

國立交通大學

網路工程研究所

碩士論文

合作與安全傳輸於不可信任之點對點系統

Cooperative and Secure Transmission in Unreliable Peer-to-Peer
System

研究生：李旻璟

指導教授：蕭旭峯 教授

中華民國 一 百 年 五 月

合作與安全傳輸於不可任之點對點系統

Cooperative and Secure Transmission in the Unreliable

Peer-to-Peer System

研究生：李旻璟

Student : Min-Ching Li

指導教授：蕭旭峯

Advisor : Hsu-Feng Hsiao

國立交通大學
網路工程研究所
碩士論文



A Thesis
Submitted to Institute of Network Engineering
College of Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of Master
In Computer Science

November 2010

Hsinchu, Taiwan, Republic of China

中華民國一百年五月


合作與安全傳輸於不可信任之點對點系統

研究生：李旻璟

指導教授：蕭旭峯

國立交通大學網路工程研究所

摘要



點對點系統技術的發展趨勢已漸漸走向合作網路(cooperative network)，並讓合作網路中的使用者分享資源，包含資料儲存空間、電腦計算資源...等。而在合作網路中常常會出現免費使用者(free-rider)，該使用者使用了系統中的資源卻僅分享少量資源或不分享資源，此種行為使得使用者之間的合作意願下降。在這篇論文中，我們提出一個新的賽局(game)來促進使用者之間的合作。一開始我們先從兩人資訊完全賽局(two-player complete information game)來分析賽局之平衡點(Nash equilibrium)，然後到資訊不完全賽局(incomplete information game)，最後擴展到多人資訊不完全賽局，並且在賽局當中考慮惡意使用者與詐欺使用者(cheating peer)的影響。最後，我們將以多人資訊不完全賽局之不同使用者的獲利做為客觀的分析比較。

Cooperative and Secure Transmission in the Unreliable Peer-to-Peer System

Student: Min-Ching Li

Advisor: Hsu-Feng Hsiao

Institute of Network Engineering
National Chiao Tung University

Abstract

Cooperative network has become one of the main trends of the research of peer-to-peer system. A peer in the cooperative network shares its resource including the storage of information, CPU, memory...etc. However, free-riders usually appears in the systems. Free-riders obtain the resources from the system and do not share any resource. The behavior of free-riders decreases the incentives for sharing resources. In this thesis, we propose a novel game to encourage the cooperation between peers. At first, we analyze the Nash equilibrium for two-player complete information game, incomplete information game, and multi-player incomplete information game respectively. And then we consider the impacts of malicious peers and cheating peers. Finally, we will compare objectively with each rewards of each kind of peers in the multi-player incomplete information game.

Acknowledgement

能夠完成碩士論文，首先必須要感謝的是蕭教授的指導。當在研究方面遇到思考上的困境時，教授總是可以給我合適的尋找解答的方向，讓我可以從困境中順利解決問題。在研究的過程中，蕭教授也經常耳提面命要注意的研究態度與求知精神，讓我獲益良多，最終完成這篇碩士論文。同時也要感謝實驗室的同仁，讓我在研究上有共同討論的對象，另一方面也要感謝交大資工系計中助教同仁，讓我在碩士生涯中學到許多知識與技術。最後，謹將這篇論文獻給我最摯愛的父母與家人。



List of Content

摘要.....	ii
Abstract.....	iii
Acknowledgement.....	iv
List of Content.....	v
List of Figures.....	viii
1. Introduction.....	1
2. Related Work.....	3
2.1 Reputation System.....	3
2.2 Network Coding.....	5
2.3 Signature-Based Network Coding.....	8
2.4 Game Theory.....	9
3. Proposed Rank-Based Game.....	17
3.1 Rank-Based Game.....	17
3.1.1 Two Player Rank-Based Game with Complete Information .	17
3.1.2 Two Player Rank-Based Game with Incomplete Information	21
3.1.3 Multi Player Rank-Based Game with Complete Information	26
3.1.4 Multi Player Rank-Based Game with Incomplete Information	29
3.1.5 Rank-Based Game with Malicious Players and Cheating Players	30
3.2 Proposed System Architecture.....	36
3.2.1 Multi-Player Rank-Based Game.....	37
3.2.2 Exchange stage.....	39
3.2.3 Update stage.....	42
3.3 Verification of Rank-Based Game.....	45
3.3.1 The Verification of Nash Equilibrium with Two-Player Game	45
3.3.2 The Impacts of The Non-used Blocks.....	47
3.3.3 The Proof of Algorithm of Estimating Private Information ..	49
4. Simulation and Discuss.....	57
4.1 The Coefficient of Expected Rank at Specific Rank k, C_{ik}	57
4.2 The Impacts of Malicious Players and Cheating Players.....	59
4.2.1 The Impact of Malicious Player.....	60

4.2.2	The Impact of Cheating Behavior	64
4.2.3	The Impacts of Malicious Player and Cheating Player	68
5.	Conclusion	74
6.	References:.....	75



List of Tables

Table 2.4-1: The payoff matrix of prisoner's dilemma	11
Table 3.1.2-1: The coefficient of two-player game: example 1	25
Table 3.1.2-2: The process of negotiation of two-player incomplete information game: example 1	25
Table 3.1.2-3: The coefficient of two-player game: example 2	25
Table 3.1.2-4: The process of negotiation of two-player incomplete information game: example 2	26
Table 3.1.5-1: The normal situation of estimated process	32
Table 3.1.5-2: The cheating situation of estimated process	32
Table 3.1.5-3: The initial coefficient of 4-player game	35
Table 3.1.5-4: The result of 4-player game	36
Table 3.3.3-1: The process of estimation private information: example 1	54
Table 3.3.3-2: The difference between estimation $_{i,t}$ and real value: example 1	54
Table 3.3.3-3: The common ratio between the differences between estimation $_{i,t}$ and real value: example 1	55
Table 3.3.3-4: The process of estimation private information: example 2	55
Table: 3.3.3-5: The difference between estimation $_{i,t}$ and real value: example 2	56
Table 3.3.3-6: The common ratio between the differences between estimation $_{i,t}$ and real value: example 2	56
Table 4.1-1: The simulation environment	57
Table 4.2.1-1: The simulation environment	61
Table 4.2.2-1: The simulation environment	65
Table 4.2.3-1: The simulation environment	69

List of Figures

Figure 2.2-1: Sample description of Avalanche	6
Figure 3.1.1-1: The coordinate of utility	19
Figure 3.1.4-1: The flow charts of multi player incomplete information game.....	30
Figure 3.1.5-1: The product of utility with different algorithm	36
Figure 3.2-1: The proposed architecture	37
Figure 3.2.1-1: The flow charts of rank-based game	38
Figure 3.2.2-1: The flow charts of upload procedure	40
Figure 3.2.2-2: The flow charts of download procedure	41
Figure 3.2.3-1: The flow charts of update procedure	42
Figure 3.3.2-1: The situation of estimating private information.....	50
Figure 4.1-1: 100 nodes with different connective probability $p=7.5%$, $10%$, and $12.5%$	58
Figure 4.1-2: 200 nodes with different connective probability $p=3.5%$, $5%$, and $6.5%$	58
Figure 4.1-3: 300 nodes with different connective probability $p=2%$, $2.5%$, and $3%$	59
Figure 4.2.1-1: The average utility of each section with 30% malicious players and attack rate 50%	62
Figure 4.2.1-2: The average of the logarithm of product of utility of each section with 30% malicious players and different attack rate 50%	64
Figure 4.2.2-1: The average utility of each section with 30% cheating player and cheating parameter 0.3	67
Figure 4.2.2-2: The average of the logarithm of product of utility of each section with 30% cheating player and cheating parameter 0.3	68
Figure 4.2.3-1: The average utility of each section with 30% cheating player and 30% malicious player.....	72
Figure 4.2.3-2: The average of the logarithm of product of utility of each section with 30% cheating player and 30% malicious player	73

1. Introduction

Typical content distribution systems are based on a super server to support the entire systems. In the recent years, the new type of content distribution systems, such as peer-to-peer distribution systems, has become the main trend of research, in which they collect a large number of computers to form a cooperative network and share their resources.

Since the peer-to-peer content distribution systems have become popular, some of the critical problems in the system have been taken seriously such as free-rider problem and content pollution. The free-rider problem is the problem in economics which means that free riders want to obtain the public resources for free, and the problem, in peer-to-peer systems, means that a node can obtain the utility and does not share any file. The content pollution problem means that the polluter tampers with the content of the file, and the file will be useless. The content pollution problem leads to the file destruction and the free-rider problem decreases the incentives for sharing file.

Network coding technique is appropriate for peer-to-peer systems and wireless sensor network. Network coding technique can not only enhance the efficiency of transmission in peer-to-peer systems, but also improve the scheduling problem. The extra overheads caused by network coding technique can be similar to the overhead caused by the scheduling problem if we use the appropriate network coding techniques. Network coding technique also enhances the impacts of the content pollution problem. However, the traditional signature is inappropriate to network coding technique. The signature will be destroyed. Signature-based network coding

offers a method to verify the integrity of encoded block and the signature can be legitimately generated by the client.

The reputation system can reduce the impact of the content pollution problem, but it needs some technique to help it verify the normal item. The signature-based network coding can verify the integrity of item. However, the reputation system cannot deal with the free-rider problem.

Since 1938, the game theory has been researched in economic. In recent years, the game theory has been applied to solve the power management problem. It also deals with the free-rider problem because in the game theory, the players must contribute their resources to bargain for some utilities.

In this study, we will propose a novel rank-based game architecture to deal with the content pollution and the free-rider. Our focus is offering a platform under the unreliable environment to distribute the file securely.

The rest of this paper is organized as follows. In Chapter 2 we introduce the related works of reputation system, network coding and game theory. In Chapter 3 we describe our proposed method, followed by Chapter 4, the simulation results and discussion. The concluding remarks are presented in Chapter 5.

2. Related Work

Content pollution problem is a common problem in a peer-to-peer file distribution system. The polluter tampers with the content of the file, and the file will be useless. This polluted situation is more serious in the peer-to-peer system with network coding technique. In this study, our focus is distributing the file in the peer-to-peer system using the network coding technique with polluted environment. In the following chapter we will introduce the previous researches about reputation system, network coding technique and game theory.

2.1 Reputation System

Reputation System is a technique for evaluating the characteristic such as peer's behaviors and player's honesty...etc. As above mentioned, we know that the reputation system can reduce the influence of the content pollution problem. In the following, we will introduce two decentralized reputation systems, Credence [9] and Scrubber [10]. Credence is a decentralized reputation system which evaluates the authenticity of disseminated files (the Credence's author calls it object). It is based on a distributed vote protocol for transporting the object reputation in the network and on a correlation schemes which decide the vote by peers who share the same mind. When a peer receives an object, the peer can calculate the probability that the object is correct. However, in our proposed method, we want to evaluate the behavior of players, so the Credence is inappropriate for our proposed method.

Scrubber is another decentralized reputation system which evaluates the authenticity of the peer behavior. Scrubber can identify and isolate the malicious peers that actively spread the polluted content. In Scrubber, each peer assigns reputations to each other. There are two critical components in this reputation system, *individual experience* and *peer testimonial*. The individual experience of peer i with respect to peer j is the quantity of trust that peer i has evaluated from its previous downloads received from peer j . After each download from peer j , peer i updates its individual experience $I_{i(j)}$, as follows:

$$I_{i(j)} = \begin{cases} \max(0, I_{i(j)} - \alpha_d n^2) & \text{if download is polluted} \\ \min(1, I_{i(j)} + \alpha_i) & \text{otherwise} \end{cases} \quad (1)$$

where n is the number of consecutive polluted downloads from peer j , α_d is the penalty given to peer j for each polluted download and α_i is the reward given to peer j for each unpolluted download. We normally set $\alpha_d > \alpha_i$.

Because the increased speed of individual experience is slower than the decreased speed, scrubber can identify the malicious peer quickly and easily. Although the peer receives a good reputation, it will quickly decrease once the peer makes malicious behaviors.

The peer testimonial of peer i with respect to peer j can be captured on the other peers' opinion. Periodically, each peer i sends a query to a number of randomly selected known peers to ask for their individual experience with respect to other peers. Before each new download, peer i updates the peer testimonial, as follows:

$$T_{i(j)} = \frac{\sum_{k \in N_{i(j)}} \min\{I_{k(j)}, R_{i(k)}\} * R_{i(k)}}{\sum_{k \in N_{i(j)}} R_{i(k)}} \quad (2)$$

Where $N_{i(j)}$ is the list of peers that responded to the queries from peer i with their individual experience on peer j and $R_{i(j)}$ is the current reputation of peer j on peer i .

Before and after each download, peer i can compute the reputation of each other peer j , as follows:

$$R_{i(j)} = \beta T_{i(j)} + (1 - \beta) I_{i(j)} \quad (3)$$

where $\beta(0 \leq \beta \leq 1)$ controls the weights given to individual experience and peer testimonial.

In this study, we use the reputation system modified from Scrubber to help us to evaluate the reliability of network coding encoded blocks.

2.2 Network Coding

Network coding is a popular forwarding technique which is used with the transmission of peer-to-peer systems and wireless sensor networks. According to Ahlswede et al. [1], network coding technique can achieve the maximum throughput of multicast networks, in which a source peer intends to send its messages to multiple client peers simultaneously. Using network coding, a peer can encode its incoming packets to generate a new outgoing packet. Koetter et al. [2] have shown that by coding on a field, linear codes are sufficient to achieve the multicast capacity, and Ho et al. [3] have shown that using randomized network coding is a more practical way to design linear codes to be used. Gkantsidis et al. [4] have proposed the principles of randomized network coding with peer-to-peer content distribution systems, and have

shown that file download times can be reduced.

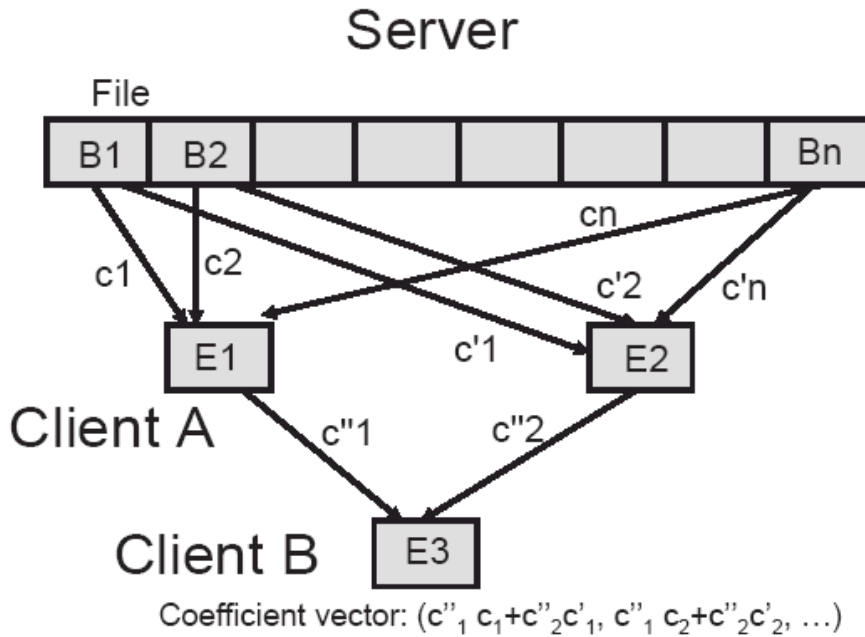


Figure 2.2-1: Sample description of Avalanche

The operation of *Avalanche* is described in Figure 2.2-1. All these operations take place in a finite field. Assume that client A contacts the server to get a block. The server will generate a new encoded block E_1 which consists of the entire original block B_i as follows. First, the server will select some random coefficients c_1, c_2, \dots, c_n , then multiply each original block B_i with c_i , and finally add the result together. We can calculate E_1 as follows:

$$E_1 = \sum_{i=1}^n c_i * B_i \pmod{p} \quad (4)$$

where p is the primer. The server will respond the result, E_1 , and the *coefficient vector* $\vec{c} = (c_i)$ to the client A.

As above mentioned, network coding can achieve a special ability that a peer can generate a new encoded block by its received encoded blocks. Assume that the client

A already receives two encoded blocks, E_1 and E_2 , and two coefficients, \vec{c} and \vec{c}' , and the client B contacts the client A to query an encoded block. The client A will generate a new encoded block E_3 which is a linear combination of E_1 and E_2 as follows. The client A selects two random coefficients c''_1 and c''_2 , multiplies E_1 with c''_1 and multiplies E_2 with c''_2 , and adds the results together. The new coefficient vector \vec{c}'' associated with E_3 is equal to $c''_1 * \vec{c} + c''_2 * \vec{c}'$. We can mathematically illustrate the procedure which the client A does above.

The client A knows

$$E_1 = \sum_{i=1}^n c_i * B_i \pmod{p}, \vec{c} = (c_1, c_2, \dots, c_n) \quad (5)$$

And

$$E_2 = \sum_{i=1}^n c'_i * B_i \pmod{p}, \vec{c}' = (c'_1, c'_2, \dots, c'_n) \quad (6)$$

The client A can compute the new encoded block E_3 as follows:

$$\begin{aligned} E_3 &= c''_1 * E_1 + c''_2 * E_2 \pmod{p} \\ &= c''_1 * \sum_{i=1}^n c_i * B_i + c''_2 * \sum_{i=1}^n c'_i * B_i \pmod{p} \\ &= \sum_{i=1}^n c''_1 * c_i * B_i + \sum_{i=1}^n c''_2 * c'_i * B_i \pmod{p} \\ &= \sum_{i=1}^n (c''_1 * c_i + c''_2 * c'_i) * B_i \pmod{p} \end{aligned} \quad (7)$$

The new coefficients vector can calculate as follows:

$$\vec{c}'' = (c_1'' * c_1 + c_2'' * c_1', c_1'' * c_2 + c_2'' * c_2', \dots, c_1'' * c_n + c_2'' * c_n') \quad (8)$$

2.3 Signature-Based Network Coding

Traditional signature approaches based on hash functions such as SHA-1 or MD5 are not suitable for network coding, because the signature will be destroyed at the encoding process. The signature-based network coding can address the pollution attacks against network coding applications. Gkantsidis and Rodriguez proposed a homomorphic hashing scheme [5] which relies on extra secure channels to transmit hash data. Charles, Jain and Lauter proposed a homomorphic signature scheme [6] which is based on public-key cryptography over elliptic curves, but the client peer needs a lot of computation to verify the signature because of lots of exponential operations at the verification process. Yu, Wei, Ramkumar and Guan proposed another homomorphic signature scheme [7] which is based on public-key cryptography over RSA. Kehdi and Li proposed a novel signature scheme for network coding [8] which is based on the null space of the original content and has a polynomial-time verification process. In this study, we use nullkey [8] to verify the unpolluted encoded block.

The null space of a given matrix A is the set of all the vectors z for which $Az=0$. According to the rank-nullity theorem, we have $rank(A) + nullity(A) = n$ for any given $m \times n$ matrix A , where the dimension of the null space of A is named the nullity of A . In the network coding, the server has r blocks, each represented by d elements

which are on the finite field F_q . The server extends block i with r symbols to form the vector x_i . The x_i can be defined as follows:

$$x_i = (0, 0, \dots, 1, \dots, 0, b_1 b_2, \dots, b_d)$$

where b_i is a part of contents of block i , and the one is at position i . And then we can denote by X the $r \times (r + d)$ matrix whose i^{th} row is x_i . All the x_i form a set of r independent vectors which can span a subspace Π_X . Because any linear combination of the vectors $\{x_1, x_2, \dots, x_r\}$ belongs to Π_X , we know that the Π_X is closed under randomized linear combinations.

In the nullkey, the set of the signature called null key is the set of the null space of Π_X , denoted as Π_X^\perp . According to rank-nullity theorem, the dimension of Π_X^\perp is equal to d . The subspace Π_X^\perp is spanned by the vectors $\{z_1, z_2, \dots, z_d\}$, so we denote by Z the $d \times (r + d)$ matrix whose i^{th} row is z_i . With network coding, all the encoded blocks are randomized linear combination of $\{x_1, x_2, \dots, x_r\}$, and belong to Π_X . Each encoded block is orthogonal to randomized linear combination of $\{z_1, z_2, \dots, z_d\}$ which belongs to Π_X^\perp . The client verifies an encoded block is valid if the encoded block w satisfies the following condition:

$$K_i w^T = 0 \tag{9}$$

where K_i is the matrix which is formed by the null keys.

2.4 Game Theory

Game Theory is a branch of mathematics which is used in social sciences, economics especially, as well as in biology engineering, political science,

international relations, computer science, and philosophy. Game theory aspires to mathematically catch behavior in strategic situations, or *game*, in which an individual's success depends on the other's options.

