



## 저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

Master's Thesis  
석사 학위논문

# A Game Theoretic Power Allocation Strategy for Secrecy Capacity Optimization

Suhyeon Kim(김 수 현 金 守 顯)

Department of  
Information and Communication Engineering

DGIST

2021

Master's Thesis  
석사 학위논문

# A Game Theoretic Power Allocation Strategy for Secrecy Capacity Optimization

Suhyeon Kim(김 수 현 金 守 顯)

Department of  
Information and Communication Engineering

DGIST

2021

# A Game Theoretic Power Allocation Strategy for Secrecy Capacity Optimization

Advisor: Professor Jihwan Choi  
Co-advisor: Professor Donghoon Shin

by

Suhyeon Kim  
Information and Communication Engineering  
DGIST

A thesis submitted to the faculty of DGIST in partial fulfillment of the requirements for the degree of Master of Science in the Department of Energy Science & Engineering. The study was conducted in accordance with Code of Research Ethics<sup>1</sup>

12. 14. 2020

Approved by

Professor Jihwan Choi (Advisor)	(signature)
Professor Donghoon Shin (Co-Advisor)	(signature)

---

<sup>1</sup> Declaration of Ethical Conduct in Research: I, as a graduate student of DGIST, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance of my thesis advisor.

# A Game Theoretic Power Allocation Strategy for Secrecy Capacity Optimization

Suhyeon Kim

Accepted in partial fulfillment of the requirements for the degree of Master of  
Science.

12. 14. 2020

Head of Committee Prof. Jihwan Choi (signature)

Committee Member Prof. Donghoon Shin (signature)

Committee Member Prof. Jeongho Kwak (signature)

## ABSTRACT

Secrecy capacity is related to Physical Layer Security (PLS) and a large PLS implies good security in the physical layer. Therefore, secrecy capacity optimization is a foremost objective for the PLS. In this paper, we consider a power allocation strategy for a physical layer system in a GEO satellite multibeam channel environment to impair secrecy capacity. In such a system, the satellite sends the information to a receiver that is threatened by eavesdroppers which have made several attacks.

To solve this, we formulate a secrecy capacity minimization problem and suggest a Convex-Concave Procedure (CCP) algorithm. After that, we consider smart eavesdropper to select or not select eavesdrop. Then, the Nash Equilibrium (NE) of the PLS game is derived. The simulation results show that the proposed power allocation strategy in the satellite model efficiently affects.

Keywords: Multibeam satellite, Secrecy capacity, CCP algorithm, Nash equilibrium.

## List of Contents

Abstract .....	i
List of contents .....	ii
List of figures .....	iii
List of tables .....	vi
I. Introduction .....	1
1.1 Motivation .....	1
1.2 Background .....	2
1.2.1 Secrecy capacity .....	2
1.2.2 Jamming .....	3
1.2.3 Game theory .....	4
1.3 Related work .....	7
II. System model .....	9
2.1 Channel model .....	9
2.2 Signal model .....	11
III. Proposed secrecy capacity minimization scheme .....	14
3.1 CCP Algorithm method .....	14
3.2 Game theoretic approach .....	18
IV. Numerical results and analysis .....	22
V. Conculusion .....	25
Reference .....	26

## List of Figures

Fig. 1: The seven layers of OSI and the physical link. ....	2
Fig. 2: Wiretap channel and eavesdrop Terminal $\mathbf{T}_3$ between Terminal $\mathbf{T}_1$ and $\mathbf{T}_2$ .....	3
Fig. 3: Two player zero sum game model representation. ....	4
Fig. 4: Satellite system and jamming attack scenario. ....	10
Fig. 5: Channel and signal model. ....	13
Fig. 6: Satellite system and dual-mode jamming attack scenario. ....	19
Fig. 7: Game theoretic values about satellite and jamming attack scenario. ....	20
Fig. 8: Comparison of CCP algorithm performance. ....	23
Fig. 9: Secrecy capacity in mixed strategies at the satellite and the jammer. ....	24



## List of tables

Algorithm. 1: Basic CCP algorithm. ....	17
Table 1: The global navigation satellites information. ....	13
Table 2: Parameters of the multibeam satellite system. ....	22

# I. INTRODUCTION

## 1.1 Motivation

Nowadays, Physical Layer Security (PLS) technology has received much attention. In the Open System Interconnect (OSI) model, which mainly deals with computer networking, PLS is a field that studies the achievement of security at the physical layer, which is the lowest layer.

In the past, security in communication systems mainly dealt with high-level processing problems: private key and public key encryption system transformation for authentication, confidentiality, and information protection. However, today many security systems such as information theory and signal processing are designed by exploiting PLS [1],[2]. At this time, security performance can be improved or degraded by attack or defense in the physical layer. Of course, it is possible to lower the security capacity through intentional interference, and we intend to approach the security problem of the physical layer considering these cases. This is because, in case of cyber wars, such as electronic warfare, jammers in specific locations can attack effectively if there is information on communication devices or communication networks used by the enemy.

The secrecy capacity maximization problem, that is, the defender perspective problem, has already been tried many times with several different methods, but the attacker is not [3]. Therefore, we consider how to allocate resource from the limited power perspective of the attacker in a given situation. There is a factor that must be checked, which is that attackers and defenders can change their power allocation strategies independently in some cases. From this, we solve the problem by taking these parts into account with each other's reasonable results.

# The Seven Layers of OSI

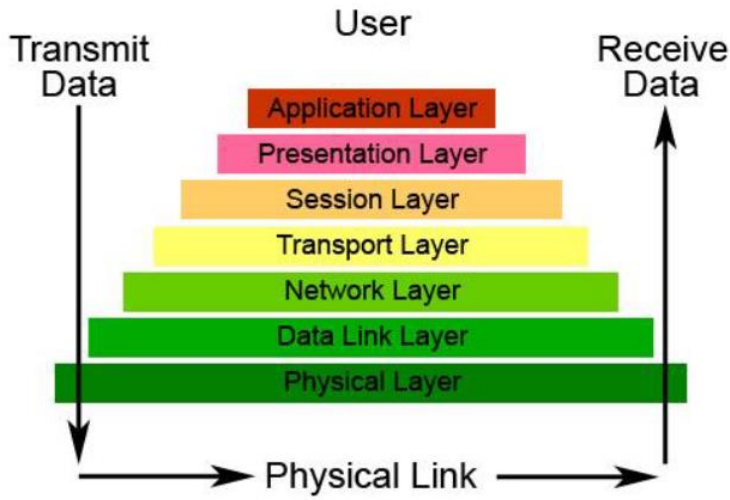


Fig. 1. The seven layers of OSI and the physical link.

