}h_{id}^*\gamma_i h_{si}\right|^2}{\left(\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum\limits_{k=N_c+1}^{N}|x_k^{(1)}|^2\right)\sum\limits_{i=1}^{N_c}|h_{id}|^2|\gamma_i|^2+\beta}\right)\right]\right] \quad (27)$$

$$\mathbf{E}_{\tilde{Z}|\mathbf{h}_{cd},\mathbf{h}_{md}}\left[C\left(\frac{\sum\limits_{i=1}^{N_c}\sigma_s^2\sigma_{sc}^2|h_{id}|^2|\ell_i|^2\left|\tilde{Z}\right|^2}{\left(\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum\limits_{k=N_c+1}^{N}|x_k^{(1)}|^2\right)\sum\limits_{i=1}^{N_c}|h_{id}|^2|\ell_i|^2+\beta\left(\sigma_{sc}^2\sigma_s^2+\sigma_{\mathbf{z}_c}^2+\sigma_{mc}^2\sum\limits_{j=N_c+1}^{N}|x_j^{(1)}|^2\right)}\right)\right], \quad (28)$$

G_{AF} is given by $(f_s^*, \mathbf{L}_c^*)$ for Player 1 and $(f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)}, f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)})$ for Player 2, where $\boldsymbol{\alpha}^*$ is the optimal power allocation between Phases 1 and 2 at the malicious relays, $f_s^* \sim \mathcal{CN}(0, P_s)$, $\mathbf{L}_c^* = \mathrm{diag}(\sqrt{P_1}e^{j\phi_1}, \ldots, \sqrt{P_{N_c}}e^{j\phi_{N_c}})$ with $\{\phi_i\}_{i=1}^{N_c}$ chosen arbitrarily, $f_{\mathbf{x}_m^{(1)}}^{(\boldsymbol{\alpha}^*)}$ is the density of a constant random vector $\mathbf{x}_m^{(1)} = \mathbf{U}\mathbf{p}^{(\boldsymbol{\alpha}^*)}$ with $\mathbf{U}$ being an arbitrary unitary matrix and $\mathbf{p}^{(\boldsymbol{\alpha}^*)} = [\sqrt{\alpha_{N_c+1}^* P_{N_c+1}}, \ldots, \sqrt{\alpha_N^* P_N}]^T$, and $f_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)} \sim \mathcal{CN}(\mathbf{0}, \Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)})$ with $\Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha}^*)} = \mathrm{diag}((1 - \alpha_{N_c+1}^*)P_{N_c+1}, \ldots, (1 - \alpha_N^*)P_N)$. The optimal power allocation $\boldsymbol{\alpha}^*$ is given by (29), shown at the bottom of the page, where $\mathbf{D}^{(\boldsymbol{\alpha})} = \mathrm{diag}(\mathbf{E}[|r_1|^2]^{-1/2}, \ldots, \mathbf{E}[|r_{N_c}|^2]^{-1/2})$ with $\mathbf{E}[|r_i|^2] = \sigma_{sc}^2\sigma_s^2 + \sigma_{\mathbf{z}_c}^2 + \sigma_{mc}^2\sum_{j=N_c+1}^{N}\alpha_j P_j$.

Following arguments given in the proof of Theorem 2, the above theorem can be proved similarly from Lemmas 5 and 6, which state that the strategies described are optimal for each player when the other player is fixed. That is, no player can gain by unilaterally altering its own strategy and, thus, is the NE of the system. Interestingly, we can see, from the NEs stated in Theorems 2 and 3, that the strategy adopted by each cooperative relay depends only on its own power constraint. Therefore, the result is not affected if knowledge of the local channel statistics and power constraints are kept private at each relay.

VI. Computer Simulations

In this section, we provide computer simulations to verify our theoretical claims. In Figs. 2–5, we set the power constraints of all terminals to be P, i.e., $P_s = P_1 = \cdots = P_N = P$, and define the signal-to-noise (SNR) as $P/\sigma_{z_d}^2$. The power constraints of the remaining figures are specified separately.

