Winter 11-21-2011

Power Control and Security Games for Wireless Communication Networks

Bo Liang
University of Nebraska-Lincoln, bxws1128@gmail.com

POWER CONTROL AND SECURITY GAMES FOR WIRELESS COMMUNICATION NETWORKS

by

Bo Liang

A THESIS

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfilment of Requirements

For the Degree of Master of Science

Major: Electrical Engineering

Under the Supervision of Professor Mustafa Cenk Gursoy

Lincoln, Nebraska

December, 2011

POWER CONTROL AND SECURITY GAMES FOR WIRELESS COMMUNICATION NETWORKS

Bo Liang, M. S.

University of Nebraska, 2011

Adviser: Mustafa Cenk Gursoy

In this thesis, game theoretic analysis of wireless communication networks has been performed. Game theory provides valuable tools can be used to solve problem of conflict and cooperation in wireless communication networks. Game theoretic tools can be applied to multiple layers of wireless networks. First, we consider power control issues at the physical layer of wireless networks. A game theoretic analysis for resource allocation policies in fading interference channels in the presence of quality of service (QoS) constraints is performed. We model a two player non-cooperative power control game and assume that both transmitters and receivers know the channel side information. The transmitters in this game are selfish and rational with QoS limitations and average power constraints. We prove that there is a unique admissible Nash equilibrium of this non-cooperative power control game. Secondly, a pseudonym change game which is used to protect location information in mobile networks has been proposed. In mobile networks, in order to track the location of mobile nodes, an adversary will monitor the pseudonym of each node. Therefore, mobile nodes are encouraged to change their pseudonyms in mix zones to increase their location security level and get rid of the tracker. However, pseudonyms are costly so some mobile nodes may not cooperate and change their pseudonyms when they already have high location security level. In order to achieve an optimal security level, game theoretical models

have been used. The goal of each mobile user in this game is to maximize its location security level with a minimum pseudonym change cost. We consider non-cooperative incomplete information game, where mobile nodes do not know their opponents' payoff function and types. We numerically demonstrate that a mobile user becomes selfish when the pseudonym change cost is small. Oppositely, if the cost is high, mobile nodes cooperate more. A game-theory-based anti-tracking protocol is also proposed at the end.

ACKNOWLEDGMENTS

I would like to thank my advisor, Professor Mustafa Cenk Gursoy for his guidance throughout my graduate program. I thank him for helping me at some critic time. I also appreciate the research environment he provided, which I believe is very helpful for our creative work.

I also want to thank Professors Senem Velipasalar and Wenbo He for serving on my Master thesis committee and providing many valuable suggestions which brought insightful perspectives into my research.

Throughout my graduate program, I have been surrounded by an amazing group of colleagues at UNL. My countless conversations with them have been invaluable to my research and to learning about other fields. I especially thank my fellow students from both the Wireless Communications and Networking Laboratory as well as the Integrated Circuit and Systems Laboratory. The discussions, chats and laughters with them made my life in Nebraska much more fun.

Last but not least, I would like to thank my parents Zongshan Liang and Linhong Li for their consistent support and encouragement. I am really glad that I can always rely on their advices. Without their love and faith, I would never have accomplished the research I have done.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Wireless Ad Hoc Networks

Unlike traditional infrastructure networks which is shown in Fig. 1.1, wireless ad hoc network [1][2] is a network that does not rely on a predefined infrastructure. It has a set of wireless nodes which have the ability to build and form a network. Based on the explanation from Webster, the two definitions for ad hoc are: ”formed or used for specific or immediate problems”, and ”fashioned from whatever is immediately available.” These definitions tell us that the ad hoc network can be set up for a specific application and they can also be built by several immediate available nodes. Other than basic features above, ad hoc network can avoid the installation and maintenance of network infrastructure and be set up very quickly. Overall, ad hoc network is a robust, dynamic and self-organizing network architecture with a distributed nature and node redundancy, as shown in Fig. 1.2. Since the wireless ad hoc network has the decentralized nature, it suits for a lot of applications. Over the last several years, many design principles for ad hoc network have been developed

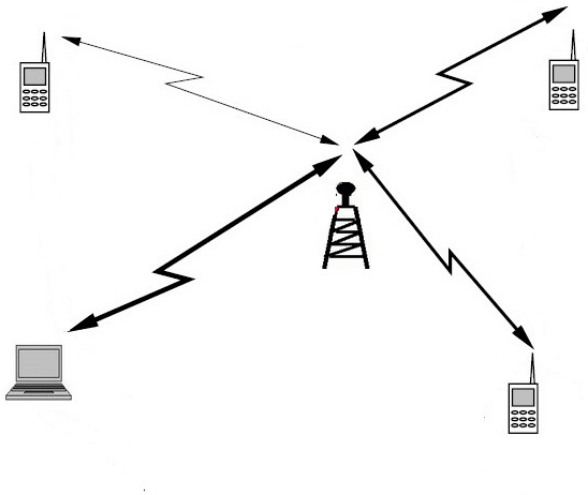

Figure 1.1: Infrastructure network.

[3][4][5]. However, more research still needs to be done to improve the capability and performance of this type network. In the following sections, I will briefly talk about the major applications for wireless ad hoc networks together with the challenges.

Generally, wireless ad hoc networks can be classified by their applications. First, the self-configuring wireless network with mobile devices is named mobile ad hoc network (MANET) [6]. It's a network that can achieve the goal of "getting connected anywhere and at any time". The mobile devices in MANET can establish links between each devices when they move in any direction at any selected time. For example, a group of people with cell phones and laptops are having a meeting in a conference room where no network service is available. In this case, they can easily build an ad hoc network using their devices so that they can share the information they have regardless of their physical

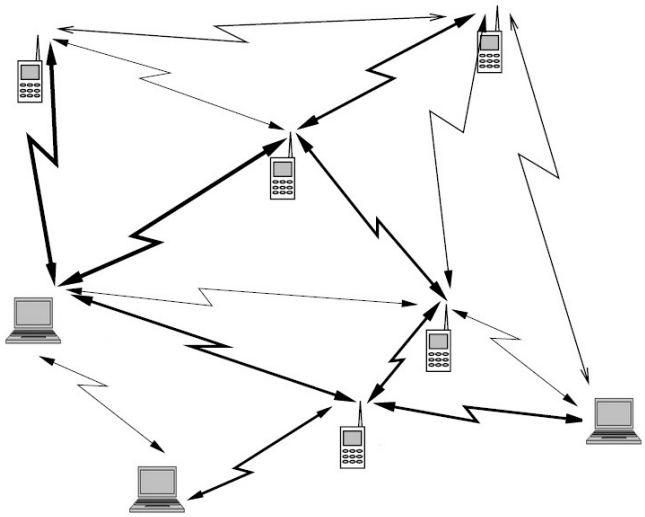

Figure 1.2: Wireless Ad Hoc Network.

location. MANETs has been a really hot topic for 15 years because of the huge numbers of laptops and cell phones. Basically, there are three types of MANET for different application scenarios: Vehicular Ad Hoc Networks (VANETs) [7], Intelligent vehicular ad hoc networks (InVANETs) [8] and Internet Based Mobile Ad Hoc Networks (iMANET) [9]. VANETs are used for communication between vehicles and roadside stations. They fully use the self-configuring feature of ad hoc network to develop connection between a set of vehicles and roadside equipment. InVANETs are an upgraded version of VANETs. They can make the vehicles behave smarter with the features of artificial intelligence setup so that the possibility of having a traffic accident is decreased. iMANET are ad hoc networks which link mobile nodes. Second, a communication network with radio nodes organized in a mesh topology is called wireless mesh network (WMN) [10]. It can be considered as a special type of ad hoc network.