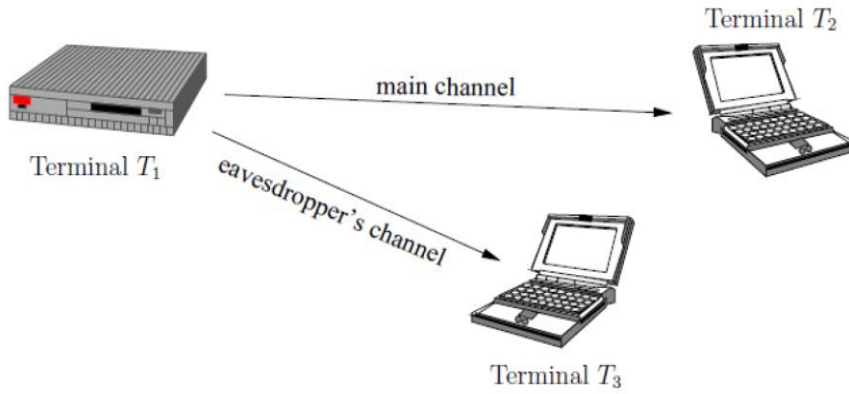
## 1.2 Background

### 1.2.1 Secrecy capacity

One of the Physical Layer Security (PLS) technologies was suggested in 1975 by Wyner using a wiretap channel[4]. Through the wiretap channel, Wyner defined secrecy capacity as the transceiver channel capacity minus the eavesdropper's channel capacity if it is not negative; otherwise its value is zero. Channel capacity was described by Shannon as the channel capacity theory [5]:

$$C = \log_2 \left( 1 + \frac{S}{N} \right) \quad (1)$$

Where  $S$  is the signal factor related to the transceiver's transmitting power and channel,  $N$  is the noise factor related to nature noise plus artificial noise. Channel capacity refers to the maximum amount of information that can be reliably transmitted through a channel, so reliable transmission is



more

Fig. 2. Wiretap channel and eavesdrop Terminal  $T_3$  between Terminal  $T_1$  and  $T_2$ .

effective as  $S$  increases and  $N$  decreases. The channel capacity from the perspective of the transceiver indicates the communication performance of the transceiver for the transmitted signal. On the other hand, the greater the value of the eavesdropper's channel capacity, the higher the risk of being eavesdropped on, so the definition of secrecy capacity is reasonable.

### 1.2.2 Jamming

Jamming is an electronic interference measure and is an electronic attack in the classical sense. This proceeds in the form of a disturbance that rejects the use of a specific frequency or radio wave by radiating ultra-high frequencies, or a form of transmitting false information deliberately. It can be hard to believe, however, there is something to be careful about. Unlike in general channel capacity, secrecy capacity requires more detailed power allocation. From a defender's perspective in the eavesdropping scenario in Fig.2, it interferes with terminals  $T_2$  and  $T_3$  in order to be able to maximize secrecy capacity using artificial noise [6]; this kind of jamming is called friendly jamming. What this suggests is that if the attacker makes the wrong power allocation, the secrecy capacity


will rise. Therefore, to minimize this, accurate power allocation must be made.

### 1.2.3 Game Theory

Game theory models strategic behavior by players who understand that their actions affect the actions of other players, and a game theoretical situation is an interdependent situation in which the actions of one player affect other's payoff. There are many game models depending on the number of players, cooperation or noncooperation, number of trials, and payoff of agents and so on.

For example, two players, I and II, assume a two player noncooperative zero sum game in which player I can choose  $n$  possible strategies and player II can choose  $m$  possible strategies. Then if player I chooses a strategy  $i$ ,  $i = 1, \dots, n$ , then player II chooses a strategy  $j$ ,  $j = 1, \dots, m$ . As each of strategy with players, if player I chooses strategy  $i$  and player II chooses strategy  $j$ , then player I has payoff  $a_{ij}$  and player II has payoff  $-a_{ij}$ , because a zero sum game means the sum of the payoff for all players. In case of a nonzero sum game, we consider a payoff matrix with all the players. In this way, we can represent the play of the game and the payoff is computed and expected. In addition, there is one very important property of game theory: The optimal strategy choice depends on the opponent's strategy.

Player I	Player II			
	Strategy 1	Strategy 2	...	Strategy $m$
Strategy 1	$a_{11}$	$a_{12}$	...	$a_{1m}$
Strategy 2	$a_{21}$	$a_{22}$		$a_{2m}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Strategy $n$	$a_{n1}$	$a_{n2}$	...	$a_{nm}$



$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix}$$

Fig. 3. Two player zero sum game model representation.

There are two types of strategy: pure and mixed. A pure strategy is as follows.

A vector  $X=(0,0,...,1,...,0) \in S_n$  for player I and  $Y=(0,0,...,1,...,0) \in S_m$  for player II where

$$x_i = 1, \sum_{i=1}^n x_i = 1 \text{ and } y_j = 1, \sum_{j=1}^m y_j = 1.$$

That means that a pure strategy chooses only one strategy. If the optimal outcome is the same regardless of the player's strategy selection order, that named value of the game, whereas, a mixed

strategy is a vector  $X=(x_1, x_2, \dots, x_n) \in S_n$  for player I and  $Y=(y_1, y_2, \dots, y_m) \in S_m$  for player II

where  $x_i \geq 0, \sum_{i=1}^n x_i = 1$  and  $y_j \geq 0, \sum_{j=1}^m y_j = 1$ .

The mixed strategy concept contains a pure strategy, and all strategies are chosen with a certain probability.

Next, we have one of the most important elements of game theory, the Nash equilibrium. The Nash equilibrium, named after the mathematician John Forbes Nash Jr., is a proposed solution of a non-cooperative game involving two or more players in which each player is assumed to know the equilibrium strategies of the other players, and no player has anything to gain by changing only their own strategy [7]. If each player has chosen a strategy, an action plan chooses its own action based on what it has seen happen so far in the game and no player can increase its own expected payoff by changing its strategy while the other players keep theirs unchanged, then the set of strategy choices constitutes a Nash equilibrium. In other words, in a given situation, if my competitor's strategy holds, my strategy has no benefit even if I change it. The mathematical explanation is as follows. If  $E(X, Y^*) \leq E(X^*, Y^*)$  for every mixed  $X \in S_n$  and  $E(X^*, Y^*) \leq E(X^*, Y)$  for every mixed  $Y \in S_m$ , then  $X^*$  and  $Y^*$  is a Nash strategy,  $(X^*, Y^*)$  is a Nash equilibrium,  $v(A) = X^* A Y^{*T}$  is the optimal payoff of

the game.