Traditional applications of game theory attempt to find equilibriums in their games. In equilibrium, each player of the game has chosen a strategy, or made a decision. The types of games include cooperative or non-cooperative, symmetric or asymmetric, zero-sum or non-zero-sum, complete information or incomplete information...etc.

A non-cooperative game is a game that each player in the game makes decisions independently. A cooperative game is a game where groups of players enforce cooperative behavior. A symmetric game is a game where the rewards for playing a particular strategy depend only on the other strategies, not on the other's identity. A zero-sum game means a game has a situation in which a player's gain or cost is exactly equal to the other's cost or gain. In non-zero-sum games, a player's gain does not necessarily correspond with another. The difference between complete information games and incomplete information games is that in complete information game, every player knows the strategies and payoffs of the other player. For instance, Poker is a non-cooperative, asymmetric, incomplete information and zero-sum game, prisoner's dilemma is a non-cooperative, symmetric, complete information and non-zero-sum game.

In game theory, Nash equilibrium is a solution of a game involving two players or multi player game. In Nash equilibrium situation, each player knows the equilibrium strategies of the other players and for each player, and no other strategy can reward more utility than equilibrium strategy. If each player has chosen a strategy and no player can reward by changing his or her strategy and the other player keep

their strategy unchanged, then the current set of strategy and the utility constitute Nash equilibrium.

The prisoner's dilemma is a fundamental problem in game theory. This problem illustrates why two people might not cooperate. If the payoff matrix of prisoner's dilemma is as following:

	Prisoner B stays silent	Prisoner B betrays
Prisoner A stays silent	Each serves 6 months	Prisoner A: 10 years Prisoner B: goes free
Prisoner A betrays	Prisoner A: goes free Prisoner B: 10 years	Each serves 5 years

Table 2.4-1: The payoff matrix of prisoner's dilemma

In table 2.4-1, if both prisoner A and prisoner B stay silent, they just only server 6 months, but if one of them betrays, the betrayer can go free and the other must server 10 years. If both prisoner A and prisoner B betray each other, they must serve 5 years. According to above table description, the best strategy in the table 2.4-1 is that both of them stay silent. However, we obtain that either prisoner A or prison B chooses the strategy of betraying is better than staying silent. If they want to choose the best strategy, they must satisfy the cooperative situation. The cooperative situation does not exist in the prisoner dilemma problem because the strategy of staying silent has fewer benefits than the strategy of betraying. In this game, the Nash equilibrium is both prisoner A and prisoner B choose the strategy of betraying. The prisoner dilemma illustrates that the best strategy may not be the Nash equilibrium in the game theory.

In 2003, Buragohain et al. proposes a game theoretic framework for incentive in the peer-to-peer system [11]. In [11], the author assumes that all players are rational under the game environment given by the author. The players are rational because they wish to maximize their own benefit. There are three key components in this framework: strategy, utility and Nash equilibrium. The strategy for each player is the behavior interacting with other players. The player's utility is the benefit derived from his interaction with other players. If no player can improve his utility by changing his strategy, the collection of players are said to be at Nash equilibrium. The reaction function is the best reaction for player, given a strategy for other. If the result of reaction function is equal to the result of reaction function at past, then the Nash equilibrium is found.

In 2008, K. J. Ray Liu *et al.* proposes another game theoretic framework for incentive-based peer-to-peer live streaming social network [12]. In [12], it illustrates two-player peer-to-peer live streaming game with complete information and different optimality criteria such as Pareto-Optimality, proportional fairness and absolute fairness. The author considers the cheating behaviors that the player gives the cheating information to mislead the players into disadvantageous situation. The author proposes the cheating-proof strategy in which the player in game should not send more data than what the other has sent. However, there is a contradiction at the cheating-proof strategy if the two-player game is incomplete information game. The contradiction means that the player in the game will not offer the better strategy because of the restriction of the cheating-proof strategy. In our study, we attempt to find Nash equilibrium under the complete information situation and incomplete information situation with network coding environment. On the other hand, we also consider the content pollution problem situation. However, in [12], it is based on

peer-to-peer live-streaming social network without content pollution problem and the author only considers the complete information situation.

In 2008, M. K. H. Yeung *et al* have proposed the packet exchange game for scalable peer-to-peer media streaming system [13]. In the packet exchange game, the author uses the punish- k strategy to achieve the equilibrium strategy. It is different from the above frameworks in which they tend to give some incentive strategy to reward more utility, and the punish- k strategy offers the punishment to prevent the players from changing their strategy. The author mathematically demonstrates that the loss utility of punishment is larger than the reward of leaving the Nash equilibrium.

Recent results in [13], [19], [20], and [21] have focused on using game theory to solve packet forwarding problem in mobile ad hoc networks or peer-to-peer system without network coding technique or with network coding technique. The packet forwarding problem means the procedure to route the packets from the source to the destination. Recent results in [17] have focused on using game theory to solve the resource distribution problem based on network coding technique. Recent results in [22] and [26] have focused on using game theory to solve the joint optimization problem. In [22], the author attempts to increase the capacity of multi-channel mesh network and proposes the joint optimization problem which is concerned with routing, channel assignment, and network coding. In [26], the author attempts to improve the bandwidth efficiency in OFDMA based wireless network and proposes the joint optimization problem is concerned with dynamic subcarrier assignment and network coding. Recent results in [23] and [27] have focused on using game theory to solve the rate allocation and control problem. Recent results in [24] have focused on using game theory to solve the power management problem in ad-hoc opportunistic radio. Recent results in [25] have focused on using game theory to solve the open spectrum

sharing problem. In 2008, C. Wu *et al* have proposed a dynamic auction game for multi-overlay peer-to-peer streaming using network coding [17]. The game attempts to resolve the conflicts among coexisting streaming overlays in their bandwidth competition. The player in the dynamic auction game can minimize their streaming cost and satisfy the streaming rate for each coexisting streaming overlay.

In 2009, X. Zhang *et al* seek to use a novel concept to describe the coding based peer-to-peer content distribution system as a peer-to-peer market system [18]. The authors have proposed entry price and expected payoff for each coded block, and claimed that this market system can maintain stability if peer follows the operation guidelines for a peer-to-peer market. Finally, the author characterizes the pricing strategies as many subgame perfect Nash equilibrium.

In 2010, T. Chen *et al* have proposed INPAC for the wireless mesh network using network coding [19]. The authors attempt to solve the incentive compatible packet forwarding problem and incentive compatible routing problem by the analysis of game theory. The author assumes the players in this game are required by the MORE protocol and considers this game as a repeated game. They claim INPAC is the first incentive scheme for packet forwarding in wireless mesh networks using network coding.

However, the dynamic auction game focuses on the optimal distribution of streaming rate based on the minimum of streaming cost, but not considers the malicious or cheating situation on its game. In our study, we pay attention to the maximum of player's reward based on the Nash Bargaining Solution [15] and also consider the malicious and cheating situation. In [18], the author focuses on a theoretical framework that quantifies the market power of network coding in a non-cooperative P2P content distribution system. In our study, we focus on how to

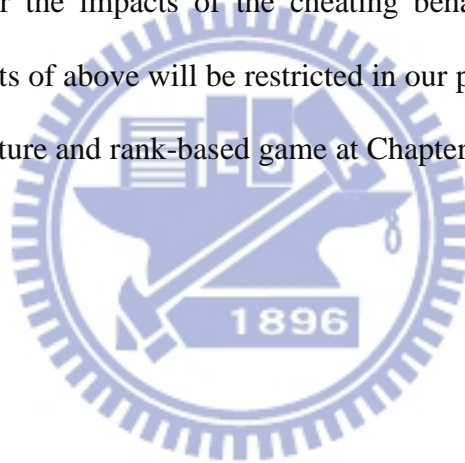
distribute the resource to maximize the player's reward based on the Nash Bargaining Solution. The game in the INPAC is the repeated game to deal with the incentive compatible packet forwarding problem under the wireless Networks using network coding. However, the author does not consider the content pollution problem on their environment. In our study, we have proposed the learning-based game under the coded-based peer-to-peer system to deal with the resources distribution problem with the malicious situation which is the malicious player will randomly modify the contents of encoded block. According to the bargaining procedure, the player in our proposed game will update the coefficient to evaluate a player's property and share the part of message to other players.

In our study, we attempt to address the problem on the network coding environment. The network coding technique is a branch of the channel coding technique. The channel coding technique is popular and suitable for the content distribution system; especially the transmission type is broadcast as wireless network. Most of the channel coding techniques can be regarded as the procedure of finding the solution from the set of the linear equations. If the peer can receive enough encoded blocks, the peer can decode the part or all of the original blocks. As above mentioned, we know the proposed rank-based game is also suitable for the environment with channel coding technique.

In this thesis, we consider how to maximize player's utility through the negotiation of game theory even if there are some of players who maybe perform malicious or cheating behavior. According to the above mentioned, we know our problem is belonging with resource distribution problems and security problems. The resource distribution problems under network coding technique concerned with security is a novel opinion. It is essential and important in the future. If there is no

effective method to restrict to malicious behaviors, the effect of resource distribution will be reduced or even the whole network based on network coding technique will destroy. To solve this problem, we consider both of malicious behaviors and cheating behaviors with network coding technique and attempt to use the game theory to analyze the player's behavior.

In our study, we consider the content pollution problem with network coding technique and after completing each game, measure the alteration of each player's contribution and update the player's information of game. We will start from the analysis of two-player game and then extend the two-player game to the multi-player game. We also consider the impacts of the cheating behaviors and the malicious behaviors and the impacts of above will be restricted in our proposed method. We will propose a novel architecture and rank-based game at Chapter 3.



3. Proposed Rank-Based Game

In this chapter, we will describe our proposed novel architecture and rank-based game in detail. In the proposed rank-based game, the reputation is required in the reward coefficient which evaluates the malicious behavior. For this purpose, we require a reputation system to evaluate the characteristic of player's behavior.

3.1 Rank-Based Game

The rank-based game is a strategic game that models the interactions of a set of players. We assume players are selfish and rational which independently decide their strategy to optimize their own utility in the rank-based game. To simplify the illustration, we will describe the rank-based game from simpler situation to more complex situation. Final, we will discuss the impacts of cheating behavior in our game.

3.1.1 Two Player Rank-Based Game with Complete Information

In this section, we will describe the simplest situation of rank-based game. There are two players in this game, denoted by N_1 and N_2 . Each player needs its opponent to exchange a certain number of their encoded blocks. For each player i , the cost of

generating a new encoded block and uploading to its opponent is c_i . The gain of receiving new encoded blocks from its opponent is evaluated by rewarded rank. It has three components such as unpolluted probability, p_{ji} , the coefficient of expected rank from specific opponent, r_{ji} , and typical coefficient of expected rank at rank k , C_{ik} , which is the rank number of player i 's independently encoded blocks. The unpolluted probability p_{ji} means that the probability of receiving an unpolluted block from player j . The coefficient of expected rank r_{ji} means that expected reward of rank when the player i receives a new encoded block from player j . Let B_i be the total number of blocks that player i will offer to exchange with others. The strategy a_{ij} mean that player i can offer a_{ij} encoded blocks to player j . The coefficient of gain is to measure the expected reward of rank with an incoming encoded block. The coefficient of expected rank at rank k , C_{ik} , means the expected rank income when the player i receives an encoded block randomly. The utility can be calculated as the following formula.

$$\begin{aligned}
 u_{ij}(a_i, a_j) &= P_{ji} * a_{ji} * C_{ik} * r_{ji} - c_i * a_{ij} + \delta_i * a_{ii} \\
 &\cong P_{ji} * a_{ji} * C_{ik} * r_{ji} - c_i * a_{ij}
 \end{aligned} \tag{10}$$

where a_i is the set of strategy of player i , denoted by $a_i=(a_{i1}, a_{i2})$, where a_{ii} is the storage of exchanged blocks which does not be used, δ_i is the reward coefficient that store an exchanged block which is not used. We assume that δ_i must satisfy

$$\begin{aligned}
 0 &< \delta_i * B_i \ll L \\
 L &= \min_{\forall j \neq i, \{x = P_{ji} * a_{ji} * C_{ik} * r_{ji} - c_i * a_{ij} | a_{ij}, a_{ji} > 0, x > 0\}}
 \end{aligned} \tag{11}$$

where L is the value of minimum utility of all possible strategy which the utility is larger than zero.

Now, we will start to analyze the two-player complete information rank-based game. For player 1, its utility function is shown in (12)

$$\begin{aligned} u_{12}(a_1, a_2) &= P_{21} * a_{21} * C_{1k} * r_{21} - c_1 * a_{12} + \delta_1 * a_{11} \\ &\cong P_{21} * a_{21} * C_{1k} * r_{21} - c_1 * a_{12} \end{aligned} \quad (12)$$

For player 2, its utility function is shown in (13)

$$\begin{aligned} u_{21}(a_1, a_2) &= P_{12} * a_{12} * C_{2k} * r_{12} - c_2 * a_{21} + \delta_2 * a_{22} \\ &\cong P_{12} * a_{12} * C_{2k} * r_{12} - c_2 * a_{21} \end{aligned} \quad (13)$$

So we can plot the both utilities as two coordinate axes into a coordinate like figure 3.1.1-1.

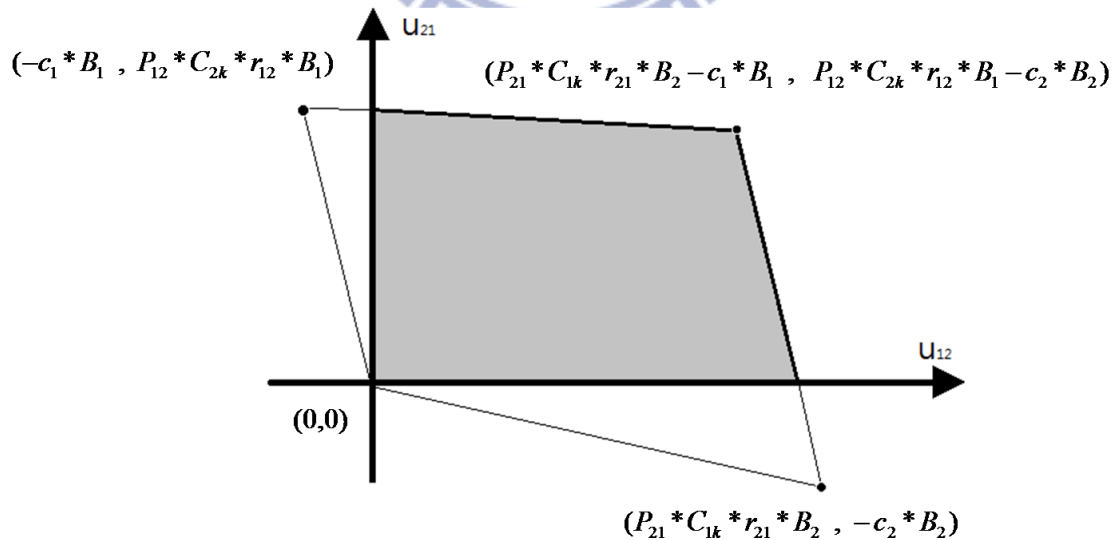


Figure 3.1.1-1: The coordinate of utility

In figure 3.1.1-1, the vertical axis denotes player 2's utility and the horizontal

axis denotes player 1's utility. The possible strategy pair inside the convex hull of $\{(0, 0), (-c_1 * B_1, P_{21} * C_{2k} * B_1), (P_{12} * C_{1k} * B_2 - c_1 * B_1, P_{21} * C_{2k} * B_1 - c_2 * B_2), (P_{12} * C_{1k} * B_2, -c_2 * B_2)\}$. However, for each player, it wishes its utility is a positive value. So, the possible strategy pair inside the gray area in figure 3.1.1-1.

As above mentioned, there are many possible strategy sets, but not all the obtained strategy sets are better. Next we show how to select the better strategy set and find the Nash equilibrium. In our study, we refine the strategy set with optimality criteria of proportional fairness and it can reduce the set of strategy set to a unique point that we call Nash equilibrium.

According to [14], [15] and [16], we know that the optimality criterion which is the maximal product of both utilities is the solution for the bargaining game. The solution means that a determination of how much it should be worth to each of these individuals to have this opportunity to bargain [15]. To satisfy the bargaining game, the game must have 3 properties as follows,

1. $d = (d_1, d_2) \in U$
2. $\exists u = (u_1, u_2) \in U$, such $u_1 > d_1$ and $u_2 > d_2$
3. U is convex, bounded and closed

Where U denotes the set of attainable utility pairs, u_i denotes the utility of player i , d is the utility pairs that the players reward the utility if the players fail to achieve an agreement, and d_i is that the player i rewards the utility when the players fail to achieve an agreement. In figure 3.1.1-1, it is obvious that our proposed rank-based game can satisfy the first property of bargaining game, $d = (0,0)$, and the second property of bargaining game, and the graph of utility pairs in the figure 3.1.1-1 is convex, bounded and closed. Our proposed rank-based game also can satisfy the third property of bargaining game.

According to the above mentioned, our proposed rank-based game belongs with the bargaining game. The selected strategy set is proportional fairness if $u_{12}(a_1, a_2) * u_{21}(a_1, a_2)$ can be maximized. The Nash equilibrium can be derived as follows.

$$\begin{aligned}
& \text{If } \frac{1}{2} \left[\frac{P_{12} * C_{2k} * r_{12}}{c_2} + \frac{c_1}{P_{21} * C_{1k} * r_{21}} \right] < \frac{B_2}{B_1} \\
& \quad a_1^* = (0, B_1), a_2^* = \left(\frac{1}{2} \left[\frac{P_{12} * C_{2k} * r_{12}}{c_2} + \frac{c_1}{P_{21} * C_{1k} * r_{21}} \right] * B_1, 0 \right) \\
& \text{If } \frac{2}{\frac{P_{21} * C_{1k} * r_{21}}{c_1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}}} \leq \frac{B_2}{B_1} \leq \frac{1}{2} \left[\frac{P_{12} * C_{2k} * r_{12}}{c_2} + \frac{c_1}{P_{21} * C_{1k} * r_{21}} \right] \\
& \quad a_1^* = (0, B_1), a_2^* = (B_2, 0) \\
& \text{If } \frac{B_2}{B_1} < \frac{2}{\frac{P_{21} * C_{2k} * r_{21}}{c_1} + \frac{c_2}{P_{12} * C_{1k} * r_{12}}} \\
& \quad a_1^* = \left(0, \frac{1}{2} \left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} \right] * B_2 \right), a_2^* = (B_2, 0)
\end{aligned} \tag{14}$$

where a_i^* is the set of strategy which is the Nash equilibrium. With complete information game, because we know the opponent's private information such as P_{ji} , r_{ji} , and c_i , we can immediately calculate the Nash equilibrium. However, a player may not offer the private information easily. In the next section, we will introduce how to estimate the opponent's private information with incomplete information game.

3.1.2 Two Player Rank-Based Game with Incomplete Information

In this section, we will introduce the algorithm of estimating the opponent's

private information. With incomplete information game, a player only knows its private information but does not know another's private information. Before we introduce the algorithm of estimating private information, we must know the algorithm of negotiation with incomplete information that means how to respond a strategy with incomplete information when a player receives the opponent's strategy.

According to optimality criteria of proportional fairness, we know the product of both utilities is shown in (15).

$$\begin{aligned}
& u_{12}(a_1, a_2) * u_{21}(a_1, a_2) \\
& \cong (P_{12} * C_{2k} * r_{12} * P_{21} * C_{1k} * r_{21} + c_1 * c_2) * a_{12} * a_{21} \\
& - P_{21} * C_{1k} * r_{21} * c_2 * (a_{12})^2 - P_{12} * C_{2k} * r_{12} * c_1 * (a_{21})^2
\end{aligned} \tag{15}$$

To simply the formula, we ignore the impact of storing the non-used block, and we will describe the impact at the chapter 3.3. To find the maximum of the product, we separately perform the partial differential of (15) with respect to variable a_{12} and a_{21} , respectively, and let it equal to zero as follows.