It provides a solution that uses a number of access points connected point to point. The mobile nodes in WMN can forward data from gateways without internet connection. The coverage area of the mobile nodes is named a mesh cloud. With this mesh cloud, even if one node can no longer operate, the other mobile nodes can still forward information to each other. The WMN is a new wireless LAN technology that addresses the market's requirement of highly scalable and cost-effective networks. It offers users secure, seamless roaming anytime and anywhere. Third, wireless sensor networks are developed to monitor certain environmental conditions. It is a network with numerous sensor nodes. For each node, it has a circuit board with low power transceiver, microcontroller, antenna, and certain sensor devices. The cost of one sensor node varies based on the complexity of the structure. There are various types of topologies for sensor networks. The simple topology can be a small star network and the complex one can be a multi-hop mesh network. Such sensor arrays systems have great potential for use in many application scenarios. For example, they can be set up in home and detect the location of the smoke and can also track the spread of the smoke. It can also be used to monitor a traffic tunnel and see if there is any accident happening.

1.2 Design Challenges

Based on the above introduction, the main characteristic of wireless ad hoc networks is their lack of infrastructure. This means that unlike the cellular systems, the mobile nodes of the wireless ad hoc network all have control functions and communication functions. Thus, with a number of mobile nodes, wireless ad hoc network can form a network hierarchy at any place and any

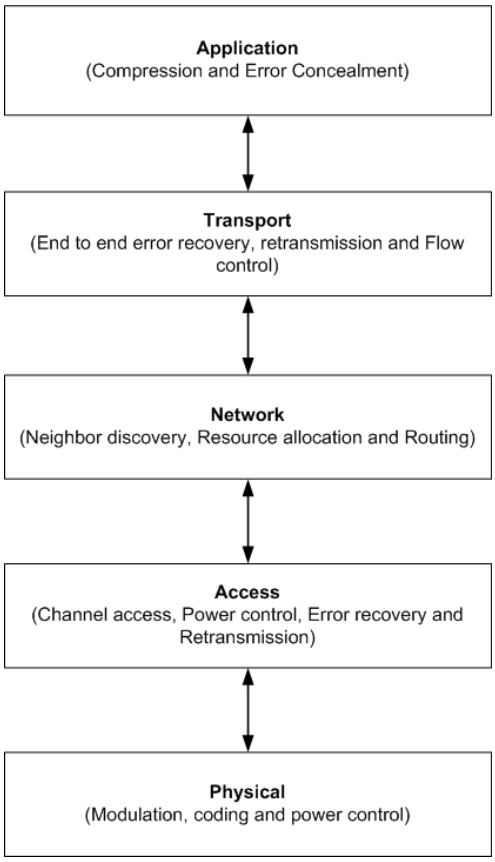

Figure 1.3: Re-created from Andrea Goldsmith 2005, "Wireless ad hoc network five layer model".

time. In networks, a five-layer model is used [2]. The five layers are application layer, transport layer, network layer, access layer, and physical layer. These layers are described in Fig. 1.3 [2]. In different layers, there are different issues which also bring different challenges to the network design. The first challenge is the power control issue [11] for mobile nodes. If the node has enough power, the node can transmit data to any other node. However, in reality, the power of one node cannot be considered as infinity. In fixed transmit power condi-

tion, the SINR between two nodes will decrease when distance between nodes increases. Furthermore, the SINR also changes randomly due to fading and interference. If the SINR of the link is very low, the bit error will increase and the node will not transmit due to this poor channel condition. Since the transmission between each node may have poor performance due to the low SINR and interference from other links, it's better to select a power adaption scheme to dynamicly change transmission power for each node so that it can assure that its SINR is large enough to transmit data. The power adaption scheme choice becomes a key to solve power control issue. Secondly, the energy constraint for mobile node is also a significant challenge. The mobile nodes are equipped with batteries. It is hard to replace the batteries or recharge them especially for some underground or underwater applications. It is obvious that the constrained energy of mobile nodes highly impacts the design of wireless ad hoc networks. In this case, the mobile nodes can only transmit finite number of bits and hence the data transmission should be more efficient. The sleep mode has to be introduced in the design of mobile nodes in order to save some energy because the node cannot transmit or stand by all the time otherwise the batteries will die soon. However, if the node has a sleep mode, the wireless ad hoc network design will be more complicated. Overall, the energy consumption is a key issue that needs to be optimized over all layers. Thirdly, scalability issue [2] is always a problem for wireless ad hoc network. As the network grows based on its application, protocols needs to scale as well. The protocol processing requires a lot of energy in mobile nodes which brings a trade off that how much load should be processed for single node versus transferring processing load to centralized node to deal with. Finally, the security is always a key issue to consider while designing a wireless network [12]. Usually, we

need to consider this problem on three aspects: availability, confidentiality and authentication. Availability guarantees that the network can handle denial of services attacks which can be introduced at any layer. Confidentiality ensures the information like data and routing information must be never exposed to unauthorized users. The authentication ensures that a node knows the identity of the node it is communicating with. Therefore, the adversary cannot use a third party unauthorized node to access the sensitive information or interfere with the operation. Since the wireless ad hoc network has the characteristic of the lack of infrastructure, this also brings a number of challenges. As the mobile nodes of wireless ad hoc network sometimes work in poor environments, the ad-hoc network should choose a distributed architecture. If the ad-hoc network uses central entity architecture, it may bring a significant security problem. Moreover, the trust relationship between each node will change due to ad hoc network's lack of infrastructure. Therefore, dynamic security mechanisms are needed for wireless ad hoc networks.

Chapter 2

Game Theory in Wireless Communication

2.1 Game Theory

Game theory provides variable tools can be used to solve the problem of conflict and cooperation. The first discussion about game theory was provided by James Waldegrave in 1838. In 1944, Von Neumann and Oskar Morgenstern established the connection between economic behavior and game theory [13]. In 1950, John Nash provided the concept of Nash equilibrium [14] which is a list of strategies for each player in the game. Nash equilibrium demonstrates the property that no player can unilaterally change his own strategy in order to get a better payoff. It is the central concept of a non cooperative game. The goal of game theory is finding the best actions for individual players in various scenarios. The game should have at least two players. Depending on the application scenarios, the player can be a company, a poker card or, in our case, a wireless node. Each player has some strategies which will determine the out-

come of the game. The outcome caused by different players will be expressed by a number of payoffs.

Games can be classified into two types [15][16]: Cooperative game and non-cooperative game.

2.1.1 Cooperative Game

A cooperative game is a game in which players can make binding commitment. Therefore, the players in the game will demonstrate cooperative behavior and the game is not a competition between individual players. The cooperative game [13][17] pays attention to the fairness and effectiveness. For example, two cars are running on the same narrow road head to head. In this situation, the drivers should choose a side to swerve in order to avoid the accident. If the drivers cooperate with each other and choose different sides to swerve, they can avoid the accident. If they choose the same side, they cannot pass each other. This is a typical cooperative game example. If we assign the payoff of pass for one driver as "0", then the payoff of collide will be "5". In this case, there are two Nash equilibrium: driver A swerve to left and driver B swerve to right, or driver A swerve to right and driver B swerve to left. As long as they choose different side, they can have a Pareto efficient solution. Table 2.1 illustrates the result of this case.

Table 2.1: Choosing sides for cars.

	left	right
left	(0,0)	(5,5)
right	(5,5)	(0,0)

2.1.2 Non-Cooperative Game

In non-cooperative game [18][13], players make decisions independently. The focus of non cooperative games is player's individual optimal strategy. Based on different criteria, non cooperative games can be divided into two types: Complete information game and incomplete information game. For complete information game, the player has full knowledge of its opponent including strategies and payoff function. The typical example of non cooperative game is prisoner's dilemma. In this story, two persons are arrested in the jail. The attorney wants them to confess their crime so she offered them a deal separately: "With enough evidences, if both of you do not confess the crime, you two will stay in jail for 1 year. If you confess the crime and the other guy confesses the crime too, you two will have to stay in jail for 5 years. However, if you confess the crime and the other guy does not confess, you don't have to stay in the jail but the other guy have to stay in jail for 11 years. It also works in the opposite way which means if you do not confess but the other guy does, you will stay in jail for 11 years." Table 2.2 demonstrates the situation of prisoner's dilemma.

