Two-Way Physical Layer Security Protocol for Gaussian Channels

Masahito Hayashi, *Fellow, IEEE*, and Ángeles Vázquez-Castro, *Senior Member, IEEE*

***Abstract*— In this paper we propose a two-way protocol of physical layer security using the method of privacy amplification against eavesdroppers. First we justify our proposed protocol by analyzing the physical layer security provided by the classic wiretap channel model (i.e. one-way protocol). In the Gaussian channels, the classic one-way protocol requires Eve's channel to be degraded w.r.t. Bob's channel. However, this channel degradation condition depends on Eve's location and whether Eve's receiving antenna is more powerful than Bob's. To overcome this limitation, we introduce a two-way protocol inspired in IEEE TIT (1993) that eliminates the channel degradation condition. In the proposed two-way protocol, on a first phase, via Gaussian channel, Bob sends randomness to Alice, which is partially leaked to Eve. Then, on a second phase, Alice transmits information to Bob over a public noiseless channel. We derive the secrecy capacity of the two-way protocol when the channel to Eve is also Gaussian. We show that the capacity of the two-way protocol is always positive. We present numerical values of the capacities illustrating the gains obtained by our proposed protocol. We apply our result to simple yet realistic models of satellite communication channels.**

***Index Terms*— Physical layer security, space links, wiretap coding, one-way protocol, two-way protocol.**

I. Introduction

PHYSICAL layer security for wireless communications has become a major research topic in recent years because it does not need the computational assumption [1]–[3]. Different properties of the wireless channel can be exploited using information theoretical tools to prevent leakage of information towards potential eavesdroppers. The classic wiretap model as first proposed by Wyner [4] and then generalised by Csiszár and J. Körner [5] was later strengthened to meet cryptographic security standards in [6] and [7], the latter framed within spectrum information-theoretic methods [8]. We adopt such approach here: we assume the physical layer security realized by a stochastic wiretap encoder [9]–[11] based on the privacy amplification method [12], [13]. This method decouples reliability and secrecy, enabling the implementation of different security protocols.

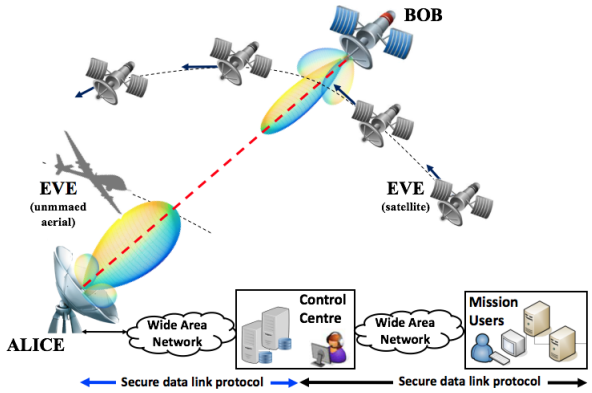

Fig. 1. Illustration for our satellite communication scenario.

In its simplest implementation, the wiretap channel model using privacy amplification can be realized as a one-way security protocol whereby Alice sends a keyless secret message to Bob protected with universal$_2$ hash functions [14]–[16]. In the Gaussian wiretap channel, secrecy capacity is positive as long as Eve's channel has a worse signal to noise ratio than the channel between Alice and Bob, i.e., Eve's channel is degraded w.r.t the main channel between Alice and Bob [17]. The same holds to ensure positive secrecy rate in the finite-length [18], [19]. However, when the channel between Alice and Bob has a worse signal to noise ratio than the channel to Eve, we cannot realize secure communication in this scenario [20]–[22]. For example, in the satellite communication, Eve's satellite usually stays in lower orbit than the orbit of Bob's satellite like in the example scenario in Fig. 1, which implies that Eve has better signal to noise ratio than Bob. That is, it is hard to realize secure satellite communication with the above proposals of wiretap codes if we cannot identify Eve's spatial locations. This type of attack is often called passive man-in-the-middle attack [44].

To resolve this problem, the papers [23]–[26] introduced two-way protocols, in which, the channels of both directions are noisy Gaussian channels. However, when both channels are noisy Gaussian channels, there still exists a possibility that we cannot realize secure communication dependently of Eve's and Bob's spatial locations. To overcome this limitation,

Manuscript received July 12, 2019; revised November 18, 2019 and January 18, 2020; accepted February 6, 2020. Date of publication February 13, 2020; date of current version May 15, 2020. MH was supported in part by JSPS Grant-in-Aid for Scientific Research (A) No.17H01280 and for Scientific Research (B) No.16KT0017, and Kayamori Foundation of Informational Science Advancement. The associate editor coordinating the review of this article and approving it for publication was R. Thobaben. *(Corresponding author: Masahito Hayashi.)*

Masahito Hayashi is with the Graduate School of Mathematics, Nagoya University, Nagoya 464-8601, Japan, also with the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China, also with the Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518066, China, and also with the Centre for Quantum Technologies, National University of Singapore, Singapore 119077 (e-mail: masahito@math.nagoya-u.ac.jp).

Ángeles Vázquez-Castro is with the Department of Telecommunications and Systems Engineering, Autonomous University of Barcelona, 08193 Barcelona, Spain, and also with the Centre for Space Research (CERES), Institut d'Estudis Espacials de Catalunya (IEEC-UAB), Autonomous University of Barcelona, 08193 Barcelona, Spain (e-mail: angeles.vazquez@uab.es).

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

Digital Object Identifier 10.1109/TCOMM.2020.2973618

Maurer [27] proposed a two-way protocol based on the binary symmetric channel. In this paper, inspired by Maurer's idea, we propose a two-way protocol with Gaussian wiretap channel and public noiseless feedback, in which, the feedback channel is given as a public noiseless channel with discrete variable. In the proposed two-way protocol, on the first phase, via Gaussian channel, Bob sends randomness to Alice, which is partially leaked to Eve. Then, on the second phase, combining the received information and the message to be sent, Alice transmits information to Bob over a public noiseless channel. This paper assumes that the noise in the channel of the initial transmission from Bob to Alice is independent of the noise in that to Eve while the paper [29] considers the case when these two noises are correlated. Under this assumption, unless the channel of the initial transmission to Eve is noiseless, this protocol always has positive secure transmission rate regardless Eve's and Bob's spatial locations. In particular, we focus on the simple but realistic (for fixed user terminals) Gaussian-channel satellite system scenarios. Our results demonstrate that our two-way protocol greatly outperforms state-of-the-art one-way and two-way protocols because our two-way protocol always realize secure communication under passive man-in-the-middle attack independently of Eve's spatial location. Note that extension of our results to channels with fading is straightforward, but we take this purely averaging calculation problem out of the scope of our paper, here we focus on the protocols for the Gaussian channel without fading. More specifically, on the application to the Gaussian with BPSK satellite channel, which is considered in current satellite communication standards [41]. Further, we can equip authentication in our protocol by attaching universal$_2$ hash function [14], [15]. This protocol can prevent active man-in-the-middle attack. Therefore, the advantages of our protocol are summarized as follows.

Contribution 1) We address wiretap channel security problem (i.e. eavesdropping) and propose for the first time a novel practical Gaussian wiretap protocol implementing theoretical ideas in Maurer's paper [27].

Contribution 2) Our novel two-way protocol greatly outperforms state-of-the-art one-way protocol because our protocol shows always positive secrecy capacity independently of Eve's location (i.e. it does not require channel degradation condition of one-way wiretap channel). This is our main technical result based on novel and rigorous information theoretical proof.

Contribution 3) Our practical two-way protocol outperforms other proposals of two-way protocols [23]–[25] in the following sense. First, because while other two-way protocols require several communication rounds, our protocol only requires two rounds. Second, because other two-way protocols while outperforming one-way protocol, they still may have negative secrecy capacity. Finally, because our protocol only requires two rounds, our protocol is highly suitable to secure communication channels with large delay, e.g. satellite channels.

Contribution 4) We show the performance of our protocol with meaningful numerical results for the realistic Gaussian BPSK modulated satellite channel, which is included in current satellite communication standards [41]. For this, we use our system modeling which allows to evaluate the security capacity as a function of the system parameters. Hence, our method and results are useful for secure communication design.

One might consider that the real feedback channel is also a noisy channel. However, if we choose sufficiently strong intensity and a suitable error correcting code, the information transmission of the feedback channel can be regarded as a noiseless channel. In this case, we can regard the feedback channel as a noiseless public channel with discrete variable. In contrast, the noise of the initial Gaussian channel is essential because its presence makes the difference between mutual informations from Alice to Bob and Eve. Furthermore, the information leakage in the channel during the second phase does not need to be considered because information leakage is only relevant on the first phase. Hence, it is allowed to make the power of the transmission signal very strong in the second phase while we cannot use such a strong power in the first phase to control the secrecy. Since the information transmission rate with the strong power is much larger than that with the weak power, the consuming time of the first phase is dominant in comparison with that of the second phase. That is, the first phase is the bottleneck in this setting. Therefore, this paper optimizes the amount of noise in the initial Gaussian channel to maximize the wiretap capacity in this model.