With variable a_{12} :

$$\begin{aligned}
& \frac{\partial u_{12}(a_1, a_2) * u_{21}(a_1, a_2)}{\partial a_{12}} \\
& = (P_{12} * C_{2k} * r_{12} * P_{21} * C_{1k} * r_{21} + c_1 * c_2) * a_{21} \\
& - 2 * P_{21} * C_{1k} * r_{21} * c_2 * a_{12} \\
& = 0
\end{aligned} \tag{16}$$

Then

$$\begin{aligned}
a_{12} & = \frac{(P_{12} * C_{2k} * r_{12} * P_{21} * C_{1k} * r_{21} + c_1 * c_2)}{2 * P_{21} * C_{1k} * r_{21} * c_2} * a_{21} \\
& = \frac{1}{2} * \left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} \right] * a_{21}
\end{aligned} \tag{17}$$

$$\leq B_1$$

With variable a_{21} :

$$\begin{aligned} & \frac{\partial u_{12}(a_1, a_2) * u_{21}(a_1, a_2)}{\partial a_{21}} \\ &= (P_{12} * C_{2k} * r_{12} * P_{21} * C_{1k} * r_{21} + c_1 * c_2) * a_{12} \\ & \quad - 2 * P_{12} * C_{2k} * r_{12} * c_1 * a_{21} \\ &= 0 \end{aligned} \tag{18}$$

Then

$$\begin{aligned} a_{21} &= \frac{(P_{12} * C_{2k} * r_{12} * P_{21} * C_{1k} * r_{21} + c_1 * c_2)}{2 * P_{12} * C_{2k} * r_{12} * c_1} * a_{12} \\ &= \frac{1}{2} * \left[\frac{P_{12} * C_{2k} * r_{12}}{c_2} + \frac{c_1}{P_{21} * C_{1k} * r_{21}} \right] * a_{12} \\ &\leq B_2 \end{aligned} \tag{19}$$

According to (17) and (19), we can know the reaction function for player 1 and player 2 as follows.

For player 1:

$$a_{1,t} = \left(0, \min \left\{ B_1, \frac{1}{2} * \left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} \right] * a_{21,t-1} \right\} \right) \tag{20}$$

where $a_{21,t-1}$ is the strategy which the player 2 respond to player 1 at time $t-1$, $a_{1,t}$ is the set of strategy that the player 1 calculates at time t according to the strategy $a_{21,t-1}$.

For player 2:

$$a_{2,t} = \left(\min \left\{ B_2, \frac{1}{2} * \left[\frac{P_{12} * C_{2k} * r_{12}}{c_2} + \frac{c_1}{P_{21} * C_{1k} * r_{21}} \right] * a_{12,t-1} \right\}, 0 \right) \tag{21}$$

where $a_{12,t-1}$ is the strategy which the player 1 respond to player 2 at time $t-1$, $a_{2,t}$ is the set of strategy that the player 2 calculates at time t according to the strategy $a_{12,t-1}$.

Now, let us introduce the algorithm of estimating private information. According to (20) and (21), we can rewrite (20) and (21) with unknown information as follows.

$$\begin{aligned} a_{1,t} &= \left(0, \min \left\{ B_1, \frac{1}{2} * \left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + estimation_{1,t} \right] * a_{21,t-1} \right\} \right) \\ a_{2,t} &= \left(\min \left\{ B_2, \frac{1}{2} * \left[estimation_{2,t} + \frac{P_{12} * C_{2k} * r_{12}}{c_2} \right] * a_{12,t-1} \right\}, 0 \right) \end{aligned} \quad (22)$$

where $estimation_{i,t}$ is the estimated private information which is estimated at time t . We consider this situation that the player 1 sends the set of strategy $a_{1,t-1}=(0,a_{12,t-1})$ to player 2 and then the player 2 responds the set of strategy $a_{2,t-1}=(a_{21,t-1},0)$ to player 1. The player 1 can estimate the $estimation_{1,t}$ as follows.

$$estimation_{1,t} = \left[2 * \frac{a_{21,t-1}}{a_{12,t-1}} - \frac{c_1}{P_{21} * C_{1k} * r_{21}} \right]^{-1} \quad (23)$$

How the estimating private information can estimate accurately and rapidly will be verified at chapter 3.3.3.

Now, let us compare two-player complete information game with two-player incomplete information game. There are two examples to show that the obtained Nash equilibrium of complete information game is the same as incomplete information game. Without loss of generality, we assume the player 1 starts the estimation algorithm and $a_{12,0}=a_{21,0}=1$.

Table 3.1.2-1: The coefficient of two-player game: example 1

	$P_{ji} * C_{ik} * r_{ji}$		c_i	$P_{ji} * C_{ik} * r_{ji} / c_i$	B_i
player 1	0	0.7	0.28	2.5	1000
player 2	0.52	0	0.29	1.793103448	1000

According to (14), we know the Nash equilibrium of two-player complete information game is $a_1^* = (0,1000), a_2^* = (1000,0)$.

Table 3.1.2-2: The process of negotiation of two-player incomplete information game:
example 1

Negotiation	t=1	t=2	t=3	t=4	t=5	t=6	t=7
$a_{12,t}$	1.45	2.57	4.32	7.23	12.13	20.33	34.09
$a_{21,t}$	1.7	2.82	4.73	7.93	13.3	22.3	37.38

Negotiation	t=8	t=9	t=10	t=11	t=12	t=13	t=14
$a_{12,t}$	57.15	95.81	160.62	269.27	451.42	756.79	1000
$a_{21,t}$	62.67	105.06	176.13	295.27	495.01	829.86	1000

In table 3.1.2-2, we obtain the Nash equilibrium, $a_1^* = (0,1000), a_2^* = (1000,0)$, at t=14.

Table 3.1.2-3: The coefficient of two-player game: example 2

	$P_{ji} * C_{ik} * r_{ji}$	c_i	$P_{ji} * C_{ik} * r_{ji} / c_i$	B_i
--	----------------------------	-------	----------------------------------	-------

player 1	0	0.5	0.16	3.125	1000
player 2	0.83	0	0.14	5.928571429	1000

According to (14), we know the Nash equilibrium of two-player complete information game is $a_1^* = (0,1000), a_2^* = (1000,0)$.

Table 3.1.2-4: The process of negotiation of two-player incomplete information game:

example 2

Negotiation	t=1	t=2	t=3	t=4	t=5
$a_{12,t}$	1.72	8.66	44.55	229.23	1000
$a_{21,t}$	5.25	27.05	139.19	716.18	1000

In table 3.1.2-4, we obtain the Nash equilibrium, $a_1^* = (0,1000), a_2^* = (1000,0)$, at t=5.

According to above examples, in the two-player game, the negotiation of incomplete information can obtain a unique Nash equilibrium and this equilibrium is the same as the one of complete information game.

3.1.3 Multi Player Rank-Based Game with Complete Information

In this section, we will describe the multi-player rank-based game. There are m players in this game, denoted by (N_1, N_2, \dots, N_m) . Each player needs its opponent to exchange a certain number of their encoded blocks at next exchange stage. For each

player i , the cost of generating a new encoded block and uploading to its opponent is c_i . The gain of receiving new encoded blocks from its opponent is evaluated by rewarded rank. It has three components such as unpolluted probability P_{ji} , the coefficient of expected rank of specific opponent, r_{ji} , and typical coefficient of expected rank at rank k , C_{ik} , which is the rank number of player i 's independently encoded blocks. The unpolluted probability P_{ji} means that the probability of receiving an unpolluted block from player j . The expected rank coefficient r_{ji} means that expected reward of rank when the player i receives a new encoded block from player j . Let B_i be the total number of blocks that player i will offer to exchange with other and let B_{ij} be the number of blocks that player i will offer to exchange with player j . The strategy a_{ij} mean that player i can offer a_{ij} encoded blocks to player j at next exchange stage. The coefficient of gain is to measure the expected reward of rank with an incoming encoded block. Because the multi-player game is based on the two-player game, the utility of multi-player game is equal to the sum of the utility of each player. The utility function of player i in multi-player game can be calculated as follows.

$$u_i(a_1, a_2, \dots, a_m) = \sum_{k=1}^m u_{ik}(a_i, a_k) + \delta_i * a_{ii} \quad (24)$$

$$u_{ij}(a_i, a_j) = P_{ji} * a_{ji} * C_{ik} * r_{ji} - c_i * a_{ij}$$

where a_i is the set of strategy of player i , denoted by $a_i=(a_{i1}, a_{i2}, \dots, a_{im})$, where a_{ii} is the storage of exchanged blocks which is not used, δ_i is the reward coefficient that stores an exchanged block which is not used. The definition of δ_i is the same as in the two-player game.

Because of the complex dimension it is too difficult to plot all utilities into the

coordinate system like figure 3.1.1-1. According to figure 3.1.1-1, we can speculate that there are many possible strategies in the multi-player game like two-player game. In the multi-player game, we also require the optimality criteria to refine the possible strategy sets. The optimality criterion of proportional fairness is selecting the strategy pair which satisfies the maximum of the product of all utilities as follows.

$$\max_{\forall a_i, i=[1,m]} \prod_{k=1}^m u_k(a_1, a_2, \dots, a_m) \quad (25)$$

In two-player game, the same optimality criteria can reduce the set of strategy set to a unique point and can easily obtain the Nash equilibrium by (14). However, in multi-player game, this optimality criterion can also reduce to a unique point, but it requires horrible computing time to obtain by full search. To avoid the horrible computing time of full search, we propose a method to obtain the suboptimal Nash equilibrium of multi-player game: the proportional distribution strategy.

In proportional distribution strategy, according to each potential contribution of each opponent, a player can distribute the upload bandwidth for each opponent. Now, we define how to calculate the potential contribution as follows. The intuition of potential contribution is the ratio of the reward of a received block and the cost of an upload block. At personal reaction function which described in chapter 3.1.2, the higher ratio is meaning that the player is willing to offer a better strategy to a specific opponent and also meaning that the specific opponent maybe give better resources to the player. According to above mentioned, we define the potential contribution as (26). Let us take player i as an example.

$$v_{ij} = \frac{P_{ji} * C_{ik} * r_{ji}}{c_i} \quad (26)$$

where v_{ij} is the value of potential contribution for player j . The distribution of upload bandwidth can be calculated as follows.

$$B_{ij} = \frac{v_{ij}}{\prod_{k=1}^m v_{ik}} * B_i \quad (27)$$

According to distributed upload bandwidth, player i has many two-player games with each opponent.

3.1.4 Multi Player Rank-Based Game with Incomplete Information

In this section, we will introduce how to negotiation with multi player incomplete information.

The flow chart of proportional distribution strategy is shown in figure 3.1.4-1.

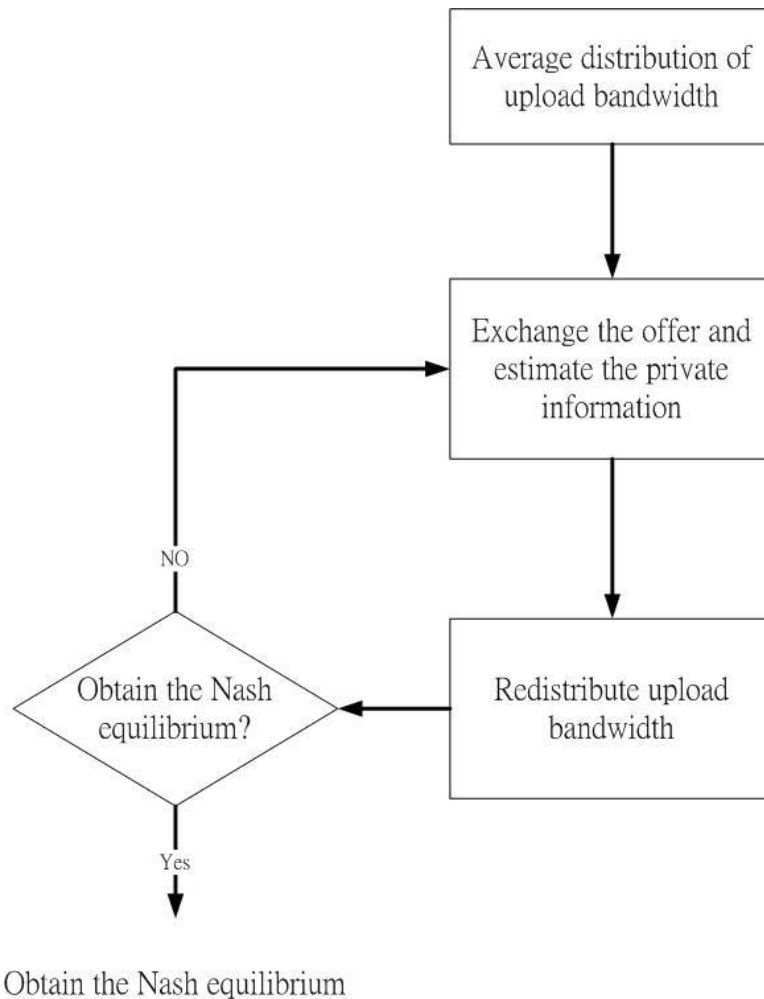


Figure 3.1.4-1: The flow charts of multi player incomplete information game

The player distributes the average distribution of upload bandwidth for each opponent at first. Next, the player exchanges their offer once with their opponent and performs the algorithm of estimating private information. Then, according to the estimated private information, the player redistributes the upload bandwidth for each opponent. Finally, the player repeats the above behavior until the player will not change their offers. The offer is the suboptimal Nash equilibrium.

3.1.5 Rank-Based Game with Malicious

Players and Cheating Players

Because of the assumption in which we assume the players are selfish, if a player can reward more utility through cheating behavior, we believe the player may cheat.

Let us describe the cheating behavior. We assume the player 2 will perform the cheating behavior which is responding the offer with the lower private information.

The both reaction functions which are described at chapter 3.1.2 is rewritten as following.

For player 1

$$a_{1,t} = \left(0, \min \left\{ B_1, \frac{1}{2} * \left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} * \frac{1}{\text{cheating}_2} \right] * a_{21,t-1} \right\} \right)$$

For player 2, who is cheating.

$$a_{2,t} = \left(\min \left\{ B_2, \frac{1}{2} * \left[\frac{c_1}{P_{21} * C_{1k} * r_{21}} + \frac{P_{12} * C_{2k} * r_{12}}{c_2} * \text{cheating}_2 \right] * a_{12,t-1} \right\}, 0 \right)$$

When player 2 assigns cheating parameter, cheating_2 , to a positive value which is smaller than 1, player 2 will respond the lower offer to player 1 and player 1 will respond the high offer to player 2. According to above mentioned, we know that the cheating behavior is effective.

We classify the cheating behavior in two categories: knowledgeable cheating behavior and unknowledgeable cheating behavior. The unknowledgeable cheating behavior means the cheating player only knows that responding the lower offer is better. The knowledgeable cheating behavior means the cheating player knows responding the offer with lower private information is better. To reduce the impact of cheating behavior, we propose two methods to detect cheating behavior.

First, according to the proof of algorithm of estimating private information in the chapter 3.3.3, we know the estimated value must be more approaching to the real

value than the estimated value in the past and never crosses the real value. There is an example as follows.

Table 3.1.5-1: The normal situation of estimated process

	real private information
player 1	0.453333
player 2	0.205128

Number of estimating	t=1	2	3	4
estimation _{1,t}	0.184445	0.204948	0.205127	0.205128
estimation _{2,t}	0.457624	0.45337	0.453334	0.453333

The unknowledgeable cheating behavior will respond with the lower offer by multiplying the original offer by a parameter p , $p=[0.5,1)$. There is an example as follows. We assume the player 2 is the unknowledgeable cheating player.

Table 3.1.5-2: The cheating situation of estimated process

	real private information
player 1	0.390805
player 2	0.159574

Number of estimating	t=1	2	3	4
estimation _{1,t}	0.219755	0.166896	0.230669	0.197642

estimation _{2,t}	0.381825	0.38969	0.38024	0.385076
---------------------------	----------	---------	---------	----------

In table 3.1.5-2, the estimated value of player 1 from $t = 1$ to $t = 2$ is incremental, but from $t = 2$ to $t = 3$ is decreasing. Player 1 can detect the cheating behavior of player 2.

Another detective method is shown as follows. For each possible strategy set, it must satisfy (28).

$$\frac{P_{12} * C_{1k} * r_{12}}{c_1} * \frac{P_{21} * C_{2k} * r_{21}}{c_2} > 1 \quad (28)$$

Proof of (28):

$$\because P_{21} * a_{21,t} * C_{1k} * r_{21} - c_1 * a_{12,t} > 0, \forall t > 0$$

$$\therefore \frac{P_{21} * C_{1k} * r_{21}}{c_1} > \frac{a_{12,t}}{a_{21,t}}$$

$$\text{And } \because P_{12} * a_{12,t} * C_{2k} * r_{12} - c_2 * a_{21,t} > 0, \forall t > 0$$

$$\therefore \frac{P_{12} * C_{2k} * r_{12}}{c_2} > \frac{a_{21,t}}{a_{12,t}}$$

$$\therefore \frac{P_{21} * C_{1k} * r_{21}}{c_1} * \frac{P_{12} * C_{2k} * r_{12}}{c_2} > \frac{a_{12,t}}{a_{21,t}} * \frac{a_{21,t}}{a_{12,t}} = 1$$

However, both of the above methods cannot detect all of cheating behaviors absolutely. The knowledgeable cheating player can perform the cheating behavior which responds with the offer by calculating the product of private information and the reciprocal of private information. This cheating behavior can be undetectable by the methods mentioned above.

As above analysis, in two-player game, there are some undetectable cheating behaviors. However, in multi-player game, the impacts of cheating situation may be

reduced. According to the above analysis, the knowledgeable cheating player will respond with the lower offer by the product of cheating parameter and private information. And then the normal player will estimate the fake private information which is equal to the product of the cheater's cheating parameter and the cheater's private information for normal players. This estimated private information will be always smaller than the real one. So if we consider the potential contribution to include the cheating behavior, we can modify (26) as follows,

$$v_{ij} = \frac{P_{ji} * C_{ik} * r_{ji}}{c_i} + \frac{P_{ij} * C_{jk} * r_{ij}}{c_j} \quad (29-1)$$

$$v_{ij} = \frac{P_{ji} * C_{ik} * r_{ji}}{c_i} * \frac{\frac{P_{ij} * C_{jk} * r_{ij}}{c_j}}{\sum_m \frac{P_{im} * C_{mk} * r_{im}}{c_m}} \quad (29-2)$$

where m means all of player i can negotiate with.

We attempt to use (29) to estimate the potential contribution of player j and according to above mentioned, we know the potential contribution is concerned with the ratio of the reward of a received block and the cost of an upload block, and the opponent's private information. The difference between (26) and (29) is considering the opponent's private information at (29). We think that the estimated private information can be the parameter used the weighted sum because we believe that considering both advantage between players will lead to the better utility. In (29-1), we think the opponent's private information must be considered because the utility of game is also concerned with the opponent's private information. In (29-2), we normalize all of estimated private information and perform the weighted sum with the ratio of the reward of a received block and the cost of an uploaded block. If an opponent performs the cheating behaviors, the estimated private information will be

decreased because the effective cheating behavior is responding by the fake private information which is lower than real one. So the potential contribution of cheating player will be decreased when the cheating player responds with the lower offer by lower private information. The lower potential contribution leads to the lower distribution of bandwidth in proportional distribution strategy.

We can detect the unknowledgeable cheating player by above detection methods and use the (29) to reduce the impacts of cheating behavior. The potential contribution evaluating by (26) does not consider the impacts of cheating behavior. As above analysis, the potential contribution evaluating by (29) can not only reduce the impacts of cheating behaviors but also reduce the impacts of malicious behaviors.

In the following, the two algorithms mentioned above will be compared with each other. In the simulations, there are four players in the game, and we show full search and proportional distribution strategy. We assume all of the players are normal player, so we assume both unpolluted probability and expected rank coefficient are one. The cost coefficient and total upload bandwidth is shown as table 3.1.5-3. In this program, there is one section which is encoded in 40 encoded blocks. The initial number of encoded block which each player has is 15 blocks, the situation A, and 10 blocks, the situation B. In figure 3.1.5-1, we can observe the full search algorithm estimated the highest product of estimated utility and real utility. The proportional distribution strategy has the similar result at this program.

