

Secrecy Analysis on Network Coding in Bidirectional Multibeam Satellite Communications

Ashkan Kalantari *Student Member, IEEE*, Gan Zheng *Senior Member, IEEE*,
Zhen Gao *Member, IEEE*, Zhu Han *Fellow, IEEE*,
and Björn Ottersten, *Fellow, IEEE*

Abstract—Network coding is an efficient means to improve the spectrum efficiency of satellite communications. However, its resilience to eavesdropping attacks is not well understood. This paper studies the confidentiality issue in a bidirectional satellite network consisting of two mobile users who want to exchange message via a multibeam satellite using the XOR network coding protocol. We aim to maximize the sum secrecy rate by designing the optimal beamforming vector along with optimizing the return and forward link time allocation. The problem is non-convex, and we find its optimal solution using semidefinite programming together with a 1-D search. For comparison, we also solve the sum secrecy rate maximization problem for a conventional reference scheme without using network coding. Simulation results using realistic system parameters demonstrate that the bidirectional scheme using network coding provides considerably higher secrecy rate compared to that of the conventional scheme.

Index Terms—Physical layer security, network coding, bidirectional satellite communications, secrecy rate, semidefinite programming.

I. INTRODUCTION

Satellite communications (SATCOM) is getting more and more integrated into communication networks to compliment the current terrestrial communication systems. Satellite services have to support increasing demands for data transfer. To realize bidirectional satellite communications, traditionally orthogonal resources either in frequency or time domain should be used to avoid interference between users. To save the precious wireless resources, network coding has been used in this work as an efficient protocol to exchange information

between two mobile satellite users. The basic principle is that the received information from users are combined on the satellite or gateway (GW), and then the mixed signal is broadcast to users at the same time and using the same frequency. Because each user can subtract its own message, it can easily decode the message from the other user.

However, due to the broadcast nature and immense area coverage, satellite communications systems, e.g., in military and commercial applications, are vulnerable to security attacks such as eavesdropping. Currently, security in SATCOM is achieved at upper layers by means of encryption such as the Advanced Encryption Standard [1], [2]. Nevertheless, traditional security is based on the assumption of limited computational capability of the malicious nodes, and thus there exists the risk that a malicious node can successfully break an encryption, and get access to sensitive satellite data [3]. In contrast to the upper layer encryption techniques, recently there has been significant interest in securing wireless communications at the physical layer using an information-theoretic approach named “*secrecy rate*” [4]. The main advantage of this approach is that the malicious nodes cannot even get access to protected information regardless of their computational capabilities.

While network coding can greatly improve the system throughput, whether it is more secure than the conventional scheme, which does not use network coding, is largely unknown in SATCOM. In this work, we will leverage the physical layer security approach to address the confidentiality issue in bidirectional SATCOM using the principle of network coding. Below, we provide an overview on the applications of network coding to SATCOM and the related work in the physical layer security literature.

A. Literature Review

1) *Network coding related works*: Network coding technique, first introduced in [5], can considerably reduce delay, processing complexity and power consumption, and can significantly increase the data rate and robustness [6]. In the popular XOR network coding scheme, the received signals at an intermediate node are first decoded into bit streams, and then XOR is applied on the bit streams to combine them. The processed bits are re-encoded and then broadcast. Utilization of network coding has been studied in both terrestrial and satellite networks. The authors in [7] apply superposition coding and XOR network coding to a bidirectional terrestrial relay

Copyright (c) 2013 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org

This work was supported by the National Research Fund (FNR) of Luxembourg under AFR grant for the project “Physical Layer Security in Satellite Communications (ref. 5798109)”, SeMIGod, the National Natural Science Foundation of US (Grant No. CCF-1456921, CMMI-1434789, CNS-1443917, and ECCS-1405121), and the National Natural Science Foundation of China (Grant No. 61428101).

Ashkan Kalantari and Björn Ottersten are with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), The University of Luxembourg, 4 rue Alphonse Wecker, L-2721 Luxembourg-Kirchberg, Luxembourg, E-mails: ashkan.kalantari@uni.lu, bjorn.ottersten@uni.lu.

Gan Zheng is with the School of Computer Science and Electronic Engineering, University of Essex, UK, E-mail: ganzheng@essex.ac.uk. He is also affiliated with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg.

Zhen Gao is with School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China, Email: zgao@tju.edu.cn.

Zhu Han is with the Electrical and Computer Engineering Department, University of Houston, USA, E-mail: zhan2@uh.edu.

network. A multi-group multi-way terrestrial relay network is considered in [8] where superposition coding and XOR network coding are investigated and compared to each other. Network coding can also considerably improve the spectral efficiency in bidirectional SATCOM in which two mobile users exchange information via the satellite. The work in [9] compares the amplify-and-forward (AF) method with the XOR network coding scheme in a satellite scenario. A joint delay and packet drop rate control protocol without the knowledge of lost packets for mobile satellite using network coding is studied in [10]. In [11], buffers are designed for satellites when the network coding scheme is employed. Random linear network coding is used in [12] to minimize the packet delivery time. Satellite beam switching for mobile users is tackled in [13] where the network coding scheme increases the robustness in delivery of the packets when mobile terminals move from beam to beam. The XOR network coding protocol is demonstrated in a satellite test bed in [14].

2) *Physical layer security related works:* Wyner in [4] first showed that secure transmission is possible for the legitimate user given the eavesdropper receives noisier data compared to the legitimate receiver. Inspired by Wyner's work, [15] extended the idea of physical layer secrecy rate from the discrete memoryless wiretap channel to Gaussian wiretap channel. The Wyner's wiretap channel was generalized in [16] to the broadcast channel. After the seminal works done in [4], [15], [16], there have been substantial amount of works in physical layer secrecy. Here, we only review those most relevant to network coding and bidirectional communications. The authors in [17] consider a relay utilizing the XOR network coding protocol where joint relay and jammer selection is done to enhance the secrecy rate. A bidirectional AF relay network with multiple-antenna nodes is considered in [18] where the relay beamforming vector is designed by the waterfilling method to improve the secrecy rate. The authors in [19] consider random relay selection in a bidirectional network in which the relay performs both data transmission and jamming the eavesdropper at the same time to increase the secrecy. The work in [20] performs selection over AF relays and jammers in a bidirectional network for the single-antenna case, and precoding in the multiple-antenna case to enhance the secrecy. To maximize the secrecy in a bidirectional network, the authors in [21] consider the location and distribution of nodes while joint relay and jammer selection is performed. Distributed beamforming along with artificial noise and beamforming is studied in [22] for a bidirectional AF relay network. The work in [23] designs the distributed beamforming weights for a bidirectional network where one intermediate node acts as a jammer. In contrast to the terrestrial literature, there are very few works in physical layer security for SATCOM. The problem of minimizing the transmit power on a multibeam satellite while satisfying a minimum per user secrecy rate is studied in [24]. Iterative algorithms are used to jointly optimize the transmission power and the beamforming vector by perfectly nulling the received signal at the eavesdropper. Both optimal and suboptimal solutions are developed in [25] where the use of artificial noise is also studied.

Despite the physical layer security and network coding

works in the terrestrial and SATCOM scenarios, some un-addressed issue are left. In [7], only downlink bottlenecks are considered when designing the beamforming weights for the XOR network coding case. The uplink bottlenecks also need to be considered when optimizing the uplink-downlink time allocation. In [8], the authors consider the decoding-re-encoding and designing the beamforming vector separately. The works in [19], [21] consider single-antenna relay where the AF protocol is used in a bidirectional network. The authors in [18], [22], [23] use the analog network coding protocol in a two-way relay network to facilitate secure information exchange between two users. Furthermore, the mentioned terrestrial works in physical layer security for bidirectional communications assume one eavesdropper in the environment. The works in [24], [25] design the beamforming weights for unidirectional service for fixed users in the forward link (FL).

B. Our Contribution

In this work, we study the network coding based bidirectional SATCOM in which two mobile users exchange data via a transparent multibeam satellite in the presence of two eavesdroppers. There is an eavesdropper present for each user who overhears the bidirectional communications. The users employ omnidirectional antennas and the communication is prone to eavesdropping in both the return link (RL) and FL. In the RL, two users send signals using two orthogonal frequency channels; the signals collected by the satellite are passed to the GW, where they are decoded, XOR-ed and then the produced stream is re-encoded. This combined stream is multiplied by the beamforming vector which contains the designed weight of each feed. Consequently, each element of the resultant vector is transmitted to the satellite using the feeder link. Each element which includes both the feed weight and the data signal is applied to the corresponding feed to adjust the beams for broadcasting to both users simultaneously in the FL. This scheme is more power-efficient than the conventional method where network coding is not utilized and the power is splitted into two data streams. This benefit is extremely vital for SATCOM because of the limited on-board power.

Our main contributions in this work are summarized below to differentiate it from the prior work:

- 1) We incorporate XOR network coding into SATCOM in order to enable both efficient and secure bidirectional data exchange.
- 2) The end-to-end sum secrecy rate is first derived, and then maximized by designing the optimal beamforming vector and the RL and FL time allocation. The optimization problem regarding the beamforming vector is solved using semi-definite programming (SDP) along with 1-D search.
- 3) We provide comprehensive simulation results to demonstrate the advantage of the bidirectional scheme over the conventional scheme using realistic SATCOM parameters.

The remainder of the paper is organized as follows. In Section II, we introduce the SATCOM network topology as well as deriving the signal model and defining the secrecy

rates. The problems for maximizing the sum secrecy rate are defined and solved in Section III. In Section IV, numerical results are presented. The conclusion is drawn in Section V.

Notation: Upper-case and lower-case bold-faced letters are used to denote matrices and column vectors, respectively. Superscripts $(\cdot)^T$ and $(\cdot)^H$ represent transpose and Hermitian operators, respectively. $\mathbf{I}_{N \times N}$ denotes an N by N identity matrix. $\mathcal{CN}(\mathbf{m}, \mathbf{K})$ denotes the complex Gaussian distribution with mean vector \mathbf{m} and covariance matrix \mathbf{K} . $\lambda_{\max}(\mathbf{A}, \mathbf{B})$ is the maximum eigenvalue of the matrix pencil (\mathbf{A}, \mathbf{B}) . $\mathbf{A} \succeq \mathbf{0}$ means that the Hermitian matrix \mathbf{A} is positive semidefinite. $\|\cdot\|$ is the Frobenius norm and $|\cdot|$ represents the absolute value of a scalar.