The channel vectors (or matrices) $\mathbf{h}_{cd}, \mathbf{h}_{sc}, \mathbf{h}_{md}, \mathbf{h}_{sm}$ and $\mathbf{H}_{mc}$ are assumed to have entries that are i.i.d. Gaussian with unit variance (unless mentioned otherwise) and all noise variances are set to unity. Each simulation result is obtained by averaging over 100000 channel realizations.

In Fig. 2, the utility of Player 1 (i.e., $u_1 = -u_2$) achieved under the proposed NE strategy is shown for the case with "Full CSI" and the case with "Unknown $\mathbf{H}_{mc}$" at the destination (i.e., the utility obtained with the strategies given in Theorems 2 and 3, respectively). The results are compared with the case where Player 2 can only select from the action subset $\mathcal{A}_{2l}$ (i.e., the malicious relays are required to listen in Phase 1). The latter scheme can be viewed as an extension of the results in [7] to the multirelay scenario, with additional optimization of the source distribution. We set the number of cooperative relays as $N_c = 2$ and the number of malicious relays as $N - N_c = 3$. The optimal power allocation $\boldsymbol{\alpha}^*$ at the malicious relays is obtained by line search. We can see that, by allowing Player 2 to select among the action set $\mathcal{A}_2$ (instead of just $\mathcal{A}_{2l}$), Player 2 is able to more

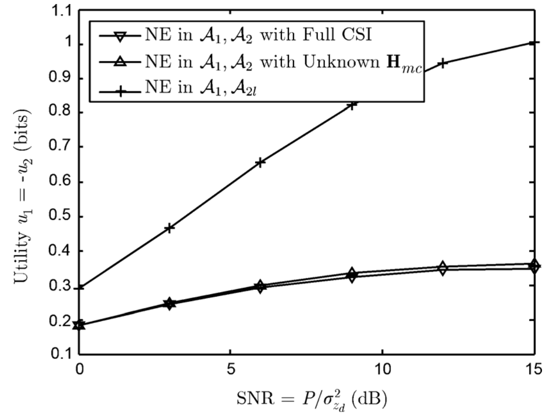


Fig. 2. With $N_c = 2$, $N - N_c = 3$, and equal power constraint P at all terminals, the utility of Player 1, i.e., $u_1 = -u_2$, versus SNR is shown for the case with Full CSI, the case with Unknown $\mathbf{H}_{mc}$, and the case where Player 2 can select only from the action subset $\mathcal{A}_{2l}$.

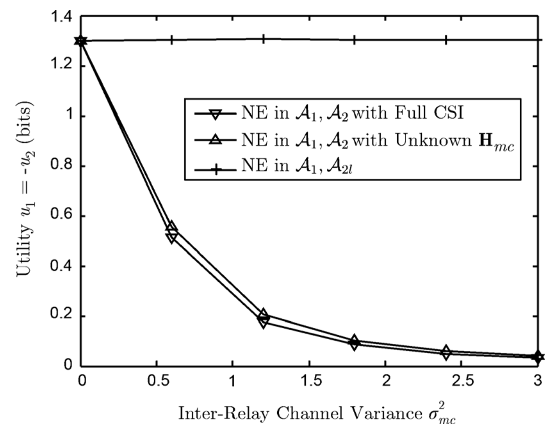


Fig. 3. With $N_c = N - N_c = 3$, $SNR = 15$ dB, and equal power constraints at all terminals, the utility of Player 1 versus different values of σ_{mc}^2 is shown for the case with Full CSI, the case with Unknown $\mathbf{H}_{mc}$, and the case where Player 2 can select only from the action subset $\mathcal{A}_{2l}$.

successfully decrease the utility of Player 1. Here, we see that the case with Full CSI and the case with Unknown $\mathbf{H}_{mc}$ achieve similar utilities. However, this is not always the case as we show in later examples. In Fig. 3, the utility of Player 1 with respect to the interrelay channel variance σ_{mc}^2, i.e., the variance of each entry of $\mathbf{H}_{mc}$, is shown for the different schemes mentioned above. We can see that the impact of malicious behaviors on the utility of Player 1 increases as the interrelay channel variance σ_{mc}^2 increases.