Table 3.1.5-3: The initial coefficient of 4-player game

player i	c_i	B_i
Player 1	0.29	30
Player 2	0.15	35
Player 3	0.3	30
Player 4	0.11	35

Table 3.1.5-4: The result of 4-player game

full_search	j=1	j=2	j=3	j=4	utility	product	rank_income_A	rank_income_B
i=1	0	16	6	8	25.3	442937.9	25	30
i=2	17	0	17	1	25.75		25	30
i=3	3	6	0	21	26		25	30
i=4	14	9	12	0	26.15		25	30
proportional-(29-1)	j=1	j=2	j=3	j=4	utility	product	rank_income_A	rank_income_B
i=1	0	10	7	13	18.3	371365.3	25	27
i=2	10	0	10	15	28.75		25	30
i=3	7	10	0	13	19		25	28
i=4	10	14	11	0	37.15		25	30
proportional-(29-2)	j=1	j=2	j=3	j=4	utility	product	rank_income_A	rank_income_B
i=1	0	11	5	14	14.3	248118.6	23	23
i=2	8	0	7	20	32.75		25	30
i=3	6	10	0	14	12		21	21
i=4	9	17	9	0	44.15		25	30

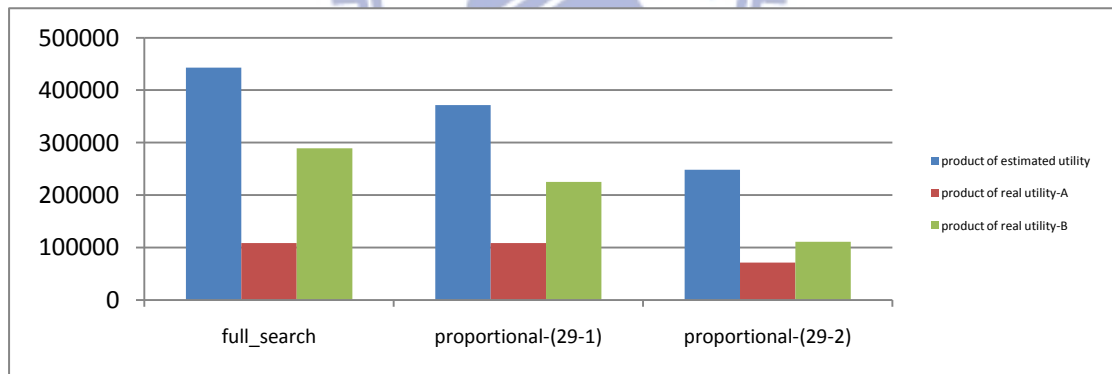


Figure 3.1.5-1: The product of utility with different algorithm

3.2 Proposed System Architecture

In this section, the proposed architecture will be described in detail. The proposed architecture and the flow chart of the peer are shown in figure 3.2-1. There are three stages for each peer in our proposed architecture such as multi-player rank-based

game, exchange stage and update stage. In our proposed architecture, each peer in the peer-to-peer systems is regarded as a player in a game.

First, they perform the multi-player rank-based game. The player will negotiate with other players until all players in a game accept their strategy. When all players accept their strategy, they perform the exchange stage. In exchange stage, each player will exchange their encoded block to others according to their accepted strategy. If they finish the exchange stage, they begin the update stage. In update stage, the player will exchange their reputation score by observing the exchange stage.

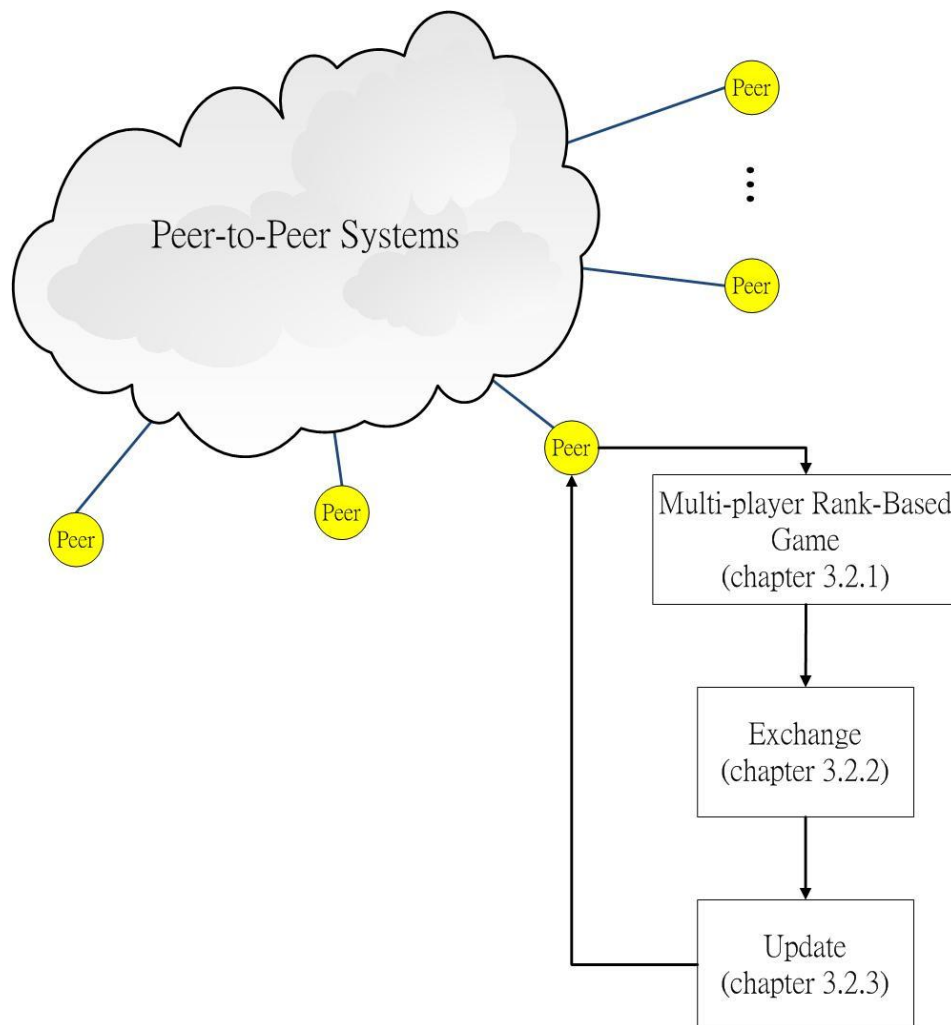


Figure 3.2-1: The proposed architecture

3.2.1 Multi-Player Rank-Based Game

In multi-player rank-based game, the player needs to exchange their offer (we called it *strategy* on the following thesis) to find a set of acceptable strategy for each. The flow chart of multi-player rank-based game is shown in figure 3.2.1-1. In figure 3.2.1-1, it is a flow chart that a play responds a strategy and decides an acceptable strategy of specific player. First, the player decides to accept the opponent's strategy or not. If not, according to the opponent's strategy, the player can estimate the opponent's private information by estimating algorithm described at 3.1.2. And then the player will calculate the best reaction strategy according to the opponent's strategy and estimated private information of opponent, and send to the opponent until both of them find an acceptable strategy. If the player decides to accept, both the player and its opponent find an acceptable strategy. However, the player must find a set of acceptable strategy with a set of other players following by above mentioned.

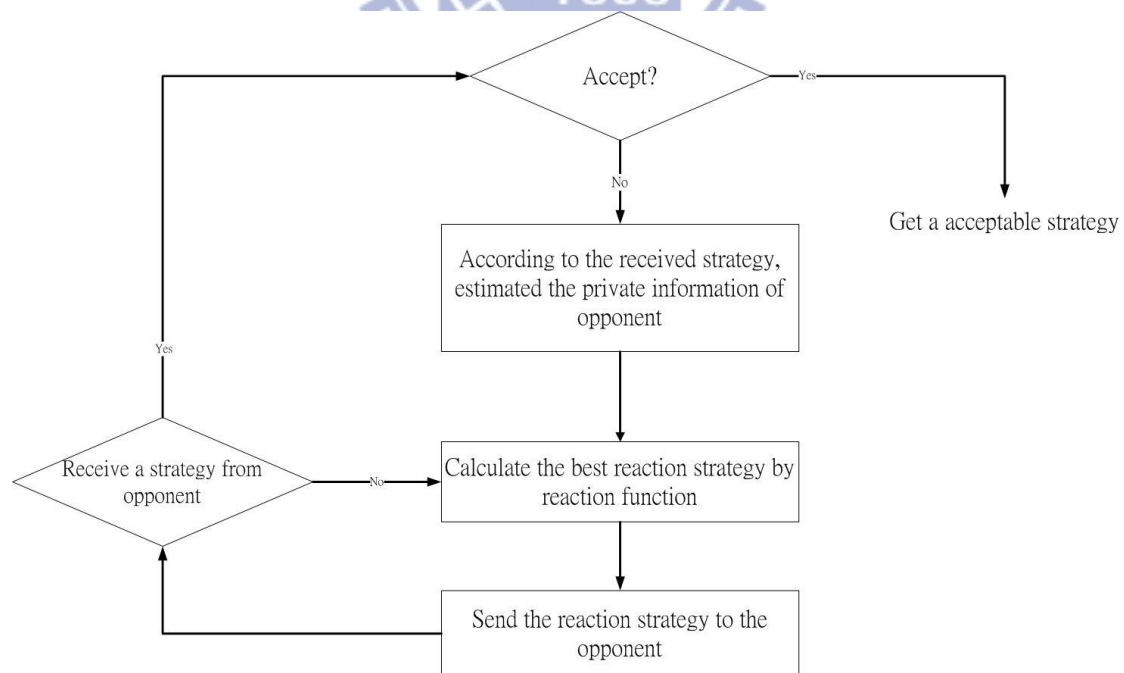


Figure 3.2.1-1: The flow charts of rank-based game

3.2.2 Exchange stage

There are two components in the exchange stage such as upload procedure and download procedure. When both of them are finished, the exchange stage is complete. The encoding and decoding algorithms use randomized linear network coding described in chapter 2. The verification of legal encoded block in the download procedure uses the nullkey algorithm [8].

The flow chart of the upload procedure is shown in figure 3.2.2-1. First, the player checks that the upload offers for each other are non-zero. The upload offers means the set of offer that the player must offer to its opponents decided in the multi-player rank-based game. Secondly, the player selects an opponent randomly and the upload offer for opponent must be larger than zero. Next, the player generates a new encoded block from the set of encoded block received by the player and subtracts one from the upload offer for opponent. Finally, upload a new encoded block to the opponent. Until all of upload offers for each other are zero, the upload procedure is complete.

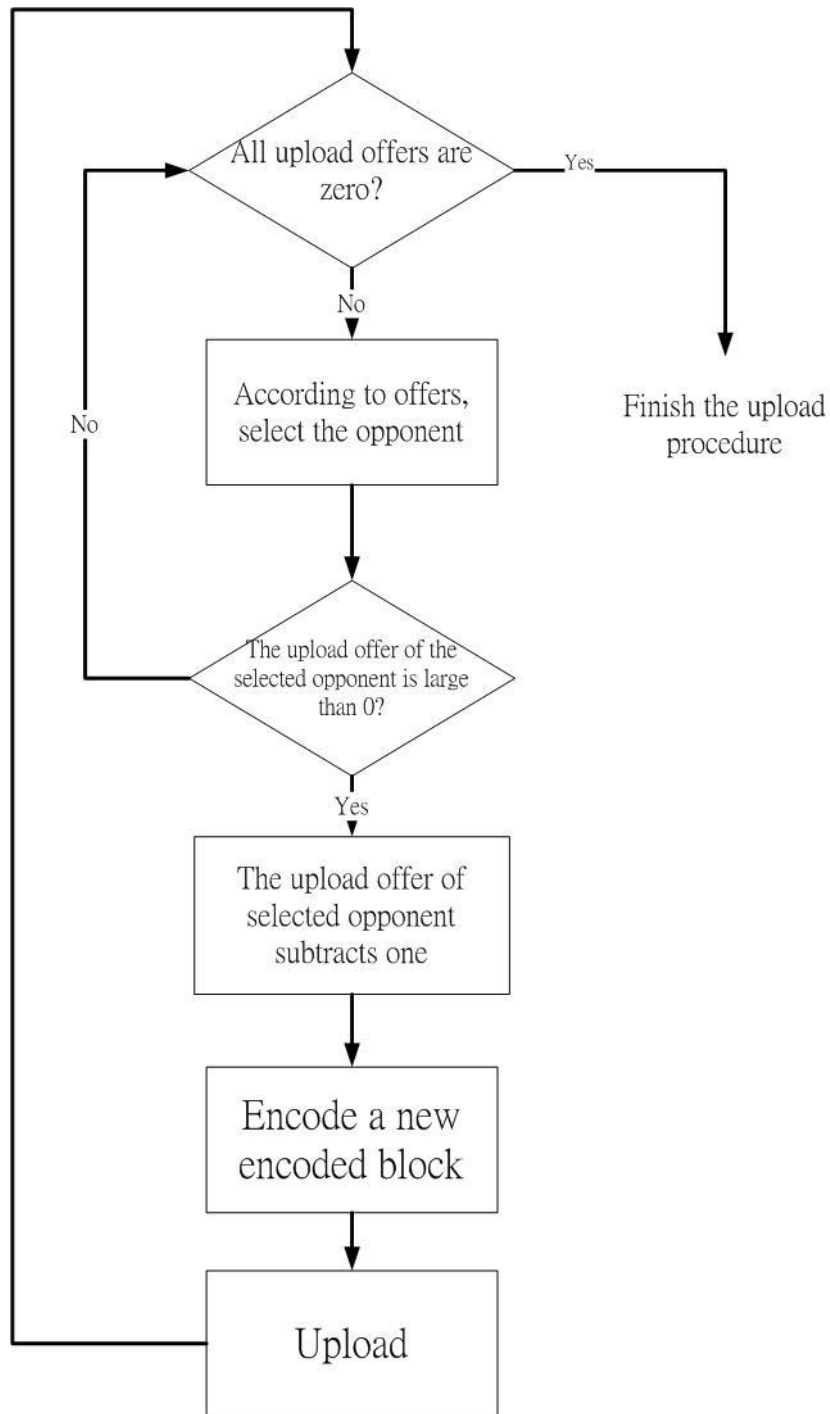


Figure 3.2.2-1: The flow charts of upload procedure

The flow chart of the download procedure is shown in figure 3.2.2-2. First, the player checks that if the download offers for each other are non-zero, and the player's download buffer is empty or not. The download offers means the set of offer that the

player's opponents must offer to the player decided in the multi-player rank-based game. Next, according to the download block from buffer, the player selects the download offer of specific opponent and subtracts one. Third, the player verifies the encoded block which is unpolluted and decodes the legal encoded block. And then record the number of polluted blocks and the usability of encoded block. Until all of download offers for each other are zero, the download procedure is complete.

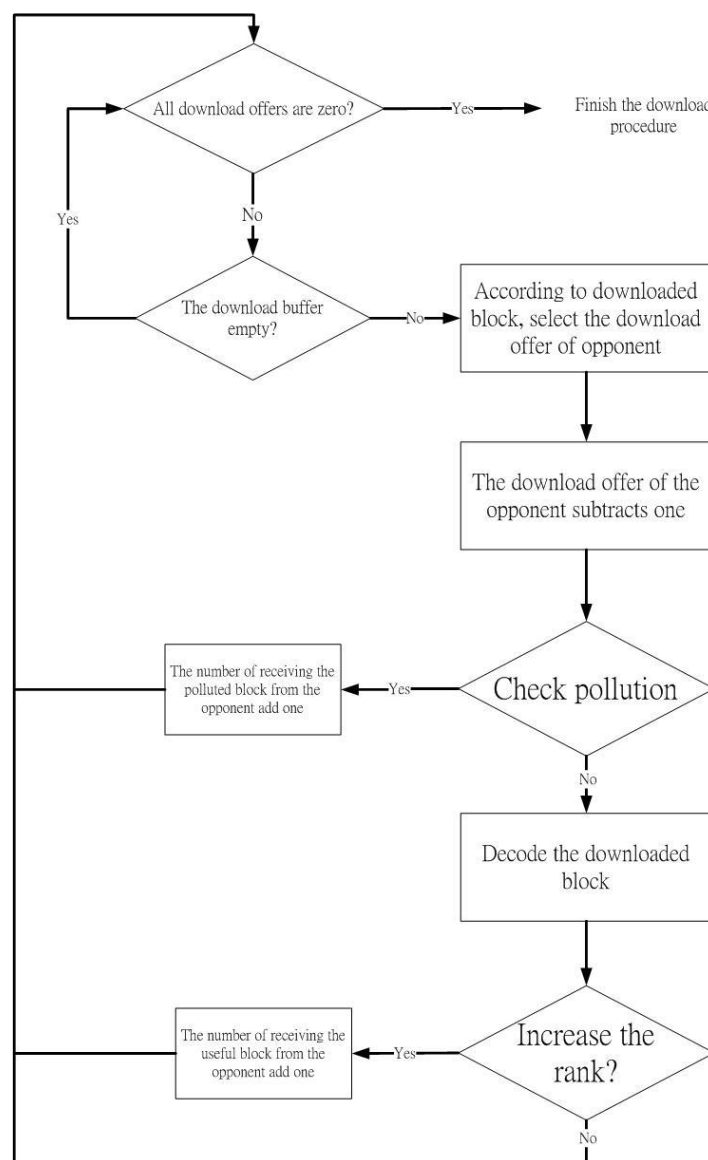


Figure 3.2.2-2: The flow charts of download procedure

3.2.3 Update stage

The flow chart of update stage is shown in figure 3.2.3-1. First, according to the recording coming from the exchange stage, the player can update their expected-rank coefficient and the individual experiment. Next, the players send a query to their neighbors to exchange the individual experiment. Finally, according to exchanged individual experiment, the player can calculate the unpolluted probability of specific player, and the unpolluted probability is regarded as the probability of receiving an unpolluted block from that specific player.

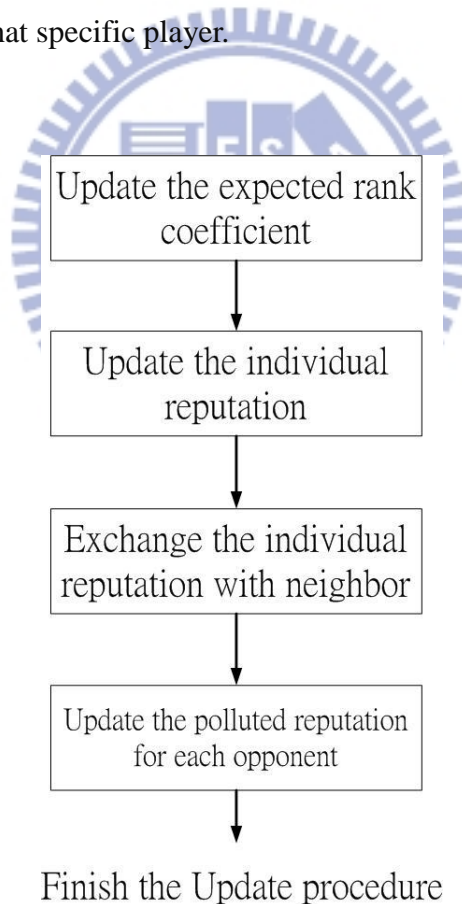


Figure 3.2.3-1: The flow chats of update procedure

The expected-rank coefficient means the expected reward of rank when the player receives a new encoded block. Let us take player i as an example. The formula of updating the expected-rank coefficient is as follows.

$$r_{ji,new} = (1 - \text{weight}_{er}) * r_{ji,old} + \text{weight}_{er} * \frac{N_{rank,j}}{N_{total,j} - N_{polluted,j}} \quad (30)$$

where $r_{ji,new}$, $r_{ji,old}$ is the new expected-rank coefficient and the old one for player j , $N_{total,j}$ is the total number of received blocks from player j , $N_{rank,j}$ is the number of increasing ranks when the player i decodes the encoded block coming from player j , $N_{polluted,j}$ is the number of polluted blocks receiving from player j and weight_{er} is the weighting factor of updating expected-rank coefficient.

In our study, we want the reputation systems to evaluate the characteristic of sending encoded blocks. The reputation evaluation is based on Scrubber. We also take player i as an example.

$$I_{ji,new} = (1 - \text{weight}_{Ir}) * I_{ji,old} + \text{weight}_{Ir} * \frac{N_{total,j} - N_{polluted,j}}{N_{total,j}} \quad (31)$$

where $I_{ji,new}$, $I_{ji,old}$ is the new individual experiment and the old one for player j , $N_{total,j}$ is the total number of receiving the encoded block from player j , $N_{polluted,j}$ is the number of polluted blocks from player j and weight_{Ir} is the weighting factor of updating individual experiment.

In the update stage, the peer testimonial of Scrubber is regarded as the procedure of exchanging individual experiment. Let us take player i as an example again. The formula of peer testimonial is as follows.

$$T_{ji} = \frac{\sum_{k \in N_i} I_{jk} * P_{ki}}{\sum_{k \in N_i} P_{ki}} \quad (32)$$

where N_i is the list of player i 's neighbor that responded to queries from player i with their individual experience on peer j and P_{ji} is the current unpolluted probability of peer j on peer i .

If the player i has updated the new individual experiment and the peer testimonial, the player i can update its unpolluted probability as follows.

$$P_{ji} = \text{weight}_{Pr} * T_{ji} + (1 - \text{weight}_{Pr}) * I_{ji} \quad (33)$$

where P_{ji} is the unpolluted probability for player j , T_{ji} is the peer testimonial for player j , I_{ji} is the individual experiment for player j and weight_{Pr} is the weighting factor of updating unpolluted probability.