II. SYSTEM MODEL

Consider a satellite communication system comprised of two users denoted by U_1 and U_2 who exchange information with each other, one multibeam transparent satellite denoted by S , one GW, two eavesdroppers denoted by E_1 and E_2 as depicted in Fig. 1. Users are located in different beams of the satellite, and they transmit the RL signals using different frequency channels simultaneously. We assume that each user and each eavesdropper is equipped with a single omnidirectional antenna. Because of the long distance between the users, there is no direct link between them; furthermore, eavesdroppers cannot cooperate and E_i can only overhear U_i for $i = 1, 2$. Contemporary orbiting satellites such as *ICO*, *SkyTerra*, and *Thuraya* have limited power, here defined as P_S , and some of them do not have the on-board processing ability to decode the received messages or perform on-board beamforming, so they have to forward the received signal to the GW to get it processed [26]–[28]. Using the GW to process the signal and designing the feed weights is referred to as the ground-based beamforming technique. The ground-based beamforming technique is perceived as the most convenient and economical approach [28]. In this paper, we consider a commercial satellite without digital processing ability and follow the ground-based beamforming paradigm.

In our satellite network model, we assume that the eavesdropper is a regular user which is part of the network. However, it is considered as an unintended user, potential eavesdropper, which the information needs to be kept secret from it. Due to the fact that the eavesdropper is part of the network, it is possible to estimate the channels to it. Hence, similar to the works [29]–[33], we assume that the eavesdropper's channel state information (CSI) is known. Based on the mentioned assumption, we assume that the users and eavesdropper know all the CSIs. Further, all communication channels are known and fixed during the period of communication. It is worth mentioning that in the secrecy rate analysis of XOR network coding, only the CSI of the eavesdroppers in the RL is required. Although we assume the availability of the eavesdropper's CSI, there are methods such as null-space artificial noise transmission [34], random beamforming [35]–[37], or effective channel coding design to strengthen the cryptography [38] in order to sustain secrecy without having the knowledge of the eavesdropper's CSI. Another alternative

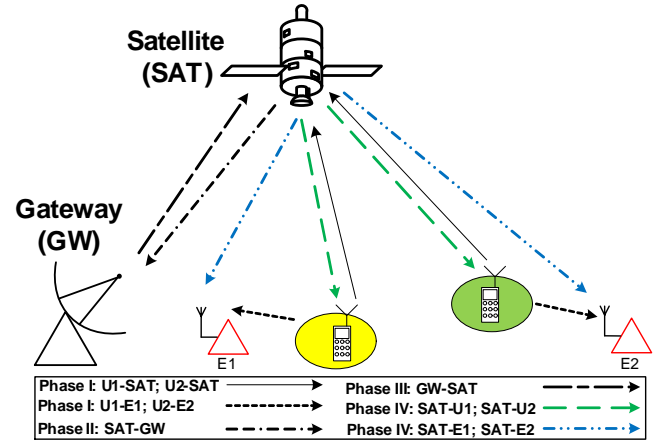


Fig. 1. Bidirectional satellite communication network.

can be using the statistical knowledge of the eavesdropper's CSI in order to improve the secrecy [39]–[42]. Also, the interference alignment technique can be used along with statistical knowledge of the eavesdropper's CSI to enhance the secrecy [43]. In the situations when the geographical area of the eavesdropper is known, the worst-case scenario can be considered. In this scenario, the best CSI from the user to the eavesdropper's area is considered for the design. One possible example for the worst-case scenario can be when the occupied zone by the enemy is known. This example can be one of the applications of this paper.

To acquire the RL channel state information (CSI) at the GW, the users send the pilot signals along with the data toward the satellite. For the FL CSI, the GW sends pilots to the users. Afterwards, the estimated CSI by the users is sent back to the GW. Therefore, getting the FL CSI takes more time compared to the RL CSI [44]. The GWs are equipped with advanced transceivers and antennas and because of this reason, the communication link between the GW and the satellite (feeder link) is modeled as an ideal link. Hence, similar to the works [27], [45]–[48] which are carried out in the satellite communications literature, we assume that the channel between the satellite and the GW, which is referred to as the feeder link, is ideal with abundant bandwidth.

The complete communication phases of the network coding based scheme are summarized in Table I. The conventional scheme without using network coding is also included for comparison and details are given in Section II-B. The first two phases for the RL are the same for both schemes while the main difference lies in the FL transmission. In the conventional scheme, signals are sent in different time slots for each user in the FL, so this scheme has less available transmission time for each user. In the bidirectional scheme, signal streams are combined, and then sent in the FL using the XOR network coding protocol, therefore, the spectral efficiency is significantly improved compared to the conventional scheme.

A. Network coding based bidirectional SATCOM

1) *Signal model:* In this case, the whole communication takes place in four phases. In Phase I, both users transmit

TABLE I
COMMUNICATION STAGES FOR THE XOR NETWORK CODING AND THE
CONVENTIONAL SCHEMES.

Conventional reference scheme	XOR network coding scheme
Phase I: U_1 and U_2 simultaneously send their signals, s_1 and s_2 , to the satellite while they are overheard by E_1 and E_2 , respectively.	
Phase II: The satellite passes the received signal to the gateway for processing. At the gateway, the users signals are separately decoded.	
Phase III: The intended signal for U_1 , decoded s_2 , is re-encoded at the gateway and the corresponding feed weights are designed. Then, the feed weights multiplied by the data signal are sent to the satellite.	Phase III: The gateway applies XOR operation on the decoded streams from s_1 and s_2 to create a merged stream of bits and the feed weights are designed. Then, the feed weights multiplied by the data signal are sent to the satellite.
Phase IV: The satellite passes the re-encoded signal through the corresponding beam to U_1 while E_1 is listening to it.	
Phase V: The intended signal for U_2 , decoded s_1 , is re-encoded at the gateway and the corresponding feed weights are designed. Then, the feed weights multiplied by the data signal are sent back to the satellite.	Phase IV: The satellite broadcasts the merged stream toward the users through the corresponding beams which is wiretapped by both E_1 and E_2 .
Phase VI: The satellite passes the re-encoded signal through the corresponding beam to U_2 while E_2 is listening to it.	

signals using different frequencies simultaneously. The signals received at the satellite and the eavesdroppers are

$$\mathbf{y}_{S_1} = \sqrt{P_{U_1}} \mathbf{h}_{U_1,S} s_1 + \mathbf{n}_{S_1}, \quad (1)$$

$$\mathbf{y}_{S_2} = \sqrt{P_{U_2}} \mathbf{h}_{U_2,S} s_2 + \mathbf{n}_{S_2}, \quad (2)$$

$$\mathbf{y}_{E_1}^{RL} = \sqrt{P_{U_1}} h_{U_1,E_1} s_1 + n_{E_1}, \quad (3)$$

$$\mathbf{y}_{E_2}^{RL} = \sqrt{P_{U_2}} h_{U_2,E_2} s_2 + n_{E_2}, \quad (4)$$

where P_{U_i} is the transmitted power by the users for $i = 1, 2$, h and \mathbf{h} represent the user-eavesdropper and user-satellite channels, respectively, and the corresponding source and destination are denoted by the subscript. The channel for the satellite is a $N_S \times 1$ vector where N_S is the number of the satellite feeds. Additive white Gaussian noises (AWGN) are denoted by n and \mathbf{n} with $n \sim \mathcal{CN}(0, \sigma^2)$ and $\mathbf{n} \sim \mathcal{CN}(\mathbf{0}, \sigma^2 \mathbf{I}_{N_S \times N_S})$, respectively. We consider the noise power for users, satellite and eavesdroppers as KTB , where K is the Boltzman's constant which is -226.8 dBW/K/Hz, T is the on-board temperature and B is the carrier bandwidth. We assume that s_1 and s_2 are independent and identically distributed (i.i.d.) Gaussian random source signals with zero mean and unit variance. For convenience, we use the noise variance, σ^2 , instead of KTB and omit the bandwidth, B , in the rate expressions throughout the paper. Note that we consider different temperatures for ground nodes and the satellite. The satellite forwards the received signal to the GW using the

feeder link in Phase II and thanks to the ideal link between the satellite and the GW, the same signals as (1) and (2) are present at the GW to be processed.

At the GW, the received signal is filtered and users' data are separated and decoded into two bit streams denoted by x_1 and x_2 , respectively. The GW applies the bit-wise XOR algebraic operation to the decoded bit streams of the users to get the combined stream

$$x_{GW} = x_1 \oplus x_2. \quad (5)$$

Note that before applying the XOR network coding, the GW uses zero-padding to add zeros to the shorter bit stream in order to make equal length bit streams out of the two different bit streams sent by the users [49], [50]. In Phase III, x_{GW} is encoded into s_{GW} with unit power, and then multiplied by the beamforming vector, \mathbf{w} . Using the ideal feeder link, each element, $w_i s_{GW}(t)$, of the produced vector, $\mathbf{w} s_{GW}$, at the GW which both includes the feed weight, w_i , and the data signal, s_{GW} , is transmitted from the GW to the satellite. Since the codebook used at the GW to encode x_{GW} can be different in the XOR network coding scheme, the RL and FL transmission times are generally different for the XOR network coding. The received signal by satellite is denoted as $\mathbf{s}_S = \mathbf{H}_{GW,S} \mathbf{w} s_{GW}$. The model $\mathbf{s}_S = \mathbf{H}_{GW,S} \mathbf{w} s_{GW}$ encapsulates the process of transmitting each element of the vector $\mathbf{w} s_{GW}$ from the GW to the satellite. Since the feeder link is considered to be ideal, $\mathbf{H}_{GW,S}$ is a $N_S \times N_S$ identity matrix. Finally, in Phase IV, each feed weight designed at the gateway, which includes the data signal, is applied to the corresponding feed at the satellite. Hence, the beams are adjusted and the signal \mathbf{s}_S is broadcast through the antennas. The received signals at two users are, respectively,

$$\mathbf{y}_{U_1}^{FLXOR} = \mathbf{h}_{S,U_1}^T \mathbf{s}_S + n_{U_1}, \quad (6)$$

$$\mathbf{y}_{U_2}^{FLXOR} = \mathbf{h}_{S,U_2}^T \mathbf{s}_S + n_{U_2}. \quad (7)$$

Similarly, the received signals at the eavesdroppers in Phase IV are, respectively,

$$\mathbf{y}_{E_1}^{FLXOR} = \mathbf{h}_{S,E_1}^T \mathbf{s}_S + n_{E_1}, \quad (8)$$

$$\mathbf{y}_{E_2}^{FLXOR} = \mathbf{h}_{S,E_2}^T \mathbf{s}_S + n_{E_2}. \quad (9)$$

In the following, we shall define the sum secrecy rate. We first introduce the users' rates and eavesdroppers' channel capacities.