In Fig. 4, the utility of Player 1 with respect to SNR is compared for cases with $N_c = 1$ and $N_c = 6$, respectively. We can see that, for the case with $N_c = 1$, Player 1 achieves a higher utility when Full CSI is available at the destination, but

$$\boldsymbol{\alpha}^* = \arg\min_{\boldsymbol{\alpha}\in[0,1]^{N-N_c}} \mathbf{E}_{\mathcal{H}'}\left[C\left(\frac{P_s|\mathbf{h}_{cd}^\dagger \mathbf{L}_c^* \mathbf{D}_c^{(\boldsymbol{\alpha})}\mathbf{h}_{sc}|^2}{\left(\sigma_{\mathbf{z}_c}^2 + \sigma_{mc}^2\|\mathbf{p}^{(\boldsymbol{\alpha})}\|^2\right)\left|(\mathbf{D}_c^{(\boldsymbol{\alpha})})^\dagger(\mathbf{L}_c^*)^\dagger\mathbf{h}_{cd}\right|^2 + \mathbf{h}_{md}^\dagger\Sigma_{\mathbf{x}_m^{(2)}}^{(\boldsymbol{\alpha})}\mathbf{h}_{md} + \sigma_{z_d}^2}\right)\right], \tag{29}$$

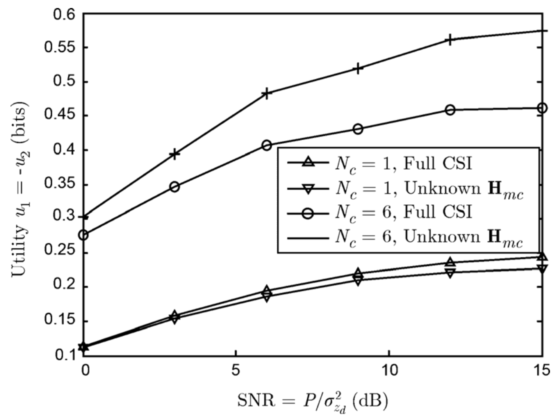


Fig. 4. For $N_c = 1$ and 6, the utility of Player 1 versus SNR is shown for the case with Full CSI and the case with Unknown $\mathbf{H}_{mc}$. Here, the number of malicious relays is set as $N - N_c = 3$ and equal power constraints are assumed at all terminals.

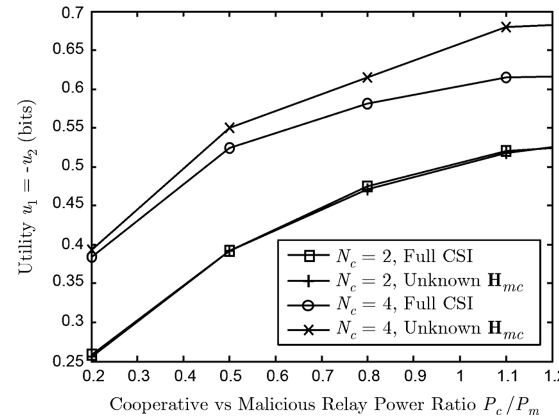


Fig. 6. For $N_c = 2, 4$ and for $N - N_c = 2$, the utility of Player 1 with respect to the cooperative and malicious relay power ratio P_c/P_m, where P_c is the power constraint at each cooperative relay and P_m is the power constraint at each malicious relay as well as the source.

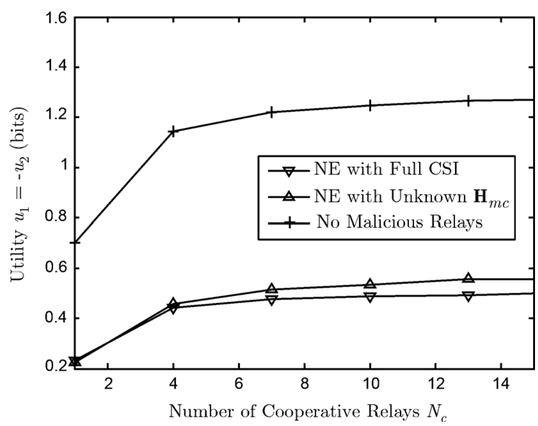


Fig. 5. For $N - N_c = 2$, $SNR = 3$ dB, and equal power constraints at all terminals, the utility of Player 1 versus the number of cooperative relays, i.e., N_c, is shown for the case with Full CSI, the case with Unknown $\mathbf{H}_{mc}$, and the case with no malicious relays.