This chapter describes the update stage for the expected-rank coefficient and the probability of receiving an unpolluted block from specific player. It is different from the estimation algorithm described at chapter 3.1.2. The estimation algorithm attempts to estimate the specific opponent's private information which is concerned for the specific player ($\frac{P_{ij} * C_{jk} * r_{ij}}{c_j}$ in (29)). And this private information leads to an optimal strategy with incomplete information two-player game. The procedure of exchanging individual experiment attempts to collect the individual experiment without a specific player and then the player can calculate the peer testimonial of specific player which is concerned about the other player without specific player. And then the player can calculate the unpolluted probability of specific player (P_{ji} in (29)).

3.3 Verification of Rank-Based Game

In this chapter, we will describe in detail the verification of Nash equilibrium with two-player game, the impact of the non-used block and the proof of algorithm of estimating private information.

3.3.1 The Verification of Nash Equilibrium with Two-Player Game

In this section, will show the Nash equilibrium with two-player game satisfies the maximum of the product of both utilities. Assume the Nash equilibrium of player i is shown as $a^*_i = (a^*_{i1}, a^*_{i2})$. According to the utility function, we can calculate the utility of each player as follows.

$$a^*_1 = (a^*_{11}, a^*_{12})$$

$$a^*_2 = (a^*_{21}, a^*_{22})$$

$$\begin{aligned} u^*_{12}(a^*_1, a^*_2) &= P_{21} * a^*_{21} * C_{1k} * r_{21} - c_1 * a^*_{12} + \delta_1 * a^*_{11} \\ &\cong P_{21} * a^*_{21} * C_{1k} * r_{21} - c_1 * a^*_{12} \end{aligned}$$

$$\begin{aligned} u^*_{21}(a^*_1, a^*_2) &= P_{12} * a^*_{12} * C_{2k} * r_{12} - c_2 * a^*_{21} + \delta_2 * a^*_{22} \\ &\cong P_{12} * a^*_{12} * C_{2k} * r_{12} - c_2 * a^*_{21} \end{aligned}$$

We assume that there exists another strategy $a'_1 = (a'_{11}, a'_{12}) = (a^*_{11}, a^*_{12} + k)$ for player 1, where $k = [-a^*_{12}, B_1 - a^*_{12}]$ as follows.

$$u'_{12}(a'_1, a_2^*) * u'_{21}(a'_1, a_2^*) > u^*_{12}(a_1^*, a_2^*) * u^*_{21}(a_1^*, a_2^*) \quad (34)$$

Now, we will show the contradiction of this assumption as follows.

$$\begin{aligned}
& u'_{12}(a'_1, a_2^*) * u'_{21}(a'_1, a_2^*) \\
&= (P_{21} * C_{1k} * r_{21} * a_{21}^* - c_1 * (a_{12}^* + k)) \\
&\quad * (P_{12} * C_{2k} * r_{12} * (a_{12}^* + k) - c_2 * a_{21}^*) \\
&= (u^*_{12}(a_1^*, a_2^*) - c_1 * k * a_{12}^*) * (u^*_{21}(a_1^*, a_2^*) + P_{12} * C_{2k} * r_{12} * k) \\
&= u^*_{12}(a_1^*, a_2^*) * u^*_{21}(a_1^*, a_2^*) - c_1 * k * u^*_{21}(a_1^*, a_2^*) + P_{12} * C_{2k} * r_{12} * k \\
&\quad * u^*_{12}(a_1^*, a_2^*) - c_1 * P_{12} * C_{2k} * r_{12} * k^2 \\
&= u^*_{12}(a_1^*, a_2^*) * u^*_{21}(a_1^*, a_2^*) \\
&\quad + k((P_{21} * C_{1k} * r_{21} * P_{12} * C_{2k} * r_{12} + c_1 * c_2) * a_{21}^* - 2 \\
&\quad * c_1 * P_{12} * C_{2k} * r_{12} * a_{12}^*) - c_1 * P_{12} * C_{2k} * r_{12} * k^2
\end{aligned}$$

According to the reaction function of player 1, we know

$$(P_{21} * C_{1k} * r_{21} * P_{12} * C_{2k} * r_{12} + c_1 * c_2) * a_{21}^* = 2 * c_1 * P_{12} * C_{2k} * r_{12} * a_{12}^* \quad (35)$$

So according to (35),

$$\begin{aligned}
& u^*_{12}(a_1^*, a_2^*) * u^*_{21}(a_1^*, a_2^*) \\
&\quad + k((P_{21} * C_{1k} * r_{21} * P_{12} * C_{2k} * r_{12} + c_1 * c_2) * a_{21}^* - 2 \\
&\quad * c_1 * P_{12} * C_{2k} * r_{12} * a_{12}^*) - c_1 * P_{12} * C_{2k} * r_{12} * k^2 \\
&= u^*_{12}(a_1^*, a_2^*) * u^*_{21}(a_1^*, a_2^*) \\
&\quad + k(2 * c_1 * P_{21} * C_{2k} * r_{21} * a_{12}^* - 2 * c_1 * P_{21} * C_{2k} * r_{21} \\
&\quad * a_{12}^*) - c_1 * P_{21} * C_{2k} * r_{21} * k^2
\end{aligned}$$

$$\begin{aligned}
&= u_{12}^*(a_1^*, a_2^*) * u_{21}^*(a_1^*, a_2^*) - c_1 * P_{21} * C_{2k} * r_{21} * k^2 \\
&\leq u_{12}^*(a_1^*, a_2^*) * u_{21}^*(a_1^*, a_2^*)
\end{aligned}$$

As above analysis, we can know that there is no other strategy can change the decision when player 1 selects the Nash equilibrium and the Nash equilibrium satisfies the optimality criteria of proportional fairness.

3.3.2 The Impacts of The Non-used Blocks

Let us take player 1 as an example. Because we consider the impacts of the non-used blocks, we can rewrite the reaction function of player 1 as follows.

$$\begin{aligned}
a_{1,t} &= (a_{11,t}, a_{12,t}) \\
a_{11,t} &= B_1 - a_{12,t} \\
a_{12,t} &= \min \left\{ B_1, \frac{1}{2} * \left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} \right] * a_{21,t-1} + \frac{1}{2} \right. \\
&\quad \left. * \left[\frac{\delta_1}{c_1} * a_{11,t-1} - \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * a_{22,t-1} \right] \right\}
\end{aligned} \tag{36}$$

According to the definition of δ_i in (11), we know

$$0 < \delta_1 * B_1 \ll P_{21} * C_{1k} * r_{21} * a_{21,t-1} - c_1 * a_{12,t-1} \quad \forall t - 1 > 0 \tag{37-1}$$

$$0 < \delta_2 * B_2 \ll P_{12} * C_{2k} * r_{12} * a_{12,t-1} - c_2 * a_{21,t-1} \quad \forall t - 1 > 0 \tag{37-2}$$

And then

$$0 < \frac{\delta_1}{c_1} * B_1 \ll \frac{P_{21} * C_{1k} * r_{21}}{c_1} * a_{21,t-1} - a_{12,t-1} \tag{38-1}$$

$$0 < \frac{\delta_2}{c_2} * B_2 \ll \frac{P_{12} * C_{2k} * r_{12}}{c_2} * a_{12,t-1} - a_{21,t-1} \tag{38-2}$$

$$0 < \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * B_2 \ll a_{12,t-1} - \frac{c_2}{P_{12} * C_{2k} * r_{12}} * a_{21,t-1}$$

Add (38-1) to (38-2), and we get

$$\begin{aligned} 0 < \frac{\delta_1}{c_1} * B_1 + \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * B_2 \\ \ll \frac{P_{21} * C_{1k} * r_{21}}{c_1} * a_{21,t-1} - \frac{c_2}{P_{12} * C_{2k} * r_{12}} * a_{21,t-1} \end{aligned} \quad (39)$$

Because the value of P_{ji} , r_{ji} , $a_{ij,t-l}$, and c_i are both positive number, we know

$$\begin{aligned} \left| \frac{P_{21} * C_{1k} * r_{21}}{c_1} * a_{21,t-1} - \frac{c_2}{P_{12} * C_{2k} * r_{12}} * a_{21,t-1} \right| \\ < \left| \frac{P_{21} * C_{1k} * r_{21}}{c_1} * a_{21,t-1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} * a_{21,t-1} \right| \end{aligned} \quad (40)$$

Because $a_{ij,t-l} \leq B_i$ for all $t-l$, we know

$$\left| \frac{\delta_1}{c_1} * a_{11,t-1} + \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * a_{22,t-1} \right| \leq \left| \frac{\delta_1}{c_1} * B_1 + \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * B_2 \right| \quad (41)$$

$$\text{And } \left| \frac{\delta_1}{c_1} * a_{11,t-1} - \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * a_{22,t-1} \right| < \left| \frac{\delta_1}{c_1} * a_{11,t-1} + \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * a_{22,t-1} \right|$$

$$\therefore \left| \frac{\delta_1}{c_1} * a_{11,t-1} - \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * a_{22,t-1} \right| < \left| \frac{\delta_1}{c_1} * B_1 + \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * B_2 \right| \quad (42)$$

According to (39) and (42), we know

$$\begin{aligned} 0 < \left| \frac{\delta_1}{c_1} * a_{11,t-1} - \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * a_{22,t-1} \right| \\ \ll \left| \frac{P_{21} * C_{1k} * r_{21}}{c_1} * a_{21,t-1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} * a_{21,t-1} \right| \end{aligned} \quad (43)$$

And then

$$\begin{aligned}
a_{12,t} &= \min \left\{ B_1, \frac{1}{2} * \left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} \right] * a_{21,t-1} + \frac{1}{2} \right. \\
&\quad \left. * \left[\frac{\delta_1}{c_1} * a_{11,t-1} - \frac{\delta_2}{P_{12} * C_{2k} * r_{12}} * a_{22,t-1} \right] \right\} \quad (44) \\
&\cong \min \left\{ B_1, \frac{1}{2} * \left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} \right] * a_{21,t-1} \right\}
\end{aligned}$$

According to above mentioned, we can ignore the impact of the non-used block.

3.3.3 The Proof of Algorithm of Estimating Private Information

In this section, we will proof the algorithm of estimating private information can estimate accurately and rapidly. We consider the situation as figure 3.3.2-1. The player 1 sends the set of strategy $a_{1,t-1}=(0,a_{12,t-1})$ to player 2 and then the player 2 respond with the set of strategy $a_{2,t-1}=(a_{21,t-1},0)$ to player 1. The player 1 can calculate $estimation_{1,t-1}$. According to $estimation_{1,t-1}$, the player 1 sends the set of strategy $a_{1,t}=(0,a_{12,t})$ to player 2 and then the player 2 can calculate $estimation_{2,t}$ and respond with the set of strategy $a_{2,t}=(a_{21,t},0)$ to player 1. Finally, the player 1 can calculate $estimation_{1,t}$.

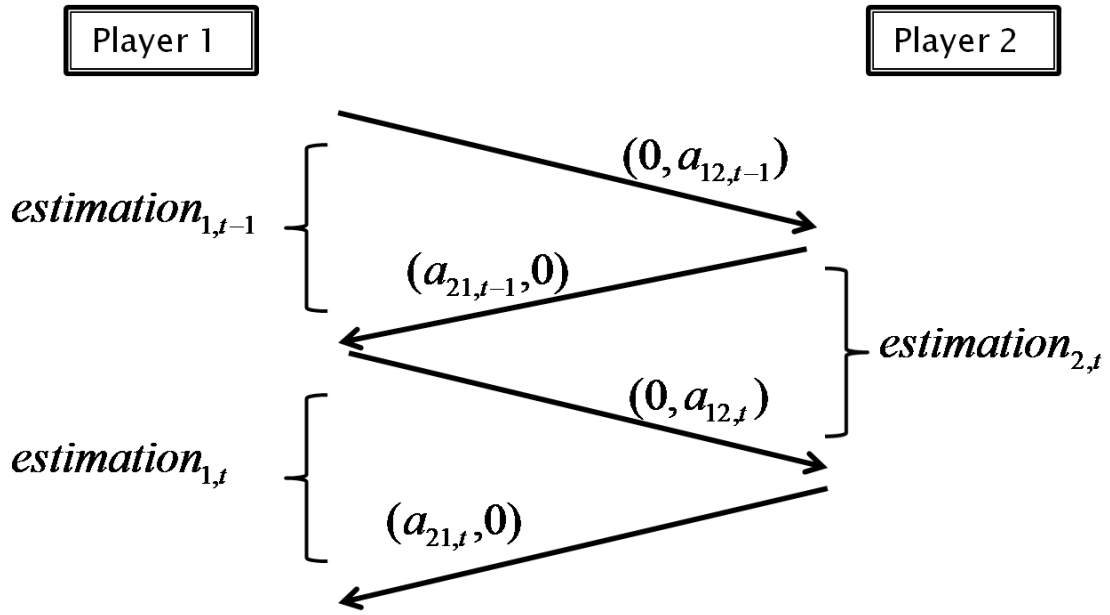


Figure 3.3.2-1: The situation of estimating private information

According to (23), we know

$$estimation_{1,t-1} = \left[2 * \frac{a_{21,t-1}}{a_{12,t-1}} - \frac{c_1}{P_{21} * C_{1k} * r_{21}} \right]^{-1} \quad (45)$$

$$estimation_{2,t} = \left[2 * \frac{a_{12,t}}{a_{21,t-1}} - \frac{c_2}{P_{12} * C_{2k} * r_{12}} \right]^{-1} \quad (46)$$

$$estimation_{1,t} = \left[2 * \frac{a_{21,t}}{a_{12,t}} - \frac{c_1}{P_{21} * C_{1k} * r_{21}} \right]^{-1} \quad (47)$$

According to reaction function, we know

$$a_{12,t} = \frac{1}{2} * \left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + estimation_{1,t-1} \right] * a_{21,t-1} \quad (48)$$

$$a_{21,t} = \frac{1}{2} * \left[estimation_{2,t} + \frac{P_{12} * C_{2k} * r_{12}}{c_2} \right] * a_{12,t} \quad (49)$$

According to (47) and (49), we can get

$$2 * \frac{a_{21,t}}{a_{12,t}} = estimation_{2,t} + \frac{P_{12} * C_{2k} * r_{12}}{c_2} = \frac{1}{estimation_{1,t}} + \frac{c_1}{P_{21} * C_{1k} * r_{21}} \quad (50)$$

According to (46) and (48), we can get

$$2 * \frac{a_{12,t}}{a_{21,t-1}} = \frac{P_{21} * C_{1k} * r_{21}}{c_1} + estimation_{1,t-1} = \frac{1}{estimation_{2,t}} + \frac{c_2}{P_{12} * C_{2k} * r_{12}} \quad (51)$$

According to (50) and (51), we can get

$$\left[\frac{P_{21} * C_{1k} * r_{21}}{c_1} + estimation_{1,t-1} - \frac{c_2}{P_{12} * C_{2k} * r_{12}} \right]^{-1} + \frac{P_{12} * C_{2k} * r_{12}}{c_2} \quad (52)$$

$$= \frac{1}{estimation_{1,t}} + \frac{c_1}{P_{21} * C_{1k} * r_{21}}$$

Let $b_1 = \frac{P_{21} * C_{1k} * r_{21}}{c_1}$, $b_2 = \frac{P_{12} * C_{2k} * r_{12}}{c_2}$

$$estimation_{1,t} = \frac{b_1 * [b_2 * estimation_{1,t-1} + b_1 * b_2 - 1]}{b_1 * b_2 + (b_1 * b_2 - 1) * [b_2 * estimation_{1,t-1} + b_1 * b_2 - 1]} \quad (53)$$

The difference between $estimation_{1,t}$ and the real value $\frac{c_2}{P_{12} * C_{2k} * r_{12}}$ is shown in (54).

$$estimation_{1,t} - \frac{1}{b_2}$$

$$= \frac{estimation_{1,t-1} - \frac{1}{b_2}}{b_1 * b_2 + (b_1 * b_2 - 1) * [b_2 * estimation_{1,t-1} + b_1 * b_2 - 1]} \quad (54)$$

Let us consider the denominator in (54).

$$\therefore P_{21} * C_{1k} * r_{21} * a_{21,t} - c_1 * a_{12,t} > 0, \forall t > 0$$

$$\therefore b_1 = \frac{P_{21} * C_{1k} * r_{21}}{c_1} > \frac{a_{12,t}}{a_{21,t}}$$

And

$$\therefore P_{12} * C_{2k} * r_{12} * a_{12,t} - c_2 * a_{21,t} > 0, \forall t > 0$$

$$\therefore b_2 = \frac{P_{12} * C_{2k} * r_{12}}{c_2} > \frac{a_{21,t}}{a_{12,t}}$$

$$\therefore b_1 * b_2 = \frac{P_{21} * C_{1k} * r_{21}}{c_1} * \frac{P_{12} * C_{2k} * r_{12}}{c_2} > 1$$

So

$$b_1 * b_2 + (b_1 * b_2 - 1) * [b_2 * estimation_{1,t-1} + b_1 * b_2 - 1] > b_1 * b_2 > 1$$

Then

$$\frac{1}{b_1 * b_2 + (b_1 * b_2 - 1) * [b_2 * estimation_{1,t-1} + b_1 * b_2 - 1]} < \frac{1}{b_1 * b_2} < 1$$

According to above mentioned, (54) can be shown as geometric progression with common ratio $\frac{1}{b_1 * b_2}$ as follows.

$$\text{If } estimation_{1,t-1} - \frac{1}{b_2} > 0$$

$$estimation_{1,t} - \frac{1}{b_2}$$

$$\begin{aligned} &= \frac{estimation_{1,t-1} - \frac{1}{b_2}}{b_1 * b_2 + (b_1 * b_2 - 1) * [b_2 * estimation_{1,t-1} + b_1 * b_2 - 1]} \\ &< \frac{1}{b_1 * b_2} \left[estimation_{1,t-1} - \frac{1}{b_2} \right] \\ &< \left[\frac{1}{b_1 * b_2} \right]^{t-1} \left[estimation_{1,0} - \frac{1}{b_2} \right] \end{aligned}$$

If $estimation_{1,t-1} - \frac{1}{b_2} < 0$

$$\begin{aligned}
estimation_{1,t} - \frac{1}{b_2} &= \frac{estimation_{1,t-1} - \frac{1}{b_2}}{b_1 * b_2 + (b_1 * b_2 - 1) * [b_2 * estimation_{1,t-1} + b_1 * b_2 - 1]} \\
&> \frac{1}{b_1 * b_2} \left[estimation_{1,t-1} - \frac{1}{b_2} \right] \\
&> \left[\frac{1}{b_1 * b_2} \right]^{t-1} \left[estimation_{1,0} - \frac{1}{b_2} \right]
\end{aligned}$$

So

$$\begin{aligned}
\left| estimation_{1,t} - \frac{1}{b_2} \right| &= \frac{\left| estimation_{1,t-1} - \frac{1}{b_2} \right|}{b_1 * b_2 + (b_1 * b_2 - 1) * [b_2 * estimation_{1,t-1} + b_1 * b_2 - 1]} \\
&< \frac{1}{b_1 * b_2} \left| estimation_{1,t-1} - \frac{1}{b_2} \right| \\
&< \left[\frac{1}{b_1 * b_2} \right]^{t-1} \left| estimation_{1,0} - \frac{1}{b_2} \right|
\end{aligned}$$

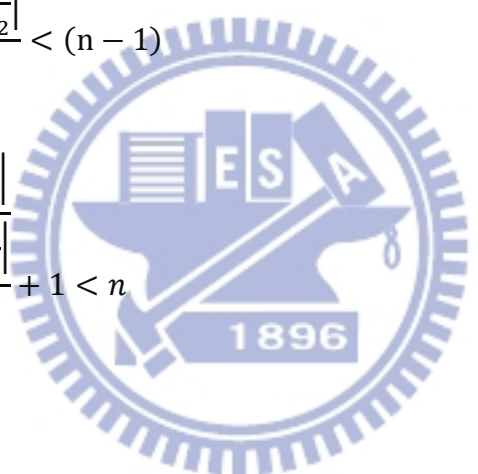
$$\therefore 0 < \frac{1}{b_1 * b_2} < 1$$

$$\therefore \left[\frac{1}{b_1 * b_2} \right]^t \rightarrow 0 \text{ as } t \rightarrow \infty$$

\therefore the difference between $estimation_{1,t}$ and $\frac{c_2}{P_{12} * C_{2k} * r_{12}}$ will approach zero

As above analysis, we proof the algorithm of estimating private information can be estimated as closer as possible and the approaching speed depends on the common ratio $\frac{1}{b_1 * b_2}$.