2) *Users' RL rates:* Consider t_1 and t_2 for the RL (Phase I) and FL (Phase IV) transmission time, respectively. In Phase I, we can characterize the RL rates ($R_{U_1}^{RL}, R_{U_2}^{RL}$) by the following equations [51, Chapter 5]:

$$R_{U_1}^{RL} \leq I_{U_1}^{RL} = t_1 \log \left(1 + \frac{P_{U_1} \|\mathbf{h}_{U_1,S}\|^2}{\sigma_S^2} \right) \quad (10)$$

$$R_{U_2}^{RL} \leq I_{U_2}^{RL} = t_1 \log \left(1 + \frac{P_{U_2} \|\mathbf{h}_{U_2,S}\|^2}{\sigma_S^2} \right), \quad (11)$$

where I denotes channel capacity or the maximum supported rate and R is the maximum achievable rate.

3) *Users' FL rates:* After receiving the FL signal, users decode s_S . As each user knows its own transmitted bits, it can use the XOR operation to retrieve the intended bits. Subsequently, using (6) and (7), the FL rates can be expressed as

$$R^{FL_{XOR}} = \min \left\{ I_{U_1}^{FL_{XOR}}, I_{U_2}^{FL_{XOR}} \right\}, \quad (12)$$

$$I_{U_1}^{FL_{XOR}} = t_2 \log \left(1 + \frac{|\mathbf{h}_{S,U_1}^T \mathbf{w}|^2}{\sigma_{U_1}^2} \right), \quad (13)$$

$$I_{U_2}^{FL_{XOR}} = t_2 \log \left(1 + \frac{|\mathbf{h}_{S,U_2}^T \mathbf{w}|^2}{\sigma_{U_2}^2} \right). \quad (14)$$

Since the data for both users have gone through a bit-wise XOR operation at the GW and a combined signal is broadcast, the GW has to adjust the combined signal's data rate to match both users' channel capacities. This rate should be equal to the minimum FL channel rate between the satellite and the users in Phase IV before sending s_S to the satellite.

4) *Eavesdroppers' channel capacities:* Using (3) and (8), the channel capacity from U_1 to E_1 , $I_{E_1}^{RL}$, and from satellite to E_1 , $I_{E_1}^{FL_{XOR}}$, can be expressed, respectively, as

$$I_{E_1}^{RL} = t_1 \log \left(1 + \frac{P_{U_1} |h_{U_1,E_1}|^2}{\sigma_{E_1}^2} \right), \quad (15)$$

$$I_{E_1}^{FL_{XOR}} = t_2 \log \left(1 + \frac{|\mathbf{h}_{S,E_1}^T \mathbf{w}|^2}{\sigma_{E_1}^2} \right). \quad (16)$$

The channel capacities for E_2 can be derived in a similar way.

5) *Secrecy rate definition:* First, we derive the the secrecy rate for the RLs and FLs, and then the end-to-end secrecy rate. In [52], the result of [4] is extended to fading channels with multiple-antenna transmitter, receiver, and eavesdropper. Using the special case of the result in [52] for single-antenna transmitter, multiple-antenna receiver, and single-antenna eavesdropper along with employing (10) and (15), the secrecy rate for the RL of U_1 is calculated as

$$SR_{U_1}^{RL} = I_{U_1}^{RL} - I_{E_1}^{RL}, \quad (17)$$

where the notation "SR" means "secrecy rate".

To calculate the secrecy rate in the FL, first, we derive the information that E_1 can recover during the RL transmission in Lemma 1.

Lemma 1: Independent of getting a positive or zero secrecy rate defined for the RL of U_1 in (17), E_1 cannot recover any bits from U_2 transmitted message using the FL transmission.

Proof: To recover bits from U_2 , E_1 has to apply XOR operation between the bits recovered from U_1 in the RL transmission and the bits derived from the satellite broadcast in the FL transmission. Hence, the information detected by E_1 in the FL depends on the bits recovered from U_1 in the RL transmission. The recovered bits from U_1 in the RL depend on the sign of the secrecy rate defined in (17). The sign of the RL secrecy rate in (17) has the following possibilities:

- 1) If $I_{U_1}^{RL} - I_{E_1}^{RL} > 0$, then U_1 can establish a perfectly secured connection so that the eavesdropper cannot get any bits from U_1 in the RL [52]. Hence, E_1 does not

have the bits transmitted by U_1 in the RL and it cannot recover any bits from U_2 using the FL transmission.

- 2) If $I_{U_1}^{RL} - I_{E_1}^{RL} \leq 0$, then the secrecy rate is zero. Therefore, U_1 cannot establish a secure connection in the RL. In this case, U_1 remains silent during the corresponding time slot. In this time slot, GW generates random bits instead of the bits from U_1 and applies XOR between them and the bits from U_2 . As a result, E_1 cannot recover any bits from U_2 using the FL transmission.

Note that since the RL time, t_1 , is always positive and all the channels are known, the sign of the expression $I_{U_1}^{RL} - I_{E_1}^{RL}$ is known prior to the beamformer design. ■

A similar argument as in Lemma 1 can be applied to E_2 .

Consequently, using Lemma 1, the secrecy rate for the FL is given in Lemma 2.

Lemma 2: Assume that there exists at least one RL with a positive secrecy rate. Then, the secrecy rate in the FL is given as below:

$$SR^{FL_{XOR}} = \begin{cases} \min \left\{ I_{U_1}^{FL_{XOR}}, I_{U_2}^{FL_{XOR}} \right\} & SR_{U_1}^{RL} > 0, \\ & SR_{U_2}^{RL} > 0, \\ I_{U_1}^{FL_{XOR}} & SR_{U_1}^{RL} = 0, \\ & SR_{U_2}^{RL} > 0, \\ I_{U_2}^{FL_{XOR}} & SR_{U_1}^{RL} > 0, \\ & SR_{U_2}^{RL} = 0. \end{cases} \quad (18)$$

Proof: Excluding the case that both RLs have zero secrecy rate, i.e., the total secrecy rate is zero, the secrecy rate for the FL transmission for different signs of the secrecy rate in the RL is given as follows:

- 1) If $SR_{U_1}^{RL} > 0$ and $SR_{U_2}^{RL} > 0$, then according to Lemma 1, E_1 and E_2 cannot wiretap any bits from U_2 and U_1 , respectively, using the FL transmission. Therefore, using (12), the secrecy rate in the FL is $\min \left\{ I_{U_1}^{FL_{XOR}}, I_{U_2}^{FL_{XOR}} \right\}$.
- 2) If $SR_{U_1}^{RL} > 0$ and $SR_{U_2}^{RL} = 0$, then according to Lemma 1, E_1 cannot wiretap any bits from U_2 using the FL transmission. Further, since the RL of U_2 is not secure, U_2 does not transmit and E_2 does not get any bits from U_2 . Hence, E_2 cannot recover bits from U_1 using the FL transmission. Since U_1 is not expected to receive any message because of $SR_{U_2}^{RL} = 0$, the FL secrecy rate is $I_{U_2}^{FL_{XOR}}$.
- 3) If $SR_{U_1}^{RL} = 0$ and $SR_{U_2}^{RL} > 0$, similar to the procedure as in Case 2, the secrecy rate in the FL is $I_{U_1}^{FL_{XOR}}$.

According to the results in Cases 1, 2, and 3, the secrecy rate of the FL is derived as in (18). ■

According to Lemma 2, when the XOR protocol is used, the FLs are totally secured. Note that for the Cases 2 and 3, the GW creates random bits instead of the message from the user with insecure link, i.e., zero secrecy rate in the RL. Then, the GW applies XOR between the received message from the user which has a positive secrecy rate in the RL and the randomly generated bits. This way, the eavesdropper still receives a

combined message when the secrecy rate is zero in one of the RLs.

To derive the end-to-end secrecy rate for U_1 , we invoke Theorem 1 in [53], which states that, when decoding and re-encoding is performed by an intermediate node, the secrecy rate of each hop needs to be taken into account as a bottleneck to derive the end-to-end secrecy rate. Since decoding and re-encoding is performed at the GW, the result of Theorem 1 in [53] can be applied. Consequently, using the mentioned theorem and the secrecy rate derived in (17) and the result of Lemma 2 in (18), the end-to-end secrecy rate for U_1 is calculated by

$$SR_{U_1}^{XOR} = \min \{SR_{U_1}^{RL}, SR_{U_1}^{FLXOR}\}. \quad (19)$$

The end-to-end secrecy rate for U_2 can be derived in a similar way. The sum end-to-end secrecy rate is expressed as

$$SR^{XOR} = SR_{U_1}^{XOR} + SR_{U_2}^{XOR}. \quad (20)$$

B. Conventional SATCOM

A conventional scheme without using network coding is described here as a performance benchmark.