vice versa for the case with $N_c = 6$. This is because Player 2 is allowed to adapt its strategy according to the available CSI at the destination. In particular, Player 2 can utilize destination's knowledge of $\mathbf{H}_{mc}$ to work against Player 1 and more effectively disrupt the reception at the destination. This phenomenon is actually more pronounced as N_c increases since more replicas of the jamming signals are forwarded to the destination in this case. This may seem counter-intuitive, but is actually reasonable since the destination does not adapt its decoding strategy in favor of any player. If the destination is indeed allowed to adapt its decoding strategy (e.g., in favor of Player 1), it can sometimes gain by decoding without the additional CSI $\mathbf{H}_{mc}$, even if it is available. Indeed, parallel to our results, the results in [11] show that lack of CSI feedback from the destination to the transmitters may not always be bad when a jammer exists in the system.

In Fig. 5, the utility of Player 1 versus the number of cooperative relays N_c is shown for the case with Full CSI, the case with Unknown $\mathbf{H}_{mc}$, and the case with no malicious relays. In the first two cases, the number of malicious relays, $N - N_c$, is fixed as 2 whereas the number of cooperative relays, N_c, is varied from 1 to 15. Notice that it is indeed the case in most practical scenarios that the number of malicious relays, $N - N_c$, is smaller than the number of cooperative relays, N_c. Notice that the advantages of increasing N_c saturates rapidly since, for large N_c, the jamming signals emitted by the malicious relays become the dominate source of noise and, thus, the effective receive SNR no longer increases with N_c.

In Fig. 6, the utility of Player 1 is shown versus increasing power constraints at the cooperative relays. Suppose that the power constraints of the cooperative relays are given uniformly by P_c and that of the source and the malicious relays are given by P_m. We can see, for the case with $N_c = 2$ and 4 and with $N - N_c = 2$, that the utility of Player 1 increases as P_c increases, but the advantage saturates rapidly since the power of the jamming signal is amplified proportionally as P_c increases and, thus, becomes the dominant source of noise.

In Figs. 7 and 8, the utility of Player 1 versus SNR is shown for heterogeneous power constraints at the relays. This is shown for the case with Full CSI in Fig. 7 and for the case with Unknown $\mathbf{H}_{mc}$ in Fig. 8. Three cases are considered: (i) $P_1/P_2 = 16$ and $P_3/P_4 = 1$, (ii) $P_1/P_2 = 1$ and $P_3/P_4 = 1$, and (iii) $P_1/P_2 = 1$ and $P_3/P_4 = 16$. We set $N_c = N - N_c = 2$ and $P_1 + P_2 = P_3 + P_4 = 2P$. In case (i), the power of cooperative relay R_2 is negligible compared to that of R_1. In this case, diversity is lost and, thus, Player 1 is not able to achieve as high a utility as the case with equal power constraints. Similarly, in case (iii), the power of malicious relay R_4 is negligible compared to that of R_3 and, thus, Player 2 is not able to achieve as high a utility as the case with equal power constraints (i.e., the utility of Player 1 is therefore higher).

VII. Conclusion

In this work, we aim to provide an improved understanding of the interaction between cooperative and malicious relays in an AF multirelay network compared with previous works. The problem was formulated as a zero-sum game and the optimal transmission strategies for the source, the cooperative relays, and the malicious relays were found by identifying the NE of the game. In the two-phase transmission protocol under consideration, malicious relays can either listen in Phase 1 and attack in Phase 2 or simply attack in both phases. When full CSI is available at the destination, we showed that the optimal