According to above mentioned, we can calculate the approaching speed as follows when we use the common ratio, $\frac{1}{b_1 * b_2}$.

$$\begin{aligned}
 \left| estimation_{1,t} - \frac{1}{b_2} \right| &< \left[\frac{1}{b_1 * b_2} \right]^{n-1} \left| estimation_{1,0} - \frac{1}{b_2} \right| \\
 \frac{\left| estimation_{1,t} - \frac{1}{b_2} \right|}{\left| estimation_{1,0} - \frac{1}{b_2} \right|} &< \left[\frac{1}{b_1 * b_2} \right]^{n-1} \\
 \log \frac{\left| estimation_{1,t} - \frac{1}{b_2} \right|}{\left| estimation_{1,0} - \frac{1}{b_2} \right|} &< (n - 1) * \log \left[\frac{1}{b_1 * b_2} \right] \\
 \frac{\log \frac{\left| estimation_{1,t} - \frac{1}{b_2} \right|}{\left| estimation_{1,0} - \frac{1}{b_2} \right|}}{\log \left[\frac{1}{b_1 * b_2} \right]} &< (n - 1) \\
 \frac{\log \frac{\left| estimation_{1,t} - \frac{1}{b_2} \right|}{\left| estimation_{1,0} - \frac{1}{b_2} \right|}}{\log \left[\frac{1}{b_1 * b_2} \right]} + 1 &< n
 \end{aligned}
 \tag{55}$$


Finally, there are two examples to verify the above mentioned. The coefficient of table 3.3.3-1 and table 3.3.3-4 is the same as table 3.2.2-1 and table 3.2.2-3.

Table 3.3.3-1: The process of estimation private information: example 1

estimation _{i,t}	t=1	t=2	t=3	t=4	t=5
player 1	0.512611	0.555417	0.557579	0.557687	0.557692
player 2	0.407345	0.400364	0.400018	0.400001	0.4

Table 3.3.3-2: The difference between estimation_{i,t} and real value: example 1

estimation _{i,t} - real value	t=1	t=2	t=3	t=4	t=5	real value
player 1	-0.04508	-0.00228	-0.00011	-5.8E-06	-1.7E-07	0.4
player 2	0.007345	0.000364	1.81E-05	9.6E-07	0	0.557692

Table 3.3.3-3: The common ratio between the differences between estimation_{i,t} and real value: example 1

$\frac{\text{estimation}_{i,t} - \text{real value}}{\text{estimation}_{i,t-1} - \text{real value}}$	t=2	t=3	t=4	t=5
player 1	0.050471	0.049822	0.050899	0.02974
player 2	0.0496	0.049627	0.053095	0

And $\frac{1}{b_1 * b_2} = 0.2230769$. In table 3.3.3-3, the common ratio between the differences between estimation_{i,t} and real value are smaller than $\frac{1}{b_1 * b_2}$. And according to (55), we know

$$\frac{\log \frac{|-1.7E-07|}{|-0.04508|}}{\log[0.2230769]} + 1 = 9.324107 < n$$

In our proposed algorithm of estimation, it needs to estimate 5 times. It needs to estimate at least 9 times when we use the common ratio, $\frac{1}{b_1 * b_2}$.

Table 3.3.3-4: The process of estimation private information: example 2

estimation _{i,t}	t=1	t=2	t=3	t=4
player 1	0.173093	0.168688	0.168674768	0.168675
player 2	0.319548	0.319999	0.32	0.32

Table: 3.3.3-5: The difference between estimation_{i,t} and real value: example 2

estimation _{i,t} - real value	t=1	t=2	t=3	t=4	real value
player 1	0.004418	1.29E-05	6.91E-08	1.22E-08	0.32
player 2	-0.00045	-1.3E-06	0	0	0.168675

Table 3.3.3-6: The common ratio between the differences between estimation_{i,t} and real value: example 2

$\frac{\text{estimation}_{i,t} - \text{real value}}{\text{estimation}_{i,t-1} - \text{real value}}$	t=2	t=3	t=4
player 1	0.002914	0.005367	0.176471
player 2	0.002947	0	

And $\frac{1}{b_1 * b_2} = 0.053976$. In table 3.3.3-6, the common ratio between the differences between estimation_{i,t} and real value are smaller than $\frac{1}{b_1 * b_2}$. And according to (55), we know

$$\frac{\log \frac{|1.22E - 08|}{|0.004418|}}{\log[0.053976]} + 1 = 5.384656 < n$$

In our proposed algorithm of estimation, it needs to estimate 4 times. It needs to estimate at least 5 times when we use the common ratio, $\frac{1}{b_1 * b_2}$.

4. Simulation and Discussion

In this chapter, we will show the result of C_{ik} and the impacts of the malicious behaviors and the cheating behaviors. The simulation environment is ns2 and the version of ns2 is 2.34.

4.1 The Coefficient of Expected Rank at Specific Rank k , C_{ik}

In this section, we want to obtain the expected rank income per received block at specific rank under the random distribution of resource environment. The simulation environment is shown as table 4.1-1.

Table 4.1-1: The simulation environment

Node number	100, 200,300
The probability of connecting between two nodes	P
Total number of original encoded blocks in the system	200 blocks
Size of each block	1000 Bytes
Upload bandwidth of each node	10 blocks per second

The original encoded blocks are distributed randomly to the node. Total number of independent encoded block is 200. Figure 4.1-1, 4.1-2 and 4.1-3 are 100, 200 and

300 nodes, with different connective probability respectively. It shows that the expected rank incomes are almost higher than 0.95. It can be regarded as 1.

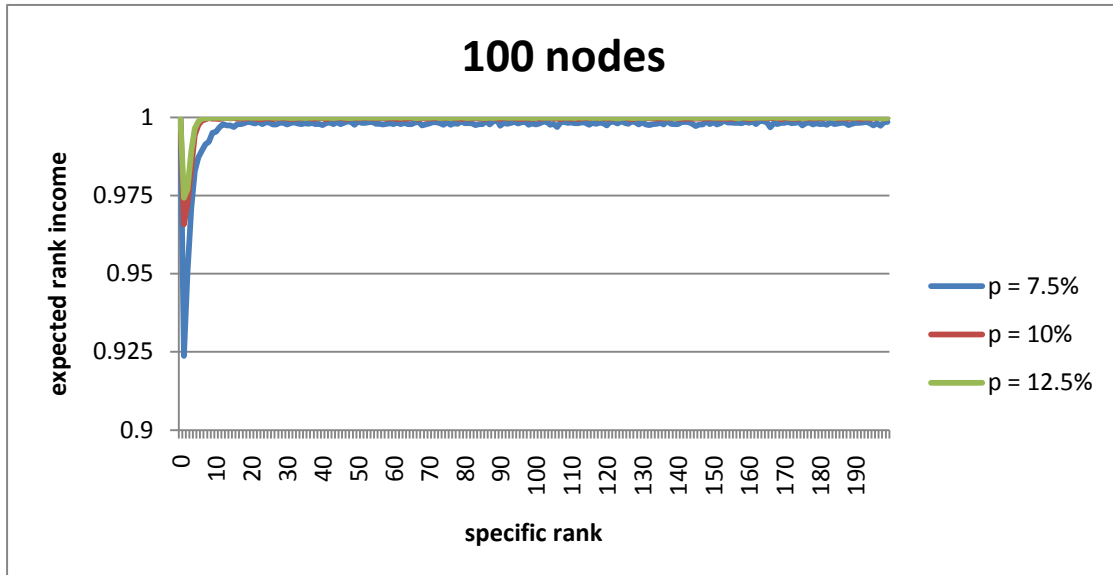


Figure 4.1-1: 100 nodes with different connective probability $p=7.5\%$, 10% , and 12.5%

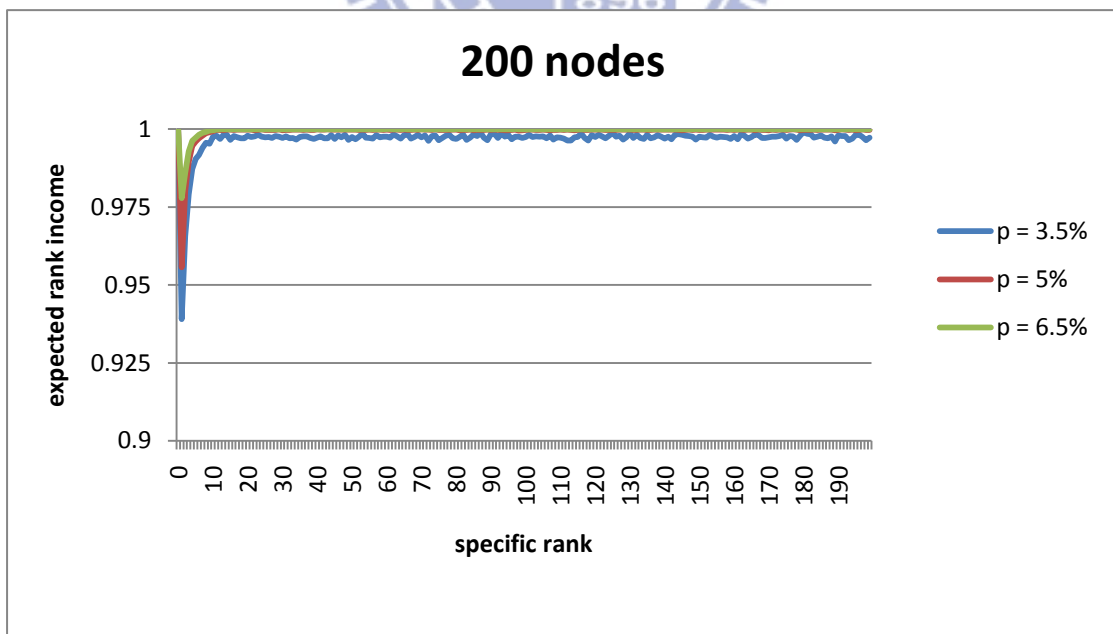


Figure 4.1-2: 200 nodes with different connective probability $p=3.5\%$, 5% , and 6.5%

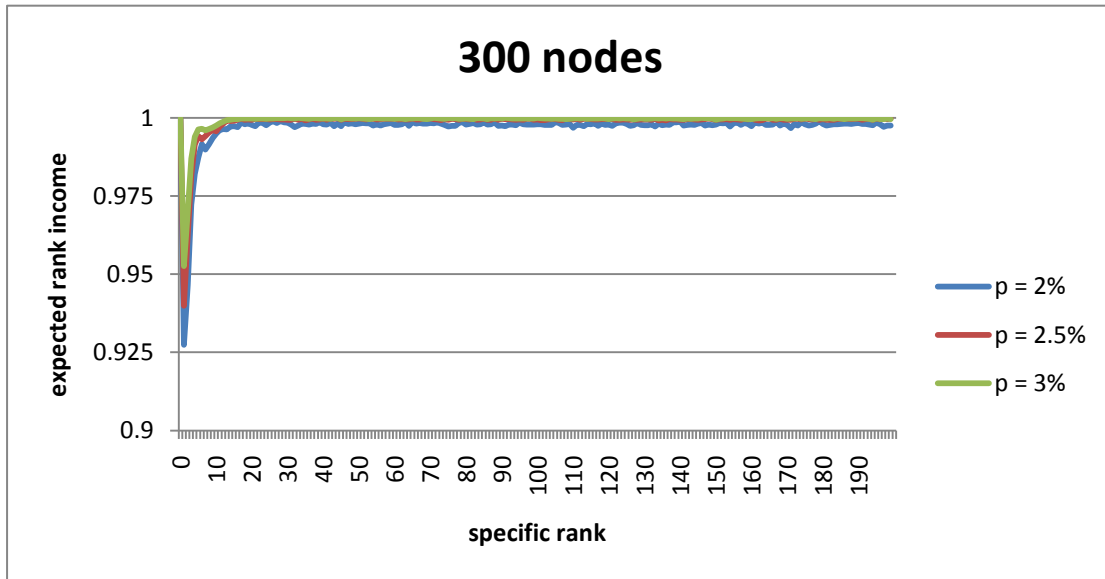


Figure 4.1-3: 300 nodes with different connective probability $p=2\%$, 2.5% , and 3%

4.2 The Impacts of Malicious Players and Cheating Players

In this section, we will discuss the impacts of malicious player and cheating player. The behavior of malicious player is the behavior of content pollution. The malicious player will randomly change the content of encoded block. The behavior of cheating player is the knowledgeable cheating behavior described in section 3.1.5. The algorithm of multi-player game is proportional distribution strategy. The network coding operations is performed in Galois Field, $GF(2^8)$. In $GF(2^8)$, the range of element is between 0 and 255, so each element in $GF(2^8)$ can be stored in one byte. The reducing polynomial for multiplication is $q(x) = x^8 + x^4 + x^3 + x^2 + 1$.

The “estimated utility” means the utility of player is evaluated by the (24). The “utility” means the utility of normal player is evaluated by the number of increased

ranks subtract the cost of upload encoded blocks.

The “proportional with (26)” means a player perform the proportional distribution strategy according to (26). The “proportional with (29-1)” means a player perform the proportional distribution strategy according to (29-1). The “proportional with (29-2)” means a player perform the proportional distribution strategy according to (29-2).

4.2.1 The Impact of Malicious Player

The simulation environment is shown as table 4.2.1-1. The duration of each section is 10 seconds. There are 20% players whose upload bandwidth is 640Kbps and 80% players whose upload bandwidth is 384Kbps. This bandwidth setting refers to the range of ADSL of CHT. The distributed section size is 360KB at each round. The number of block of each section is 300 blocks. The size of each original block is 1200Bytes, and the size of each original encoded block is 1500Bytes. The 300Bytes overhead is due to the coefficients of each original block. Each original block needs at least one coefficient to be encoded in encoded process, and one coefficient in $GF(2^8)$ is one byte. The 300 original encoded blocks are distributed randomly to the nodes. The system will randomly distribute the encoded blocks which are encoded by the original block of specific section to the players in one section. The attack rate means the probability that the malicious player performs the malicious behavior. The malicious behavior means a player randomly changes the content of encoded block.

In figure 4.2.1-1 and 4.2.1-2, the normal players’ average utility and the logarithm of the product of utility is better than the malicious player. Of course, the normal players’ average rank-utility and the average logarithm of the product of rank

utility is also better than the malicious players. The lower utility means the player must use more resources to exchange the fewer encoded blocks. The proportional distribution strategy is better on the restriction of the impact of the malicious behaviors.

Table 4.2.1-1: The simulation environment

The number of player	100
The size of section which is distributed at each round	360KB
The number of block of each section	300 blocks
Size of each block	1200Bytes
Upload bandwidth of each node per round	640, 384Kbps
Initial unpolluted probability, P_{ji}	1
Initial coefficient of expected rank, r_{ji}	1
Initial cost coefficient, c_i	0.1~0.4
Number of section	8
The weighting coefficient at update stage: $weight_{er}$, $weight_{lr}$, $weight_{pr}$	0.5, 0.5, 0.5

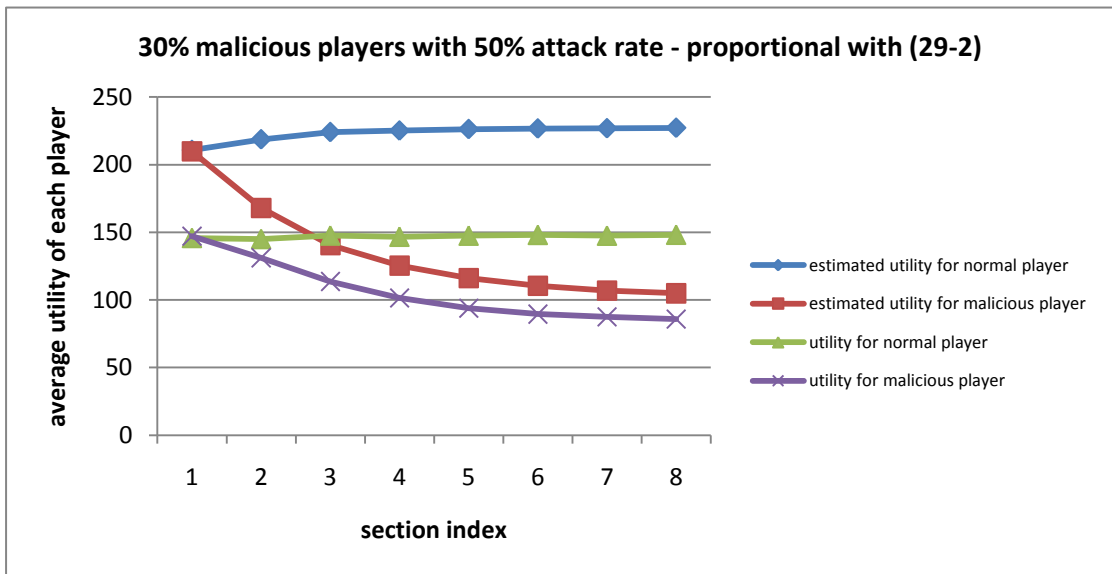
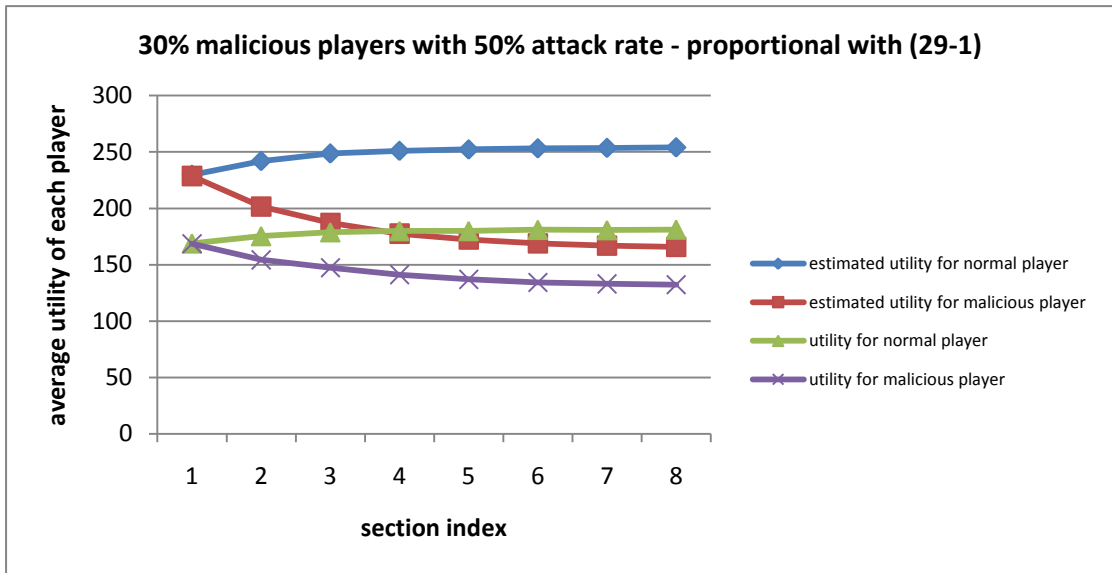
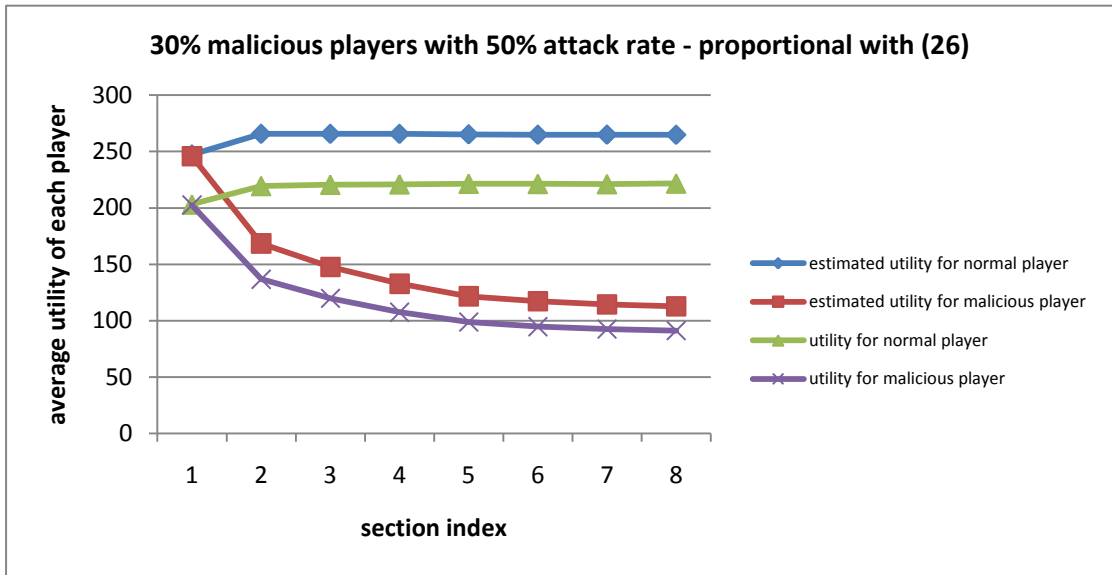
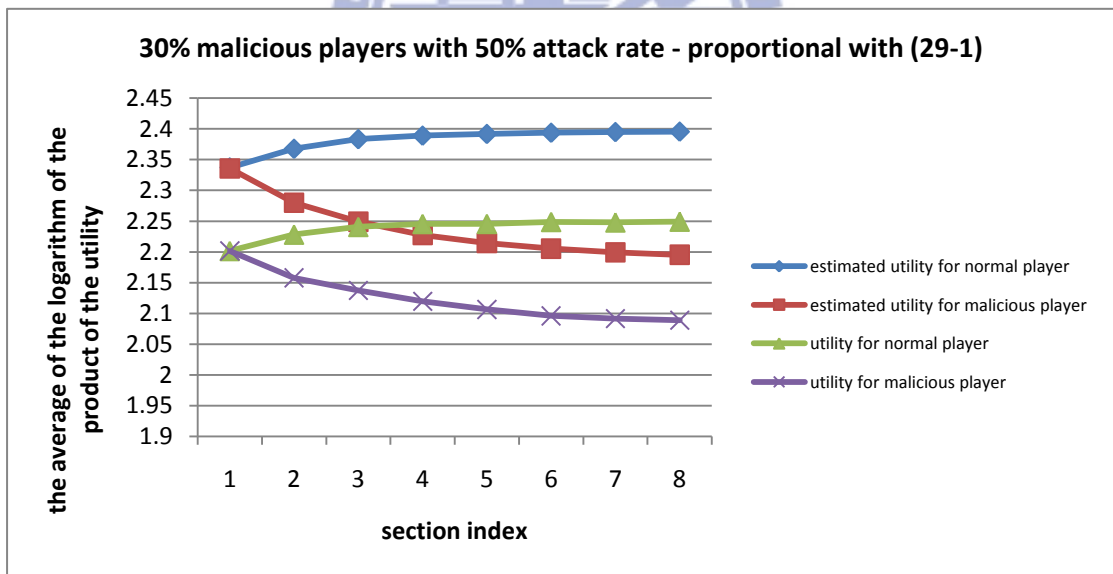
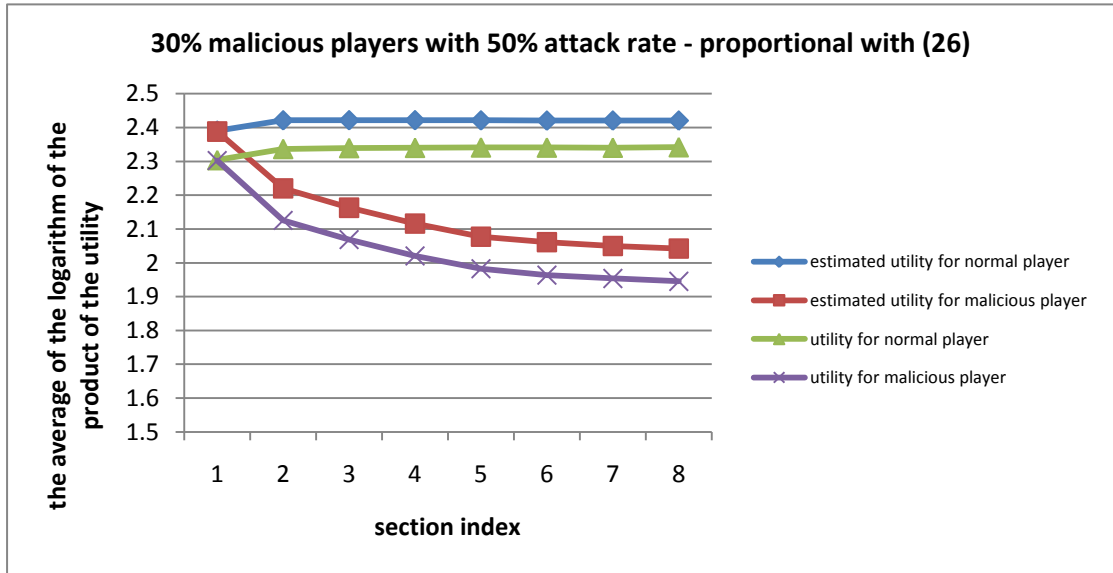