1) *Signal model*: As shown in Table I, the Phases I and II are the same for the conventional and the XOR network coding schemes, which result in the same signal model for both schemes. In Phases III and V, the GW sends back each element of the processed \mathbf{s}_2 and \mathbf{s}_1 to the satellite, respectively, using the ideal feeder link where \mathbf{s}_1 and \mathbf{s}_2 are $N_S \times 1$ vectors containing both the feed weights and the users' data signals. \mathbf{s}_1 and \mathbf{s}_2 are defined as $\mathbf{s}_1 = \mathbf{w}_1 \hat{\mathbf{s}}_1$ and $\mathbf{s}_2 = \mathbf{w}_2 \hat{\mathbf{s}}_2$, where $\hat{\mathbf{s}}_1$ and $\hat{\mathbf{s}}_2$ are the decoded and re-encoded versions of the data signals received from U_1 and U_2 at the GW with unit power, and \mathbf{w}_1 and \mathbf{w}_2 are beamforming vectors to be designed at the GW. Note that since different Gaussian codebooks are used at the GW to re-encode the signals for U_1 and U_2 , the generated signals at the GW are different from those received from the users. Therefore, generated signals at the GW are shown by $\hat{\mathbf{s}}_1$ and $\hat{\mathbf{s}}_2$.

The satellite applies each component of the vector \mathbf{s}_2 , containing the feed weight multiplied by the data signal, to the corresponding feed. Then, the beam is adjusted and $\hat{\mathbf{s}}_2$ is sent toward U_1 in Phase IV, and the received signals at U_1 and E_1 are, respectively,

$$y_{U_1}^{FLCon} = \mathbf{h}_{S,U_1}^T \mathbf{s}_2 + n_{U_1}, \quad (21)$$

$$y_{E_1}^{FLCon} = \mathbf{h}_{S,E_1}^T \mathbf{s}_2 + n_{E_1}. \quad (22)$$

Similarly, at the end of Phase VI, the received signals at U_2 and E_2 are, respectively,

$$y_{U_2}^{FLCon} = \mathbf{h}_{S,U_2}^T \mathbf{s}_1 + n_{U_2}, \quad (23)$$

$$y_{E_2}^{FLCon} = \mathbf{h}_{S,E_2}^T \mathbf{s}_1 + n_{E_2}. \quad (24)$$

The beamformer weights in the conventional scheme are exclusively designed at the GW for each user. Hence, when data is being transmitted for U_1 , the satellite's main lobe is focused toward U_1 . Since E_2 is outside the beam directed toward U_1 and the beamformers are designed to maximize the

signal strength toward U_1 , E_2 receives the signal from side lobes. As a result, the signal received by E_2 is weak. Similar conditions hold for E_1 when transmitting to U_2 . To make the derivation tractable, we neglect these weak signals received by E_2 and E_1 in Phases IV and VI, respectively. As a result, the sum secrecy rate derived for the conventional scheme shall be an upper-bound.

2) *Users' rates*: The RL rates for the conventional SATCOM are the same as the XOR network coding scheme in (10) and (11). Using (21) and (23), the FL rates to U_1 and U_2 after self-interference cancellation can be derived, respectively, as

$$I_{U_1}^{FLCon} = t_2 \log_2 \left(1 + \frac{|\mathbf{h}_{S,U_1}^T \mathbf{w}_2|^2}{\sigma_{U_1}^2} \right), \quad (25)$$

$$I_{U_2}^{FLCon} = t_3 \log_2 \left(1 + \frac{|\mathbf{h}_{S,U_2}^T \mathbf{w}_1|^2}{\sigma_{U_2}^2} \right). \quad (26)$$

In order to make the conventional method comparable to the bidirectional one, we assume that the total available transmission time for both the network coding and the conventional schemes are the same. In other words, the RL time for the users is t_1 and the FL for U_1 and U_2 are t_2 and $t_3 = 1 - t_1 - t_2$, respectively.

3) *Eavesdroppers' channel capacities*: The RL capacities for E_1 and E_2 in the conventional SATCOM are the same as the ones derived for the XOR network coding scheme. Using (22) and (24), the FL capacity from the satellite toward E_1 and E_2 to overhear the signals sent in Phases IV and VI, respectively, are

$$I_{E_1}^{FLCon} = t_2 \log_2 \left(1 + \frac{|\mathbf{h}_{S,E_1}^T \mathbf{w}_2|^2}{\sigma_{E_1}^2} \right), \quad (27)$$

$$I_{E_2}^{FLCon} = t_3 \log_2 \left(1 + \frac{|\mathbf{h}_{S,E_2}^T \mathbf{w}_1|^2}{\sigma_{E_2}^2} \right). \quad (28)$$

4) *Secrecy rate definition*: The RL secrecy rate for U_1 and U_2 are the same as the XOR network coding scheme in Section II-A5. In the conventional scheme, the messages that E_1 receives in the RL and FL are different and can be decoded independently. Hence, the FL secrecy rate for U_1 can be defined using (25), (27) and the result from [52] as

$$SR_{U_1}^{FLCon} = I_{U_1}^{FLCon} - I_{E_1}^{FLCon}. \quad (29)$$

Utilizing (17), (29), and Theorem 1 in [53], the end-to-end secrecy rate for U_1 is derived as

$$SR_{U_1}^{Con} = \min \{SR_{U_1}^{RL}, SR_{U_1}^{FLCon}\}. \quad (30)$$

The end-to-end secrecy rate for U_2 can be defined in a similar way. Like in Section II-A5, the sum secrecy rate is

$$SR^{Con} = SR_{U_1}^{Con} + SR_{U_2}^{Con}. \quad (31)$$

III. PROBLEM FORMULATION AND THE PROPOSED SOLUTION

In this section, we study the problem of maximizing the sum secrecy rate by optimizing the precoding vectors at the GW to shape the satellite beams along with the RL and FL

time allocation, given the maximum available power P_S at the satellite. We consider both the XOR network coding and the conventional schemes. For the XOR network coding, we just solve the optimal beamformer design for the secrecy rate derived from the first case of the FL secrecy rate in (18). The solutions for the optimal beamformer design for the other two cases of (18) are similar to the first case of (18).

A. Network coding for bidirectional SATCOM

Using the sum secrecy rate defined in (20), the optimization problem for the XOR network coding scheme is defined as

$$\begin{aligned} \max_{\mathbf{w}, t_1, t_2} \quad & \min \left\{ I_{U_1}^{RL} - I_{E_1}^{RL}, \min \left\{ I_{U_1}^{FLXOR}, I_{U_2}^{FLXOR} \right\} \right\} \\ & + \min \left\{ I_{U_2}^{RL} - I_{E_2}^{RL}, \min \left\{ I_{U_1}^{FLXOR}, I_{U_2}^{FLXOR} \right\} \right\} \\ \text{s.t.} \quad & t_1 + t_2 = 1, \\ & \|\mathbf{w}\|^2 \leq P_S. \end{aligned} \quad (32)$$

To transform (32) into a standard convex form, we apply the following procedures. First, we assume that t_1 and t_2 are fixed and study the beamforming design. After designing the optimal beamformer, the optimal time allocation is found by performing 1-D search of t_1 over the range $(0, 1)$. Second, after considering a fixed transmission time for the RL and FL, the RL secrecy rate expressions in (32) are fixed and can be dropped without loss of generality. Hence, (32) boils down into

$$\begin{aligned} \max_{\mathbf{w}} \quad & \min \left\{ I_{U_1}^{FLXOR}, I_{U_2}^{FLXOR} \right\} \\ \text{s.t.} \quad & \|\mathbf{w}\|^2 \leq P_S. \end{aligned} \quad (33)$$

Next, we introduce the auxiliary variable u to remove the “min” operators. Then, (33) yields

$$\begin{aligned} \max_{\mathbf{w}, u > 0} \quad & u \\ \text{s.t.} \quad & \|\mathbf{w}\|^2 \leq P_S, \\ & \sigma_{U_1}^2 \left(2^{\frac{u}{t_2}} - 1 \right) \leq |\mathbf{h}_{S,U_1}^T \mathbf{w}|^2, \\ & \sigma_{U_2}^2 \left(2^{\frac{u}{t_2}} - 1 \right) \leq |\mathbf{h}_{S,U_2}^T \mathbf{w}|^2. \end{aligned} \quad (34)$$

The last two constraints in (34) are not convex. By introducing $\mathbf{W} = \mathbf{w}\mathbf{w}^H$, we rewrite (34) as

$$\begin{aligned} \max_{\mathbf{W} \succeq 0, u > 0} \quad & u \\ \text{s.t.} \quad & \text{tr}(\mathbf{W}) \leq P_S, \\ & \sigma_{U_1}^2 \left(2^{\frac{u}{t_2}} - 1 \right) \leq \text{tr}(\mathbf{W}\mathbf{A}), \\ & \sigma_{U_2}^2 \left(2^{\frac{u}{t_2}} - 1 \right) \leq \text{tr}(\mathbf{W}\mathbf{B}), \end{aligned} \quad (35)$$

where $\mathbf{A} = \mathbf{h}_{S,U_1}^* \mathbf{h}_{S,U_1}^T$ and $\mathbf{B} = \mathbf{h}_{S,U_2}^* \mathbf{h}_{S,U_2}^T$. The rank constraint, $\text{rank}(\mathbf{W}) = 1$, in (35) is dropped. The optimal beamforming weight in (35) is designed for the FL transmission. However, since the RL secrecy rates, which can be bottlenecks for the total end-to-end secrecy rate, are not considered in (35), extra unnecessary power at the satellite

may be utilized. To fix this, one last constraint is added to (35) to get

$$\begin{aligned} \max_{\mathbf{W} \succeq 0, u > 0} \quad & u \\ \text{s.t.} \quad & \text{tr}(\mathbf{W}) \leq P_S, \\ & \sigma_{U_1}^2 \left(2^{\frac{u}{t_2}} - 1 \right) \leq \text{tr}(\mathbf{W}\mathbf{A}), \\ & \sigma_{U_2}^2 \left(2^{\frac{u}{t_2}} - 1 \right) \leq \text{tr}(\mathbf{W}\mathbf{B}), \\ & u \leq \max \{ I_{U_1}^{RL} - I_{E_1}^{RL}, I_{U_2}^{RL} - I_{E_2}^{RL} \}. \end{aligned} \quad (36)$$

Problem (36) is recognized as a SDP problem, thus convex and can be efficiently solved. According to Theorem 2.2 in [54], when there are three constraints on the matrix variable of a SDP problem such as (36), existence of a rank-1 optimal solution for $N_S > 2$ is guaranteed. Hence, if the solution to (36) happens not to be rank-one, we can use Theorem 2.2 in [54] to recover the rank-one optimal solution out of a non-rank-1 solution.