Table 2.2: Prisoner's dilemma.

	prisoner A confess	prisoner A non-confess
prisoner B confess	(5,5)	(0,11)
prisoner B non-confess	(11,0)	(1,1)

Apparently, the prisoner's dilemma is a complete information non-cooperative game. Each player has two strategies and knows his opponent's strategies. The assumption of the game is that each player in this game is rational individually and each player also assumes their opponent is rational. The years one player will stay in the jail are payoff of the player. Thus, a smaller payoff value is

preferred by both prisoners individually. The case that both prisoners confess the crime will be the best strategy that they can choose by themselves without cooperation. Therefore, (confess,confess) is the Nash equilibrium in this case but it is not Pareto optimal because (not confess, not confess) have a better result.

2.2 Game Theoretic Analysis of Wireless Communications

Wireless ad hoc network has a dynamic and self-organizing architecture. This dynamic characteristic increases the difficulty of using analytical models to analyze the performance of wireless ad hoc networks. Game theory offers several mathematical tools to solve this issue. With game theory, we can model the interaction and competition between wireless nodes of an ad hoc network [19].

For the last ten years, game theory has been widely used as an efficient analysis tool in the telecommunication area. Most of the time, the object is the traditional network. In recent years, as the interest in wireless ad hoc network increases, developing communication games for ad hoc networks become an attractive topic. For example, considering a problem in the MAC layer, the Aloha protocol has been implemented in a wireless ad hoc network. Because of the dynamic architecture of wireless ad hoc network, the total number of mobile nodes in the network is unknown. The optimal retransmit probability is undecided. Therefore, in order to achieve the maximum throughput, an adaptive retransmit scheme with dynamic retransmit probability needs to be

developed for this network. However, we still do not know if the adaptive scheme can reach a steady state. We are also wondering if certain perturbations will change the node behavior or cause some undesired result. Game theory provides an ideal tool to solve these issues. Game theory does not only suit for MAC layer, but also suits for physical, transport, and other layers.

In wireless ad hoc network communication, nodes make choices independently while considering their environment and other nodes' activity. It is exactly like what a player does in a game. Therefore, with reasonable mapping, we can apply game theory to wireless ad hoc network scenarios. In a game, there are three important components: players, strategy and utility function. In the wireless ad hoc network, mobile nodes will act as players and their strategies are those decisions they made such as transmiting the packets or not, the power level setting, pseudonym change or not, choice of modulation scheme. The payoff functions are the metrics like throughput, delay, or SINR. The Fig. 2.1 shows the mapping relationship between game and wireless ad hoc network.

Game theory can provide many benefits for ad hoc networks. First, it is a strong tool to analyze network protocols because it can investigate a steady state operating point of networks. Second, it can provide a good mathematical tool to model the system and solve some cross layer problems. Third, it is also a excellent candidate to design incentive mechanisms for network. Although game theory has a lot of great properties that can be performed on wireless ad hoc network, it still has challenges to be solved. Though game theory has strong ability to provide a mathematical model for the network problem, it is still not perfect. It is also difficult to design a utility function to evaluate different performance levels. Finally, game theoretic analysis on ad hoc networks is

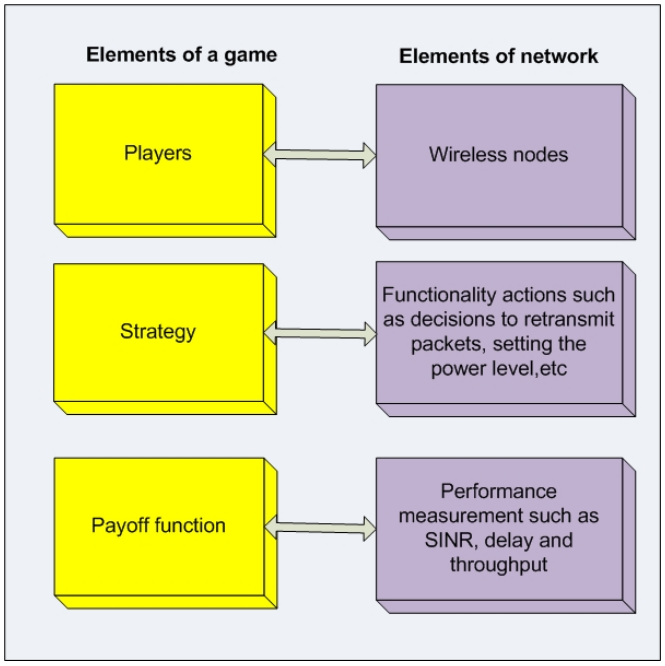

Figure 2.1: The relation between games and ad hoc networks.

based on the assumption that players act rationally. Although we can program this behavior for wireless nodes, it does not accurately reflect the practical occasions. It is possible that wireless nodes do not perform rationally. The list of benefits and challenges are shown in Fig. 2.2.

When we use game theory to analyze the wireless ad hoc network, selfish behavior of nodes becomes a big issue because it may make network reach an undesirable suboptimal equilibrium [20][21][22]. In order to limit the selfish behavior of nodes, incentive mechanisms are introduced to wireless ad hoc network design so nodes can have less selfish moves and the network can reach a desirable optimal result. As mentioned in the literature, incentive mechanisms can be divided into two categories: credit-exchange systems and reputation

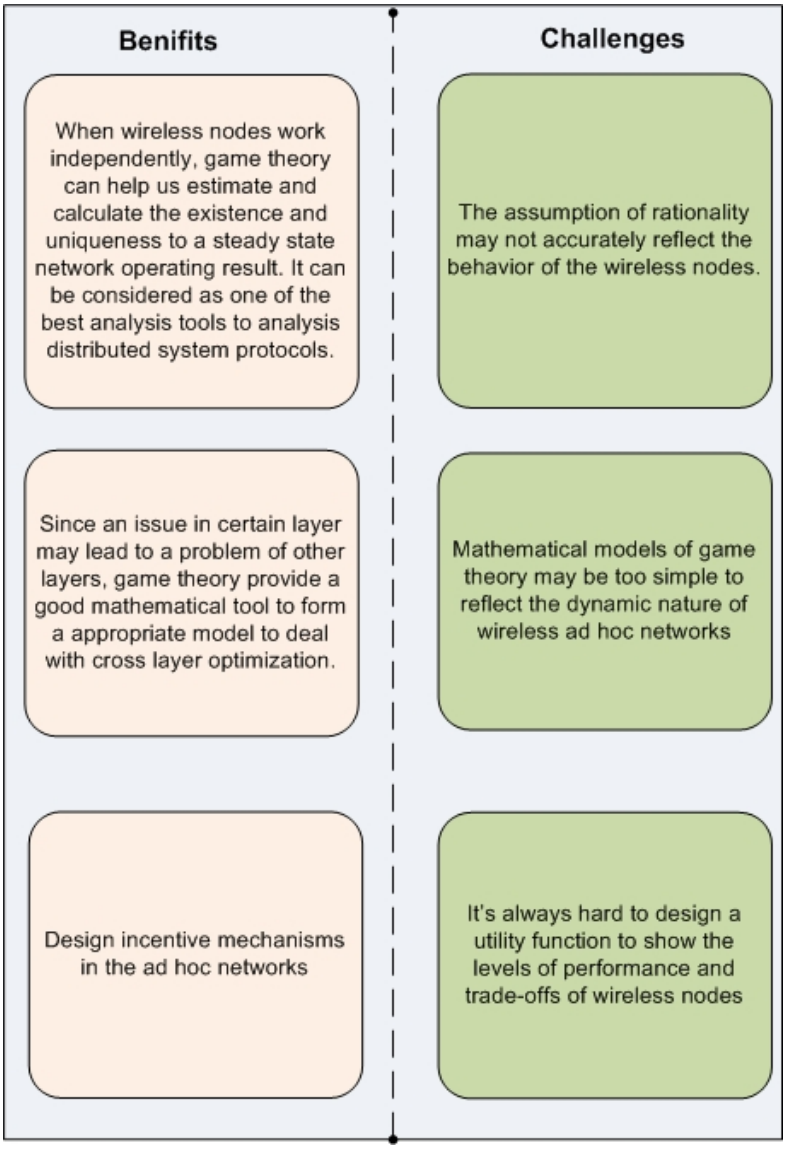

Figure 2.2: Benefits and Challenges of the game.

systems.