In fact, the paper [31] considers a similar topic. It is a follow up of this submission with practical focus. Hence, it contains only the brief description of the two-way protocol without proper proof. Also, the analysis of the secure satellite communication in [31] is different from our analysis in Sections IV and V. That is, it did not consider the optimization while the analysis in this paper is based on the optimization given in Section IV.

Relations to other studies are summarized as follows. While the paper [26] discusses two-way wiretap channels, it considers a new scheme cooperative jamming. The scheme in [26] has several users that are cooperative while this paper has only two cooperative users, the legitimate sender and the legitimate receiver. Therefore, the method in this paper cannot be compared with [26]. In the paper [45], Bob feeds back some randomness that is used as a secret key, exactly like the present manuscript. However, it assumes that the feedback is noiseless and secure, so Eve does not observe it, which is different from here. In the paper [46], unlike the present work, Bob does not control the feedback link. However, it allows all players to observe everything. Hence, the method in this paper cannot be compared with the results [45], [46].

Our work is structured as follows. In Section II, we review the results of one-way standard protocol. In Section III, we propose our two-way protocol. In Section IV, we make numerical optimization for our obtained secret capacities. In Section V, we apply our result to simple realistic models of satellite communication. Finally in Section VI we discuss the protocol and draw some conclusions.

II. One-Way Physical Layer Security Protocols

A. Signal and Channel Model

First, we review the results of one-way standard protocol with Gaussian channels, which model wireless channels in

relevant realistic communication scenarios such as satellite radiofrequency communication channels. The signal variables received by Bob and Eve can be modeled as

$$Y' = \sqrt{E_s}V + \sqrt{n_B}N_1, \quad Z' = \gamma_g\sqrt{E_s}V + \sqrt{\gamma_n n_B}N_2, \tag{1}$$

where V is a variable modeling the transmitted signal and E_s is the energy per symbol expressed in Joules. Y' is the random variable representing the signal received at the legitimate receiver, Z' the random variable representing the signal received at the eavesdropper's receiver and N_1 and N_2 are zero-mean circular complex Gaussian random variables with unit variance. n_B is the noise spectral density power of Bob's receiver expressed in Joules per Hertz. The coefficient γ_g models the amplitude attenuation of the wiretapper's channel w.r.t. the legitimate channel. The analytical expression of γ_g will depend on the system under analysis as well as the channel assumptions and corresponding time scale. The multiplicative coefficient γ_n expresses wiretapper's receiver noise with respect to Bob's receiver noise. Denote the signal-to-noise ratio (SNR) for Bob as

$$\eta_B = \frac{E_s}{n_B} = \frac{P}{N_B}$$

where P and N_B are the system and noise power at Bob's receiver, respectively both expressed in Watts. We can then rewrite the signal model as

$$Y = \sqrt{\eta_B}V + N_1, \quad Z = \gamma_B\sqrt{\eta_B}V + N_2; \tag{2}$$

where $Y = Y'/\sqrt{n_B}$, $Z = Z'/\sqrt{\gamma_n n_B}$ and $\gamma_B := \gamma_g/\sqrt{\gamma_n}$. Hence, N_1 and N_2 are zero-mean circular complex Gaussian random variables with unit variance.

B. Secrecy Capacity With BPSK Modulation and Soft Decision

In the one-way model, Alice sends the encoded information to Bob via channel (2) as Fig. 2. Now, we assume the BPSK modulation, in which, Alice encodes her binary information $A \in \mathbb{F}_2$ to $V = (-1)^A$. In this scenario, the secrecy capacity $C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma_B, \eta_B)$ for the one-way protocol is given as [19, (46)]

$$\begin{aligned} &C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma_B, \eta_B) \\ &= I(A;Y) - I(A;Z) \\ &= \int_{-\infty}^{\infty} u\left[\frac{1}{\sqrt{8\pi}}\left(e^{-\frac{(y-\sqrt{\eta_B})^2}{2}} + e^{-\frac{(y+\sqrt{\eta_B})^2}{2}}\right)\right]dy \\ &\quad - \int_{-\infty}^{\infty} u\left[\frac{1}{\sqrt{8\pi}}\left(e^{-\frac{(z-\gamma_B\sqrt{\eta_B})^2}{2}} + e^{-\frac{(z+\gamma_B\sqrt{\eta_B})^2}{2}}\right)\right]dz, \end{aligned}$$

where $u(x) := -x\log x$ when

$$\gamma_B < 1, \quad \text{i.e., } \gamma_g^2 < \gamma_n. \tag{3}$$

Also, when the condition (3) does not hold, the capacity is zero. In this case, we cannot realize secure communication in this scheme. Here, Bob and Eve are assumed to store the sequence of the received continuous signals and apply the decoder to them. This type of information processing is called soft decision decoding [42, pp. 457 – 460].

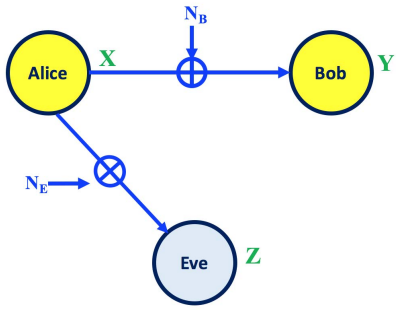

Fig. 2. Graphical illustration of the one way protocol with Gaussian channels. N_B and N_E are noise powers at Bob's and Eve's receivers.

C. Secrecy Capacity With BPSK Modulation and Hard Decision

To save the cost of decoding, the receiver converts the received continuous signal to a binary signal in the reception and applies the decoder to the sequence of the binary signals. This type of information processing is called hard decision decoding [42, pp. 457 – 460]. When the receiver applies this method, it is sufficient to store only binary signals, which saves the memory of the receiver. Here, as another scenario, we consider the case when Bob and Eve obtain B and E using hard decision detection on their received signals Y and Z as defined in the previous sections, respectively. The crossover probability between Alice and Bob induced by the Bernoulli random variable X_1 is given as $\epsilon_B^* = 0.5\mathrm{erfc}(\sqrt{\eta_B/2})$ and the crossover probability between Alice and Eve induced by the Bernoulli random variable X_2 is given as $\epsilon_E^* = 0.5\mathrm{erfc}(\gamma_B\sqrt{\eta_B/2})$ with

$$\mathrm{erfc}(t) := \frac{2}{\sqrt{\pi}}\int_t^{\infty} e^{-t^2}dt. \tag{4}$$

In this scenario, by using the binary entropy function $h(x) := -x\log x - (1-x)\log(1-x)$, the secrecy capacity for the one-way protocol is given as

$$C^{\mathrm{OW}}_{\mathrm{hard}}(\gamma_B, \eta_B) = h(\epsilon_E^*) - h(\epsilon_B^*), \tag{5}$$

which is positive only when $\epsilon_E^* > \epsilon_B^*$, which is equivalent to (3).

III. Two-Way Physical Layer Security Protocol With Gaussian Channels and BPSK Modulation

A. Signal and Channel Model

One-way model requires the condition that the mutual information between the sender and the legitimate receiver is larger than that between the sender and the eavesdropper. This assumption does not hold when the eavesdropper performs passive man-in-the-middle attack. To resolve this problem, we consider two-way protocol for the Gaussian channel and BPSK modulation as follows. In an initial step, Bob sends a random variable V to Alice. In this case, Alice and Eve obtain the variables Y and Z, respectively, as follows.

$$Y = \sqrt{\eta_A}V + N_1, \quad Z = \gamma_A\sqrt{\eta_A}V + N_2, \tag{6}$$

where N_1 and N_2 are zero-mean circular complex Gaussian random variables with unit variance and the coefficient γ_A

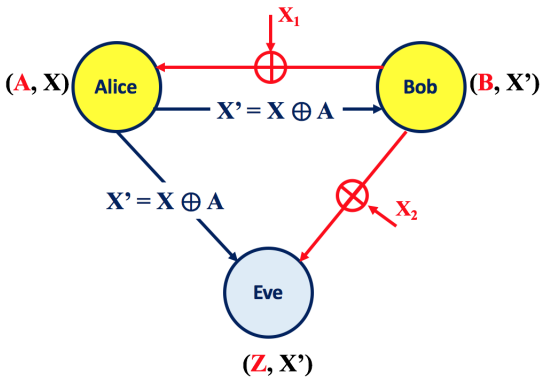

Fig. 3. Graphical illustration of the two-way protocol with Gaussian channels. Phase 1 is shown in red and Phase 2 is shown in black.

models the amplitude attenuation of the wiretapper's channel w.r.t. the legitimate channel (which is now between Bob and Alice and not between Alice and Bob). Notice that the transmitter of the noisy Gaussian channel (6) is not Alice who is the sender of the secret message of this protocol. Therefore η_A is now

$$\eta_A = \frac{E_s}{n_A} = \frac{P}{N_A},$$

where n_A is the noise spectral density power of Alice's receiver expressed in Joules per Hertz.