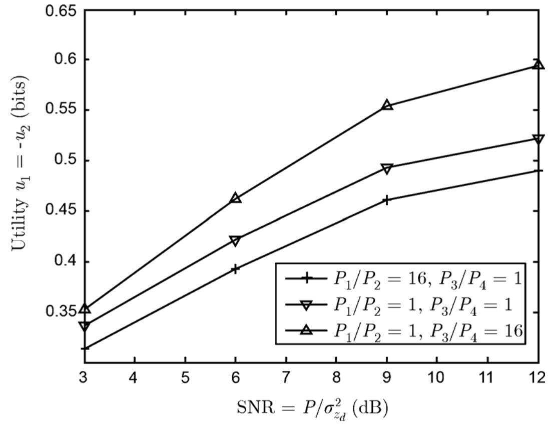


Fig. 7. For $N_c = N - N_c = 2$ and the case with Full CSI at the destination, the utility of Player 1 versus SNR, i.e., P/σ_d^2, is shown for different relay power constraints. Three cases are considered: (i) $P_1/P_2 = 16$ and $P_3/P_4 = 1$; (ii) $P_1/P_2 = 1$ and $P_3/P_4 = 1$; and (iii) $P_1/P_2 = 1$ and $P_3/P_4 = 16$. In all cases, we have $P_1 + P_2 = P_3 + P_4 = 2P$.

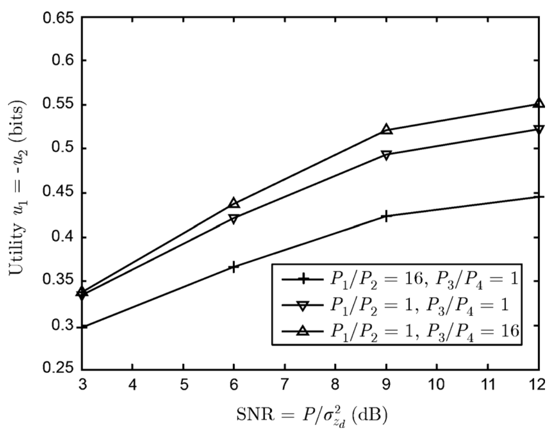


Fig. 8. For $N_c = N - N_c = 2$ and the case with unknown $\mathbf{H}_{mc}$ at the destination, the utility of Player 1 versus SNR, i.e., P/σ_d^2, is shown for different relay power constraints. Three cases are considered: (i) $P_1/P_2 = 16$ and $P_3/P_4 = 1$; (ii) $P_1/P_2 = 1$ and $P_3/P_4 = 1$; and (iii) $P_1/P_2 = 1$ and $P_3/P_4 = 16$. In all cases, we have $P_1 + P_2 = P_3 + P_4 = 2P$.

strategy for malicious relays is to emit Gaussian jamming signals in both phases. However, if the interrelay channel $\mathbf{H}_{mc}$ is not known at the destination, the malicious relays should instead attack with a constant jamming signal in Phase 1 and a Gaussian jamming signal in Phase 2. In both cases, the source should employ Gaussian signaling and all terminals should transmit with full power. The theoretical claims were verified through numerical simulations. Note that based on the fundamental results obtained in our work, one can extend the study of cooperative networks with malicious relays to more complicated game formulation.

APPENDIX
PROOF OF LEMMA 1

(a) The following proof is given by mathematical induction.

(i) Let us first consider the case with $M = 2$, where $\mathcal{J}(\mathbf{K})$ in (13) can be written as (30), shown at the bottom of the page. Notice that, since h_1 and h_2 are independent zero-mean Gaussian, the expectation in (30) would not change by replacing h_1 with $-h_1$. Therefore, with $\{\mathbf{K}\}_{11} = p_1$ and $\{\mathbf{K}\}_{22} = p_2$, the expectation in (30) can be written as

$$\begin{aligned}
&\mathbf{E}_\mathbf{h}\left[C\left(\frac{u}{v+|h_1|^2p_1+|h_2|^2p_2+h_1^*\{\mathbf{K}\}_{12}h_2+h_2^*\{\mathbf{K}\}_{21}h_1}\right)\right]\\
&=\frac{1}{2}\left\{\mathbf{E}_\mathbf{h}\left[C\left(\frac{u}{v+|h_1|^2p_1+|h_2|^2p_2+2\mathrm{Re}\{h_1^*\{\mathbf{K}\}_{12}h_2\}}\right)\right]\right.\\
&\left.+\mathbf{E}_\mathbf{h}\left[C\left(\frac{u}{v+|h_1|^2p_1+|h_2|^2p_2-2\mathrm{Re}\{h_1^*\{\mathbf{K}\}_{12}h_2\}}\right)\right]\right\}\\
&=\frac{1}{2}\mathbf{E}_\mathbf{h}\left[C\left(\frac{u\left[u+2\left(v+|h_1|^2p_1+|h_2|^2p_2\right)\right]}{\left(v+|h_1|^2p_1+|h_2|^2p_2\right)^2-\left(2\mathrm{Re}\{h_1^*\{\mathbf{K}\}_{12}h_2\}\right)^2}\right)\right].
\end{aligned}$$