One technique to provide incentives is called credit exchange[23][24]. For this mechanism, a charge and reward system has been adopted into the wireless ad hoc network. If a wireless node cooperates with other same type nodes (nodes with the same network goal), it will be credited. If a node does not cooperate or cooperates with other nodes, it will be debited. In [23], a "token reward" method has been introduced to implement this credit exchange mechanism. If the nodes provide services, they will be rewarded a token. If they request services, the token they have will be decreased. Reputation based mechanism [25] is another technique to create incentive. Based on the communication between wireless nodes, the wireless nodes interact with other nodes in the network and assign the reputation value to their neighbors. The goal of the player is to try to build a good reputation by cooperating with other players. If the node's reputation value is low, it will be isolated from the network. Game theory is used to analyze this mechanism and try to improve the reputation value of the nodes in the network in order to stimulate the nodes to cooperate with each other.

Chapter 3

Non-Cooperative Power Control Games for Wireless Communication Networks

In this chapter, we will perform a game theoretic analysis of the physical layer of a wireless communication system. At the physical layer analysis, the transmit power of wireless nodes has a huge impact. Ideally, two random nodes in the network can communicate with each other with sufficient power. However, if the transmit power is too high, significant interference will be generated to other nodes which will degrade other node's performance. Furthermore, in practical scenarios, a wireless node has limited energy and hence cannot afford high power consumption. Recently, game theory has been introduced to solve the transmit power and resource allocation issues. For instance, in [26], an iterative water-filling power control algorithm through a non-cooperative game in the digital subscriber lines has been presented. A game theoretic analysis on multi-access fading channel is also provided by Lai and Gamal [27]. They

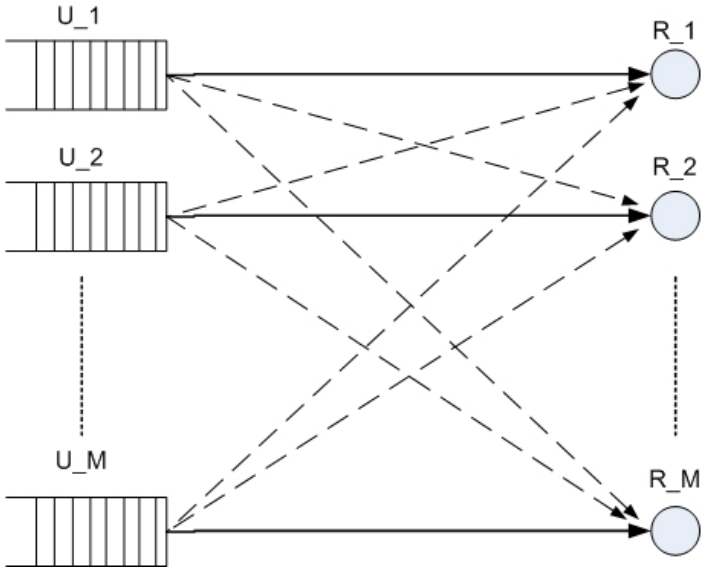

Figure 3.1: System model.

prove that the maximum sum rate of the capacity region is the unique Nash equilibrium. Qiao also provided a power control game analysis on multiple-access channel with the consideration of quality of service (QoS) constraints [28]. Therefore, the multiple access channel has been considered many times from a game-theoretic perspective. It is interesting to apply game theoretic analysis the game to other channel models.

We focus on a non-cooperative power control game on interference channels with QoS constraints. The effective capacity is employed as the throughput metric in our game.

3.1 System Model

The scenario we consider is that M users communicate with M receivers with individual power constraints and QoS constraints. The system model is shown in Fig. 3.1. We assumed that data sequences that are generated by transmitters have been divided into frames of duration T. At the transmitter side, there is a buffer which is used to store data frames before they are transmitted over the wireless channel. The discrete-time signal received at the first receiver in the i^{th} symbol duration is given by

$$y_1[i] = \sum_{j=1}^{M} h_{j1}[i]x_j[i] + n[i], \quad i = 1, 2, \ldots \tag{3.1}$$

where M is the number of users, $x_j[i]$ denotes the complex-valued channel input and $h_{j1}[i]$ is the fading coefficient between the jth user and the first receiver. We assume that $h_{j1}[i]$ is jointly stationary and ergodic discrete-time process and so is the other fading coefficient, and we denote the magnitude-square of the fading coefficients by $z_{j1}[i] = |h_{j1}[i]|^2$. Additionally, we assume that the bandwidth available in the system is B. Therefore, average energy constraint can be expressed as $\mathcal{E}\{|x_j[i]|^2\} \leq \bar{P}_j/B$ for all i, indicating that the average power of the system is constrained by $\bar{P}$ and the channel input of user j should be subject to the average energy constraint in this model. Since the bandwidth is B, symbol rate is assumed to be B complex symbols per second. $y[i]$ is the channel output and $n[i]$ is a zero-mean, circularly symmetric, complex Gaussian random variable with variance $\mathcal{E}\{|n[i]|^2\} = N_0$. The additive Gaussian noise samples $\{n[i]\}$ are assumed to form an independent and identically distributed (i.i.d.) sequence.

In this system model, we assume that both the transmitters and the receivers know the channel state $\mathbf{z} = \{z_{11}, z_{12} \ldots, z_{MM}\}$. It is possible that one node broadcasts the estimated perfect $\mathbf{z}$ to all the other users. Although implicitly, the channel state varies much more slowly than the data rate so that tracking the channel can be done exactly with negligible cost and feedback [29]. Under this condition, dynamic power and rate allocation can be performed in accordance with the changing channels.