Bob generates the binary variable $B \in \mathbb{F}_2$ subject to the binary uniform distribution, and sends $V = (-1)^B$ via the above RF channel. Applying hard decision decoding to Y, Alice obtains the binary variable A. In the next step, Alice prepares another binary variable X, and sends $X' := X \oplus A$ to Bob via a public channel. When X is regarded as the channel input information, the legitimate receiver's output is B and X' while the eavesdropper's output is Z and X'. The overall process along with the generated random variables is shown in Fig. 3.

B. Protocol

Based on the above discussion, we fully describe our concrete protocol. For this aim, we fix an error correction code, i.e., the pair of the encoder $\phi_{e,n}$ and the decoder $\phi_{d,n}$ with block length n. Then, combining the error correction code and universal$_2$ hash functions [14]–[16], we employ the wiretap code given in [19, Appendix A] using random seed S and we have the wiretap encoder $\phi_{e,n|S}$ and the wiretap decoder $\phi_{d,n|S}$. This code construction achieves the strong secrecy even in the continuous system [9], [18], [19].

Then, we propose the following two-way protocol.

(1) Bob generates the binary data sequence $B_1, \ldots, B_n \in \mathbb{F}_2$. Then, sends $(-1)^{B_1}, \ldots, (-1)^{B_n}$ via the channel described in (6).

(2) Alice makes the hard decision. Then, she obtains the binary data $A_1, \ldots, A_n$. In this case, A_i and B_i are connected via the binary symmetric channel with crossover probability ϵ_A, whose mathematical expression will be given later.

(3) To send the secret message M, using an auxiliary variable L, Alice applies the code $X^n = (X_1, \ldots, X_n) := \phi_{e,n|S}(M, L) \in \mathbb{F}_2^n$. Then, Alice sends $X'^n = (X'_1, \ldots, X'_n)$ to Bob via public channel, where $X'_i := A_i \oplus X_i$. Here, an auxiliary variable L is a variable independent of the message M, and is used to realize the secrecy of M.

(4) Bob decodes M by $\phi_{d,n|S}(X^{n\prime\prime})$, where $X^{n\prime\prime} = (X''_1, \ldots, X''_n)$ and $X''_i := X'_i \oplus B_i$.

To realize the public channel from Alice to Bob in the second phase, they employ the RF channel (2) with an error correcting code $(\hat{\phi}_{e,\hat{n}}, \hat{\phi}_{d,\hat{n}})$ different from the error correction $\phi_{e,n|S}$ so that the decoding error probability of the code $(\hat{\phi}_{e,\hat{n}}, \hat{\phi}_{d,\hat{n}})$ is close to zero (i.e., the bit error rate is e.g. below 10^{-6}). Here, if the coding rate of the code $(\hat{\phi}_{e,\hat{n}}, \hat{\phi}_{d,\hat{n}})$ is $\hat{R}$, they use the RF channel (2) $\hat{n} = n/\hat{R}$ times in Step (3) physically. That is, in Step (3), Alice sends $\hat{X}^{\hat{n}} = \hat{\phi}_{e,\hat{n}}(X'^n)$ to Bob via the RF channel (2) of coefficient η_B. Also, in Step (4), to get X'^n, Bob applies the decoder $\hat{\phi}_{d,\hat{n}}$ to the received $\hat{n}$ symbols via the RF channel (2) of coefficient η_B. Indeed, when the bit error rate of the public channel (i.e., the bit error rate of the code $(\hat{\phi}_{e,\hat{n}}, \hat{\phi}_{d,\hat{n}})$) is e.g. below 10^{-6}, it can be negligible in comparison with the bit error rate between A and B. Hence, we can consider that the bit error rate of the channel from X_i to X''_i given in Steps (3) and (4) almost equals that between A and B, in practice.

The above description has no authentication. However, it is possible by using universal$_2$ hash function [14], [15], which prevents active man-in-the-middle attack [44], while it is difficult to avoid active man-in-the-middle attacks without authentication [43]. The detail is discussed in [28] and the arXiv version of [29].

C. Secrecy Capacity When Eve Uses Hard Decision

When Eve has limited memory, it is natural that Eve uses hard detection decoding when receiving Z so that Eve obtains the binary variable E.

Indeed, the first phase can be regarded as a preparation step for the secure communication. In order to prevent Eve to make soft decision, Alice and Bob can consider the following strategy. Before starting the second phase, Alice and Bob continue the first phase so that the length of their obtained random numbers $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ is close to the limitation of their memory. In this case, the length of their obtained random numbers is across several coding blocks. Since satellite has a limitation of size of memory due to the limitation of physical space. it is natural that the size of Eve's memory is similar to that of Alice and Bob. In this case, it is difficult for Eve to keep the all the outcomes of soft decision, i.e., Eve needs to choose hard decision in this case. For example, the preceding paper [47], which is oriented to an application side, analyzed the security for the Poisson wiretap channel when Eve has limited memory, i.e., Eve uses hard detection decoding.

Using two independent Bernoulli random variables X_1 and X_2 on $\mathbb{F}_2$, we have

$$A = B \oplus X_1, \quad E = B \oplus X_2. \tag{7}$$

The crossover probability between A and B is $\epsilon_A = 0.5\mathrm{erfc}(\sqrt{\eta_A/2})$ and the crossover probability between E and B is $\epsilon_E = 0.5\mathrm{erfc}(\gamma_A\sqrt{\eta_A/2})$, where $\mathrm{erfc}(t)$ is defined in (4).

Hence, the problem is reduced to the case with BSC channels, which was discussed by Maurer [27]. Hence, the capacity $C^{\rm TW}_{\rm hard}(\gamma_A,\eta_A)$ when Eve uses hard detection is calculated to

$$\begin{aligned} C^{\rm TW}_{\rm hard}(\gamma_A,\eta_A) &= I(A;B|E) = I(A;B) - I(A;E) \\ &= H(B) - H(B|A) - (H(E) - H(E|A)) \\ &= H(E|A) - H(B|A) \\ &= h(\epsilon_E+\epsilon_A - 2\epsilon_E\epsilon_A) - h(\epsilon_A) \end{aligned} \tag{8}$$

because $H(B) = H(E) = h(\frac{1}{2})$ and the probability of $E \neq A$ is $\epsilon_E(1-\epsilon_A)+(1-\epsilon_E)\epsilon_A = \epsilon_E+\epsilon_A-2\epsilon_E\epsilon_A$. When $\gamma_A = \gamma_B$ and $\eta_A = \eta_B$, i.e., $\epsilon^*_B = \epsilon_A$ and $\epsilon^*_E = \epsilon_E$, we have

$$C^{\rm TW}_{\rm hard}(\gamma_A,\eta_A) \geq C^{\rm OW}_{\rm hard}(\gamma_B,\eta_B) \tag{9}$$

because $h(\epsilon_E+\epsilon_A-2\epsilon_E\epsilon_A) = h(\epsilon_E+\epsilon_A(1-2\epsilon_E)) \geq h(\epsilon_E) = h(\epsilon^*_E)$.