According to [55], the complexity of problem (36) is

$$O \left((3 + N_S^2) \left(\frac{N_S^2 (N_S^2 + 1)}{2} \right)^3 \right). \quad (37)$$

Solving (36) is accompanied along with a 1-D exhaustive search over the time variable t . We assume that the time variable is divided into m bins between 0 and 1. The overall computational complexity for designing the beamformer for the XOR network coding scheme is m times the complexity mentioned in (37). This is typically affordable since the optimization is performed at the GW on the ground.

B. Conventional SATCOM

According to the secrecy rate defined in (31), the optimization problem for the conventional scheme is

$$\begin{aligned} \max_{\mathbf{w}_1, \mathbf{w}_2, t_1, t_2} \quad & \min \left\{ I_{U_1}^{RL} - I_{E_1}^{RL}, I_{U_2}^{FLCon} - I_{E_2}^{FLCon} \right\} \\ & + \min \left\{ I_{U_2}^{RL} - I_{E_2}^{RL}, I_{U_1}^{FLCon} - I_{E_1}^{FLCon} \right\} \\ \text{s.t.} \quad & \|\mathbf{w}_1\|^2 + \|\mathbf{w}_2\|^2 \leq P_S. \end{aligned} \quad (38)$$

Assume that the power split between the beamforming vectors \mathbf{w}_1 and \mathbf{w}_2 is βP_S and $(1 - \beta) P_S$ where β is a given parameter with $0 \leq \beta \leq 1$. Using the parameter β , the beamforming vectors \mathbf{w}_1 and \mathbf{w}_2 in the power constraint of (38) can be separated. Hence, (38) can be rewritten as

$$\begin{aligned} \max_{\mathbf{w}_1, \mathbf{w}_2, t_1, t_2} \quad & \min \left\{ I_{U_1}^{RL} - I_{E_1}^{RL}, I_{U_2}^{FLCon} - I_{E_2}^{FLCon} \right\} \\ & + \min \left\{ I_{U_2}^{RL} - I_{E_2}^{RL}, I_{U_1}^{FLCon} - I_{E_1}^{FLCon} \right\} \\ \text{s.t.} \quad & \|\mathbf{w}_1\|^2 \leq \beta P_S, \\ & \|\mathbf{w}_2\|^2 \leq (1 - \beta) P_S. \end{aligned} \quad (39)$$

The problem (39) can be expanded as

$$\begin{aligned} \max_{\mathbf{w}_1, \mathbf{w}_2, t_1, t_2} \quad & \min \left\{ SR_{U_1}^{RL}, t_2 \log \left(\frac{\sigma_{E_2}^2 \sigma_{U_2}^2 + |\mathbf{h}_{S,U_2}^T \mathbf{w}_1|^2}{\sigma_{U_2}^2 \sigma_{E_2}^2 + |\mathbf{h}_{S,E_2}^T \mathbf{w}_1|^2} \right) \right\} \\ & + \min \left\{ SR_{U_2}^{RL}, t_3 \log \left(\frac{\sigma_{E_1}^2 \sigma_{U_1}^2 + |\mathbf{h}_{S,U_1}^T \mathbf{w}_2|^2}{\sigma_{U_1}^2 \sigma_{E_1}^2 + |\mathbf{h}_{S,E_1}^T \mathbf{w}_2|^2} \right) \right\} \\ \text{s.t.} \quad & \|\mathbf{w}_1\|^2 \leq \beta P_S, \\ & \|\mathbf{w}_2\|^2 \leq (1 - \beta) P_S. \end{aligned} \quad (40)$$

Before further simplifying (40), we first mention the following theorem.

Theorem 1: If the achievable secrecy rate is strictly greater than zero, the power constraints in (40) are active at the optimal point \mathbf{w}_1^* and \mathbf{w}_2^* , i.e., $\|\mathbf{w}_1\|^2 = \beta P_S$ and $\|\mathbf{w}_2\|^2 = (1 - \beta) P_S$.

Proof: The proof is given in Appendix A. ■

Using Theorem 1, we can show that the constraints in (40) are active which enables us to write (40) as

$$\begin{aligned} \max_{\mathbf{w}_1, \mathbf{w}_2, t_1, t_2} \quad & \min \left\{ I_{U_1}^{RL} - I_{E_1}^{RL}, t_2 \log \left(\frac{\sigma_{E_2}^2 \mathbf{w}_1^H \mathbf{U}_2 \mathbf{w}_1}{\sigma_{U_2}^2 \mathbf{w}_1^H \mathbf{E}_2 \mathbf{w}_1} \right) \right\} \\ & + \min \left\{ I_{U_2}^{RL} - I_{E_2}^{RL}, t_3 \log \left(\frac{\sigma_{E_1}^2 \mathbf{w}_2^H \mathbf{U}_1 \mathbf{w}_2}{\sigma_{U_1}^2 \mathbf{w}_2^H \mathbf{E}_1 \mathbf{w}_2} \right) \right\} \\ \text{s.t.} \quad & \|\mathbf{w}_1\|^2 = \beta P_S, \\ & \|\mathbf{w}_2\|^2 = (1 - \beta) P_S, \end{aligned} \quad (41)$$

where $\mathbf{U}_1 \triangleq \frac{\sigma_{U_1}^2}{(1-\beta)P_S} \mathbf{I} + \mathbf{h}_{S,U_1}^* \mathbf{h}_{S,U_1}^T$, $\mathbf{U}_2 \triangleq \frac{\sigma_{U_2}^2}{\beta P_S} \mathbf{I} + \mathbf{h}_{S,U_2}^* \mathbf{h}_{S,U_2}^T$, $\mathbf{E}_1 \triangleq \frac{\sigma_{E_1}^2}{(1-\beta)P_S} \mathbf{I} + \mathbf{h}_{S,E_1}^* \mathbf{h}_{S,E_1}^T$, $\mathbf{E}_2 \triangleq \frac{\sigma_{E_2}^2}{\beta P_S} \mathbf{I} + \mathbf{h}_{S,E_2}^* \mathbf{h}_{S,E_2}^T$.

The benefit of (41) is that given β , \mathbf{w}_1 and \mathbf{w}_2 can be optimized separately. To be specific, the optimal \mathbf{w}_1 and \mathbf{w}_2 corresponds to the eigenvectors associated with the maximum eigenvalues of matrices $\mathbf{C} = \mathbf{L}_1^{-1} \mathbf{U}_1 \mathbf{L}_1^{-H}$ and $\mathbf{D} = \mathbf{L}_2^{-1} \mathbf{U}_2 \mathbf{L}_2^{-H}$ where $\mathbf{E}_1 = \mathbf{L}_1 \mathbf{L}_1^H$ and $\mathbf{E}_2 = \mathbf{L}_2 \mathbf{L}_2^H$, respectively. As a result, (41) can be simplified into

$$\begin{aligned} \max_{\substack{0 < t_1 < 1 \\ 0 < t_2 < 1}} \quad & \min \left\{ I_{U_1}^{RL} - I_{E_1}^{RL}, t_2 \log \left(\frac{\sigma_{E_2}^2}{\sigma_{U_2}^2} \lambda_{\max}(\mathbf{C}) \right) \right\} \\ & + \min \left\{ I_{U_2}^{RL} - I_{E_2}^{RL}, t_3 \log \left(\frac{\sigma_{E_1}^2}{\sigma_{U_1}^2} \lambda_{\max}(\mathbf{D}) \right) \right\}. \end{aligned} \quad (42)$$

Note that the constraints of (41) are dropped in (42) due to the homogeneity of the objective function. To solve (42), we introduce auxiliary variables as u_1 and u_2 to remove the “min”

operators as

$$\begin{aligned} \max_{t_1, t_2, u_1, u_2} \quad & u_1 + u_2 \\ \text{s.t.} \quad & u_1 \leq t_1 c, \end{aligned} \quad (43a)$$

$$u_1 \leq t_2 \log \left(\frac{\sigma_{E_2}^2}{\sigma_{U_2}^2} \lambda_{\max}(\mathbf{C}) \right), \quad (43b)$$

$$u_2 \leq t_1 d, \quad (43c)$$

$$u_2 \leq t_3 \log \left(\frac{\sigma_{E_1}^2}{\sigma_{U_1}^2} \lambda_{\max}(\mathbf{D}) \right), \quad (43d)$$

$$u_1, u_2 \geq 0, \quad (43e)$$

$$0 < t_1 < 1, 0 < t_2 < 1, \quad (43f)$$

where

$$c \triangleq \log \frac{1 + \frac{P_{U_1} \|\mathbf{h}_{U_1,S}\|^2}{\sigma_S^2}}{\left(1 + \frac{P_{U_1} |h_{U_1,E_1}|^2}{\sigma_{E_1}^2}\right)}, \quad d \triangleq \log \frac{1 + \frac{P_{U_2} \|\mathbf{h}_{U_2,S}\|^2}{\sigma_S^2}}{\left(1 + \frac{P_{U_2} |h_{U_2,E_2}|^2}{\sigma_{E_2}^2}\right)}, \quad (44)$$

and $t_3 = 1 - t_1 - t_2$. Clearly, it is a linear programming problem and can be optimally solved. After that, we use 1-D search to find the optimal power allocation parameter β^* .

IV. SIMULATION RESULTS

In this section, we present numerical results to evaluate the secrecy rate of the XOR network coding based SATCOM protocol and compare it with the conventional scheme. We consider both i) equal RL and FL time allocation (ETA), and ii) optimized time allocation between the RL and the FL (OTA). We use labels “XOR-ETA” and “XOR-OTA” to denote equal time allocation and optimal time allocation policies, respectively.

In our simulations, B denotes the carrier bandwidth, 41.67 kHz, for both RL and FL transmissions. Since there is a main direct link from the satellite to the users as well as some diffuse components, the channel from the satellite to the users can be modeled as Rician [56]. The K -factor for the FL is determined by the multipath average scattered power and random log-normal variable using the values provided by [56]. Due to the “scintillation” effect [57], we have multipath in the RL. Moreover, there exists a direct link like the FL case. Therefore, the RL can be considered to follow Rician distribution with a higher K -factor which is assumed to be 15 dB. The rest of the link parameters are summarized in Table II [58]. The satellite’s FL transmission power in Table II shows the carrier power used in the following transmissions: 1) the broadcast in Phase IV of the XOR scheme or, 2) the transmissions in Phases IV and V of the conventional reference scheme. If the satellite’s FL transmission power is not a variable in a simulation scenario, its value provided by Table II is used.