One of the important examples of the importance of the Nash equilibrium is the prisoner's dilemma. If both players confess, then the two players have a payoff of 2, if they both do not confess, then the two players have a payoff of 1. Otherwise, the one who chose to confess gets a payoff of 0, and the other who chose not to confess gets a payoff of 3. We can check the game model of the prisoner's dilemma for the case in which the payoff indicates the period of time in prison to pay for crimes. That is, in that case, players want to get a minimized payoff. If the two players do not confess, they have to be in prison for only one year. Of course, the two players can get a minimum payoff of 0 if one player confesses, and the other does not confess. But the problem is, from another point of view, it is better to live in prison for two years than to live in prison for three years. Therefore, if the opponent confesses, then the two players live in jail for two years. But there is something strange. Consider the case in which the two players do not confess, then they live in jail for only one year, so it is better for them not to confess than to confess. However, players will not accept these punishments and will choose to confess to obtain release. Except when both confess, if one changes the strategy when the other does not change it, then one gets a benefit. Therefore, in this non Nash equilibrium, players will try to change to gain advantage. However, when both confess, neither changes their strategy because even if they change their strategy, there is no gain, that is, this state satisfies the Nash equilibrium. For these reasons, we apply game theory to various fields: mathematics, economics, evolutionary biology, communications and so on. In particular, we pay attention to the use of game theory in a communication jamming scenario case.

### 1.3 Related Work

As mentioned previously, PLS is one of the major problems to be dealt with in wireless communication engineering, and many studies have been conducted on the security capacity, which has a close relationship to the security of the physical layer. In general, if the Signal-to-Noise Ratio (SNR) of the eavesdropper channel is higher than the SNR of the sender channel, it is easy to think that eavesdropping will be easily performed if messages are exchanged due to degradation of security performance. However, in this case, even if the SNR of the eavesdropper channel is higher than the SNR of the sender channel, it can be seen that perfect security is possible. Through this, it can be seen that the possibility of perfect security for any radio channel condition is implied [2].

Moreover, many methods address the secrecy capacity maximization problem. Representatively, assuming that all channel information is completely known, Semidefinite Programming (SDP) relaxation and Second-Order Cone Programming (SOCP) are methods that solve the optimization problem of maximizing the security capacity by using the limited power of the transmitter when transmitting a message through beamforming in the transmitter [8]. According to [8], SDP relaxation is a method of calculating the optimal solution and optimal value after finding the variable region in which the solution can exist by extending the existing optimization equation into a matrix and converting it into a quasi-convex optimization problem, and the SOCP method approaches in the form of a norm rather than a matrix. There is a method of obtaining the optimization problem in the same way as in SDP relaxation.

We can also consider the satellite system: Assuming all channel information is known, we think



about a situation in which a satellite transmits a message and an eavesdropper passively listens to it in a Ka-band (26.5-40GHz) multi-beam satellite system. At this time, the goal is to obtain the minimum power of the satellite that can achieve a certain level of security capacity by deliberately adding artificial noise to damage the channel capacity of the satellite rather than causing minor damage to the channel capacity of the eavesdropper [9]. Besides, in terms of game theory, the subject of the game considers attackers and defenders. The attacker has the purpose of minimizing the security capacity by becoming an eavesdropper or jammer, and when he becomes a jammer, the cost aspect is also considered by using a cost proportional to the power value to attack. The defender tries to maximize the security capacity in case the attacker is an eavesdropper or jammer. Through this non-cooperative game problem, if each game subject uses strategies with a specific probability, the most rational attack or defense strategy is found by finding the Nash Equilibrium, which in turn suffers losses when changing strategies [10], [11]. In addition, there are studies on maximizing the security capacity for various conditions, obtaining the minimum power that satisfies a specific security capacity value, or analyzing a game theory by incorporating it. However, while there are many studies to increase the security capacity, studies to minimize the security capacity are very rare. Therefore, in this paper, we propose an optimal power allocation for jammers by approaching the problem of minimizing the security capacity in case of attempting a downlink attack by a jammer. In addition, from the viewpoint of game theory, we propose the best strategy to obtain the greatest benefit from each other's point of view by obtaining the Nash equilibrium for effective jamming attacks and satellite defense strategies according to specific satellite conditions and channels.

## II. SYSTEM MODEL

Network paralysis defined in this study refers to a jamming technique aimed at degrading the performance of networking protocols and algorithms by attacking the vulnerable layers of enemy communication devices or systems. In particular, this paper aims to lower the communication capability or security of the satellite communication system by attacking the physical layer.

The jamming attack scenario is as follows. Assuming that the jammer's position and beamforming gain are fixed, when the enemy satellite (SAT) transmits a message to the destination (D), the eavesdropper passively intercepts the message around the destination (D). At this time, from an attacker's point of view, jammer (J) reduces the security performance with a limited resource(power) at the physical layer.

### 2.1 Channel model

Multibeam satellite systems operate in the high frequency range Ka band (26.5 to 40GHz), Channel h is designed in consideration of Free Space Loss, Rain Attenuation and Beam Gain.

First, we consider Free Space Loss, the propagation loss due to free space loss can be expressed as

$$C_L = \frac{\lambda}{4\pi\sqrt{d_l^2 + d_o^2}} \quad (2)$$

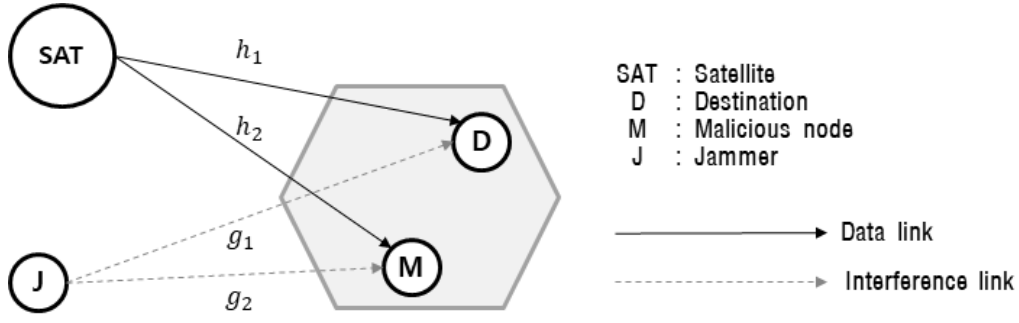


Fig. 4. Satellite system and jamming attack scenario.

where  $\lambda$  is the carrier wavelength,  $d_0$  is a distance of about 36000km in a Geostationary Orbit (GEO) satellite case, and  $d_1$  is the distance from the destination to the satellite.