In this case, the expectation is minimized by choosing $\{\mathbf{K}\}_{12} = \{\mathbf{K}\}_{21}^* = 0$. Hence, (13) is minimized by choosing $\mathbf{K} = \mathrm{diag}(p_1, p_2)$, for the case with $M = 2$.

(ii) Suppose that the statement holds for $M = k$, where $k \geq 2$. We need to show that it also holds for $M = k + 1$. Specifically, for $M = k + 1$, the objective function $\mathcal{J}(\mathbf{K})$ can be written as

$$\begin{aligned}
\mathbf{E}_\mathbf{h}\left[C\left(\frac{u}{v+\mathbf{h}^\dagger\mathbf{K}\mathbf{h}}\right)\right] &= \mathbf{E}_\mathbf{h}\left[C\left(\frac{u}{v+\sum_{i=1}^{k+1}\sum_{j=1}^{k+1}h_i^*\{\mathbf{K}\}_{ij}h_j}\right)\right]\\
&= \mathbf{E}_\mathbf{h}\left[C\left(\frac{u}{v'+2\mathrm{Re}\{\sum_{i=1}^{k}h_i^*\{\mathbf{K}\}_{i,k+1}h_{k+1}\}}\right)\right], \qquad (31)
\end{aligned}$$

where $v' \triangleq v + \tilde{\mathbf{h}}^\dagger\tilde{\mathbf{K}}\tilde{\mathbf{h}} + |h_{k+1}|^2\{\mathbf{K}\}_{k+1,k+1}$ and $\tilde{\mathbf{h}} = [h_1, \ldots, h_k]^T$ and $\tilde{\mathbf{K}}$ is a $k \times k$ matrix with $\{\tilde{\mathbf{K}}\}_{i,j} = \{\mathbf{K}\}_{i,j}$, for $i, j = 1, \ldots, k$. Then, by the fact that $-h_{k+1}$ has the same distribution as h_{k+1}, the expectation in (31) becomes

$$\frac{1}{2}\mathbf{E}_\mathbf{h}\left[C\left(\frac{u\,(u+2v')}{(v')^2-(2\mathrm{Re}\{\sum_{i=1}^{k}h_i^*\{\mathbf{K}\}_{i,k+1}h_{k+1}\})^2}\right)\right].$$

$$\mathbf{E}_\mathbf{h}\left[C\left(\frac{u}{v+|h_1|^2\{\mathbf{K}\}_{11}+|h_2|^2\{\mathbf{K}\}_{22}+h_1^*\{\mathbf{K}\}_{12}h_2+h_2^*\{\mathbf{K}\}_{21}h_1}\right)\right]. \qquad (30)$$

Here, the expectation is minimized by choosing $\{\mathbf{K}\}_{i,k+1} = \{\mathbf{K}\}^*_{k+1,i} = 0$, for $i = 1, \ldots, k$. In this case, (31) becomes

$$\mathbf{E_h}\left[C\left(\frac{u}{v + |h_{k+1}|^2\{\mathbf{K}\}_{k+1,k+1} + \tilde{\mathbf{h}}^\dagger\tilde{\mathbf{K}}\tilde{\mathbf{h}}}\right)\right]. \quad (32)$$

Since $v + |h_{k+1}|^2 P_{k+1} \geq 0$ and $\tilde{\mathbf{K}}$ is positive definite, it follows from the inductive hypothesis that (32) is minimized by choosing $\tilde{\mathbf{K}} = \mathrm{diag}(p_1, \ldots, p_k)$. This concludes the proof of (a).