D. Secrecy Capacity When Eve Uses Soft Decision

When Eve has sufficient size of memory and her computation power is unlimited, she can employ soft decision decoding. That is, to consider Eve's best strategy, we need to address the case when Eve uses the variables Z and X'. To analyze this case, we use the Markov chain $A-B-Z$ and regard the first phase as the preparation for the second phase. Then, we apply the result of wiretap channel to the communication of the second phase with the result of the first phase. In the second phase, only the variable X reflects Alice's message and the variable A cannot be chosen by Alice. Hence, the input alphabet is given as X. Since Bob decodes Alice's message based on the variables B and X', the output alphabet is given as the pair of B and X'. Therefore, in the second phase, the channel from Alice to Bob is given as the conditional distribution $W_B := P_{B,X'|X}$, as illustrated in the conceptual model of Fig. 4. Similarly, the eavesdropper channel of the second phase is given as $W_E := P_{Z,X'|X}$. Since $A = X' \oplus X$, we have $P_{B,X'|X}(b,x'|x) = P_{B|A}(b|x' \oplus x)P_A(x' \oplus x)$. Hence, the Markov chain $A-B-Z$ condition guarantees that

$$\begin{aligned} &P_{Z,X'|X}(z,x'|x) \\ &\quad= \sum_b P_{Z|B}(z|b)P_{B|A}(b|x' \oplus x)P_A(x' \oplus x) \\ &\quad= \sum_b P_{Z|B}(z|b)P_{B,X'|X}(b,x'|x). \end{aligned} \tag{10}$$

Thus, the channel W_E is a degraded channel of the channel W_B. Further, the channels W_B and W_E are symmetric, the wiretap capacity is attained when P_X is the binary uniform distribution, and the wiretap capacity $C^{\rm TW}_{\rm soft}(\gamma_A,\eta_A)$ is calculated to

$$\begin{aligned} C^{\rm TW}_{\rm soft}(\gamma_A,\eta_A) &= I(X;X'B) - I(X;X'Z) \\ &= I(X;X') + I(X;B|X') \\ &\quad -(I(X;X') + I(X;Z|X')) \\ &= I(A \oplus X';B|X') - I(A \oplus X';Z|X') \\ &= I(A;B|X') - I(A;Z|X') \overset{(a)}{=} I(A;B) \\ &\quad -I(A;Z) \\ &= I(A;BZ) - I(A;Z) = I(A;B|Z), \end{aligned} \tag{11}$$

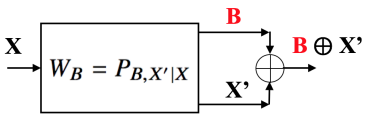

Fig. 4. Bob's computation channel model for the two-way protocol. Independently of whether Eve uses hard or soft detection, two-way secrecy capacity can be attained with this computation model.

where (a) follows from the independence of X' from A,B,Z, which can be shown by the uniformity of the conditional distribution $P_{X'|A}$. Therefore, the wiretap capacity $C^{\rm TW}_{\rm soft}$ is always positive regardless of γ_A, regardless the condition $\gamma_A < 1$ does not hold. The wiretap capacity expresses the limit of the secure transmission rate when we use a proper coding under the condition that the mutual information between the message and Eve's information goes to zero.

Further, the probability P_Z and the conditional probability $P_{B|Z}$ are calculated as

$$\begin{aligned} P_Z(z) &= \sum_{b=0}^{1} P_{Z,B}(z,b) = \sum_{b=0}^{1} P_{Z|B}(z|b)P_B(b) \\ &= \frac{1}{2\sqrt{2\pi}}(e^{-\frac{(z+\gamma_A\sqrt{\eta_A})^2}{2}} + e^{-\frac{(z-\gamma_A\sqrt{\eta_A})^2}{2}}), \end{aligned} \tag{12}$$

$$\begin{aligned} P_{B|Z}(b|z) &= \frac{P_{B,Z}(b,z)}{P_Z(z)} = \frac{P_{Z|B}(z|b)P_B(b)}{P_Z(z)} = \frac{P_{Z|B}(z|b)}{2P_Z(z)} \\ &= \frac{e^{-\frac{(z-(-1)^b\gamma_A\sqrt{\eta_A})^2}{2}}}{e^{-\frac{(z+\gamma_A\sqrt{\eta_A})^2}{2}} + e^{-\frac{(z-\gamma_A\sqrt{\eta_A})^2}{2}}}. \end{aligned} \tag{13}$$

Hence, due to the Markov chain $Z-B-A$, we can calculate the conditional mutual information;

$$I(A;B|Z=z) = h\Big(P_{B|Z}(0|z)\epsilon_A + P_{B|Z}(1|z)(1-\epsilon_A)\Big) - h(\epsilon_A).$$

Notice that $I(A;B|Z=z) = 0$ if and only if $P_{B|Z}(0|z)$ is 0 or 1. Hence, the capacity $C^{\rm TW}_{\rm soft}(\gamma_A,\eta_A)$ with Eve's soft decision is calculated as a function of η_A,γ by

$$\begin{aligned} C^{\rm TW}_{\rm soft}(\gamma_A,\eta_A) &= I(A;B|Z) \\ &= \int_{-\infty}^{\infty} P_Z(z)dz\Big(h\Big(P_{B|Z}(0|z)\epsilon_A + P_{B|Z}(1|z) \\ &\qquad (1-\epsilon_A)\Big) - h(\epsilon_A)\Big). \end{aligned} \tag{14}$$

Thus, unless $P_{B|Z}(0|z)$ is 0 or 1 for all z, (14) is strictly positive. That is, when γ_A is a finite value, $P_{B|Z}(0|z)$ is an intermediate value between 0 and 1 for all z. Hence, the capacity $C^{\rm TW}_{\rm soft}(\gamma_A,\eta_A)$ is strictly positive.

Even in this scenario, when X is also subject to the uniform distribution, $B \oplus X'$ is Bob's sufficient statistics with respect to X. Hence, we have $I(X;X' \oplus B) - I(X;X'Z) = I(X;X'B) - I(X;X'Z) = C^{\rm TW}_{\rm soft}(\gamma_A,\eta_A)$. Therefore, even when Bob uses only $B \oplus X'$ for his decoding while Eve uses the two variables Z and X', the capacity $C^{\rm TW}_{\rm soft}(\gamma_A,\eta_A)$ can be attained. Consequently, the channel W_B can be modeled as a computation channel as illustrated in Fig. 4.

Now, we compare $C^{\rm TW}_{\rm soft}(\gamma_A,\eta_A)$ and $C^{\rm OW}_{\rm soft}(\gamma_B,\eta_B)$ when $\gamma_A = \gamma_B = \gamma$ and $\eta_A = \eta_B = \eta$. For this comparison, we fix η and change γ. Due to the above discussion, when $\gamma > 1$,

$C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma,\eta)$ is larger than $C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma,\eta)$. In contrast, under the limit $\gamma \to 0$, we have

$$\begin{aligned}\lim_{\gamma\to 0} C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma,\eta) &= \log 2 - h(\epsilon_A) \\ &= I(B_{\mathrm{TW}};A_{\mathrm{TW}}) < I(B_{\mathrm{TW}};Y_{\mathrm{TW}}) \\ &= I(A_{\mathrm{OW}};Y_{\mathrm{OW}}) = I(X_{\mathrm{OW}};Y_{\mathrm{OW}}) \\ &= \lim_{\gamma\to 0} C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma,\eta), \end{aligned} \tag{15}$$

where the subscripts TW and OW of the random variables express the protocol to be considered. This opposite inequality is caused by the hard decision on Alice's received signal Y in the two-way protocol. Therefore, when γ is smaller than a certain threshold, $C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma,\eta)$ is smaller than $C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma,\eta)$. That is, the one-way protocol may have greater capacity than the two-way protocol for some threshold of γ. We have computed the value of such threshold as a function of the SNR, which is shown in Fig. 5.

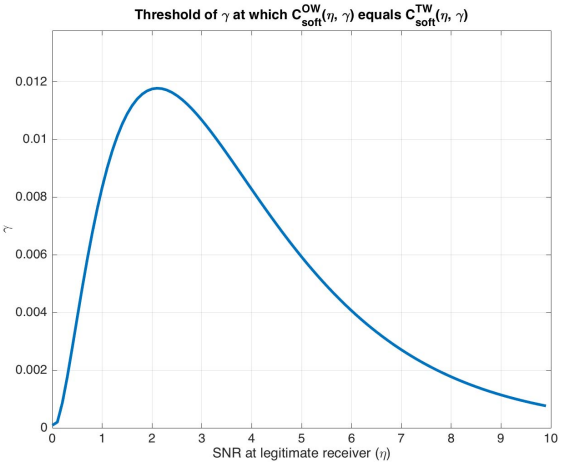

Fig. 5. Threshold values of γ at which $C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma,\eta)$ equals $C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma,\eta)$.