In addition, attenuation due to weather must be considered, and the signal is disturbed by clouds and rain in the atmosphere. According to the state-of-the-art empirical model [12], the channel  $\tilde{h}$  is given by

$$\tilde{h} = \beta^{-\frac{1}{2}} e^{-j\varphi} \quad (3)$$

where  $\varphi$  denotes an  $N \times 1$  phase vector uniformly distributed over  $[0, 2\pi)$ , and  $\beta$  is expressed as a probability distribution that satisfies  $\beta_{dB} = 20\log_{10}(\beta)$  and  $\log(\beta_{dB}) \sim N(\mu, \delta)$ .  $\log(\beta_{dB})$  follows a normal distribution with mean  $\mu$  and standard deviation  $\delta$ . The mean  $\mu$  and standard deviation  $\delta$  depend on the signal's destination, frequency, and the angle of elevation between the satellite and the destination.

The beam gain is related to the satellite's antenna pattern and the location of the destination. The

beam gain is a key performance measure that combines the directivity and electrical efficiency of an antenna. In a transmit antenna, the gain indicates how well the antenna converts the input power into a radio wave traveling in a specified direction. Therefore, beam gain from the satellite to the receiver  $m$  is expressed by

$$b(m) = b_m^{max} \left( \frac{J_1(u_m)}{2u_m} + 36 \frac{J_3(u_m)}{u_m^3} \right)^2 \quad (4)$$

$$u_m = 2.07123 \sin \theta_m / \sin (\theta_{3dB})_m \quad (5)$$

and  $J_1$  and  $J_3$  are the first-kind Bessel function of orders 1 and 3,  $b_m^{max}$  is the gain at the boresight.

Suppose that  $\mathbf{b}$  is a  $N \times 1$  beam gain vector from the satellite to the destination, then the channel for the satellite to the user is expressed as

$$\mathbf{h} = C_L \tilde{\mathbf{h}} \odot \mathbf{b}^{\frac{1}{2}} \quad (6)$$

where  $\odot$  denotes the Hadamard product.

## 2.2 Signal model

Suppose that the signals of user  $m$  are defined as  $s_m$  with an average power  $E[|s_m|^2] = 1$  for all

m, and the Beamforming vectors are  $w_k$ . The transmitted signal can be presented in vector x as

$$x = \sum_{n=1}^m w_n s_n \quad (7)$$

When  $g_i$  is defined Rayleigh fading channel over jammer, the signals received by the satellite and jammer are expressed as

$$y_m = h_m^H \sum_{n=1}^m w_n s_n + n_D \quad (8)$$

$$y_{m,k} = g_{m,k}^H \sum_{n=1}^m w_n s_n + n_E \quad (9)$$

where  $n_d$  and  $n_e$  are the noise components with an independent and identically distributed ( i.i.d.) zero mean, and the variances are  $\sigma_D^2$  and  $\sigma_E^2$ . In general, there may be multiple jammers and eavesdroppers.

From an information theory point of view, not many eavesdroppers are important, but the value of the eavesdropper with the smallest security capacity is important for each eavesdropper, and those of the jammer attacks for a receiver indicate the total noise. Thus, we consider a model with one eavesdropper and one jammer attack. Therefore, based on these formulas and assumptions, the secrecy capacity for the user m is expressed as follows:

$$C_m = \log_2 \left( 1 + \frac{|h_1^H w_1|^2}{\sigma_D^2 + |g_1^H w_2|^2} \right) - \log_2 \left( 1 + \frac{|h_2^H w_1|^2}{\sigma_E^2 + |g_2^H w_2|^2} \right) \quad (10)$$

$w_1$  is the satellite allocation power, and  $w_2$  is the jammer allocation power.

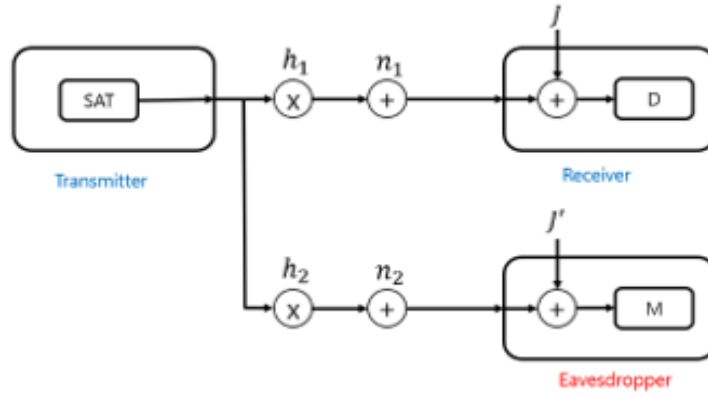


Fig. 5. Channel and signal model.

	Glionass	Glionass-M	Glionass-K	Glionass-KM
First launch		2003	2005	After 2011
Lifetime	3 years	7 years	10—12 years	improved
Mass	1415 kg	1415 kg	750 kg	(TBD)
Number of satellites per launch: - PROTON - SOYUZ	3 -	3 1	6 2	6 (TBC) 2 (TBC)
Elec. Power Subsys. output power	1000 W	1600 W	1270 W (TBC)	TBD
Vertical real time navigation accuracy (95%)	60 m	30 m	5-8 m (TBC) (40 – 60 cm, using global differential system)	TBD
Number of civil signals	1	2	3 (TBC)	3 (TBC)
Number of special signals	2	2	3 (TBC)	TBD
On-board clocks stability	$5 \cdot 10^{-13}$	$1 \cdot 10^{-13}$	$1 \cdot 10^{-13}$	TBD
Root-mean-square error of mutual synchronization of navigation signals	15 ns	8 ns	3-4 ns	TBD
Supplementary functions	-	-	Integrity signal (TBC) Different. corrections (TBC) Search&Rescue (TBC)	TBD

TBC - To Be Confirmed

TBD - To Be Defined

Table 1. The global navigation satellites information [13].

### **III. PROPOSED SECRECY CAPACITY MINIMIZATION SCHEME**

We want to solve a secrecy capacity optimization problem from an attack or defense prospective, but it is not simple because the objective function, i.e., the secrecy capacity, is nonconvex. Thus, in this paper, we suggest using slack variables and the Convex-Concave Procedure (CCP) algorithm. Then, we expand this problem to determine whether the eavesdropper is activated or not. We additionally suggest how to allocate power depending on the presence of eavesdroppers.