The ground channels between the users and the eavesdroppers are assumed to follow a Rayleigh distribution with the pathloss calculated by

$$L = 10 \log \left[\left(\frac{4\pi}{\lambda} \right)^2 d^\gamma \right], \quad (45)$$

TABLE II
LINK BUDGET AND PARAMETERS

Parameter	Value
Satellite orbit type	LEO
Operating band (1~2 GHz)	L-band
RL and FL frequency band, MHz	1616-1626.5
Beams on the Earth	48
Number of antenna arrays	318
Frequency reuse factor (FRF)	12
Number of carriers per beam	20
Carrier bandwidth, B_c , kHz	41.67
Guard bandwidth, kHz	2
Satellite's antenna gain per beam, dBi	24.3
Total power at the satellite, dBW	31.46
Satellite noise temperature, K	290
Terminal noise temperature, K	321
Satellite's FL transmission power, dBW	7.65
Mobile device radiation power, dBW	0
Mobile device antenna gain, dBi	3.5
Return and forward link pathloss, dB	151
Doppler shift due to satellite velocity, Hz	270
Envelope mean of the direct wave, m_s	0.787
The variance of the direct wave, σ_s^2	0.0671
The power of the diffuse component	0.0456

where γ is the pathloss exponent which we assume to be $\gamma = 3.7$. The maximum Doppler shift is calculated using the following relation as

$$f_{Dmax} = \frac{v}{\lambda} = \frac{vf_c}{c}, \quad (46)$$

where v is the user's speed, f_c is the maximum frequency used and c is the light speed.

Since the carrier bandwidth is 41.67 kHz, we assume that the RL operating bandwidth is 1616–1616.04167 MHz for U_1 , 1616.04367 – 1616.08534 MHz for U_2 and the FL operating bandwidth is 1616 – 1616.04167 MHz which is common between the users. Each user is supposed to move in a random direction with a 10 m/s speed. If not explicitly mentioned, each eavesdropper's distance to the user is randomly changed between 2 to 2.5 km.

We first show the average sum secrecy rate in Fig. 2 when the number of feeds used on the satellite varies from 3 to 10. As we can see, the XOR network coding scheme can achieve over 54% higher average sum secrecy rate than the conventional one. It can be observed that optimizing the RL and FL communication times improves the average sum secrecy rate for both schemes considerably, especially for the conventional scheme in higher number of feeds.

The effect of time allocation is further illustrated in Figs. 3 and 4 for the XOR network coding and the conventional schemes, respectively. It is observed in Fig. 3 that for different number of feeds, the average sum secrecy rate first increases, and then then decreases with the RL time allocation t_1 . Here, more time is allocated to the RL transmission which means that the FL transmission rate is a bottleneck for the end-to-

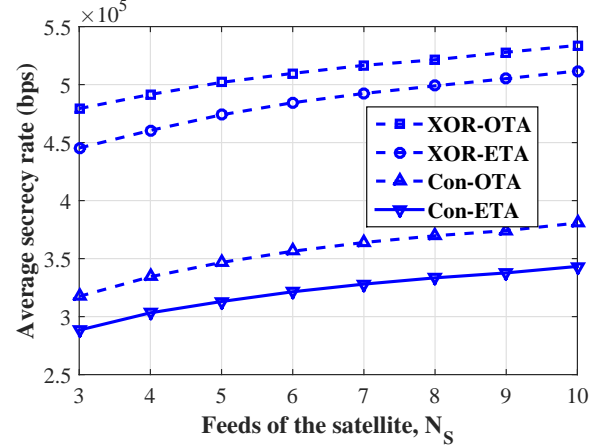


Fig. 2. Average sum secrecy rate versus different number of feeds on the satellite for the XOR network coding and conventional schemes.

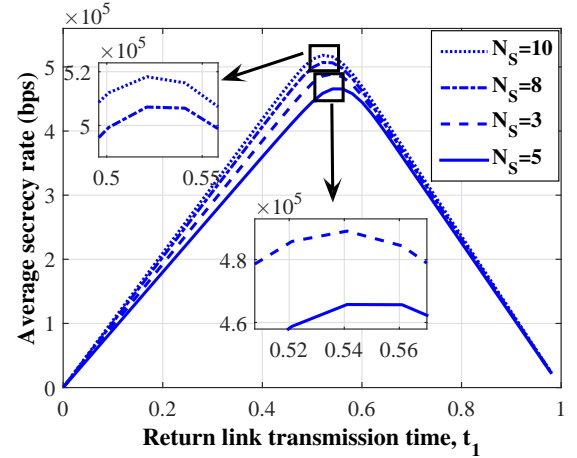


Fig. 3. Average sum secrecy rate versus the RL time allocation t_1 in the XOR network coding scheme.

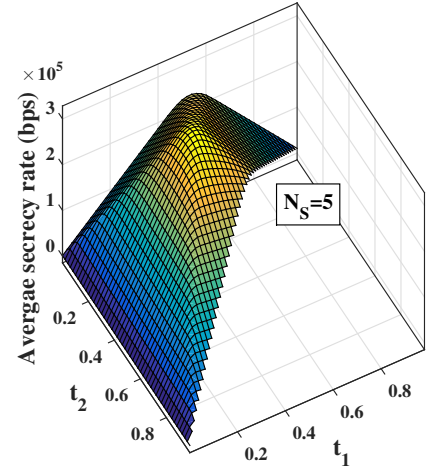


Fig. 4. Average sum secrecy rate versus different RL, t_1 , and FL, t_2 and $t_3 = 1 - t_1 - t_2$, time allocation in the conventional scheme.

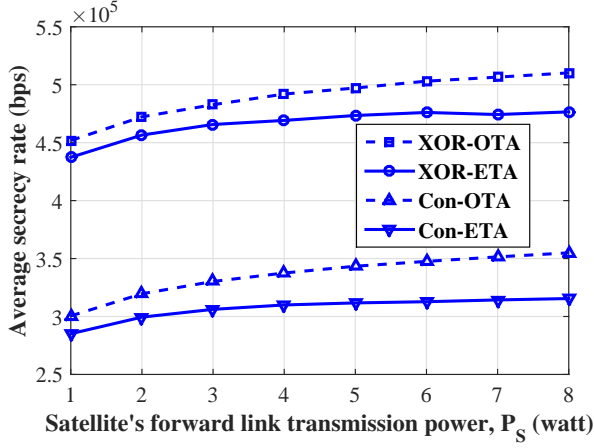


Fig. 5. Average sum secrecy rate versus the satellite's forward link transmission power.

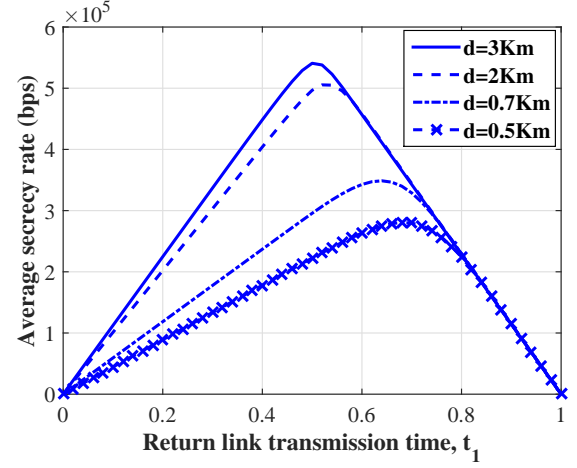


Fig. 8. Average sum secrecy rate versus different RL and FL time allocation in XOR network coding scheme for different distances between the user and eavesdropper.

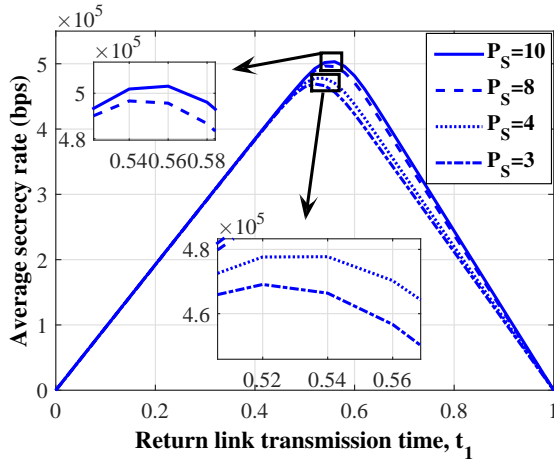


Fig. 6. Average sum secrecy rate versus RL time allocation for different satellite's forward link transmission powers.

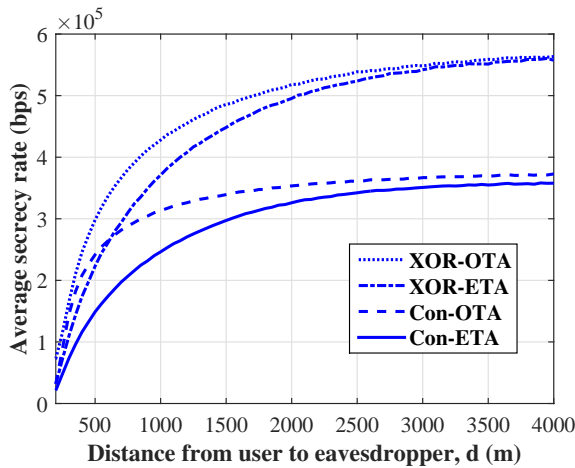


Fig. 7. Average sum secrecy rate versus the distance between the user and the eavesdropper for XOR network coding and conventional schemes while equal and optimal time allocation are employed.

end rate. The time split between the RL and FL depends on the number of feeds at the satellite. As the number of feeds increases, the time devoted to the FL transmission increases. This shows that the FL acts as a bottleneck for the end-to-end communications. The change in the RL and FL time allocation makes the channel secrecy rates closer to each other so that the overall average secrecy rate increases. The optimal time allocation for one RL slot and two FL slots in the conventional scheme can be seen in Fig. 4.