IV. Optimization

Here, to extract a higher communication speed, we consider how to optimize the channel parameters in the RF channel (6). When the power of transmitting antenna of Bob increases, the coefficient η_A increases and the ratio between the coefficients of signal in Alice's and Eve's sides is not changed. For simple analysis, we first assume that Alice and Bob can know the value of η_A by using test transmission, and control it by changing the power of transmitting antenna of Bob, where other components (e.g., the receiving antenna gains of Alice and Eve, the directions of antennas etc) are fixed. In practice, it is not so easy to know the value of the ratio γ_A because it depends on Eve's position. However, if we know the type of Eve's orbit, we know the range $\mathcal{G}$ of possible values of γ_A. In this case, we consider the worst case for Alice and Bob, i.e., $\gamma_{A,\max} := \max_{\gamma_A\in\mathcal{G}} \gamma_A$. In fact, when we have two possible values $\gamma_{A,1} > \gamma_{A,2}$ for the ratio, the channel to Eve with $\gamma_{A,2}$ is a degraded channel of the channel to Eve with $\gamma_{A,1}$. Hence [1], a secure code for the channel to Eve with $\gamma_{A,1}$ is also secure for the channel to Eve with $\gamma_{A,2}$. Therefore, it is sufficient to prepare a code with the largest value $\gamma_{A,\max}$. We optimize $C^{\mathrm{TW}}_{\mathrm{hard}}(\gamma_{A,\max},\eta_A)$ and $C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma_{A,\max},\eta_A)$ by changing η_A. Here, the parameter $\eta_A = P/N_A$ can be changed by changing the power P. The optimum secret capacities are given as

$$C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma_{A,\max}) := \max_{\eta_A} C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma_{A,\max},\eta_A) \tag{16}$$

$$C^{\mathrm{TW}}_{\mathrm{hard}}(\gamma_{A,\max}) := \max_{\eta_A} C^{\mathrm{TW}}_{\mathrm{hard}}(\gamma_{A,\max},\eta_A). \tag{17}$$

Hence, we need to find suitable value for η_A dependently of $\gamma_{A,\max}$. $\eta^{\mathrm{TW}}_{\mathrm{soft}}(\gamma_{A,\max}) := \mathrm{argmax}_{\eta_A} C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma_{A,\max},\eta_A)$ and $\eta^{\mathrm{TW}}_{\mathrm{hard}}(\gamma_{A,\max}) := \mathrm{argmax}_{\eta_A} C^{\mathrm{TW}}_{\mathrm{hard}}(\gamma_{A,\max},\eta_A)$ are the optimal intensities of η_A.

[1]Note that in a traditional communication scenario, the transmission power is designed so that the link budget can provide a required link quality (e.g. in terms of target bit error rate) is met. However, here we are designing a secure communication scenario and therefore the link budget is constrained to meet the security requirements. Such security requirement means here that the link budget is designed to provide the maximum secrecy capacity.

In fact, we can apply a similar optimization to the one way case. In this case, we consider the following optimum secret capacities;

$$C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma_{B,\max}) := \max_{\eta_B} C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma_{B,\max},\eta_B) \tag{18}$$

$$C^{\mathrm{OW}}_{\mathrm{hard}}(\gamma_{B,\max}) := \max_{\eta_B} C^{\mathrm{OW}}_{\mathrm{hard}}(\gamma_{B,\max},\eta_B), \tag{19}$$

where $\gamma_{B,\max}$ is the maximum value among possible values of γ_B. $\eta^{\mathrm{OW}}_{\mathrm{soft}}(\gamma_{B,\max}) := \mathrm{argmax}_{\eta_B} C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma_{B,\max},\eta_B)$ and $\eta^{\mathrm{OW}}_{\mathrm{hard}}(\gamma_{B,\max}) := \mathrm{argmax}_{\eta_B} C^{\mathrm{OW}}_{\mathrm{hard}}(\gamma_{B,\max},\eta_B)$ are the optimal intensities of η_B.

Now we show numerical calculations to compare the capacities of the one-way protocol and the two-way protocol. For easy visualization, we calculate numerical values assuming $\eta_B = \eta_A$ and $\gamma_A = \gamma_B$.

Fig. 6 shows the comparison among the optimum secret capacities $C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma_{A,\max})$, $C^{\mathrm{TW}}_{\mathrm{hard}}(\gamma_{A,\max})$, $C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma_{B,\max})$, and $C^{\mathrm{OW}}_{\mathrm{hard}}(\gamma_{B,\max})$. We can observe that while for the one-way protocol the capacity is zero whenever the eavesdropper has higher SNR than Bob, in the two-way protocol the capacity is always positive and greater than zero. We have computed the difference between optimal secrecy capacities $C^{\mathrm{OW}}_{\mathrm{soft}}(\gamma_{B,\max})$ and $C^{\mathrm{TW}}_{\mathrm{soft}}(\gamma_{A,\max})$ for $\gamma_{B,\max} = \gamma_{A,\max} = \gamma_{\max}$ as Fig. 7. We observe that as obtained theoretically in (15), the OW secrecy capacity is slightly bigger than the TW secrecy capacity when the channel to Bob is advantageous over that to Eve. However, also in agreement with the theoretical derivations, the TW secrecy capacity starts to be bigger than the OW when the channel to Bob is not so advantageous over that to Eve. In Fig. 7, we observe in the zoom plot that this occurs at $\gamma_{max} = 0.3185$.

Fig. 8 shows the optimal intensities $\eta^{\mathrm{TW}}_{\mathrm{soft}}(\gamma_{A,\max})$, $\eta^{\mathrm{TW}}_{\mathrm{hard}}(\gamma_{A,\max})$, $\eta^{\mathrm{OW}}_{\mathrm{soft}}(\gamma_{B,\max})$, and $\eta^{\mathrm{OW}}_{\mathrm{hard}}(\gamma_{B,\max})$. These values are the optimal choices for the intensity η_A or η_B in the respective cases.

V. Application to Real Satellite Communication

Now, we apply our analysis to the following two types of real satellite communication scenarios.

(I) The transmitter is the earth station and the legitimate receiver is the GEO satellite in the noisy Gaussian

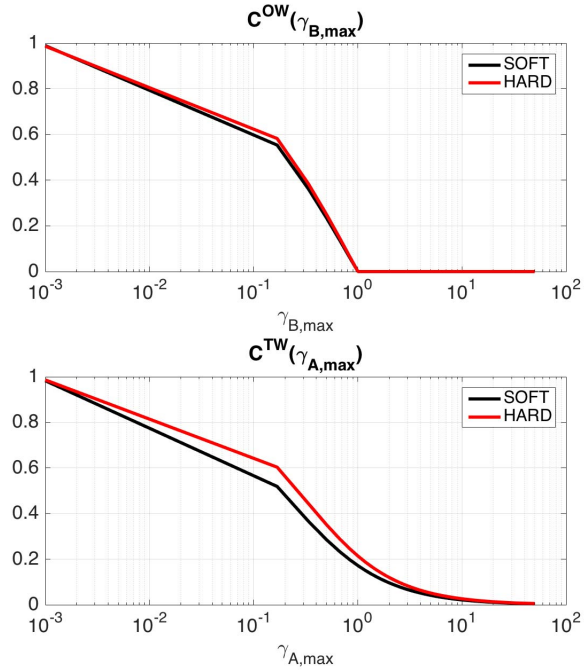

Fig. 6. Comparison among the optimum secret capacities $C_{\rm soft}^{\rm TW}(\gamma_{A,\max})$, $C_{\rm hard}^{\rm TW}(\gamma_{A,\max})$, $C_{\rm soft}^{\rm OW}(\gamma_{B,\max})$, and $C_{\rm hard}^{\rm OW}(\gamma_{B,\max})$. The vertical axis expresses these optimal capacities. The horizontal axis expresses $\gamma_{A,\max}$ and $\gamma_{B,\max}$ with log scale, which runs from 10^{-3} to 10^{2}.

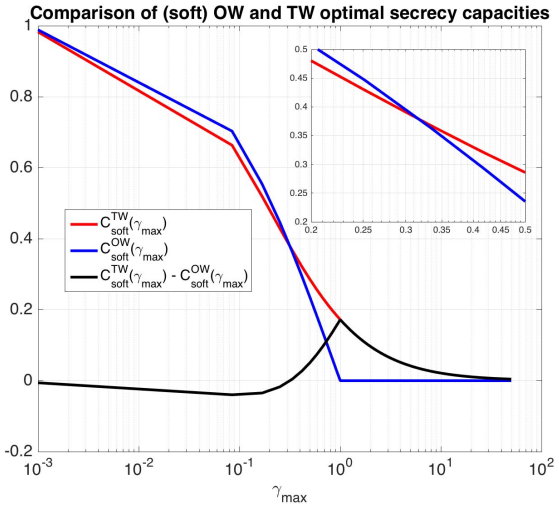

Fig. 7. Comparison of OW and TW optimal secrecy capacities assuming $\gamma_{B,\max} = \gamma_{A,\max} = \gamma_{\max}$.

channels (2) and (6). That is, Alice is the earth station and Bob is the GEO satellite in the OW, and Bob is the earth station and Alice is the GEO satellite in the TW. Notice that the noiseless public channel from the GEO satellite to the earth station is also required by using a proper combination of wireless communication and outer error correcting code in the TW. The noisy Gaussian channels (2) and (6) of these scenarios are explained in the two figures on the top in Fig 9, which describe the case when the Earth station is the information data communication source in the noisy