#### **3.1 CCP Algorithm method**

Problems related to optimization have been studied for a long time. One of the big criteria classifying these optimization problems is that this optimization problem is classified as convex and nonconvex types. Solving problems of the convex optimization form is much more accessible than solving non-convex optimization problems because if the optimization problem can be expressed as convex, the problem can be solved more easily. Looking at (10), the secrecy capacity has a nonconvex form. However, we can use the CCP algorithm as if solving convex optimization, and I will introduce the approach first, referring to the system model in Fig. 4 and (10). The basic form of secrecy capacity minimization problem is as follows.

$$\underset{w_2}{\text{minimize}} \quad \log_2 \left( 1 + \frac{|h_1^H w_1^*|^2}{\sigma_D^2 + |g_1^H w_2|^2} \right) - \log_2 \left( 1 + \frac{|h_2^H w_1^*|^2}{\sigma_E^2 + |g_2^H w_2|^2} \right) \quad (11)$$

$$\text{subject to} \quad |w_2|^2 \leq P_2 \quad (12)$$

A number of secrecy capacity maximization methods have been proposed, for example, [6] and [8], so we assume that we know the satellite allocated power  $w_1^*$ . In (12), we emphasize that we never use more power than constrained power.

We first consider a semidefinite programming (SDP) method [14]. Using the definition

$h_i h_i^H = H_i$ ,  $g_i g_i^H = G_i$ ,  $w_i w_i^H = W_i$  for  $i = 1, 2$ , we transform (11) and (12) as follows.

$$\underset{W_2}{\text{minimize}} \quad \log_2 \left( 1 + \frac{\text{tr}(H_1 W_1^*)}{\sigma_D^2 + \text{tr}(G_1 W_2)} \right) - \log_2 \left( 1 + \frac{\text{tr}(H_2 W_1^*)}{\sigma_E^2 + \text{tr}(G_2 W_2)} \right) \quad (13)$$

$$\text{subject to} \quad \text{tr}(W_2) \leq P_2 \quad (14)$$

$$W_2 \succeq 0 \quad (15)$$

Because  $W_2$  must satisfy a positive semi-definite matrix by definition, then a constrained condition (15) is added. First of all, by applying SDP relaxation, we can change the formula of the objective function and the constrained conditions from the vector form to the square matrix form. We then consider the following substitution of slack variables with a definition as

$$e^x \triangleq \sigma_D^2 + \text{tr}(G_1 W_2) + \text{tr}(H_1 W_1) \quad (16)$$

$$e^y \triangleq \sigma_D^2 + \text{tr}(G_1 W_2) \quad (17)$$

$$e^z \triangleq \sigma_E^2 + \text{tr}(G_2 W_2) + \text{tr}(H_2 W_1) \quad (18)$$

$$e^r \triangleq \sigma_E^2 + \text{tr}(G_2 W_2) \quad (19)$$



Using (15)-(19), we reformulate as follows

$$\underset{\substack{W_2 \\ x, y, z, r}}{\text{minimize}} \frac{x-y-z+r}{\log 2} \quad (20)$$

$$\text{Subject to } e^x \geq \sigma_D^2 + \text{tr}(G_1 W_2) + \text{tr}(H_1 W_1) \quad (21)$$

$$e^y \leq \sigma_D^2 + \text{tr}(G_1 W_2) \quad (22)$$

$$e^z \leq \sigma_E^2 + \text{tr}(G_2 W_2) + \text{tr}(H_2 W_1) \quad (23)$$

$$e^r \geq \sigma_E^2 + \text{tr}(G_2 W_2). \quad (24)$$

(14), (15)

The minimization problem transformed through the slack variable is as follows, and 4 constraints

(21)-(24) related to each slack variable x, y, z, r is added. The inequality sign of the constraint related to the slack variable is determined according to whether the objective function is minimized or max-

imized. Since this problem is a minimization problem, the objective function is minimized as x and r are smaller and y and z are larger. According to (20), the objective function is changed to linear form.

In addition, the constraints (14), (15), (22), and (23) have a convex form. But (21) and (24) consist of

a convex form minus the convex function form. For example,  $x^2$  and  $x^4$  are convex, but  $x^2 - x^4$

is not convex, which means these must not satisfy a convex form. Fortunately, through the CCP algo-

rithm, convex minus convex form can be approximated in a convex form, and the approximate solu-

tion is obtained by iteratively calculating the convex optimization problem created through it. The

CCP algorithm is a method in which the convex minus convex functions approximate is transformed to convex minus linear functions by first-order Taylor approximation. Since the convex-linear function is a convex function, converting the objective function and constraints to a convex form, it can be made into a convex optimization problem.

Algorithm 1. Basic CCP algorithm [15].

**Algorithm: Basic CCP algorithm**

**Given an initial feasible point  $x_0$ .**

**K := 0**

**Repeat**

1. Convexify. Form  $\widehat{g}_i(x; x_k) \triangleq g_i(x_k) + \nabla g_i(x_k)^T (x - x_k)$

*for*  $i = 0, 1, \dots, m$ .

2. Solve. Set the value of  $x_{k+1}$  to a solution of the convex problem

minimize  $f_0(x) - \widehat{g}_0(x; x_k)$

subject to  $f_i(x) - \widehat{g}_i(x; x_k) \leq 0, i = 1, \dots, m$ .

3. Update iteration.  $k := k + 1$ .

**Until stopping criterion is satisfied.**

(Criterion :  $|\frac{x-y+p-q}{\log 2} - C_s| \leq \varepsilon$ )  $C_s = \log_2 \left( 1 + \frac{|h_1^H w_1^*|^2}{\sigma_D^2 + |g_1^H w_2|^2} \right) - \log_2 \left( 1 + \frac{|h_2^H w_1^*|^2}{\sigma_E^2 + |g_2^H w_2|^2} \right)$

The basic CCP algorithm is as follows. First, the initial value is selected as a point in the feasible area. For convexify, if  $g$  is linearly approximated in the f-g form, the objective function and the constraint formula become convex, and the solution is solved by solving the following convex problem. Hence objective and constraint functions are convex functions. Then this program is convex, so it can be solved efficiently assuming the functions  $f$  can be handled tractably. Then, after adding  $k$  by 1 and substituting the solution obtained, repeat the above process to solve the problem to obtain an approximate solution. We have one thing to check, whether the value obtained through the above algorithm is feasible. The feasibility proof of the algorithm is described in [15]. For a flexible approach, we can also allow for constraints to be violated very slightly using the Penalty CCP. To use the CCP algorithm, we apply a linear approximation to  $e^r \cong e^{r_i} + e^{r_i}(r - r_i)$  ( $r_i$  is the  $i$ -th iteration value). Then, we get the following formula:

$$e^{x_i} + e^{x_i}(x - x_i) \geq \sigma_D^2 + \text{tr}(G_1 W_2) + \text{tr}(H_1 W_1) \quad (25)$$

$$e^{r_i} + e^{r_i}(r - r_i) \geq \sigma_E^2 + \text{tr}(G_2 W_2) \quad (26)$$

We replace (21) with (25) and (24) with (26) and use the CCP algorithm to get an approximate solution using a convex optimization tool such as CVX [16].