The effect of the satellite's FL transmission power on the average secrecy rate is investigated in Figs. 5 and 6. In Fig. 5, we see that the average secrecy rate for the equal time allocation approach in both schemes starts to saturate as the available power for the FL transmission increases. This can be explained by the fact that as the available power increases, the RL becomes a bottleneck for the end-to-end secrecy rate and hinders the overall improvement. On the other hand, while performing optimal time allocation over RL and FL, the average secrecy rate keeps growing for both the conventional and the XOR network coding schemes. It is seen in Fig. 6 that by increasing the power at the satellite, more time is allocated to the RL transmission in order to balance the RL and FL secrecy rates and sustaining the secrecy rate growth. However, after increasing the satellite's power beyond a specific point, the effect of the optimal time allocation fades out, and the average secrecy rate in the optimal time allocation scheme also saturates due to RL being a bottleneck. This fact can be observed in Fig. 6. As the power of the FL transmission increases, less time is exchanged between the RL and FL transmission and the average secrecy rate saturates.

The effect of the distance between each user and the corresponding eavesdropper is investigated in Figs. 7 and 8. As is seen in Fig. 7, the average secrecy rate for equal time allocation in both schemes saturates as the distance between the user and eavesdropper increases. This is because increasing the distance to the eavesdropper improves the secrecy rate in the RL, leaving the FL as a performance bottleneck. When the time allocation is optimized, the average secrecy rate

shows notable gain in both schemes. However, after a specific distance, the secrecy rate for the optimal power allocation also saturates. Increasing the distance to the eavesdropper increases the secrecy rate for the RL, but this increment is going to be quite small at some point and consequently vanishes. Consequently, as the distance increases, less time exchange is required between the RL and FL transmission. This fact can be seen in Fig. 8. Due to this limit in the RL secrecy rate, the secrecy rate can be improved using optimal time allocation up to a limited distance. Furthermore, as it is observed in Fig. 7, the average sum secrecy rate of the XOR network coding saturates in a much longer distance compared to the conventional scheme. Interestingly, when the user and the eavesdropper are close, the conventional scheme using the optimal time allocation outperforms the XOR network coding scheme using equal time allocation. This originates from the fact that there are more degrees of freedom in terms of optimal time allocation in the conventional scheme compared to the XOR network coding scheme. Hence, when it comes to picking up a secure protocol, distance plays an important role.

The results in Fig. 8 illustrate that as the distance between the user and the eavesdropper decreases, more time is allocated to the RL transmission of the XOR network coding scheme in order to balance the secrecy rates in RL and FL. It is observed that as the distance to the eavesdropper increases, less change is required in the RL and FL times. This is due to the fact that as the distance increases, the improvement rate in the secrecy rate of the RL is reduced and less regulation is required in the transmission times.

V. CONCLUSION

Network coding principle has been known to increase the throughput of bidirectional SATCOM. In this paper, we studied the use of XOR network coding to improve the sum secrecy rate of bidirectional SATCOM. The beamforming vector as well as the optimal time allocation between the RL and the FL were optimized to improve the secrecy rate. We compared the sum secrecy rate of the XOR network coding with the conventional scheme without using network coding regarding realistic system parameters. Our results demonstrated that the network coding based scheme outperforms the conventional scheme substantially, especially when the legitimate users and the eavesdroppers are not close.

APPENDIX A PROOF OF THEOREM 1

Proof: In the objective function of problem (40), only the second argument of the “min” operators, FL secrecy rates, include the beamforming vector. Hence, we focus on these terms in our optimization. Using contradiction, we shall show that $\|\mathbf{w}_1^*\|^2 = \beta P_S$ and $\|\mathbf{w}_2^*\|^2 = (1 - \beta) P_S$ must hold for the optimal solutions \mathbf{w}_1^* and \mathbf{w}_2^* . Assume that \mathbf{w}_1^* and \mathbf{w}_2^* are the optimal solutions to (40) and satisfy $\|\mathbf{w}_1^*\|^2 < \beta P_S$ and $\|\mathbf{w}_2^*\|^2 < (1 - \beta) P_S$, then there exist constants $\alpha_1 > 1$ and $\alpha_2 > 1$ that satisfy $\|\widehat{\mathbf{w}}_1^*\|^2 = \beta P_S$ and $\|\widehat{\mathbf{w}}_2^*\|^2 = (1 - \beta) P_S$ where $\widehat{\mathbf{w}}_1^* = \alpha_1 \mathbf{w}_1^*$ and $\widehat{\mathbf{w}}_2^* = \alpha_2 \mathbf{w}_2^*$. Replacing \mathbf{w}_1^* by $\widehat{\mathbf{w}}_1^*$

and \mathbf{w}_2^* by $\widehat{\mathbf{w}}_2^*$ in the FL secrecy rates of the objective in (40), we get

$$\begin{aligned} f_1(\alpha_1) &= t_2 \log \left(\frac{\sigma_{E_2}^2 \sigma_{U_2}^2 + \alpha_1^2 |\mathbf{h}_{S,U_2}^T \mathbf{w}_1^*|^2}{\sigma_{U_2}^2 \sigma_{E_2}^2 + \alpha_1^2 |\mathbf{h}_{S,E_2}^T \mathbf{w}_1^*|^2} \right), \\ f_2(\alpha_2) &= t_3 \log \left(\frac{\sigma_{E_1}^2 \sigma_{U_1}^2 + \alpha_2^2 |\mathbf{h}_{S,U_1}^T \mathbf{w}_2^*|^2}{\sigma_{U_1}^2 \sigma_{E_1}^2 + \alpha_2^2 |\mathbf{h}_{S,E_1}^T \mathbf{w}_2^*|^2} \right). \end{aligned} \quad (47)$$

Also, we assume that in the RL and FL of each user the secrecy rate is nonzero which translates into

$$\sigma_{E_2}^2 (\sigma_{U_2}^2 + |\mathbf{h}_{S,U_2}^T \mathbf{w}_1|^2) > \sigma_{U_2}^2 (\sigma_{E_2}^2 + |\mathbf{h}_{S,E_2}^T \mathbf{w}_1|^2), \exists \mathbf{w}_1, \quad (48)$$

$$\sigma_{E_1}^2 (\sigma_{U_1}^2 + |\mathbf{h}_{S,U_1}^T \mathbf{w}_2|^2) > \sigma_{U_1}^2 (\sigma_{E_1}^2 + |\mathbf{h}_{S,E_1}^T \mathbf{w}_2|^2), \exists \mathbf{w}_2. \quad (49)$$

According to the conditions in (48) and (49), we can see that $f_1(\alpha)$ and $f_2(\alpha)$ are monotonically increasing functions in the parameters α_1 and α_2 . This contradicts that \mathbf{w}_1^* and \mathbf{w}_2^* are the optimal solutions. Since adjusting the RL and FLs transmission time balances the RL and FL secrecy rates, the RL bottleneck does not limit the FL secrecy rate increment. Hence, the power constraint should be active. This completes the proof. ■

REFERENCES

- [1] A. Roy-Chowdhury, J. Baras, M. Hadjithedodiosou, and S. Papademetriou, “Security issues in hybrid networks with a satellite component,” *IEEE Wireless Commun. Mag.*, vol. 12, no. 6, pp. 50–61, Dec. 2005.
- [2] H. Cruickshank, M. Howarth, S. Iyengar, Z. Sun, and L. Claverotte, “Securing multicast in DVB-RCS satellite systems,” *IEEE Wireless Commun. Mag.*, vol. 12, no. 5, pp. 38–45, Oct. 2005.
- [3] N. Sklavos and X. Zhang, *Wireless Security and Cryptography: Specifications and Implementations*. Taylor & Francis, 2007.
- [4] A. D. Wyner, “The wire-tap channel,” *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.
- [5] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network information flow,” *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.
- [6] R. Bassoli, H. Marques, J. Rodriguez, K. Shum, and R. Tafazolli, “Network coding theory: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1–29, Fourth quarter 2013.
- [7] I. Hammerstrom, M. Kuhn, C. Esli, J. Zhao, A. Wittneben, and G. Bauch, “MIMO two-way relaying with transmit CSI at the relay,” in *IEEE Workshop on Signal Proces. Advances in Wireless Commun. (SPAWC)*, Helsinki, Finland, Jun. 2007.
- [8] A. Amah and A. Klein, “Regenerative multi-group multi-way relaying,” *IEEE Trans. Veh. Technol.*, vol. 60, no. 7, pp. 3017–3029, Sep. 2011.
- [9] F. Rossetto, “A comparison of different physical layer network coding techniques for the satellite environment,” in *Advanced Satellite Multimedia Syst. Conf. (ASMA) and the 11th Signal Proces. for Space Commun. Workshop (SPSC)*, Cagliari, Italy, Sep. 2010, pp. 25–30.
- [10] S. Sorour, S. Valaee, and N. Alagha, “Joint control of delay and packet drop rate in satellite systems using network coding,” in *Advanced Satellite Multimedia Syst. Conf. (ASMA) and the 11th Signal Proces. for Space Commun. Workshop (SPSC)*, Cagliari, Italy, Sep. 2010, pp. 46–53.
- [11] F. Rossetto and D. Lucani, “Systematic design of network coding-aware buffering strategies,” in *Military Commun. Conf. (MILCOM)*, Baltimore, MD, Nov. 2011, pp. 316–322.
- [12] F. Vieira, D. Lucani, and N. Alagha, “Codes and balances: Multibeam satellite load balancing with coded packets,” in *IEEE Int. Conf. on Commun. (ICC)*, Ottawa, Canada, Jun. 2012, pp. 3316–3321.
- [13] —, “Load-aware soft-handovers for multibeam satellites: A network coding perspective,” in *Advanced Satellite Multimedia Syst. Conf. (ASMA) and the 11th Signal Proces. for Space Commun. Workshop (SPSC)*, Baiona, Spain, Sep. 2012, pp. 189–196.

