Joint Transmission and Computation Power Allocations for Satellite Communication Security

Suhyeon Jeon*, Jeongho Kwak*, and Jihwan P. Choi†
*Dep. of Electrical Engineering and Computer Science, DGIST, Korea
†Dep. of Aerospace Engineering, KAIST, Korea
Email: jsh6327@dgist.ac.kr, jeongho.kwak@dgist.ac.kr, jhch@kaist.ac.kr

***Abstract*—Due to introduction of the non-terrestrial network (NTN) and satellite-air-terrestrial integrated network (SATIN), many applications using satellites are being expected and this will result in a severe security issue. In this paper, we propose a satellite communication security method that jointly considers signal transmission and security computation power based on the orthogonal multiple access (OMA). Before transmission, satellite estimates a security threat based on the number of eavesdroppers (Eves) in the large satellite beam coverage as wide as 50 km for LEO satellites at the L-band. With the security threat, the satellite splits onboard power for signals and security, and controls a beam size. Through the sum capacity optimization problem, we derive the optimal onboard power allocation and security algorithm selection with respect to security threats and channel conditions.**

I. Introduction

Since the global Internet service projects, such as Starlink and OneWeb, have been launched recently, the need of satellite communications is increasing drastically. Also, the non-terrestrial network (NTN) and satellite-air-terrestrial integrated network (SATIN) have been studied for 6G development. Due to the data traffic explosion by NTN and SATIN, security can be one of the important problems [1].

For the satellite network security, encryption techniques and physical layer security (PLS) have been studied, respectively. For the encryption technique, the fault-tolerant encryption method is proposed for the satellite space missions. Based on the self-recovery property, the cipher feedback (CFB) mode was combined with advanced encryption standard (AES) to relax the fault propagation by the space radiation effect [2]. For PLS, a joint design of transmission power minimization and secure beamforming weight was proposed [3]. The complete zero-forcing beamforming eliminates co-channel interference and nulls eavesdropping signals. However, the encryption technique requires additional cost of time and power, which incurs performance reduction of the power-limited satellite system. Power for security computations can be as huge as power for signal transmissions. In addition, the most of PLS literatures discuss a framework on the scenario with transmitter, receiver, and a single eavesdropper (Eve), but the satellite beam coverage is very wide and multiple Eves can hide.

This work was supported in part by a grant from the Institute of Information & Communications Technology Planning & Evaluation (IITP) funded by the Korean government, Ministry of Science and ICT (No. 2018-0-01658, Key Technologies Development for Next-Generation Satellites), and in part by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2022-0-00704).

In this paper, we propose a satellite communication security considering transmission and computation power jointly. Before signal transmissions, a security threat is estimated with respect to the number of Eves in the satellite beam. Based on the security threat, a security algorithm pair of encryption and message authentication code (MAC) is determined, an onboard power is split into three parts of non-encryption signals, encryption signals and security calculation, and then the beam size is also controlled. With this modeling, we design a joint optimization problem of onboard power allocation and security algorithm selection. For simultaneous transmission of two signals, we use a scheme of orthogonal multiple access (OMA) and equal frequency-sharing. We derive the optimal policy of onboard power according to the security threat and signal attenuation due to the rain effects.

The rest of this paper is organized as follows. Section II shows the system model and derivation of the security threat based on the number of Eves. The optimal onboard power allocation and security algorithm selection are derived in section III. The conclusion is given in section IV.

II. System Model and Problem Formulation

The satellite network system can be exposed to multiple eavesdropping attacks by Eves. The satellite transmits two signals of non-encryption (NENC) and encryption (ENC) for user i. In the beam for user i, multiple Eves $e_{i,k} \in \boldsymbol{\mathcal{K}_i}$ can hide.

Before signal transmission, satellite estimates a security threat based on the number of Eves. In this paper, we consider the non-colluding eavesdropping attack where Eves do not cooperate. Therefore, the satellite takes into account the maximum signal-to-noise ratio (SNR) value among all of Eves. The security threat is derived by [4]

$$S_i = \mathbb{P}\Big[\max_{k\in\boldsymbol{\mathcal{K}}_i} \gamma_{i,k} \geq \gamma_t\Big], \tag{1}$$

where $\gamma_{i,k} = \frac{nH_{i,k}^2\bar{P}}{\omega^2 WN_0}$ is the SNR of Eve. $H_{i,k} = \alpha_i h_{i,k}$ is the small-scale channel gain of rain attenuation α_i^2 and Nakagami-m multi-path fading $h_{i,k}$. $\bar{P}$ is uniform power, and $\omega = \frac{\lambda L}{D}$ is the satellite beamwidth with wavelength λ, satellite altitude L, and antenna size D, γ_t is a threshold for decoding the satellite signal.