## 3.2 Game theoretic approach

Game theory is method that can be applied to the field of communication as a study of predicting

what kind of results will occur in situations where the interests of various subjects are intertwined and how we can understand the results. The game consists of two or more decision-making players, strategy for situations, and payoffs. We set the satellite and jammer as the player and the security capacity  $C_s$  as the payoff to compose this as a game for the security of the physical layer. The attacker's strategy is dual-mode (jamming or eavesdropping), and the jammer attacks the jamming by assigning power directly to the destination, but when the eavesdropper has no channel capacity, it becomes a malicious node and does not directly attack the wiretap channel. It can be classified as a case of eavesdropping by generating  $h_2$ . As for the security capacity, when a jammer attacks jamming,  $C_2$  becomes 0 because there is no wiretap channel, so only  $C_1$  needs to be considered for the objective function value. If the jammer becomes a malicious node, the objective function becomes  $C_s$  due to the influence of the wiretap channel. If there are two strategies, Eve's optimal attack through jamming or eavesdropping as a malicious node, Alice's point of view is the Full Power strategy that prioritizes maximizing the channel capacity  $C_1$ , and the eavesdropper's channel capacity by generating artificial noise. The artificial noise strategy that maximizes  $C_s$  is used in a way that impairs it, but a slight blow to the receiver's channel capacity is applied, and the game model is as follows:

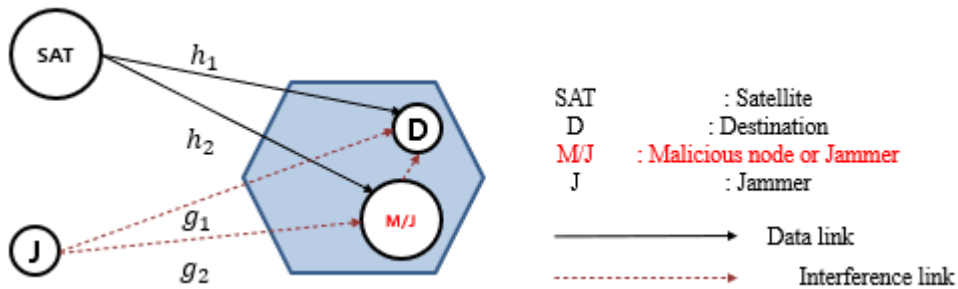


Fig. 6. Satellite system and dual-mode jamming attack scenario.

	Eavesdrop(E)	Jamming(J)
Full Power(F)	$R_{FE}$	$R_{FJ}$
Artificial Noise(A)	$R_{AE}$	$R_{AJ}$

Fig. 7. Game theoretic values about satellite and jamming attack scenario.

From the satellite's strategic point of view, if the jammer's strategy is fixed to Eavesdrop (E), the equal sign relationship of the payoff (security capacity) value is  $R_{FE} \leq R_{AE}$ , and if it is fixed as Jamming(J),  $R_{AJ} \leq R_{FJ}$  unconditionally follows, but the jammer's strategy from its point of view, even if the satellite strategy is fixed, since the channel value is set to a statistical value that satisfies a specific condition, the equal sign relationship of the payoff value is not definite. Therefore, for a satellite's specific strategy, it cannot be said that the payoff is larger. A pure strategy means that each player selects only one specific strategy. In the case of approaching pure strategy equilibria, if  $R_{AE} \leq R_{AJ}$  is satisfied, we will be satisfied with the following:

$$R_{FE} \leq R_{AE} \leq R_{AJ} \leq R_{FJ} \quad (27)$$

In addition, if the satellite changes strategy ( $R_{FE}$ ) or the jammer changes strategy ( $R_{AJ}$ ) in  $R_{AE}$ ,

$R_{AE}$  becomes a Pure Nash Equilibrium, and if  $R_{FJ} \leq R_{FE}$  is satisfied

$$R_{AJ} \leq R_{FJ} \leq R_{FE} \leq R_{AE} \quad (28)$$

If we analyze in a way similar to the previous case, we can see that  $R_{FJ}$  becomes a Pure Nash Equilibrium.

Mixed strategy means that each player chooses each strategy probabilistically, and mixed strategy equilibria can also be obtained. The mixed strategy can be obtained under the conditions of satellite strategy  $\mathbf{P}=(p,1-p)$ , jammer strategy  $\mathbf{q}=(q,1-q)$ , and  $(0 \leq p, q \leq 1)$ . If  $q=1$ , expectation of a payoff is  $P * R_{FE} + (1 - p) * R_{AE}$ , if  $q=0$ , expectation of a payoff is  $P * R_{FJ} + (1 - p) * R_{AJ}$ . Thus, the best response of satellite  $P^*$  satisfies  $P * R_{FE} + (1 - p) * R_{AE} = P * R_{FJ} + (1 - p) * R_{AJ}$ . In this way,  $q^*$  can also be obtained, and the Nash Equilibrium payoff  $v$  of the security capacity is as follows.

$$P^* = \frac{R_{AJ} - R_{AE}}{R_{FE} + R_{AJ} - R_{FJ} - R_{AE}} \quad (29)$$

$$q^* = \frac{R_{AJ} - R_{FJ}}{R_{FE} + R_{AJ} - R_{FJ} - R_{AE}} \quad (30)$$

$$v(P^*, q^*) = \frac{(R_{FE}R_{AJ} - R_{FJ}R_{AE})}{R_{FE} + R_{AJ} - R_{FJ} - R_{AE}} \quad (31)$$

The payoff  $v$  means reasonable secrecy capacity for the satellite and the attacker.

## IV. NUMERICAL RESULTS AND ANALYSIS

In this section, numerical results are provided to evaluate the performance of the proposed schemes. Table 1 indicates the channel and system parameters used for the simulations. The satellite is assumed to be equipped with  $M=3$  antenna feeds and the lognormal distribution parameters are  $\mu = -3.125$  and  $\sigma = 1.591$ . The jammer also equipped with  $M=3$  antenna feeds, but it has a Rayleigh fading channel over  $\sigma_E = 2$ . Since the satellite sends signals intensively to the receiver,  $b_m^{max}$  is corrected to 1.2. Other values of many other parameters are given in Table 1. We assume that the satellite is located in the beam center, and the distance between the satellite and the transceiver and the eavesdropper is random at a range of 36000km. The satellite power is fixed at 1000w, the jammer attacks with 1 to 10w power. Of course, several jammers may attack, but this involves a noise component, so one jammer is considered for the attack. Fig. 9 presents a comparison between the channel capacity minimization method and the secrecy capacity minimization method.