(b) From (a), we know that $\mathcal{J}(\mathbf{K})$ is minimized by choosing $\mathbf{K}$ to be a diagonal matrix. In this case, the objective function becomes $\mathbf{E_h}\left[C\left(u/(v + \sum_{i=1}^{M}|h_i|^2\{\mathbf{K}\}_{ii})\right)\right]$. Hence, given that $\{\mathbf{K}\}_{ii} \leq P_i$, for $i = 1, \ldots, M$, the objective can be further minimized by choosing $\{\mathbf{K}\}_{ii} = P_i$, for all i, since $|h_i|^2 \geq 0$.

References

[1] T. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 5, pp. 572–584, Sep. 1979.

[2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[3] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity. Part I. System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[4] Y.-W. Hong, W.-J. Huang, F.-H. Chiu, and C.-C. J. Kuo, "Cooperative communications in resource-constrained wireless networks," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 47–57, May 2007.

[5] Y.-W. P. Hong, W.-J. Huang, and C.-C. J. Kuo, *Cooperative Communications and Networking: Technologies and System Design*. New York, NY, USA: Springer, 2010.

[6] S. Farahmand, G. B. Giannakis, and X. Wang, "Max-min strategies for power-limited games in the presence of correlated jamming," in *Proc. 41st Annu. Conf. Inf. Sciences and Syst. (CISS)*, 2007, pp. 300–305.

[7] T. Wang and G. B. Giannakis, "Mutual information jammer-relay games," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 290–303, Jun. 2008.

[8] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.

[9] M.-H. Chen, S.-C. Lin, and Y.-W. Peter Hong, "A game theoretic approach for the cooperative network with the presence of malicious relays," in *Proc. IEEE Global Commun. Conf. (Globecom)*, Houston, TX, USA, 2011.

[10] S. Shafiee and S. Ulukus, "Mutual information games in multiuser channels with correlated jamming," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4598–4607, Oct. 2009.

[11] S. Wei, R. Kannan, V. Chakravarthy, and M. Rangaswamy, "CSI usage over parallel fading channels under jamming attacks: A game theory study," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 1167–1175, Apr. 2012.

[12] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA, USA: MIT Press, 1994.

[13] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[14] A. Mukherjee and A. L. Swindlehurst, "Equilibrium outcomes of dynamic games in MIMO channels with active eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Cape Town, South Africa, 2010.

[15] A. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818–830, Sep. 2011.

[16] R. Zhang, L. Song, Z. Han, and B. Jiao, "Distributed coalition formation of relay and friendly jammers for secure cooperative networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, 2011.

[17] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[18] Y.-W. Huang and P. Moulin, "On the saddle-point solution and the large-coalition asymptotics of fingerprinting games," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pt. 2, pp. 160–175, Feb. 2012.

[19] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 2, pp. 198–212, Jun. 2007.

[20] S. Dehnie and N. Memon, "Detection of misbehavior in cooperative diversity," in *Proc. Military Commun. Conf. (MILCOM)*, San Diego, CA, USA, 2008.

[21] R. Gangula and R. Bhattacharjee, "Performance of selection cooperation in the presence of a malicious relay," in *Proc IEEE Int. Symp. on Wireless Commun. Syst. (ISWCS)*, 2010, pp. 408–412.

[22] S. Dehnie, H. T. Sencar, and N. Memon, "Cooperative diversity in the presence of a misbehaving relay : performance analysis," in *Proc. IEEE Sarnoff Symp.*, Princeton, NJ, USA, 2007.

[23] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pt. 2, pp. 1875–1888, Mar. 2010.

[24] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.

[25] R. U. Nabar, H. Bolcskei, and F. W. Kneubuhler, "Fading relay channels: Performance limits and space-time signal design," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 6, p. 1099, Aug. 2004.

[26] C. S. Patel and G. L. Stuber, "Channel estimation for amplify and forward relay based cooperation diversity systems," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2348–2356, Jun. 2007.

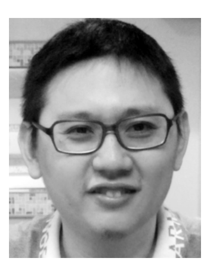
[27] T. Cover and J. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 1991.

[28] G. D. Forney, Jr, "On the role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian channels: Shannon meets Wiener," in *Proc. 41st Allerton Conf. on Comm. Control, and Comput.*, 2003, pp. 430–439.