Figure 4.2.1-1: The average utility of each section with 30% malicious players and

attack rate 50%



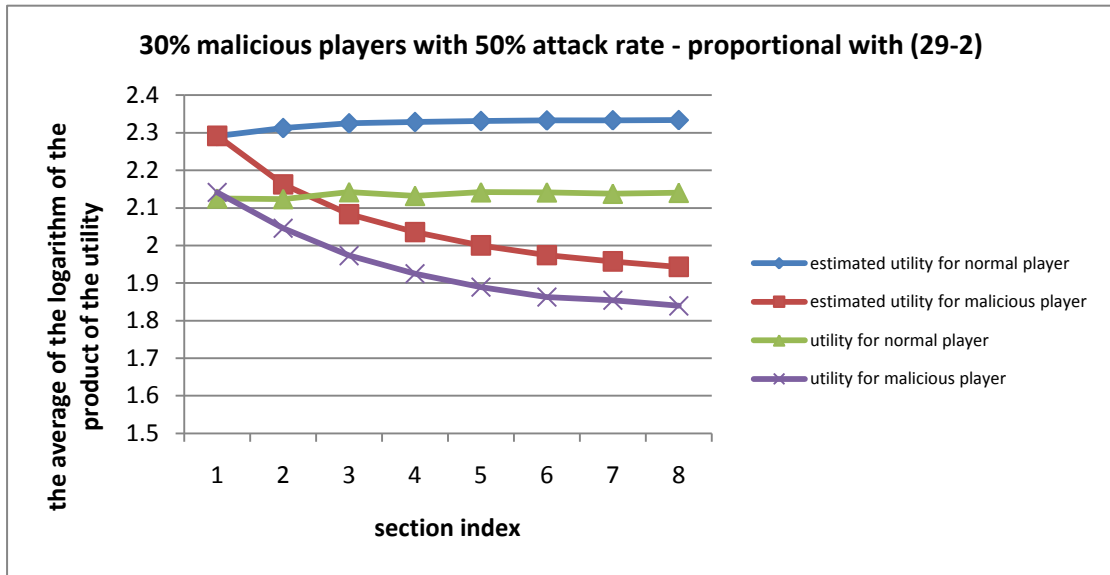


Figure 4.2.1-2: The average of the logarithm of product of utility of each section with 30% malicious players and different attack rate 50%

4.2.2 The Impact of Cheating Behavior

The simulation environment is shown as table 4.2.2-1. The duration of each section is 10 seconds. There are 20% players whose upload bandwidth is 640Kbps and 80% players whose upload bandwidth is 384Kbps. This bandwidth setting refers to the range of ADSL of CHT. The distributed section size is 360KB at each round. The number of block of each section is 300 blocks. The size of each original block is 1200Bytes, and the size of each original encoded block is 1500Bytes. The 300Bytes overhead is due to the coefficients of each original block. Each original block needs at least one coefficient to be encoded in encoded process, and one coefficient in $GF(2^8)$ is one byte. The 300 original encoded blocks are distributed randomly to the node. The system will randomly distribute the encoded blocks which are encoded by the original block of specific section to the players in one section. The cheating player

will start the cheating behavior at section 1.

In figure 4.2.2-1 and figure 4.2.2-2, show 30% cheating player with cheating parameters 0.3. The cheating parameter means the knowledgeable cheating behavior responds with the lower private information equaled to the product of its private information and the cheating parameter. It shows that the cheating players almost have the lower average utility at proportional distribution strategy with (29-1) and (29-2). The lower average utility means that the cheating players exchange the lower resources from the other. In our proposed method, the cheating behavior is unsuitable in our proposed method.

Table 4.2.2-1: The simulation environment

The number of player	100
The size of section which is distributed at each round	360 KB
The number of block of each section	300 blocks
Size of each block	1200 Bytes
Upload bandwidth of each node per round	640, 384Kbps
Initial unpolluted probability, P_{ji}	1
Initial coefficient of expected rank, r_{ji}	1
Initial cost coefficient, c_i	0.1~0.4
Number of section	8
Which section the cheating player start the cheating behavior	0
The weighting coefficient at update stage: $weight_{er}$, $weight_{lr}$, $weight_{pr}$	0.5, 0.5, 0.5

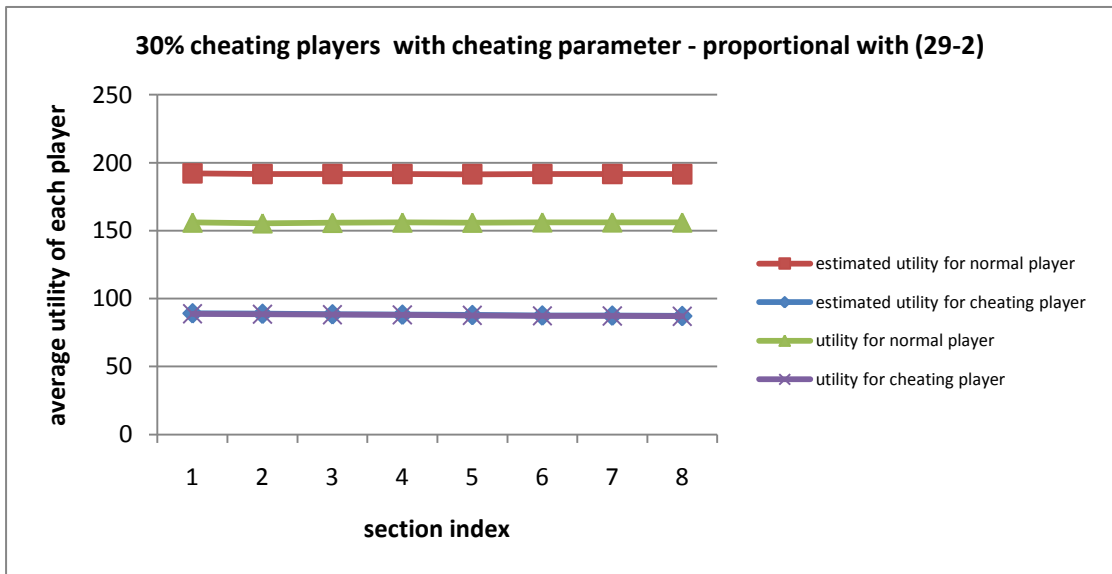
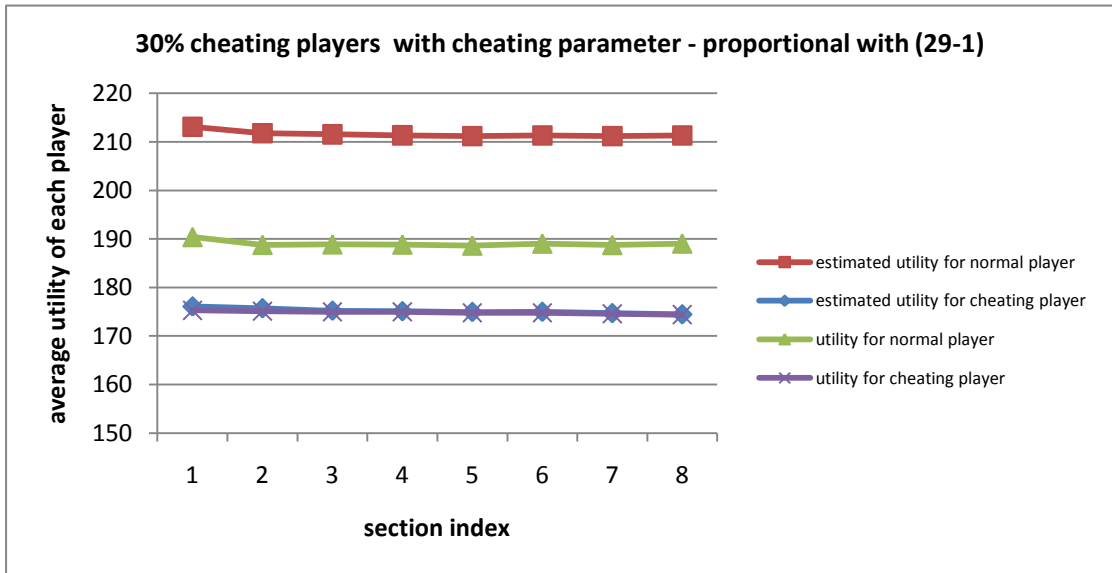
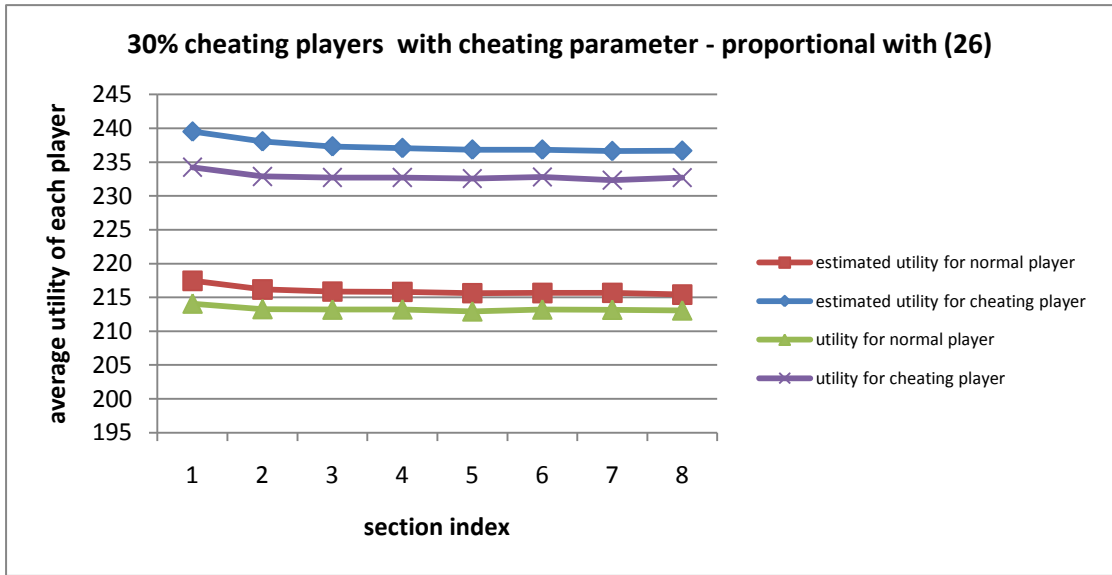
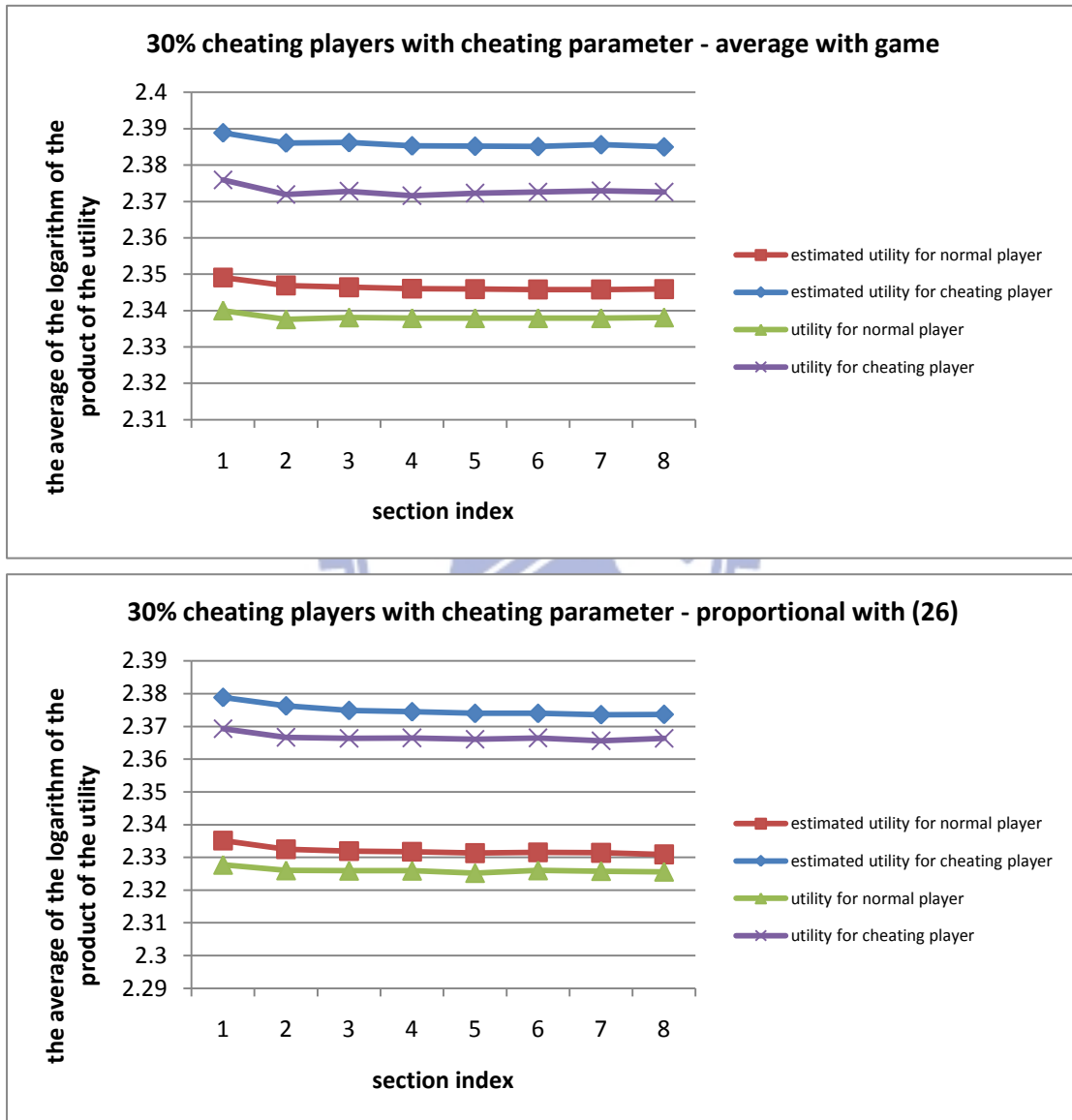


Figure 4.2.2-1: The average utility of each section with 30% cheating player and cheating parameter 0.3



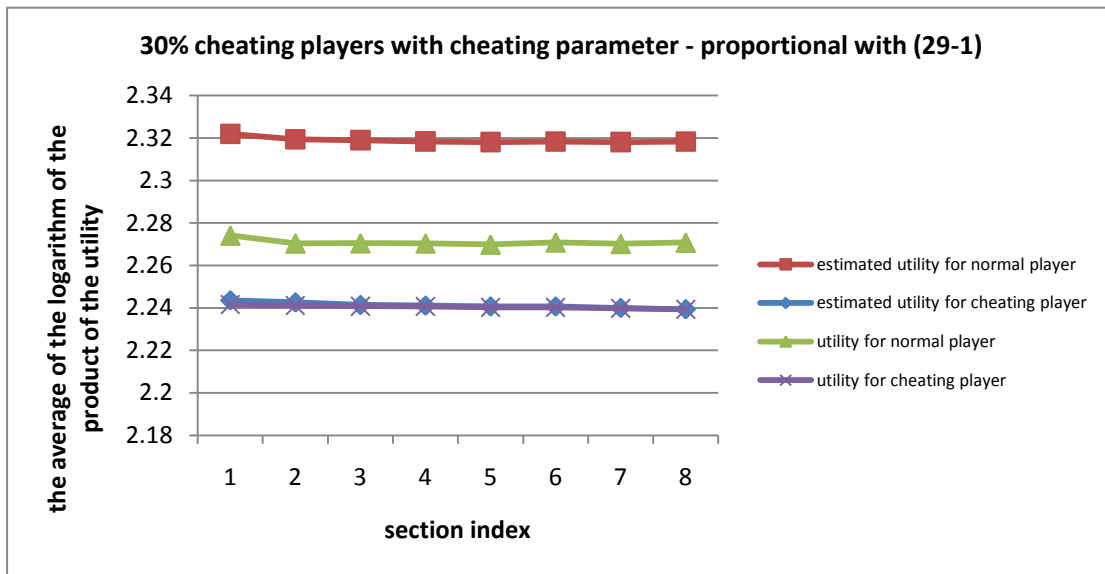


Figure 4.2.2-2: The average of the logarithm of product of utility of each section with 30% cheating player and cheating parameter 0.3

4.2.3 The Impacts of Malicious Player and Cheating Player

In this section, we will show the impacts when both of malicious player and

cheating player exist simultaneously at the environment. The simulation environment is shown as table 4.2.3-1. The duration of each section is 10 seconds. There are 20% players whose upload bandwidth is 640Kbps and 80% players whose upload bandwidth is 384Kbps. This bandwidth setting refers to the range of ADSL of CHT. The distributed section size is 360KB at each round. The number of block of each section is 300 blocks. The size of each original block is 1200Bytes, and the size of each original encoded block is 1500Bytes. The 300Bytes overhead is due to the coefficients of each original block. Each original block needs at least one coefficient to be encoded in encoded process, and one coefficient in $GF(2^8)$ is one byte. The 300 original encoded blocks are distributed randomly to the player. The system will randomly distribute the encoded blocks which are encoded by the original block of specific section to the players in one section. The cheating player will start the cheating behavior at round 1. The attack rate means the probability that the malicious player performs the malicious behavior. The malicious behavior means a player randomly changes the content of encoded block. The cheating player will cheat by cheating parameter 0.3.