Parameter	Value
Climatic conditions	Central Europe
Frequency band	$Ka$ (20 GHz)
Satellite orbit	Geostationary
Polarization	Circular
Elevation angle	$30^\circ$
Number of active beams	$M = 3$
Beam diameter	$D = 500$ km
3 dB angle	$\theta_{3dB} = 0.4^\circ$
Rain fading statistics	$\{\mu; \sigma\} = \{-3.125; 1.591\}$

Table 2. Parameters of the multibeam satellite system [12].

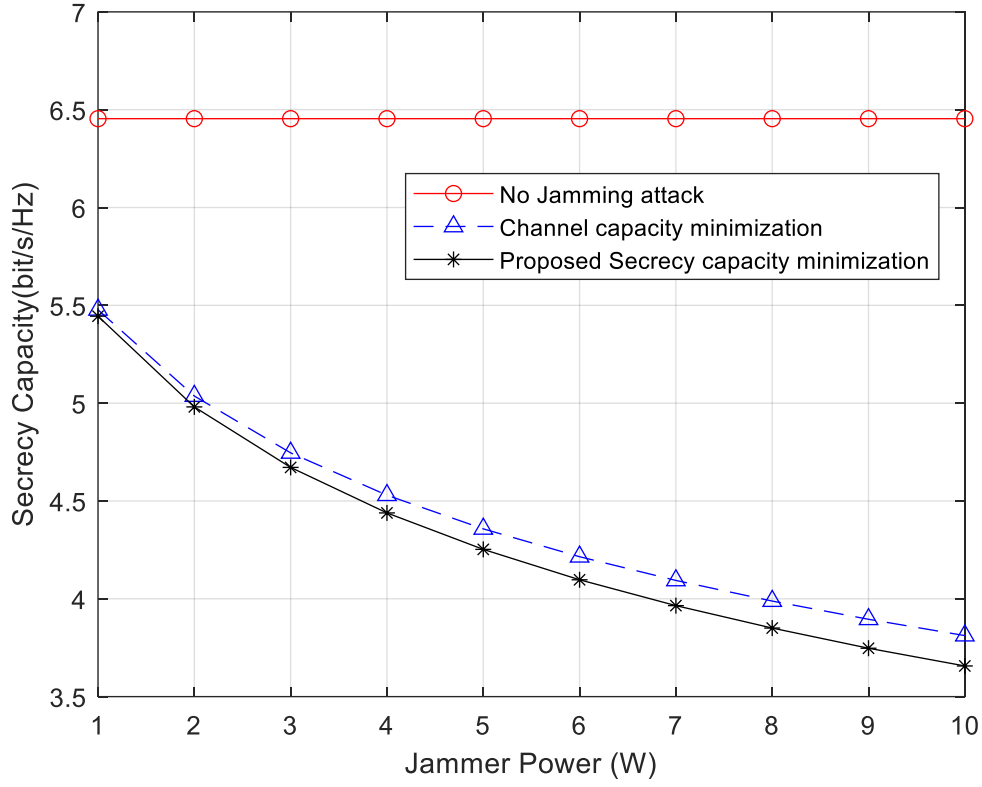


Fig. 8. Comparison of CCP algorithm performance.

The results illustrate the performance of secrecy capacity minimization using the CCP algorithm versus channel capacity minimization. Actually, the proposed method is better than channel capacity minimization method, but this requires the assumption that we know a lot of information, all of the channel conditions and  $\mathbf{w}_1$ . Channel capacity minimization is easy to use when the jammer to the receiver channel  $\mathbf{g}_1^H$  knows because of  $|\mathbf{g}_1^H \mathbf{w}_2|^2$  maximization to setting jammer power. However, this sometimes leads to a bad result that increases the secrecy capacity if the jammer channel capacity is unintentionally too big. Another point is complexity. The proposed method can be demonstrated by solving the convex optimization problem several times through the CCP algorithm, whereas the channel capacity minimization calculation considers only maximizing  $|\mathbf{g}_1^H \mathbf{w}_2|^2$ . By comparing the pros



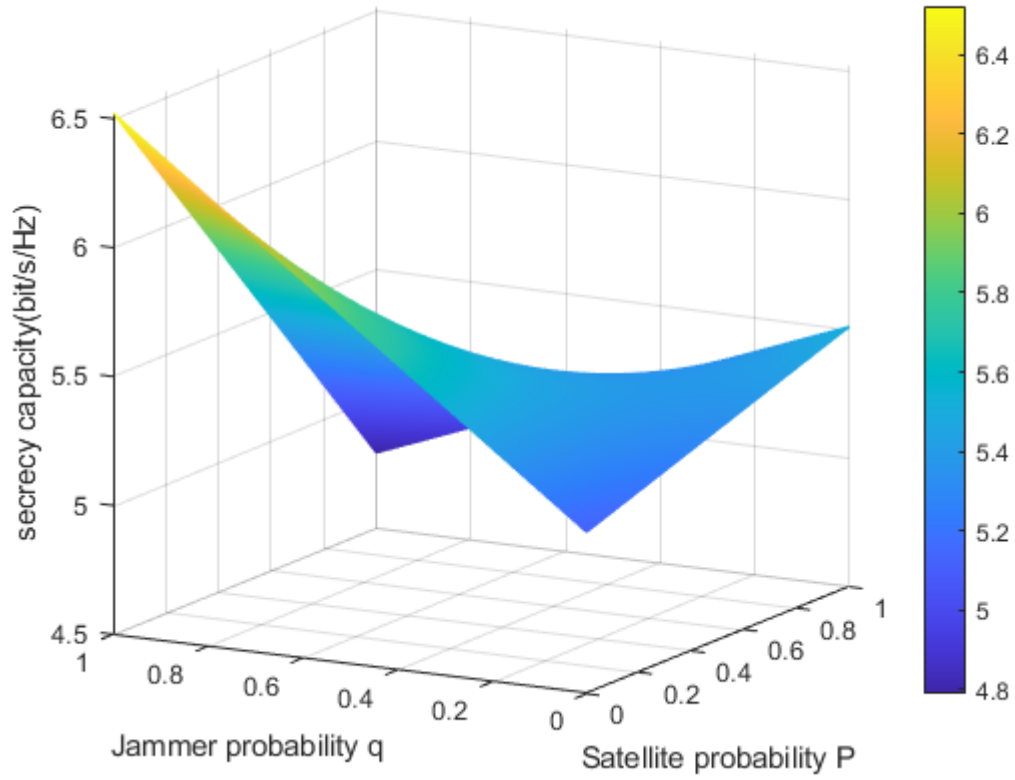


Fig. 9. Secrecy capacity in mixed strategies at the satellite and the jammer.

and cons, we can apply these.