Based on the security threat, the satellite splits onboard power into three parts of NENC and ENC signals, and security calculation, given as

$$P_i = P_i^{ne} + P_i^e + P_i^c = \{1-(\phi+1)S_i\}P_i + S_iP_i + \phi S_iP_i,\ S_i < \frac{1}{\phi+1}, \quad (2)$$

where $0 \le \phi \le 1$ is a power-splitting coefficient. Transmit power is inversely proportional to the squared beamwidth, which leads to the beamforming strategy as follows:

$$\omega_{i,ne} = \frac{\lambda L}{D\sqrt{1-(\phi+1)S_i}},\ \omega_{i,e} = \frac{\lambda L}{D\sqrt{S_i}}. \quad (3)$$

With this power splitting strategy, channel capacities of NENC and ENC signals based on the OMA are derived as

$$C_i^{ne} = \frac{W}{2n}\log_2\left(1+\frac{2nH_i^2P_i^{ne}}{\omega_{i,ne}^2WN_0}\right), \quad (4)$$

$$C_i^{e} = \frac{W}{2n}\log_2\left(1+\frac{2nH_i^2P_i^{e}}{\omega_{i,e}^2WN_0}\right). \quad (5)$$

In the OMA system, the frequency band is uniformly allocated for each signal, and W is divided by $2n$.

Given the security threat, the sum capacity maximization problem jointly optimizing onboard power allocation and security algorithm selection can be formulated as

$$\max \sum_{i=1}^{n} C_i^{sum} \quad (6a)$$

$$\text{s.t.} \sum_{i=1}^{n} P_i \le P_{total} \quad (6b)$$

$$SA_i = \begin{cases} \text{no security}, & S_i = 0 \\ (\text{AES}_{128}, \text{SHA}_{256}), & 0 \le S_i \le \frac{1}{\phi+2} \\ (\text{AES}_{192}, \text{SHA}_{384}), & \frac{1}{\phi+2} \le S_i \le \frac{1}{\phi+1} \\ (\text{AES}_{256}, \text{SHA}_{512}), & \frac{1}{\phi+1} \le S_i \le 1 \end{cases}, \quad (6c)$$

where $C_i^{sum} = C_i^{ne} + C_i^e$. Condition (6b) is the total satellite onboard power constraint. The security algorithm pair of encryption and MAC is considered in condition (6c). We use the advanced encryption standard (AES) as encryption and the secure hash algorithm (SHA) for MAC. The subscript of the security algorithm pair means security algorithm strength.

III. Optimal Onboard Power Allocation and Security Algorithm Selection

We now solve the optimization problem (6). (6a) is a concave function with respect to the onboard power, which leads to the convex optimization problem [5]. The optimal onboard power is derived as

$$P_i = \frac{W}{2n}\left[\frac{1}{\Lambda \ln 2} - \frac{\omega^2 N_0 \Delta_i}{2H_i^2\Psi_i} + \sqrt{\left(\frac{1}{\Lambda\ln 2} - \frac{\omega^2N_0\Delta_i}{2H_i^2\Psi_i}\right)^2 - \frac{\omega^2N_0}{h_i^2\Psi_i}\left(\omega^2N_0 - \frac{H_i^2\Delta_i}{\Lambda\ln 2}\right)}\right], \quad (7)$$

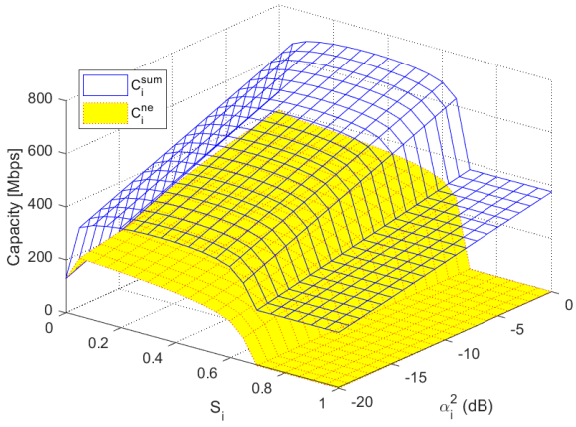

Fig. 1. Performances of sum and NENC capacities with $\phi = 0.3$ with respect to the security threat and rain attenuation.

where $\Delta_i = (\phi^2+2\phi+2)S_i^2 - 2(\phi+1)S_i + 1$, and $\Psi_i = S_i^2\{1-(\phi+1)S_i\}^2$; and Λ is a Lagrangian multiplier for the total satellite onboard power.

Fig. 1 shows the capacities of two signals. The difference between capacities of the sum and NENC implies ENC capacity. As the rain attenuation is severe, the capacities decreases and when the security threat increases, ENC capacity enhances, which means the rain attenuation and security threat play a similar role of controlling the power allocation profile. The highest sum capacity is achieved at the same power point of two signals $S_i = \frac{1}{\phi+2}$ due to the rate-splitting effect.

Given security threat, the security algorithm pair is determined and P_i^c is used for security computation. The higher security threat is, the more security computation power is allocated and the stronger security algorithm is selected.

IV. Conclusion

Security will be one of the important issue due to the data traffic explosion from NTN and SATIN. However, the solutions of cryptographic and physical layer securities for satellite network have been studied, independently. In this paper, we presented the joint satellite communication security methods of power allocation and security algorithm selection. With security threat, we derived the onboard power allocation profile and security algorithm selection.

References

[1] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 126–132, 2020.

[2] R. Banu and T. Vladimirova, "Fault-tolerant encryption for space applications," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 45, no. 1, pp. 266–279, 2009.

[3] J. Lei, Z. Han, M. A. V. Castro, and A. Hjorungnes, "Secure satellite communication systems design with individual secrecy rate constraints," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 661–671, 2011.

[4] S. Jeon, J. Kwak, and J. P. Choi, "Advanced multibeam satellite network security with encryption and beamforming technologies," in *Proc. IEEE ICC Workshop*, 2022.

[5] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.