For a given power allocation policy $\mathcal{U} = \{\mu_1(\mathbf{z}), \cdots, \mu_M(\mathbf{z})\}$, where $\mu_j \geq 0, \forall j$ can be viewed as a function of $\mathbf{z}$, the achievable rates are defined as [29]

$$\mathcal{R}(\mathcal{U}) = \left\{ \mathbf{R} : \mathbf{R}(S) \leq \mathcal{E}_{\mathbf{z}} \left\{ B \log_2 \left(1 + \sum_{j \in S} \mu_j(\mathbf{z}) \mathbf{z} \right) \right\}, \right. \\ \left. \forall S \subset \{1, \cdots, M\} \right\}, \tag{3.2}$$

If all transmitters and receivers have CSI, the rate of one transmitter is provided by

$$\mathcal{R}_{IF} = \bigcup_{\mathcal{U} \in \mathcal{F}} \mathcal{R}(\mathcal{U}) \tag{3.3}$$

where $\mathcal{F}$ is the set of all feasible power control policies satisfying the average power constraint

$$\mathcal{F} \equiv \{\mathcal{U} : \mathcal{E}_{\mathbf{z}} \{\mu_j(\mathbf{z})\} \leq \text{SNR}_j, \mu_j \geq 0, \forall j\} \tag{3.4}$$

where $\text{SNR}_j = \bar{P}_j / (N_0 B)$ denotes the average transmitted signal-to-noise ratio of user j. The maximum instantaneous rate at a given state with any decoding

order π can be obtained as

$$R_{\pi(k)} = B \log_2 \left(1 + \frac{\mu_{\pi(k)} z_{\pi(k)}}{1 + \sum_{i=k+1}^{M} \mu_{\pi(i)} z_{\pi(i)}} \right) \quad \text{bits/s}, \quad k = 1, \cdots, M. \tag{3.5}$$

3.2 Effective Capacity

In order to guarantee a statistical QoS requirement, the concept of effective capacity [30] is introduced in this section. It is the maximum constant arrival rate[1] that a given service process can support. In this problem, we describe the statistic QoS requirement by the QoS exponent θ and we define L_Q as the stationary queue length. Therefore, θ is considered to be the decay rate of the tail distribution of the queue length L_Q:

$$\lim_{q \to \infty} \frac{\log P(L_Q \geq q)}{q} = -\theta. \tag{3.6}$$

If we have a large $q_{\max}$, we can derive the buffer violation probability as: $P(L_Q \geq q_{\max}) \approx e^{-\theta q_{\max}}$. Thus, larger θ represents more strict QoS constraints, smaller θ indicates looser QoS guarantees. Furthermore, if L_D is the steady-state delay appeared in the buffer, then we can have expression $P(L_D \geq d_{\max}) \approx e^{-\theta \delta d_{\max}}$ for large $d_{\max}$ and the arrival and service processes [31] determines δ.

[1] For time-varying arrival rates, effective capacity specifies the effective bandwidth of the arrival process that can be supported by the channel.

In [31], Tang and Zhang demonstrated a method which used the effective capacity to solve a resource allocation in audio and video application problem.

The effective capacity can be expressed as

$$R_C(\theta) = -\frac{\Lambda(-\theta)}{\theta} = -\lim_{t\to\infty}\frac{1}{\theta t}\log_e \mathbb{E}\{e^{-\theta S[t]}\} \quad \text{bits/s}, \tag{3.7}$$

where $\Lambda(-\theta)$ is a function which depends on the logarithmic moment generating function of $S[t]$. $S[t] = \sum_{i=1}^{t} s[i]$ is the time-accumulated service process.

In our case, we consider a general fading distribution. We also assume that fading coefficients are constant over the frame duration in order to simplify our problem. The fading coefficients change independently for each frame and each user. Under these assumptions, $s[i] = TR[i]$, where $R[i]$ is the instantaneous service rate in the ith frame duration $[iT; (i+1)T]$. Thus, (3.7) can be denoted as

$$R_C(\theta) = -\frac{1}{\theta T}\log_e \mathbb{E}_{\mathbf{z}}\{e^{-\theta T R[i]}\} \quad \text{bits/s}. \tag{3.8}$$

The effective capacity normalized by bandwidth B is

$$\mathbf{R}_C(\theta) = \frac{R_C(\theta)}{B} \quad \text{bits/s/Hz}. \tag{3.9}$$

3.3 The Power Control Game

In this section, we discuss a two-player interference channel game. In this game, users are selfish and they all try to send data to their respective destination. The goal of them is to try to maximize their transmission rate based on their average power constraint on interference channel. Since the channel

model we consider in this game is interference channel, each node will generate interference to other transmission link, while it tries to send its own data to its own target node. We assume that (θ_1, θ_2) is a vector composed of the QoS constraints for the two users and $\beta_j = \frac{\theta_j TB}{\log_e 2}$, $j = 1, 2$ is the corresponding normalized QoS constraint.

The power control game we consider is a two-player non-cooperative game. The power control policy $\mu_j(\mathbf{z})$ can be expressed as the strategy of user j. The payoff of this game is the normalized effective capacity $\mathbf{C}_j(\mathcal{U})$. The goal of user j in this game is

$$\max_{\mu_j} \mathbf{C}_j(\mu_j, \mu_{-j}) \quad \text{s.t.} \quad \mu_j \in \mathcal{F}_j, \tag{3.10}$$

where $\mathcal{F}$ is given in (3.4), and μ_{-j} is the power control policies of the other users. In this interference channel game, one user transmits data continuously to its target destination. At the same time, it produces interference to its neighbors's objective receiver. For a given power control policy $\mu_2(z_{11}, z_{12}, z_{21}, z_{22})$ of user 2, the payoff of user 1 is given by

$$\begin{aligned}
\mathbf{C}_1(\mathcal{U}) &= -\frac{1}{\theta_1 TB} \log_e \\
&\quad \mathcal{E}\left\{ e^{-\theta_1 TB \log_2\left(1+\frac{\mu_1(z_{11},z_{12},z_{21},z_{22})z_{11}}{1+\mu_2(z_{11},z_{12},z_{21},z_{22})z_{21}}\right)} \right\} \\
&= -\frac{1}{\theta_1 TB} \log_e \left(\int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty \right. \\
&\quad \left(1 + \frac{\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) z_{11}}{1 + \mu_2(z_{11}, z_{12}, z_{21}, z_{22}) z_{21}} \right)^{-\beta_1} \times \\
&\quad \left. p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22}) dz_{11} dz_{12} dz_{21} dz_{22} \right)
\end{aligned} \tag{3.11}$$

where $p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22})$ is the joint probability density function of the

channel state. Since transmitter 2 has the same properties as transmitter 1, the payoff for user 2 is similar to the payoff of user 1 and it is expressed as

$$\begin{aligned}\mathbf{C}_2(\mathcal{U}) = & -\frac{1}{\theta_2 TB}\log_e \\ & \mathcal{E}\left\{e^{-\theta_2 TB\log_2\left(1+\frac{\mu_2(z_{11},z_{12},z_{21},z_{22})z_{22}}{1+\mu_1(z_{11},z_{12},z_{21},z_{22})z_{12}}\right)}\right\} \\ & = -\frac{1}{\theta_2 TB}\log_e\Bigg(\int_0^\infty\int_0^\infty\int_0^\infty\int_0^\infty \\ & \left(1+\frac{\mu_2(z_{11},z_{12},z_{21},z_{22})z_{22}}{1+\mu_1(z_{11},z_{12},z_{21},z_{22})z_{12}}\right)^{-\beta_2}\times \\ & p_{\mathbf{z}}(z_{11},z_{12},z_{21},z_{22})dz_{11}dz_{12}dz_{21}dz_{22}\Bigg)\end{aligned} \tag{3.12}$$

From the above equations, two strategies (μ_1, μ_2) become the dominant factors of the effective capacity payoff function of user 1 and user 2. Hence, in order to reach the goal of this game, we bring the following definition.