Table 4.2.3-1: The simulation environment

The number of player	100
The size of section which is distributed at each round	360 KB
The number of block of each section	300 blocks
Size of each block	1200 Bytes
Upload bandwidth of each node per round	640, 384Kbps
Initial unpolluted probability, P_{ji}	1
Initial coefficient of expected rank, r_{ji}	1
The cost coefficient, c_i	0.1~0.4

Cheating parameter and malicious attack rate	0.3 , 50%
Number of section	8
Which round the cheating player start the cheating behavior	1
The probability that the player is malicious player	30%
The probability that the player is cheating player	30%
The weighting coefficient at update stage: weight _{er} , weight _{Ir} , weight _{Pr}	0.5, 0.5, 0.5

In figure 4.2.3-1 and figure 4.2.3-2, it shows that both of the malicious player and the cheating player are restricted at proportional distribution strategy, especially the player who is malicious and cheating player simultaneously. In figure 4.2.3-1, we observe the cheaters at proportional distribution strategy are restricted. On the other hand, the players who are malicious and cheating player simultaneously have lower utility than the malicious players at proportional strategy. These kinds of players are still restricted at proportional distribution strategy.

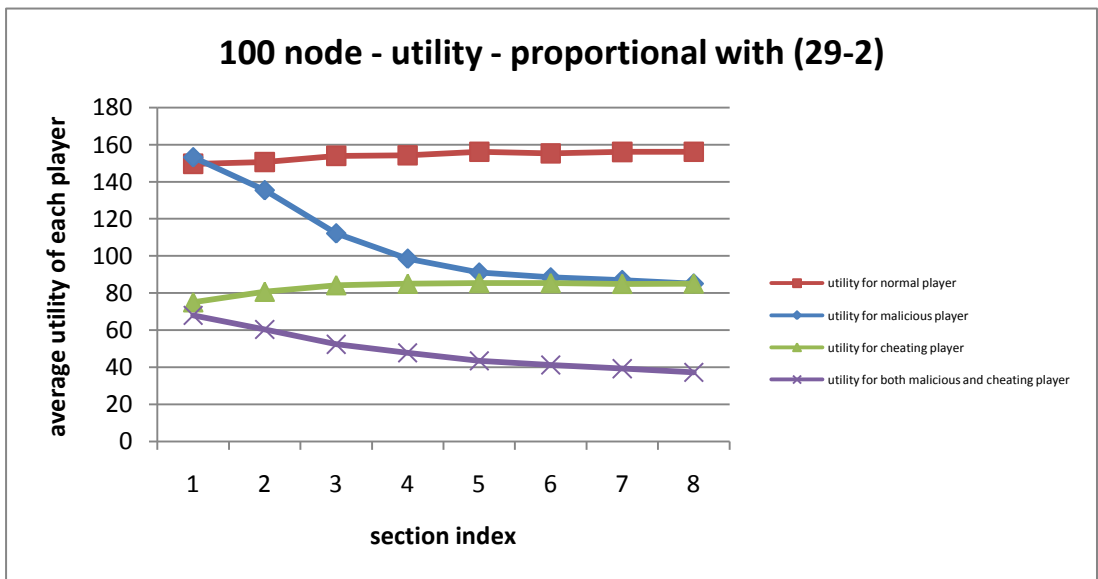
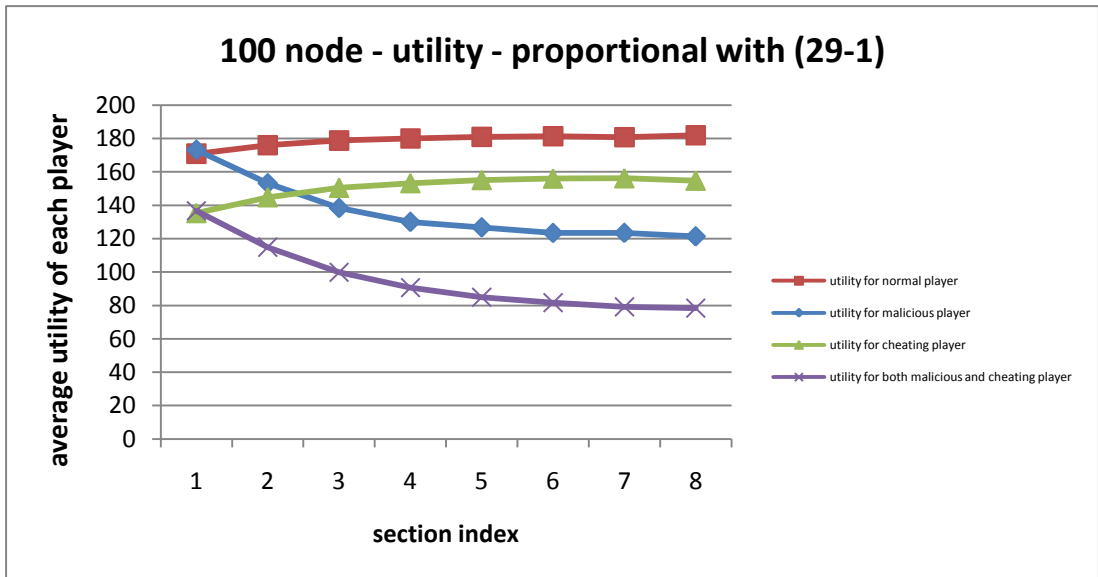
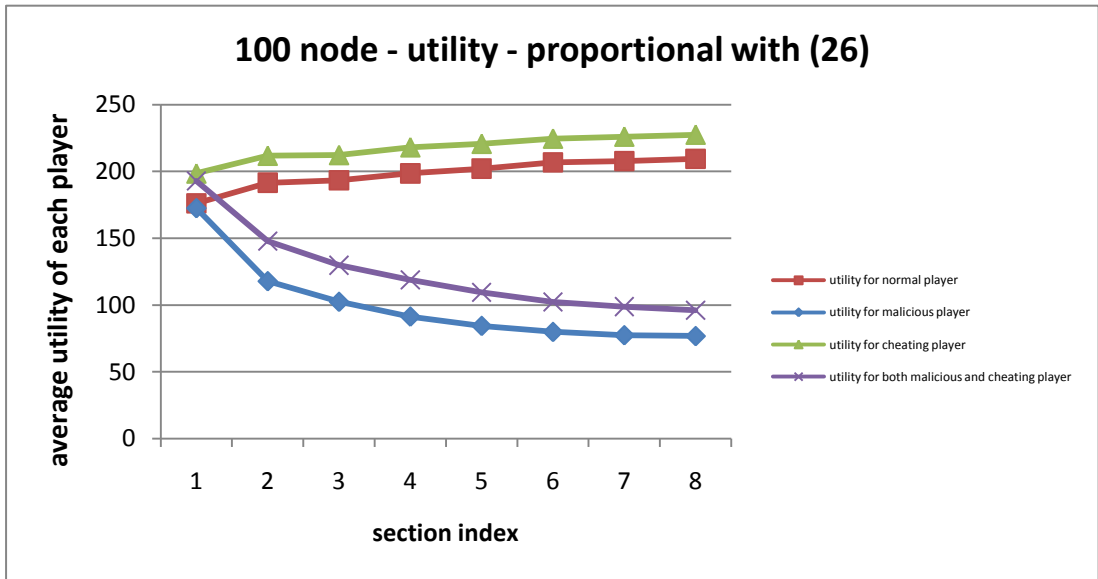
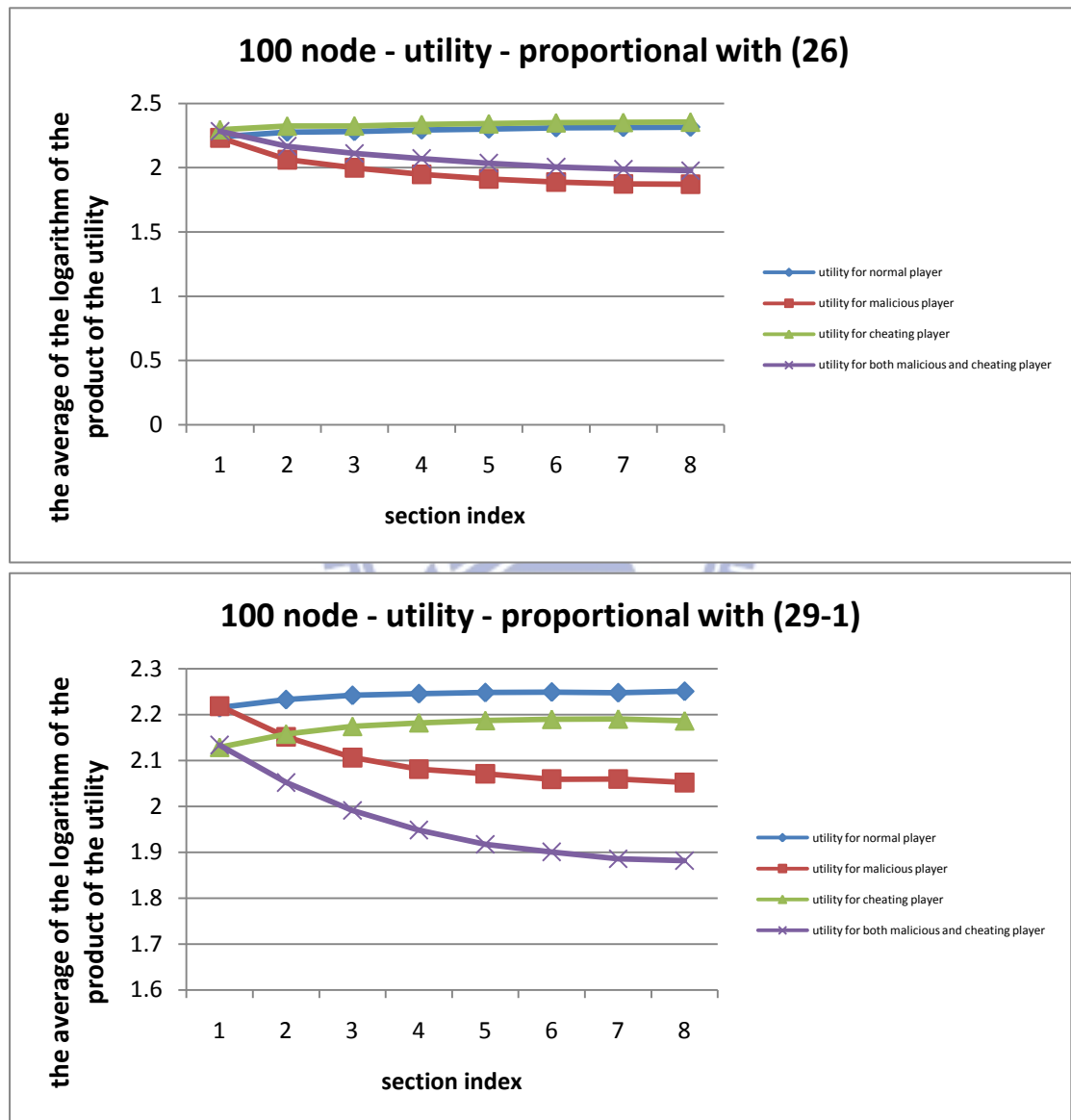


Figure 4.2.3-1: The average utility of each section with 30% cheating player and 30% malicious player



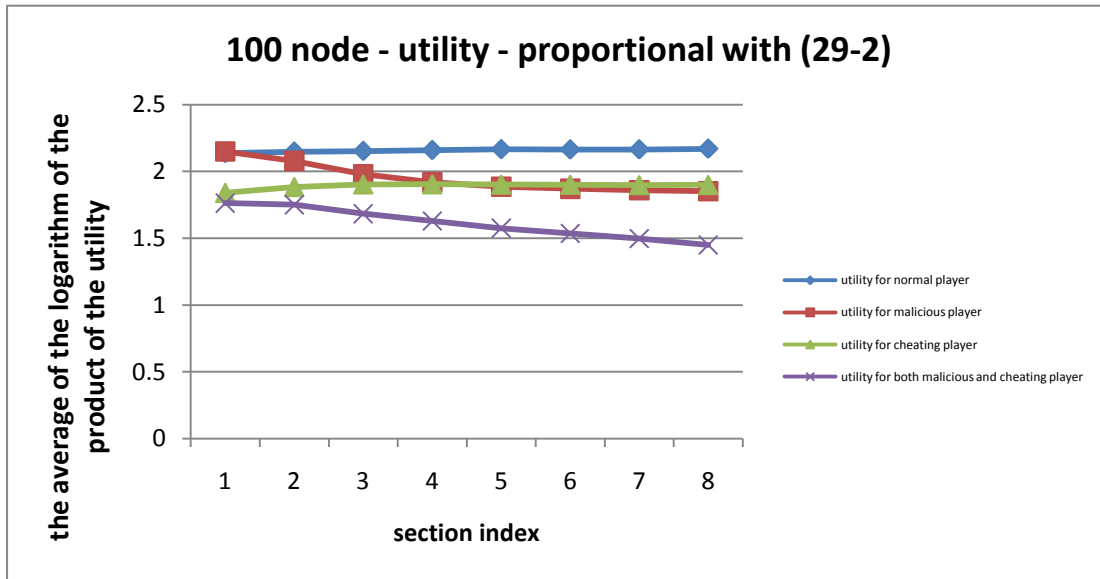


Figure 4.2.3-2: The average of the logarithm of product of utility of each section with 30% cheating player and 30% malicious player

According to above simulation, we know that both of malicious player and cheating player are not suitable at our proposed method. They will reward lower resources or be restricted. In our proposed method, the player must be cooperative and not perform the malicious behavior, or they will be restricted.

The proportional distribution strategy with (26) is only suitable for the environment in which there are some normal players and malicious players. The proportional distribution strategy with (29-1) and (29-2) is suitable for the environment in which there are some normal players, malicious players and cheating players. The proportional distribution strategy with (29-1) has higher average utility than (29-2), but the proportional distribution strategy with (29-2) is more effective than (29-1) for malicious players and cheating players.

5. Conclusion

In this thesis, we propose a novel algorithm to restrict the impacts of the problem. The problem means that how to maximize the peer's reward under the environment where some of the peers will perform the malicious behaviors and the cheating behaviors in the peer-to-peer network coding environment. We attempt to use the game theory to maximize the player's rewards and simultaneously limit the impacts of the malicious behaviors and the cheating behaviors.

The game theory is an interesting application of social sciences and computer sciences. It offers some incentive strategies for the players to encourage them to be cooperative. The cheating behavior is also an interesting problem in the game theory. The cheating player will perform cheating behavior when they believe the cheating behavior can bring more rewards.

In our proposed method, the normal players can be more cooperative with other normal players, but be more uncooperative with malicious player. The uncooperative situation leads to the consequence that the malicious player must use more resource for normal player to exchange their resource.

The effect of the cheating behavior in our proposed architecture is restricted. The proposed detective algorithm can detect part of the cheating behavior. Moreover, in multi-player game, the cheating player cannot be rewarded by any utility from other cheating players. It leads to the consequence that the total utility of the cheating players is decreasing.

6. References:

- [1]. R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung, "Network Information Flow" *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204-1216, 2000
- [2]. R. Koetter and M. Medard, "An algebraic Approach to Network Coding," *IEEE/ACM Transaction on Networking*, vol. 11, no. 5, pp.782-795, 2003
- [3]. T. Ho, R. Koetter and M. Medard, D. Karger, and M. Effros, "The Benefits of Coding over Routing in a Randomized Setting," in *Proc. Of IEEE International Symposium on Information Theory*, 2003
- [4]. C. Gkantsidis and P. Rodriguez, "Network Coding for Large Scale Content Distribution," in *Proc. of IEEE INFOCOM 2005*
- [5]. C. Gkantsidis and P. Rodriguez, "Cooperative Security for Network Coding File Distribution," in *Proc. of IEEE INFOCOM 2006*
- [6]. D. Charles, K. Jian, and K. Lauter, "Signature for Network Coding," Technique Report MSR-TR-2005-159, Microsoft, 2005
- [7]. Z. Yu, Y. Wei, B. Ramkumar and Y. Guan, "An Efficient Signature-based Scheme for Securing Network Coding against Pollution Attacks," in *Proc. of IEEE INFOCOM 2008*
- [8]. E. Kehdi, B. Li, "Null Keys: Limiting Malicious Attacks Via Null Space Properties of Network Coding," in *Proc. of IEEE INFOCOM 2009*
- [9]. K. Walsh and E. G. Sirer, "Fighting Peer-to-Peer SPAM ans Decoys with Object Reputation," in *Proc. Economics of P2P Systems*, Philadelphia, PA, Aug.2005
- [10]. C. Costa, V. Soares, J. Almeida, and V. Almeida, "Fighting Pollution Dissemination in Peer-to-Peer Networks," in *Proc. Symp. on Applied Computing*, Seoul, S. Korea, Mar. 2007
- [11]. C. Buragohain, D. Agrawal, S. Suri, "A Game Theoretic Framework for

Incentives in P2P Systems,” in *Proceedings Third International Conference on Peer-to-Peer Computing*, 2003

[12]. W. S. Lin, H. V. Zhao, K. J. R. Liu, “A Game Theoretic Framework for Incentive-based Peer-to-Peer Live-Streaming Social Networks,” in *Proc of IEEE ICASSP 2008*

[13]. M. K. H. Yeung, Y. K. Kwok, ”Game Theoretic Scalable Peer-to-Peer Media Streaming,” in *Proc of IEEE IPDPS*, 2008

[14]. E. V. Damme, *Stability and Perfection of Nash Equilibria*, Second, Revised and Enlarged Edition, New York: Springer-Verlag, 1991, ch.7

[15]. J. F. Nash, “The bargaining problem,” *Econometrica* 18, 155-162

[16]. J. W. Friedman, *GAME THEORY WITH APPLICATIONS TO ECONOMICS*, Second Edition, New York; Oxford University Press, 1990, ch.6

[17]. C. Wu, B. Li and Z. Li, ” Dynamic Bandwidth Auctions in Multi-overlay P2P Streaming with Network Coding”, in *Proc. of TPDS 2008*

[18]. X. Zhang and B. Li, “On the Market Power of Network Coding in P2P Content Distribution Systems,” in *Proc. of IEEE INFOCOM 2009*

[19]. T. Chen and S. Zhong, “INPAC: An Enforceable of Incentive Scheme for Wireless Networks using Network Coding,” in *Proc. of IEEE INFOCOM 2010*

[20]. Z. Ji, W. Yu and K. J. R. Liu, “A Game Theoretical Framework for Dynamic Pricing-Based Routing in Self-Organized MANETs,” in *IEEE J-SAC vol. 26, no. 7, Sep 2008*

[21]. W. Yu and K. J. R. Liu, “Game theoretic analysis of cooperation and security in autonomous ad hoc networks,” in *IEEE Transactions on Mobile Computing, vol. 6 no.5, May 2007*

[22]. X. Zhang and B. Li, ”On the Benefits of Network Coding in Multi-Channel

Wireless Networks,” in *Proc. of IEEE SECON 2008*

[23]. X. Zhang and B. Li, “Optimized Multipath Network Coding in Lossy Wireless Networks,” in *IEEE J-SAC vol. 27, no. 5, Jun 2009*

[24]. S. Mumtaz, P. Marques, A. Gameiro and J. Rodriguez, “Application of Game Theory in Ad-hoc Opportunistic Radios,” in *Proc. of ICNP 2009*

[25]. Y. Wu, B. Wang and K. J. R. Liu, “Repeated Open Spectrum Sharing Game with Cheat Proof Strategies,” in *IEEE Transaction on Wireless Communications, vol. 8, no. 4, Apr 2009*

[26]. X. Zhang and B. Li, “Network Coding Aware Dynamic Subcarrier Assignment in OFDMA Wireless Networks,” in *Proc. of IEEE ICC 2008*

[27]. Y. Chen, B. Wang and K. J. R. Liu, “Multiuser Rate Allocation Games for Multimedia Communications,” in *IEEE Transaction on Multimedia, vol. 11, no. 6, Oct 2009*