After that, we can extend the problem to determine whether we use a malicious node around the destination or not. With an extended problem, we can get the result form of Fig. 7. The result of the payoff is determined by the constrained power of the satellite and jammer, and the channel conditions. A graphical illustration of the saddle point in mixed strategies  $P$  and  $q$  for a specific channel is shown in Fig. 10. For the specified channel parameters, when the satellite power is 1000w, and the jammer power is 10w, the calculated payoffs are calculated as  $R_{FE} = 4.789$ ,  $R_{FJ} = 5.510$ ,  $R_{AE} = 6.522$ ,  $R_{AJ} = 5.127$ . From the satellite's perspectives, the secrecy capacity is guaranteed to be at least 5.127

if the satellite uses artificial noise, while from the attacker's perspective, the secrecy capacity is guaranteed to be at least 5.510 if the attacker uses jamming directly. However, they can each obtain a reasonable secrecy capacity through game theoretic view. From the following payoff and (29), (30), (31), we can know the mixed Nash equilibrium secrecy capacity value  $v^* = 5.379$  and optimal mixing probabilities  $P^* = 0.660, q^* = 0.181$ .

## V. CONCLUSION

In this paper, we examined physical layer security for a multibeam satellite and a malicious node network from the information theoretic perspective. Since the secrecy capacity is an important factor in the PLS problem, we aimed to optimize this value. To analyze this system, we formulated a secrecy capacity optimization problem. Attackers want to minimize the secrecy capacity, so we proposed using the CCP algorithm in order to solve the non-convexity problem. After that, we expanded the scenario to determine whether the malicious node was eavesdropping or jamming. For this purpose, we proposed using noncooperative game theoretic techniques. To solve this game, we adopted a mixed strategy Nash equilibrium. The results revealed that if we know the channel parameters and constrained power conditions, then we can confirm that the proposed method has a better effect than the channel capacity minimization method. This result gives us a reasonable power allocation strategy.

## References

- [1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550-1573, Aug. 2014.
- [2] Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 2006, pp. 356-360.
- [3] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," in *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875-1888, March 2010, doi: 10.1109/TSP.2009.2038412
- [4] A. D. Wyner "The wire-tap channel" *Bell Syst. Tech. J.* vol. 54 pp. 1355-1387 Oct. 1975.
- [5] C. E. Shannon "Communication theory of secrecy systems" *Bell Syst. Tech. J.* vol. 28 pp. 656-715 Oct. 1949.
- [6] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," in *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180-2189, June 2008, doi: 10.1109/TWC.2008.060848.
- [7] Osborne, Martin J.; Rubinstein, Ariel (12 Jul 1994). *A Course in Game Theory*. Cambridge, MA: MIT. p. 14. ISBN 9780262150415.
- [8] J. Zhang and M. C. Gursoy, "Collaborative Relay Beamforming for Secrecy," *2010 IEEE International Conference on Communications*, Cape Town, 2010, pp. 1-5, doi: 10.1109/ICC.2010.5501835.

- [9] G. Zheng, P. Arapoglou and B. Ottersten, "Physical Layer Security in Multibeam Satellite Systems," in *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 852-863, February 2012, doi: 10.1109/TWC.2011.120911.111460.
- [10] Q. Zhu, W. Saad, Z. Han, H. V. Poor and T. Başar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," 2011 - MILCOM 2011 Military Communications Conference, Baltimore, MD, 2011, pp. 119-124, doi: 10.1109/MILCOM.2011.6127463.
- [11] A. Houjeij, W. Saad and T. Basar, "A game-theoretic view on the physical layer security of cognitive radio networks," 2013 IEEE International Conference on Communications (ICC), Budapest, 2013, pp. 2095-2099, doi: 10.1109/ICC.2013.6654835.
- [12] ITU-R Recommendation P.618-10, Propagation data and prediction methods required for the design of Earth-space telecommunication systems, Geneva 2009.
- [13] G. Polischuk V. Kozlov V. Ilitchov M. Kozlov V. Bartenev V. Kossenko et al. "The global navigation satellite system GLONASS: Development and usage in the 21st century" 34th Precise Time and Time Interval (PTTI) Meeting 2002.
- [14] Fujie, T., Kojima, M. Semidefinite Programming Relaxation for Nonconvex Quadratic Programs. *Journal of Global Optimization* 10, 367–380 (1997).
- [15] T. Lipp and S. Boyd "Variations and extension of the convex-concave procedure" *Optim. Eng.* vol. 17 no. 2 pp. 263-287 Jun. 2016.
- [16] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press., 2014.

## 요 약 문

### 보안 용량 최적화를 위한 게임 이론 관점 전력 할당 전략

최근 물리 계층 보안(PLS) 기술이 많은 주목을 받고 있다. PLS 란 주로 네트워크에서 다루는 OSI 모델에서의 최하위 계층인 물리 계층의 보안성을 연구하는 분야이다. 보안 용량은 물리 계층 보안과 관련이 있는 수치이며, 보안 용량이 클수록 물리 계층의 보안성능이 우수하다는 것을 의미한다. 따라서 보안 용량은 물리 계층 보안의 가장 중요한 요소가 된다. 본 논문에서는 GEO 위성 멀티 빔 채널 환경에서 수신기에 정보를 전송하고 주변에 도청 노드가 있을 때, 물리계층의 보안성을 낮추기를 원하는 공격자의 측면에서 보안 용량을 감소시키기 위한 재밍 전력 할당 전략을 찾는다. 최적의 전력 할당 전략을 찾기 위해 보안 용량 최소화 문제를 도식화 하는데 해당 문제는 볼록 최적화(Convex optimization) 문제의 형태가 아니므로 문제를 해결하기가 까다롭다. 이러한 문제를 해결하기 위해 CCP(Convex-Concave Procedure) 알고리즘을 사용하여 기존 문제를 볼록 최적화 문제로 근사하여 해를 구하는 것을 반복하여 실제 해에 수렴시키는 것으로 재머의 최적 파워 할당 전략을 구하는 방식을 제안한다. 그 후 도청 노드의 존재여부까지 고려하는 문제로 확장하여 전개하면, 이는 위성과 재머가 도청 여부에 따라 선택할 수 있는 전력 할당 전략들을 고려하게 되는 게임 이론 관점에서의 문제가 된다. 위성과 재머는 상대방의 전략 선택에 따라 결과가 달라지므로 서로가 합리적인 결과를 이끌어 내기 위해 내쉬 평형 값을 선택하게 된다. 시뮬레이션 결과는 위성 모델에서 제안된 재머의 전력 할당 전략이 효율적으로 영향을 미칠 수 있음을 보여준다.

핵심어: 다중 빔 위성, 보안 용량, CCP 알고리즘, 내쉬 평형.