Definition 1 *A Nash equilibrium is a policy pair* (μ_1^*, μ_2^*) *such that*

$$\begin{aligned}&\mathbf{C}_1(\mu_1^*, \mu_2^*) \geq \mathbf{C}_1(\mu_1', \mu_2^*),\ \forall \mu_1' \in \mathcal{F}_1 \\ &\mathbf{C}_2(\mu_1^*, \mu_2^*) \geq \mathbf{C}_2(\mu_1^*, \mu_2'),\ \forall \mu_2' \in \mathcal{F}_2.\end{aligned} \tag{3.13}$$

As illustrated by the definition, no user can benefit by using non-optimal strategy individually. If we consider a case with fixed power policy $\mu_2(z_1, z_2)$, the optimal strategy of user 1 can be reached by solving the solution to the follow-

ing maximization problem

$$\begin{aligned}
\mathbf{C}_1 = \max_{\mu_1} & -\frac{1}{\theta_1 TB} \log_e \Bigg(\int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty \\
& \left(1 + \frac{\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) z_{11}}{1 + \mu_2(z_{11}, z_{12}, z_{21}, z_{22}) z_{21}}\right)^{-\beta_1} \\
& \times p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22}) dz_{11} dz_{12} dz_{21} dz_{22} \Bigg), \\
\text{s.t.} & \int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty \mu_1(z_{11}, z_{12}, z_{21}, z_{22}) \times \\
& p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22}) dz_{11} dz_{12} dz_{21} dz_{22} \leq \text{SNR}_1, \\
& \mu_1(z_{11}, z_{12}, z_{21}, z_{22}) \geq 0
\end{aligned} \tag{3.14}$$

It also can be further reduced to the following minimization problem

$$\begin{aligned}
& \min_{\mu_1} \int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty \left(1 + \frac{\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) z_{11}}{1 + \mu_2(z_{11}, z_{12}, z_{21}, z_{22}) z_{21}}\right)^{-\beta_1} \\
& \times p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22}) dz_{11} dz_{12} dz_{21} dz_{22}, \\
& \text{s.t.} \int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty \mu_1(z_{11}, z_{12}, z_{21}, z_{22}) \times \\
& p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22}) dz_{11} dz_{12} dz_{21} dz_{22} \leq \text{SNR}_1, \\
& \mu_1(z_{11}, z_{12}, z_{21}, z_{22}) \geq 0
\end{aligned} \tag{3.15}$$

The solution to the above optimization problem is the power allocation similar to [31]

$$\mu_1(\mathbf{z}) = \left(\frac{(1 + \mu_2(\mathbf{z}) z_{21})^{\frac{\beta_1}{\beta_1+1}}}{\alpha_1^{\frac{1}{\beta_1+1}} z_{11}^{\frac{\beta_1}{\beta_1+1}}} - \frac{1 + \mu_2(\mathbf{z}) z_{21}}{z_{11}} \right)^+ \tag{3.16}$$

$$= \frac{1 + \mu_2(\mathbf{z}) z_{21}}{z_{11}} \left(\left(\frac{z_{11}}{\alpha_1 (1 + \mu_2(\mathbf{z}) z_{21})} \right)^{\frac{1}{\beta_1+1}} - 1 \right)^+ \tag{3.17}$$

where $(x)^+ = \max\{x, 0\}$, α_1 is the threshold chosen to satisfy the following power constraint

$$\int_{\alpha_1}^{\infty}\int_{0}^{\infty}\int_{0}^{\infty}\int_{0}^{\infty}\left(\frac{(1+\mu_2(\mathbf{z})z_{21})^{\frac{\beta_1}{\beta_1+1}}}{\alpha_1^{\frac{1}{\beta_1+1}} z_{11}^{\frac{\beta_1}{\beta_1+1}}} - \frac{1+\mu_2(\mathbf{z})z_{21}}{z_{11}}\right)^+ \times p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22}) dz_{22} dz_{12} dz_{21} dz_{11} = \mathrm{SNR}_1. \tag{3.18}$$

Similarly the optimal power policy of user 2 can be derived as

$$\mu_2(z_1, z_2) = \left(\frac{(1+\mu_1(\mathbf{z})z_{12})^{\frac{\beta_2}{\beta_2+1}}}{\alpha_2^{\frac{1}{\beta_2+1}} z_{22}^{\frac{\beta_1}{\beta_2+1}}} - \frac{1+\mu_1(\mathbf{z})z_{12}}{z_{22}}\right)^+ \tag{3.19}$$

where α_2 is the threshold chosen to satisfy the power constraint

$$\int_{\alpha_2}^{\infty}\int_{0}^{\infty}\int_{0}^{\infty}\int_{0}^{\infty}\left(\frac{(1+\mu_1(\mathbf{z})z_{12})^{\frac{\beta_2}{\beta_2+1}}}{\alpha_2^{\frac{1}{\beta_2+1}} z_{22}^{\frac{\beta_2}{\beta_2+1}}} - \frac{1+\mu_1(\mathbf{z})z_{12}}{z_{22}}\right)^+ \times p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22}) dz_{11} dz_{12} dz_{21} dz_{22} = \mathrm{SNR}_2. \tag{3.20}$$

Based on the above analysis, the optimal policy of one user cannot be reached by only adjusting its own parameters. It also depends on its assumption of the other user's strategy. According to the assumption, transmitters are going to adjust their threshold value and power control policy to achieve the maximum normalized effective capacity in this game. Therefore, the above analysis shows that the power constraints of the two users must be satisfied with equality at the Nash equilibrium. Considering the expressions (3.16) and (3.19), we have the following result.

Proposition 1 *With every pair of* (α_1, α_2)*, a unique pair of strategies* (μ_1, μ_2) *should exist.*

Proof: First, we consider that if user 1 decides to transmit, or $\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) > 0$, from (3.17), we have

$$\frac{z_{11}}{\alpha_1(1 + \mu_2(z_{11}, z_{12}, z_{21}, z_{22})z_{21})} > 1. \tag{3.21}$$

The channel state of transmitter 1 is normalized by the interference from transmitter 2 and channel noise. From the above equation, we can find out that if $\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) > 0$, the channel state is greater than the threshold. Since the transmitter 2 has the same situation, we can derive the condition for transmitter 2 as the equation

$$\frac{z_{22}}{\alpha_2(1 + \mu_1(z_{11}, z_{12}, z_{21}, z_{22})z_{12})} > 1. \tag{3.22}$$

When they decide to transmit data separately, they have different conditions. Thus, we will consider the condition that they transmit data at the same time at the next step. In this situation, both conditions (3.21) and (3.22) should be satisfied. Let's consider three cases with an assumption that the pair (α_1, α_2) exist: only node 1 transmits, only node 2 transmits and both nodes transmit together.

In the case that only node 1 transmits, we have $\mu_2(z_{11}, z_{12}, z_{21}, z_{22}) = 0$, and condition (3.21) can be satisfied while (3.22) cannot. According to (3.16), we

can derive that

$$\mu_{10}(z_{11}, z_{12}, z_{21}, z_{22}) = \frac{1}{\alpha_1^{\frac{1}{\beta_1+1}} z_{11}^{\frac{\beta_1}{\beta_1+1}}} - \frac{1}{z_{11}}. \tag{3.23}$$

Then we substitute $\mu_{10}(z_{11}, z_{12}, z_{21}, z_{22})$ and $\mu_2(z_{11}, z_{12}, z_{21}, z_{22})$ into (3.21) and (3.22), we have

$$\mathbf{Z}_1 = \left\{ \mathbf{z} : z_{11} > \alpha_1, \frac{z_{22}}{\alpha_2} \leq \alpha_1(1 + \mu_{10} z_{12}) \right\} \tag{3.24}$$

The above condition illustrated the region in which only node 1 transmits. When only node 2 transmits, we have a similar situation that $\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) = 0$. Then, we have the region that only node 2 transmits as follow

$$\mu_{20}(z_{11}, z_{12}, z_{21}, z_{22}) = \frac{1}{\alpha_2^{\frac{1}{\beta_2+1}} z_{22}^{\frac{\beta_2}{\beta_2+1}}} - \frac{1}{z_{22}}, \tag{3.25}$$

$$\mathbf{Z}_2 = \left\{ \mathbf{z} : z_{22} > \alpha_2, \frac{z_{11}}{\alpha_1} \leq \alpha_2(1 + \mu_{20} z_{21}) \right\}. \tag{3.26}$$

When both nodes transmit, (3.21) and (3.22) can be satisfied. We can find out that $\mu_1(z_{11}, z_{12}, z_{21}, z_{22})$ is upperbounded by $\frac{\frac{z_{22}}{\alpha_2} - 1}{z_{12}}$ and $\mu_2(z_{11}, z_{12}, z_{21}, z_{22})$ is upperbounded by $\frac{\frac{z_{11}}{\alpha_1} - 1}{z_{21}}$. Since the region in which none of the nodes is transmitting is derived previously as

$$\mathbf{Z}_0 = \{ \mathbf{z} : z_{22} \leq \alpha_2, z_{11} \leq \alpha_1 \}, \tag{3.27}$$

the region in which both nodes transmit is $\mathbf{Z}_3$ which is the one other than the

above three regions.