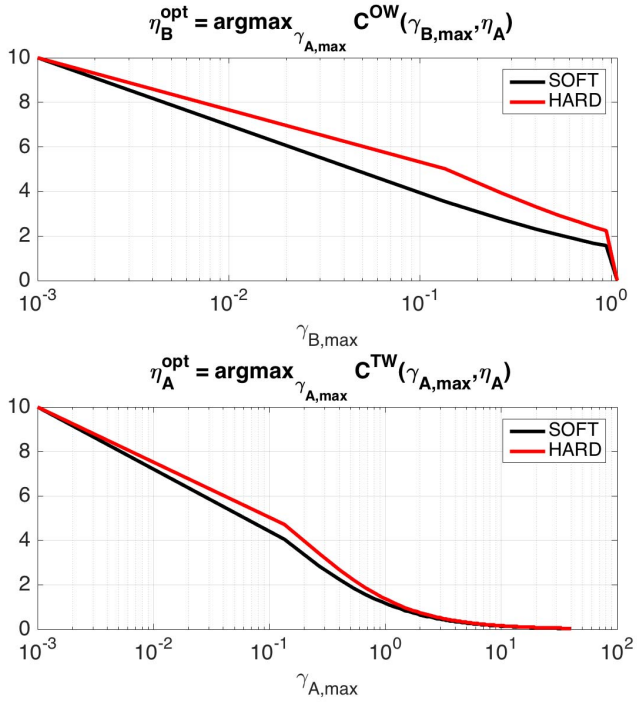

Fig. 8. Optimal intensities $\eta_{\rm soft}^{\rm TW}(\gamma_{A,\max})$, $\eta_{\rm hard}^{\rm TW}(\gamma_{A,\max})$, $\eta_{\rm soft}^{\rm OW}(\gamma_{B,\max})$, and $\eta_{\rm hard}^{\rm OW}(\gamma_{B,\max})$. The vertical axis expresses these optimal intensities with log scale. The horizontal axis expresses $\gamma_{A,\max}$ and $\gamma_{B,\max}$ with log scale, where $\gamma_{A,\max}$ runs from 10^{-3} to 10^{2}, but $\gamma_{B,\max}$ runs from 10^{-3} to 1.

Gaussian channel. In this case, the eavesdropper, Eve is a low Earth orbit (LEO) satellite or a medium Earth orbit (MEO) satellite.

(II) The transmitter is the GEO satellite and the legitimate receiver is the earth station in the noisy Gaussian channels (2) and (6). That is, Alice is the GEO satellite and Bob is the earth station in the OW, and Bob is the GEO satellite and Alice is the earth station in the TW. The noisy Gaussian channels (2) and (6) of these scenarios are explained in the two figures on the down in Fig 9, which describe the case when the GEO satellite is the information data communication source in the noisy Gaussian channel. In this case, Eve is an LEO satellite, an MEO satellite, or a GEO satellite.

Let $\alpha(\theta)$ be the normalised transmitter's antenna radiation's pattern of the earth station in response to the angle θ from the boresight axis directed to the GEO satellite to account for spatial attenuation. The function $\alpha(\theta)$ can be considered exactly in case the (normalized) antenna pattern is known, or otherwise it can be considered in terms of the allowed emission of radiation according to space regulations. A typical analytical expression for $\alpha(\theta)$ is

$$\alpha(\theta) := \frac{J_1(k\sin(\theta))}{2k\sin(\theta)} + 36\frac{J_3(k\sin(\theta))}{(k\sin(\theta))^3} \tag{20}$$

where $k = 2.0712/\sin(\theta^{3dB})$, with θ^{3dB} being the one-sided half-power angular beamwidth and J_1 and J_3 are the Bessel functions of the first kind, of order one and three respectively. Our interest is the parameter $\alpha(\theta_E)$ in the specific angle θ_E between Bob's and Eve's directions. g_L and g_E are legitimate

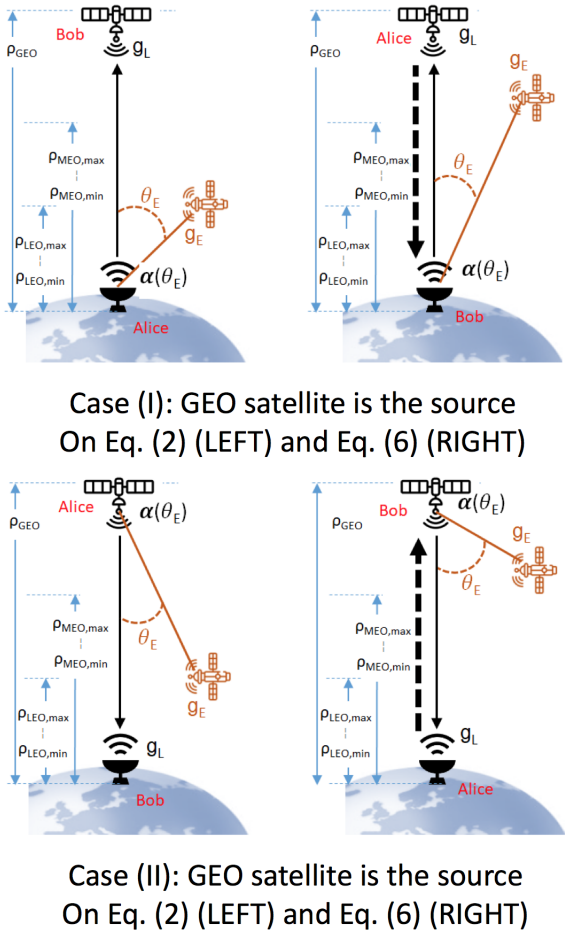

Fig. 9. Geometry considered to illustrate the real satellite communication secrecy analysis. The two figures on the top describe Case (I), in which the Earth station is the source in the noisy Gaussian channels (2) and (6). The two figures on the bottom describe Case (II), in which the satellite is the source in the noisy Gaussian channels (2) and (6). The geometries for OW (left) and TW (right) cases illustrate LEO and MEO orbit heights. The dashed line expresses the noiseless public channel from Alice to Bob in the TW case. The eavesdropper can be at any LEO or MEO orbit while the legitimate transmitter and receiver are either the earth station of the GEO satellite.

and eavesdropper's receiver's antenna gains towards Earth station. Now we introduce a model for the coefficient that gives Eve's signal strength relative to Bob's signal in (2) and (6) (see [18], [19], [31]). We first introduce the parameter μ to account for the relative antenna gain, i.e., $\mu := \sqrt{g_L/g_E}$. We also define $\beta(r, \rho_E)$ to account for relative propagation losses between Bob and Eve as

$$\beta^2(r, \rho_E) = \frac{\rho_L^2}{\rho_E^r}. \tag{21}$$

The exponent r accounts for the power attenuation decay that affects eavesdropper's propagation channel. Different values of the exponent model correspond to different assumptions about eavesdropper. Specifically, the eavesdropper can be modeled as a terrestrial, aerial or satellite station. For example, while for the satellite case $r = 2$, in case of aerial eavesdropper, a good assumption is to consider a large scale two-ray ground multipath model,with $r > 2$. Then, we discuss the parameter γ_B in the OW (2) and the parameter γ_A in the TW (6) because the channel (2) in the OW case is the same as the channel (6)

TABLE I
SUMMARY OF OPTIMUM CAPACITIES IN SATELLITE MODELS

$\gamma_{B,\max} = \gamma_{A,\max}$	$C_{\text{soft}}^{\text{TW}}$	$C_{\text{hard}}^{\text{TW}}$	$C_{\text{soft}}^{\text{OW}}$	$C_{\text{hard}}^{\text{OW}}$
$\gamma_{(\text{I})\,\text{MEO}}$	0.029	0.036	0	0
$\gamma_{(\text{I})\,\text{LEO}}$	3.6×10^{-4}	3.9×10^{-4}	0	0
$\gamma_{(\text{II})\,\text{GEO}}$	1.4×10^{-12}	1.4×10^{-12}	0	0
$\gamma_{(\text{II})\,\text{MEO}}$	0.086	0.108	0	0
$\gamma_{(\text{II})\,\text{LEO}}$	0.159	0.198	0	0

in the TW case in each scenario (I) or (II). These parameters are given as

$$\gamma(\theta_E, \rho_E, r, \mu, \gamma_n) := \frac{\alpha(\theta_E)\,\mu\beta(r, \rho_E)}{\sqrt{\gamma_n}}, \tag{22}$$

where, γ_n is the ratio between the powers of the noises in legitimate receiver's and eavesdropper's detectors. In doing a secrecy analysis, we assume in which orbit Eve is, but we don't make any assumption on which angle she is (since she is orbiting). In this case, to guarantee the security, we need to consider the worst case. For this aim, we consider the possible range $\mathcal{R}$ of the value (θ_E, ρ_E). Then, the maximums of γ_B and γ_A are calculated to

$$\gamma_{B,\max} = \gamma_{A,\max} = \max_{(\theta_E, \rho_E) \in \mathcal{R}} \gamma(\theta_E, \rho_E, r, \mu, \gamma_n). \tag{23}$$