- [14] H. Bischl, H. Brandt, and F. Rossetto, "An experimental demonstration of network coding for satellite networks," *CEAS Space Journal*, vol. 2, no. 1-4, pp. 75–83, Jun. 2011.
- [15] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [16] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [17] J. Chen, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure decode-and-forward two-way relay communications," in *IEEE Global Telecommun. Conf. (GLOBECOM)*, Houston, TX, Dec. 2011.
- [18] A. Mukherjee and A. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *IEEE 11th Int. Workshop on Signal Process. Advances in Wireless Commun. (SPAWC)*, Marrakech, Morocco, Jun. 2010.
- [19] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, Jun. 2011.
- [20] Z. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842–2848, Jul. 2012.
- [21] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.
- [22] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.
- [23] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.
- [24] L. Jiang, Z. Han, M. Vazquez-Castro, and A. Hjørungnes, "Secure satellite communication systems design with individual secrecy rate constraints," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 661–671, Sept. 2011.
- [25] G. Zheng, P. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852–863, Feb. 2012.
- [26] D. Sunderland, G. Duncan, B. Rasmussen, H. Nichols, D. Kain, L. Lee, B. Clebowicz, I. Hollis, R.W. L. Wissel, and T. Wilder, "Megagate asics for the thuraya satellite digital signal processor," in *International Symposium on Quality Electronic Design*, San Jose, CA, Mar. 2002, pp. 479–486.
- [27] B. Devillers, A. Perez-Neira, and C. Mosquera, "Joint linear precoding and beamforming for the forward link of multi-beam broadband satellite systems," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Houston, Texas, USA, Dec. 2011.
- [28] A. Khan, M. Imran, and B. Evans, "Semi-adaptive beamforming for OFDM based hybrid terrestrial-satellite mobile system," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3424–3433, Oct. 2012.
- [29] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
- [30] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.
- [31] 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, pp. 1875–1888, Mar. 2010.
- [32] M. 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.
- [33] H. Long, W. Xiang, Y. Zhang, Y. Liu, and W. Wang, "Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 229–238, Jan. 2013.
- [34] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [35] Q. Li, H. Song, and K. Huang, "Achieving secure transmission with equivalent multiplicative noise in MISO wiretap channels," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 892–895, May 2013.
- [36] A. Chorti, "Helping interferer physical layer security strategies for M-QAM and M-PSK systems," in *Annual Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, Mar. 2012.
- [37] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24–32, May 2007.
- [38] W. Harrison and S. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *IEEE International Conference on Communications*, Dresden, Germany, Jun. 2009.
- [39] J. Li and A. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861–867, Sep. 2011.
- [40] —, "On ergodic secrecy rate for gaussian miso wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.
- [41] Z. Rezki, A. Khisti, and M.-S. Alouini, "Ergodic secret message capacity of the wiretap channel with finite-rate feedback," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3364–3379, Jun. 2014.
- [42] M. Giryk, M. Vehkaperä, J. Yuan, and L. Rasmussen, "On the ergodic secrecy capacity of MIMO wiretap channels with statistical CSI," in *International Symposium on Information Theory and its Applications (ISITA)*, Melbourne, Australia, Oct. 2014, pp. 398–402.
- [43] O. Koyluoglu, H. El Gamal, L. Lai, and H. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.
- [44] B.-G. Kim, C.-S. Kim, and D.-S. Ahn, "Performance evaluation for a closed loop power control using an efficient channel estimation in SAT-CDMA," in *IEEE Veh. Technology Conf. (VTC)*, vol. 6, Melbourne, Australia, May 2006, pp. 2625–2629.
- [45] L. Cottatellucci, M. Debbah, G. Gallinaro, R. Mueller, M. Neri, and R. Rinaldo, "Interference mitigation techniques for broadband satellite systems," in *AIAA International Communications Satellite Systems Conference (ICSSC)*, San Diego, CA, Jun. 2006.
- [46] D. Christopoulos, S. Chatzinotas, G. Zheng, J. Grotz, and B. Ottersten, "Linear and nonlinear techniques for multibeam joint processing in satellite communications," *EURASIP journal on wireless communications and networking*, vol. 2012, pp. 1–13, May 2012.
- [47] J. Arnau, B. Devillers, C. Mosquera, and A. Pérez-Neira, "Performance study of multiuser interference mitigation schemes for hybrid broadband multibeam satellite architectures," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, pp. 1–19, Apr. 2012.
- [48] V. Joroughi, B. Devillers, M. Vazquez, and A. Perez-Neira, "Design of an on-board beam generation process for the forward link of a multi-beam broadband satellite system," in *IEEE Global Communications Conference (GLOBECOM)*, Atlanta, GA, Dec. 2013, pp. 2921–2926.
- [49] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "Xors in the air: Practical wireless network coding," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 497–510, Jun. 2008.
- [50] X. Zhang, A. Ghrayeb, and M. Hasna, "On hierarchical network coding versus opportunistic user selection for two-way relay channels with asymmetric data rates," *IEEE Trans. Commun.*, vol. 61, no. 7, pp. 2900–2910, Jul. 2013.
- [51] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York, NY: Cambridge University Press, 2005.
- [52] F. Oggier and B. Hassibi, "The MIMO wiretap channel," in *International Symposium on Communications, Control and Signal Processing (ISCCSP)*, St. Julians, Malta, Mar. 2008, pp. 213–218.
- [53] Z. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 359–371, Apr. 2012.
- [54] W. Ai, Y. Huang, and S. Zhang, "New results on hermitian matrix rank-one decomposition," *Mathematical Programming*, vol. 128, no. 1-2, pp. 253–283, Jun. 2011.
- [55] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY: Cambridge University Press, 2004.
- [56] B. Vucetic and J. Du, "Channel modeling and simulation in satellite mobile communication systems," *IEEE J. Sel. Areas Commun.*, vol. 10, no. 8, pp. 1209–1218, Oct. 1992.
- [57] *Propagation data and prediction methods required for the design of Earth-space telecommunication systems*, International Telecommunication Union (ITU) Std. Rec. P.618-11, Oct. 2009.
- [58] C. Fossa, R. Raines, G. Gunsch, and M. A. Temple, "An overview of the iridium low earth orbit (LEO) satellite system," in *IEEE National Aerospace and Electronics Conference*, Dayton, OH, Jul. 1998, pp. 152–159.



Ashkan Kalantari Ashkan Kalantari (AK) was born in Iran. He received his BSc and MSc degrees from K. N. Toosi University of Technology, Tehran, Iran in 2009 and 2012, respectively. He is currently working toward the Ph.D. degree with the research group SIGCOM in the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg. His research interest is physical layer security in wireless and satellite communications.



Gan Zheng (S'05-M'09-SM'12) is currently a Lecturer in School of Computer Science and Electronic Engineering, University of Essex, UK. He received the B. E. and the M. E. from Tianjin University, Tianjin, China, in 2002 and 2004, respectively, both in Electronic and Information Engineering, and the PhD degree in Electrical and Electronic Engineering from The University of Hong Kong, Hong Kong, in 2008. Before he joined University of Essex, he worked as a Research Associate at University College London, UK, and University of Luxembourg,

Luxembourg. His research interests include cooperative communications, cognitive radio, physical-layer security, full-duplex radio and energy harvesting. He is the first recipient for the 2013 IEEE Signal Processing Letters Best Paper Award.



Zhen GAO received his BS, MS and PhD degree in Electrical and Information Engineering from Tianjin University, China, in 2005, 2007 and 2011, respectively. From 2008.10 to 2010.11, he was a visiting scholar in GeorgiaTech, working on the design and implementation for OFDM based cooperative communication. From 2011.7 to 2014.11, he was an assistant researcher in the Wireless and Mobile Communication Research Center in Tsinghua University, China. He is currently an Associate Professor in Tianjin University. His focus is on mobile satellite

communications, fault-tolerant signal processing and wireless communication system.



Zhu Han (S01M04-SM09-F14) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an assistant professor in Boise State University, Idaho.

Currently, he is an Associate Professor in Electrical and Computer Engineering Department at the University of Houston, Texas. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, wireless multimedia, security, and smart grid communication. Dr. Han is an Associate Editor of IEEE Transactions on Wireless Communications since 2010. Dr. Han is the winner of IEEE Fred W. Ellersick Prize 2011. Dr. Han is an NSF CAREER award recipient 2010. Dr. Han is IEEE Distinguished lecturer since 2015.



Björn Ottersten was born in Stockholm, Sweden, 1961. He received the M.S. degree in electrical engineering and applied physics from Linköping University, Linköping, Sweden, in 1986. In 1989 he received the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA. Dr. Ottersten has held research positions at the Department of Electrical Engineering, Linköping University, the Information Systems Laboratory, Stanford University, the Katholieke Universiteit Leuven, Leuven, and the University of Luxembourg. During 96/97

Dr. Ottersten was Director of Research at ArrayComm Inc, a start-up in San Jose, California based on Otterstens patented technology. He has co-authored journal papers that received the IEEE Signal Processing Society Best Paper Award in 1993, 2001, 2006, and 2013 and 3 IEEE conference papers receiving Best Paper Awards. In 1991 he was appointed Professor of Signal Processing at the Royal Institute of Technology (KTH), Stockholm. From 1992 to 2004 he was head of the department for Signals, Sensors, and Systems at KTH and from 2004 to 2008 he was dean of the School of Electrical Engineering at KTH. Currently, Dr. Ottersten is Director for the Interdisciplinary Centre for Security, Reliability and Trust at the University of Luxembourg. Dr. Ottersten is a board member of the Swedish Research Council and as Digital Champion of Luxembourg, he acts as an adviser to the European Commission. Dr. Ottersten has served as Associate Editor for the IEEE Transactions on Signal Processing and on the editorial board of IEEE Signal Processing Magazine. He is currently editor in chief of EURASIP Signal Processing Journal and a member of the editorial boards of EURASIP Journal of Applied Signal Processing and Foundations and Trends in Signal Processing. Dr. Ottersten is a Fellow of the IEEE and EURASIP and a member of the IEEE Signal Processing Society Board of Governors. In 2011 he received the IEEE Signal Processing Society Technical Achievement Award. He is a first recipient of the European Research Council advanced research grant. His research interests include security and trust, reliable wireless communications, and statistical signal processing.