[29] Y. H. Kim and A. Lapidoth, "On the log determinant of noncentral wishart matrices," in *Proc. IEEE Int. Symp. on Inform. Theory*, Kanagawa, Japan, 2003.

Meng-Hsi Chen received the B.S. degree in electrical engineering and the M.S. degree in communications engineering from the National Tsing Hua University (NTHU), Hsinchu, Taiwan, in 2009 and 2011, respectively.

Currently, he is a Research Assistant in Electrical Engineering at the National Taiwan University, Taipei, Taiwan. His research interests are in wireless communications and signal processing.



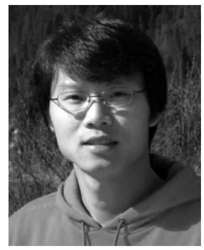
Shih-Chun Lin (M'08) received the B.S. and Ph.D. degrees in electrical engineering from National Taiwan University, Taipei, Taiwan, in 2000 and 2007, respectively. He was a Visiting Student at The Ohio State University, Columbus, OH, USA, in 2007.

After finishing his military duty during 2008, he was a Postdoctoral Researcher at National Tsing Hua University, HsinChu, Taiwan. From August 2011 to August 2012, he was an Assistant Professor at National Taipei University of Technology. He is now an Assistant Professor with the National Taiwan University of Science and Technology, Taipei, Taiwan. He also served as a TPC member of IEEE ICCC 2013, IEEE WPMC 2012, and VTC 2010-Spring. His research interests include coding/information theory, communications, and signal processing.

Y.-W. Peter Hong (S'01–M'05) received the B.S. degree in electrical engineering from National Taiwan University, Taipei, Taiwan, in 1999, and the Ph.D. degree in electrical engineering from Cornell University, Ithaca, NY, USA, in 2005.

He joined the Institute of Communications Engineering and the Department of Electrical Engineering at National Tsing Hua University, Hsinchu, Taiwan, in Fall 2005, where he is now an Associate Professor. He was also a visiting scholar at the University of Southern California during June–August of 2008. His research interests include cooperative communications, physical-layer secrecy, distributed signal processing for sensor networks, and PHY-MAC cross-layer designs for wireless networks.

Dr. Hong received the best paper award for young authors from the IEEE IT/COM Society Taipei/Tainan Chapter in 2005, the best paper award among unclassified papers in MILCOM 2005, the Junior Faculty Research Award from the College of EECS and from National Tsing Hua University in 2009 and 2010, respectively. He also received the IEEE Communication Society Asia-Pacific Outstanding Young Researcher Award in 2010, the Y. Z. Hsu Scientific Paper Award and the National Science Council (NSC) Wu Ta-You Memorial Award in 2011, and the Chinese Institute of Electrical Engineering (CIEE) Outstanding Young Electrical Engineer Award in 2012. He is a coeditor (with A. Swami, Q. Zhao, and L. Tong) of the book *Wireless Sensor Networks: Signal Processing and Communications Perspectives*, published by Wiley in 2007, and is a coauthor (with W.-J. Huang and C.-C. Jay Kuo) of the book *Cooperative Communications and Networking: Technologies and System Design*. He is also a guest editor of *EURASIP Special Issue on Cooperative MIMO Multicell Networks* and of *IJSNET Special Issue on Advances in Theory and Applications of Wireless, Ad Hoc, and Sensor Networks*. He is currently an Associate Editor for IEEE TRANSACTIONS ON SIGNAL PROCESSING and IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.



Xiangyun Zhou (S'08–M'11) is a lecturer at the Australian National University (ANU), Australia. He received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the ANU in 2007 and 2010, respectively. From June 2010 to June 2011, he worked as a postdoctoral fellow at UNIK—University Graduate Center, University of Oslo, Norway. His research interests are in the fields of communication theory and wireless networks.

Dr. Zhou serves on the editorial board of *Security and Communication Networks Journal* (Wiley) and *Ad Hoc & Sensor Wireless Networks Journal*. He has also served as the TPC member of major IEEE conferences. He is a recipient of the Best Paper Award at the 2011 IEEE International Conference on Communications.