We have

$$\begin{cases} \mu_1(\mathbf{z}) = \frac{(1+\mu_2(\mathbf{z})z_{21})^{\frac{\beta_1}{\beta_1+1}}}{\alpha_1^{\frac{1}{\beta_1+1}} z_{11}^{\frac{\beta_1}{\beta_1+1}}} - \frac{1+\mu_2(\mathbf{z})z_{21}}{z_{11}} \\ \mu_2(\mathbf{z}) = \frac{(1+\mu_1(\mathbf{z})z_{12})^{\frac{\beta_2}{\beta_2+1}}}{\alpha_2^{\frac{1}{\beta_2+1}} z_{22}^{\frac{\beta_2}{\beta_2+1}}} - \frac{1+\mu_1(\mathbf{z})z_{12}}{z_{22}} \end{cases} \tag{3.28}$$

which can be written as

$$\begin{cases} 1+\mu_1(\mathbf{z})z_{11}+\mu_2(\mathbf{z})z_{21} = \left(\frac{z_{11}}{\alpha_1}\right)^{\frac{1}{\beta_1+1}} (1+\mu_2(\mathbf{z})z_{21})^{\frac{\beta_1}{\beta_1+1}} \\ 1+\mu_1(\mathbf{z})z_{12}+\mu_2(\mathbf{z})z_{22} = \left(\frac{z_{22}}{\alpha_2}\right)^{\frac{1}{\beta_2+1}} (1+\mu_1(\mathbf{z})z_{12})^{\frac{\beta_2}{\beta_2+1}} \end{cases} . \tag{3.29}$$

With $\alpha_1, \alpha_2, z_1, z_2$, we try to establish monotonic properties for μ_1 and μ_2 (3.28) and we find that $\mu_1(z_{11}, z_{12}, z_{21}, z_{22})$ is a concave function of $\mu_2(z_{11}, z_{12}, z_{21}, z_{22})$ and $\mu_2(z_{11}, z_{12}, z_{21}, z_{22})$ is a concave function of $\mu_1(z_{11}, z_{12}, z_{21}, z_{22})$. It is clear that we may find a intersection in the $\mu_1 - \mu_2$ plane caused by these two curves. This intersection demonstrates that there is a $(\mu_1^2(\mathbf{z}), \mu_2^2(\mathbf{z}))$ satisfying the both equations. Consider the function $\mu_1(z_{11}, z_{12}, z_{21}, z_{22})$ of $\mu_2(z_{11}, z_{12}, z_{21}, z_{22})$, if $\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) > 0$, then we have $\mu_2(\mathbf{z}) \in (0, \frac{\frac{z_{11}}{\alpha_1}-1}{z_{21}})$. It means that curve has a intersection with $\mu_2 = 0$ at

$$\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) = \frac{1}{\alpha_1^{\frac{1}{\beta_1+1}} z_{11}^{\frac{\beta_1}{\beta_1+1}}} - \frac{1}{z_{11}} > 0. \tag{3.30}$$

Similarly, let's consider the function $\mu_2(z_{11}, z_{12}, z_{21}, z_{22})$ of $\mu_1(z_{11}, z_{12}, z_{21}, z_{22})$. We have $\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) \in (0, \frac{\frac{z_{22}}{\alpha_2}-1}{z_{12}})$. The curve will have a intersection at

$\mu_1 = 0$ as

$$\mu_2(z_{11}, z_{12}, z_{21}, z_{22}) = \frac{1}{\alpha_2^{\frac{1}{\beta_2+1}} z_{22}^{\frac{\beta_2}{\beta_2+1}}} - \frac{1}{z_{22}} > 0. \tag{3.31}$$

Therefore, at least one intersection $(\mu_1^2(z_{11}, z_{12}, z_{21}, z_{22}), \mu_2^2(z_{11}, z_{12}, z_{21}, z_{22}))$ between the two curves can be derived based on the above analysis.

Then we are going to see if this result is unique. We assume that another point $(\mu_1'^2(z_{11}, z_{12}, z_{21}, z_{22}), \mu_2'^2(z_{11}, z_{12}, z_{21}, z_{22}))$ is satisfying (3.28). In order to prove the result, we also assume $\mu_1'^2(z_{11}, z_{12}, z_{21}, z_{22}) < \mu_1^2(z_{11}, z_{12}, z_{21}, z_{22})$. From the equation in (3.29), we also have that $\mu_2'^2(z_{11}, z_{12}, z_{21}, z_{22}) < \mu_2^2(z_{11}, z_{12}, z_{21}, z_{22})$. Then we can see that these two points are staying on a line $\mathbf{I}$ and their slope is positive. Due to the concavity of the curve, if the interception of $\mathbf{I}$ on $\mu_1 = 0$ is not greater than 0, then the curve for $\mu_2(z_{11}, z_{12}, z_{21}, z_{22})$ as a function of $\mu_1(z_{11}, z_{12}, z_{21}, z_{22})$ will have a intersection on $\mu_1 = 0$ as a negative value so that $\mu_2(z_{11}, z_{12}, z_{21}, z_{22}) < 0$ at $\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) = 0$. However, it is not satisfied by (3.31). Similarly, if the interception of $\mathbf{I}$ on $\mu_2 = 0$ is less than 0, we can derive that $\mu_1(z_{11}, z_{12}, z_{21}, z_{22}) < 0$ at $\mu_2(z_{11}, z_{12}, z_{21}, z_{22}) = 0$, it also violates (3.30). Therefore, there is only one solution to the equations, so that we prove that there is a unique pair of (μ_1, μ_2) for a given pair (α_1, α_2).□

Based on the proof above, we will have a disjoint division of the 4-dimensional channel state, nodes will have different move and actions in different regions because of the channel states. If $\mathbf{z}$ lies in the region $\mathbf{Z}_0$, both nodes find out weak channel with strong background noise so they decide not to transmit. If $\mathbf{z}$ falls in the region $\mathbf{Z}_1$ or $\mathbf{Z}_2$, one of the nodes decides not to transmit because it predict the interference of other nodes and find out that interference of the other nodes and the noise is so high. If $\mathbf{z}$ is in the region $\mathbf{Z}_3$, both nodes find a relatively weak interference from the each other and allocate power based on

$$\mu_1^* = \begin{cases} \frac{1}{\alpha_1^{*\frac{1}{\beta_1+1}} z_{11}^{\frac{\beta_1}{\beta_1+1}}} - \frac{1}{z_{11}}, & z_{11} > \alpha_1^* \& \frac{z_{22}}{\alpha_2^*} \leq \alpha_1^* \left(1 + \left(\frac{1}{\alpha_1^{*\frac{1}{\beta_1+1}} z_{11}^{\frac{\beta_1}{\beta_1+1}}} - \frac{1}{z_{11}}\right) z_{12}\right) \\ \mu_1^*(z_{11}, z_{12}, z_{21}, z_{22}), & \text{regions other than} \mathbf{Z}_0 \& \mathbf{Z}_1 \& \mathbf{Z}_2 \\ 0, & \text{otherwise} \end{cases} \tag{3.32}$$

$$\mu_2^* = \begin{cases} \frac{1}{\alpha_2^{*\frac{1}{\beta_2+1}} z_{22}^{\frac{\beta_2}{\beta_2+1}}} - \frac{1}{z_{22}}, & z_{22} > \alpha_2^* \& \frac{z_{11}}{\alpha_1^*} \leq \alpha_2^* \left(1 + \left(\frac{1}{\alpha_2^{*\frac{1}{\beta_2+1}} z_{22}^{\frac{\beta_2}{\beta_2+1}}} - \frac{1}{z_{22}}\right) z_{21}\right) \\ \mu_2^*(z_{11}, z_{12}, z_{21}, z_{22}), & \text{regions other than} \mathbf{Z}_0 \& \mathbf{Z}_1 \& \mathbf{Z}_2 \\ 0, & \text{otherwise} \end{cases} \tag{3.33}$$

---

the best strategy.