Now, we assume representative values for Eve's possible orbits according to basic orbital mechanics [30] and usual low or medium orbit terminology. In Case (I), when Eve is MEO (LEO), we assume that the height of Eve's orbit runs from $\rho_{\text{MEO}\,\min} = 5000$ to $\rho_{\text{MEO}\,\max} = 20000$ km ($\rho_{\text{LEO}\,\min} = 150$ to $\rho_{\text{LEO}\,\max} = 2000$ km). Also, we assume that the height of our GEO orbit is $\rho_{\text{GEO}} = 36000$ km. Since the maximum of $\alpha(\theta_E)$ is realized by $\theta_E = 0°$, when Eve is MEO (LEO), we have $\gamma(0°, \rho_E, r, \mu, \gamma_n) = \frac{\mu\rho_{\text{GEO}}}{\rho_{\text{MEO}\,\min}^{r/2}\sqrt{\gamma_n}}$ ($= \frac{\mu\rho_{\text{GEO}}}{\rho_{\text{LEO}\,\min}^{r/2}\sqrt{\gamma_n}}$). For illustration, we now assume Eve equally powerful than the legitimate receiver, i.e. $\mu = 1$ and $\gamma_n = 1$. Also, we have $r = 2$ for both LEO and MEO. Hence, the maximum $\gamma_{B,\max} = \gamma_{A,\max}$ is given as $\gamma_{(\text{I})\,\text{MEO}} := \frac{\rho_{\text{GEO}}}{\rho_{\text{MEO}\,\min}} = 36000/5000 = 7.2$ for the case when Eve is MEO, and it is given as $\gamma_{(\text{I})\,\text{LEO}} := \frac{\rho_{\text{GEO}}}{\rho_{\text{LEO}\,\min}} = 36000/150 = 240$ for the case when Eve is LEO. Then, we have the capacities of the worst case as Table I. While these capacities are small in comparison with the conventional communication, we see that the secure communication is possible in these scenarios only in the TW case.

Applying same reasoning in Case (II), when Eve is MEO, the minimum of ρ_E is $\rho_{\text{GEO}} - \rho_{\text{MEO}\,\max}$ at $\theta_E = 0°$ and the maximum of $\alpha(\theta_E)$ is realized by $\theta_E = 0°$. The same observation holds when Eve is LEO or GEO. In this case, it seems reasonable to assume the legitimate receiver having a more powerful antenna gain and less detector noise than the eavesdropper. Hence, we can again assume $\mu = 1$ and $\gamma_n = 1$. Again, we also have $r = 2$. Therefore, when Eve is MEO, the maximum $\gamma_{B,\max} = \gamma_{A,\max}$ is calculated to be $\gamma_{(\text{II})\,\text{MEO}} := \frac{\rho_{\text{GEO}}}{(\rho_{\text{GEO}} - \rho_{\text{MEO}\,\max})} = 36000/(36000 - 20000) = 9/4$. When Eve is LEO, it is calculated to be $\gamma_{(\text{II})\,\text{LEO}} := \frac{\rho_{\text{GEO}}}{(\rho_{\text{GEO}} - \rho_{\text{LEO}\,\max})} = 36000/(36000 - 2000) = 18/17$. When Eve is GEO, the minimum distance between the transmitter of

the initial transmission and Eve is 1km. Hence, it is calculated as $\gamma_{(\mathrm{II})\,\mathrm{GEO}} := \frac{\rho_{\mathrm{GEO}}}{1} = 36000$.

VI. Conclusions and Further Improvements

We have introduced a two-way protocol for the BPSK modulation to overcome the limitations of the classic (one-way) wiretap physical layer security protocol. While the secrecy capacity of the one-way protocol is zero when Eve's channel is better than Bob's channel (i.e $\gamma_B > 1$), we show that the two-way protocol always provides positive capacity with higher gains even for $\gamma_A \geq 1$ and $\gamma_B \geq 1$ when the noises exist and are independent. We have shown that the one-way protocol cannot realize secure communication in realistic scenarios of satellite communication, while our two-way protocol can realize secure communication in these realistic scenarios. Notice that this conclusion does not change whenever the maximum of possible values of γ_A and γ_B is greater than 1.

For example, in the scenario (I), we have the transmission rate 3.6×10^{-4} with the worst case analysis in the two-way protocol with Eve's soft decision while the eavesdropper has an extremely stronger power in the detection process than the legitimate receiver, i.e., the eavesdropper has 240 times power in the receiving signal as the legitimate receiver. The conventional one-way method cannot realize secure communication in this case. This numerical analysis shows that even in this case, we can realize secure communication with the same physical device if we accept approximately e.g. one thousandth reduction of the speed of the conventional communication without secrecy (e.g., 1 Gbps is reduced to 1 Mbps). While this cost seems very large, the cost is still much smaller than quantum key distribution (QKD) [32] due to the following reason. Since QKD requires expensive devices, it is available only for extremely limited users (big governments and/or big military organizations). However, since the proposed method is based on the conventional satellite system, even though the transmission speed is very low, it is available for ordinary users. In fact, the user can use the proposed system when the size of communication is reduced, e.g., the user uses only e-mail instead of video. On the other hand, in the scenario (II), we assume that the receiving antenna of the earth station has almost same performance as that of Eve. Under such a worst case assumption, we obtain very small transmission speed. To improve this, the receiving antenna of the earth station needs to be more powerful than that of Eve. However, to realize this condition, the earth station needs to prepare an expensive receiving device, which may or may not imply to restrict ordinary users since such higher cost is shared by all service/users sharing the earth station. In this sense, the scenario (II) may seem less practical for ordinary users. In any case, to realize secure communication, it is sufficient to share secure keys between two users. because one-time use of shared secure key realizes secure communication with both directions. Hence, it is sufficient to establish secure communication only with one direction. Therefore, the scenario (I) of TW is enough for our purpose.

However, in the scenario (I) of TW, if Eve is an eavesdropping terrestrial node, e.g., a drone near the terrestrial earth station, she has better performance than LEO/MEO satellite. In this case, the secure transmission rate is worse than 3.6×10^{-4} when the angle θ_E is set to be 0. However, the possible minimum angle θ_E of this case in practice is larger than that in the case with an eavesdropping LEO/MEO satellite. Therefore, it is needed to evaluate the secure transmission rate with an eavesdropping terrestrial node and the possible minimum angle θ_E. However, it is not so easy to find the minimum angle θ_E among practically possible values. Therefore, this type of analysis is remained as a future study.

As the price to pay, the protocol requires higher delay to establish the secure channel when compared to the one-way. However, this cost is much cheaper than the previous two-way protocols in the papers [23]–[26] because they require many rounds of communication while our protocol requires only two rounds of communication. On the other hand, the transmission of information can be over a public channel while for randomness sharing, the channel needs to be previously authenticated like [28], [29]. As discussed in [28], [29], the required amount of the random numbers shared between Alice and Bob in advance is the logarithm order of the size of intended secure communication. Also, this cost is much cheaper than the realization of quantum key distribution. Therefore, considering the cost-benefit performance, we find that our two-way method is useful. Furthermore, the bias of the variable B may reduce the effectiveness of the protocol and reduce the secrecy capacity gains. To improve this problem, we often distill uniform random numbers from the thermal noise. It is known that it is possible to distill uniform random numbers by applying a hash function to a biased random numbers [9], [10], [12], [13]. To obtain the ultimate secure uniform random number, we may employ quantum random number generator [33]–[35], which requires much cheaper cost than quantum key distribution because it does not need quantum communication.

Unfortunately, this paper discusses only the asymptotic performance. Since the implemented communication system has finite-length codes, we need to evaluate the security of finite-length codes for its practical application [36]–[40]. Since the finite-length analysis depends on the choice of the security criterion, we need to be careful of its choice [7], [10]. As such a study is beyond the focus on this paper, it is considered as a future study. Furthermore, it is well known that a good model for the land mobile satellite (LMS) channel model is a Markov model [48]. Hence, it is a completely different channel from (6). Therefore, follow up studies also include considering different satellite channel models such as fading models accounting for frequency-dependent atmospheric effects and for the case of mobile (legitimate) users.

References

[1] Y. Liang, H. V. Poor, and S. S. Shamai (Shitz), *Information-Theoretic Security* (Foundations and Trends in Communications and Information Theory), vol. 5, nos. 1–5. Delft, Netherlands: Now Publishers, 2009.

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

[3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

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

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

[6] I. Csiszár, "Almost independence and secrecy capacity," *Problems Inf. Transmiss.*, vol. 32, no. 1, pp. 40–47, 1996.

[7] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.

[8] T. S. Han:, *Information-Spectrum Methods in Information Theory*. New York, NY, USA: Springer-Verlag, 2002.

[9] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3989–4001, Jun. 2011.

[10] M. Hayashi, "Tight exponential analysis of universally composable privacy amplification and its applications," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7728–7746, Nov. 2013.

[11] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

[12] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[13] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM J. Comput.*, vol. 28, no. 4, pp. 1364–1396, Jan. 1999.

[14] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *J. Comput. Syst. Sci.*, vol. 22, no. 3, pp. 265–279, Jun. 1981.

[15] H. Krawczyk, "LFSR-based hashing and authentication," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 839. New York, NY, USA: Springer-Verlag, 1994, pp. 129–139.

[16] M. Hayashi and T. Tsurumaru, "More efficient privacy amplification with less random seeds via dual universal hash function," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 2213–2232, Apr. 2016.

[17] 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.

[18] Á. Vázquez-Castro and M. Hayashi, "Information-theoretic physical layer security for satellite channels," in *Proc. IEEE Aerosp. Conf.*, Big Sky, MT, USA, Mar. 2017, pp. 1–14.

[19] Á. Vázquez-Castro and M. Hayashi, "Physical layer security for RF satellite channels in the finite-length regime," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 981–993, 2018.

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

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

[22] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[23] H. Wen, G. Gong, and P.-H. Ho, "Build-in wiretap channel I with feedback and LDPC codes," *J. Commun. Netw.*, vol. 11, no. 6, pp. 538–543, Dec. 2009.

[24] Y. Feng, X.-Q. Jiang, J. Hou, H.-M. Wang, and Y. Yang, "An efficient advantage distillation scheme for bidirectional secret-key agreement," *Entropy*, vol. 19, no. 9, p. 505, Sep. 2017.

[25] G. Zhang, H. Wen, J. Pu, and J. Tang, "Build-in wiretap channel I with feedback and LDPC codes by soft decision decoding," *IET Commun.*, vol. 11, no. 11, pp. 1808–1814, Aug. 2017.

[26] 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.

[27] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[28] C.-H. F. Fung, X. Ma, and H. F. Chau, "Practical issues in quantum-key-distribution postprocessing," *Phys. Rev. A, Gen. Phys.*, vol. 81, no. 1, 2010, Art. no. 012318.

[29] M. Hayashi, "Secure wireless communication under spatial and local Gaussian noise assumptions," in *Proc. IEEE Int. Symp. Inf. Theory*, Aachen, Germany, Jun. 2017, pp. 1698–1702. [Online]. Available: https://arxiv.org/abs/1604.00635

[30] V. A. Vladimir and A. Chobotov, *Orbital Mechanics* (AIAA Education Series), 3rd ed. Reston, VA, USA: AIAA, Sep. 2002, p. 460.

[31] Á. Vázquez-Castro and M. Hayashi, "One-way and two-way physical layer security protocols for the Gaussian satellite channel," in *Proc. IEEE Int. Conf. Commun. (ICC), SAC Satell. Space Commun. Track Satell. Space Commun.*, Shanghai, China, May 2019, pp. 1–7.

[32] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175–179.

[33] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, no. 1, 2017, Art. no. 015004.

[34] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *NPJ Quantum Inf.*, vol. 2, p. 16021, Jun. 2016.

[35] M. Hayashi and H. Zhu, "Secure uniform random-number extraction via incoherent strategies," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 1, 2018, Art. no. 012302.

[36] S. Watanabe and M. Hayashi, "Non-asymptotic analysis of privacy amplification via Rényi entropy and inf-spectral entropy," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, Jul. 2013, pp. 2715–2719.

[37] M. Hayashi, H. Tyagi, and S. Watanabe, "Strong converse for a degraded wiretap channel via active hypothesis testing," in *Proc. 52nd Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep./Oct. 2014, pp. 148–151.

[38] M. Hayashi, H. Tyagi, and S. Watanabe, "Secret key agreement: General capacity and second-order asymptotics," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3796–3810, Jul. 2016.

[39] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.

[40] M. Hayashi, "Semi-finite length analysis for information theoretic tasks," 2018, *arXiv:1811.00262*. [Online]. Available: http://arxiv.org/abs/1811.00262

[41] *Digital Video Broadcasting (DVB). Second Generation Framing Structure, Channel Coding and Modulation Systems for Broadcasting, Interactive Services, News Gathering and Other Broadband Satellite Applications (DVB-S2)*, Standard ETSI EN 302 307 V1.2.1 (2009-08), European Standard (Telecommunications Series), 2009.

[42] J. Proakis, *Digital Communications*, 4th ed. New York, NY, USA: McGraw-Hill, 2001.

[43] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in *Computer Security—ESORICS* (Lecture Notes in Computer Science), vol. 7459, S. Foresti, M. Yung, and F. Martinelli, Eds. Berlin, Germany: Springer, 2012.

[44] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016.

[45] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

[46] G. Bassi, P. Piantanida, and S. Shamai, "The wiretap channel with generalized feedback: Secure communication and key generation," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2213–2233, Apr. 2019.

[47] H. Endo, T. S. Han, T. Aoki, and M. Sasaki, "Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels," *IEEE Photon. J.*, vol. 7, no. 5, pp. 1–18, Oct. 2015.

[48] F. P. Fontan, M. Vázquez-Castro, C. E. Cabado, J. P. Garcia, and E. Kubista, "Statistical modeling of the LMS channel," *IEEE Trans. Veh. Technol.*, vol. 50, no. 6, pp. 1549–1567, Nov. 2001.

Masahito Hayashi (Fellow, IEEE) received the B.S. degree from the Faculty of Sciences, Kyoto University, Japan, in 1994, and the M.S. and Ph.D. degrees in mathematics from Kyoto University, Japan, in 1996 and 1999, respectively. He worked at Kyoto University as a Research Fellow of the Japan Society of the Promotion of Science (JSPS) from 1998 to 2000, and worked at the Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN, from 2000 to 2003, and worked at the ERATO Quantum Computation and Information Project, Japan Science and Technology Agency (JST), from 2000 to 2006, as the Research Head. He worked at the Graduate School of Information Sciences, Tohoku University, from 2007 to 2012, as an Associate Professor. In 2012, he joined the Graduate School of Mathematics, Nagoya University, as a Professor. Also, he worked at the Centre for Quantum Technologies, National University of Singapore, from 2009 to 2012, as a Visiting Research Associate Professor, and as a Visiting Research Professor since 2012. He has been working at the Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, China, since 2018, as a Visiting Professor, and at the Center for Quantum Computing, Peng Cheng Laboratory, China, since 2019, as a Research Scientist. His research interests include classical and quantum information theory and classical and quantum statistical inference. In 2011, he received Information Theory Society Paper Award (2011) for "Information-Spectrum Approach to Second-Order Coding Rate in Channel Coding." In 2016, he received the Japan Academy Medal from the Japan Academy and the JSPS Prize from the Japan Society for the Promotion of Science.

Ángeles Vázquez-Castro (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in telecommunications engineering from the Engineering School, Vigo University, Spain, in 1994 and 1998, respectively. Her Ph.D. was granted by the European Space Agency to develop land mobile satellite channel models, which were later used for the development of satellite Digital Video Broadcasting (DVB) satellite communication standards. Until 2002, she worked on satellite communications optimization across layers at University Carlos III University, Madrid, and University of Southern California, Los Angeles, CA, USA, as an Assistant and Visiting Professor, respectively. From 2002 to 2004, she held a Research Fellow position at the European Space Agency to work at the Space Research and Technology Centre, Noordwijk, The Netherlands, to develop scheduling algorithms, which are now a part of the guidelines of DVB-S2 standard. Since 2004, she has been an Associate Professor with the Autonomous University of Barcelona, Spain, leading research projects for the development of space technology, with results published in more than 150 peer-reviewed scientific papers (two best paper awards), 12 book chapters, one book as an editor, and holds two patents. She is a European expert in space communications of SatNEx, a scientific network funded by the European Space Agency. Her current research is focused on secure information communication and networking for space.