Since every pair of (α_1, α_2) determines a unique power strategy for each nodes, we can derive the following results.

Proposition 2 *A Nash equilibrium which can optimize the throughput always exists. (3.32) and (3.33) are optimal power control policies of the two nodes.* $(\mu_1^*(\mathbf{z}), \mu_2^*(\mathbf{z}))$ *is the optimum power allocation result (3.28) with a* (α_1^*, α_2^*) *threshold pair that satisfies the power constraints. It can be determined numerically.*

Proof: We can further write (3.18) and (3.20) as

$$\begin{aligned} &\int\int\int\int_{\mathbf{Z}_1} \left(\frac{1}{\alpha_1^{*\frac{1}{\beta_1+1}} z_{11}^{\frac{\beta_1}{\beta_1+1}}} - \frac{1}{z_{11}}\right) \times \\ &p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22}) dz_{22} dz_{21} dz_{12} dz_{11} + \\ &\int\int\int\int_{\mathcal{Z}_3} \mu_1^2(z_{11}, z_{12}, z_{21}, z_{22}) \times \\ &p_{\mathbf{z}}(z_{11}, z_{12}, z_{21}, z_{22}) dz_{22} dz_{21} dz_{12} dz_{11} = \mathrm{SNR}_1 \end{aligned} \tag{3.34}$$

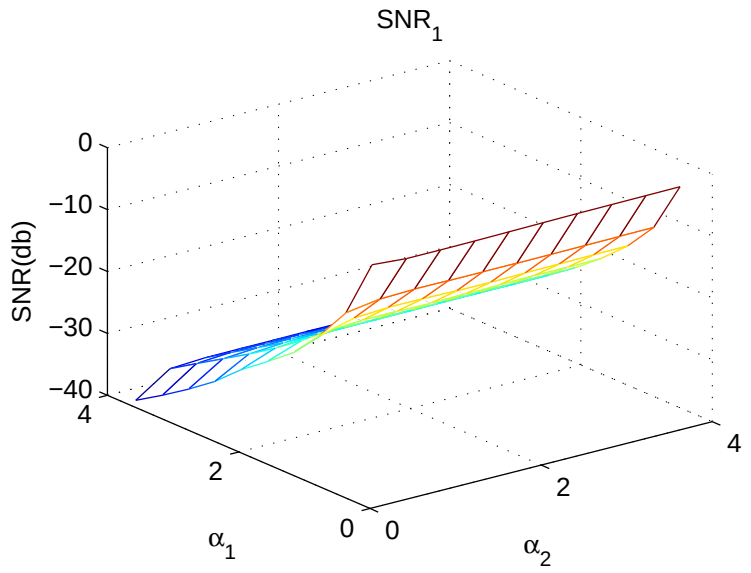

Figure 3.2: The average SNR1 with respect to α_1 and α_2.

$$\int\int\int\int_{\mathbf{z}_2}\left(\frac{1}{\alpha_2^{\frac{1}{\beta_2+1}} z_{22}^{\frac{\beta_2}{\beta_2+1}}}-\frac{1}{z_{22}}\right)\times$$
$$p_{\mathbf{z}}(z_{11},z_{12},z_{21},z_{22})dz_{22}dz_{21}dz_{12}dz_{11}+$$
$$\int\int\int\int_{\mathcal{Z}_3}\mu_2^2(z_{11},z_{12},z_{21},z_{22})\times$$
$$p_{\mathbf{z}}(z_{11},z_{12},z_{21},z_{22})dz_{22}dz_{21}dz_{12}dz_{11}=\mathrm{SNR}_2 \tag{3.35}$$

Based on the previous analysis of the channel state regions and the power allocation, we can find out that SNR_1 is a non-increasing function of α_1, and a non-decreasing function of α_2. On the other hand, $\mu_2(\mathbf{z})$ is a non-increasing function of α_2, and a non-decreasing function of α_1. The verified result is shown in the Figures (3.2) and (3.3). In order to prove the above proposition, we assume two threshold pairs (α_1', α_2') and (α_1^*, α_2^*) with $\alpha_1' = \alpha_1^*, \alpha_2' \leq \alpha_2^*$, because of the monotonic properties of the curve we can derive $\mathrm{SNR}_1(\alpha_1', \alpha_2') \geq$

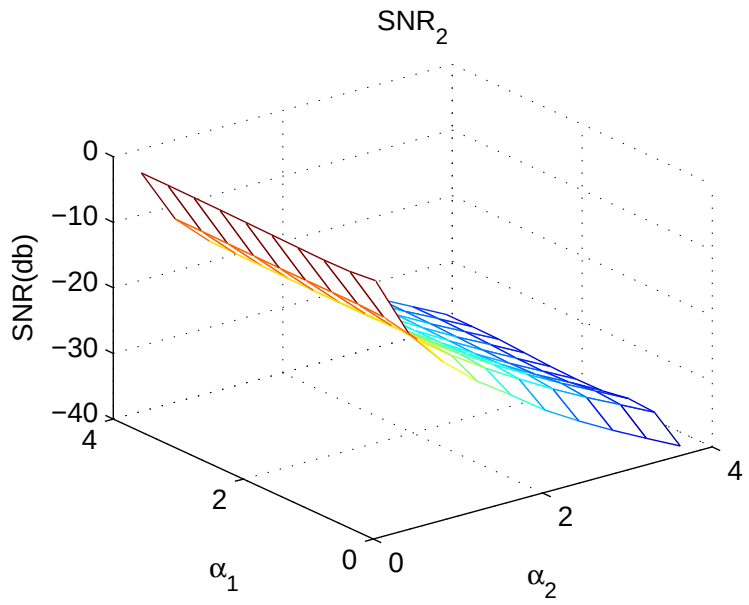

Figure 3.3: The average SNR2 with respect to α_1 and α_2.

$\text{SNR}_1(\alpha_1^*, \alpha_2^*)$ and $\text{SNR}_2(\alpha_1', \alpha_2') \leq \text{SNR}_2(\alpha_1^*, \alpha_2^*)$. $\text{SNR}_i(\alpha_1, \alpha_2)$ is the SNR of user i alone with the given threshold pair. Therefore, similar to [27], we set a starting analysis point $\alpha_1(0) = \varepsilon, \alpha_2(0) = \varepsilon$ and the value of ε is close to the maximum channel gain. From the previous verified result, $\text{SNR}_i(\alpha_1(0), \alpha_2(0))$, $i = 1, 2$ are close to 0. After finding the starting point, we fix $\alpha_1(n-1)$ and compute $\alpha_2(n)$ by considering the average power constraint of user 1, which is a solution to (3.35). Then we have $\alpha_2(n) \leq \alpha_2(n-1)$ and $\text{SNR}_1(\alpha_1(n-1), \alpha_2(n)) \leq \text{SNR}_1$. Next step, we fix $\alpha_2(n)$ to find the $\alpha_1(n)$ by considering the average power constraint of user 2, which is a solution to (3.34). Therefore, we have $\alpha_1(n) \leq \alpha_1(n-1)$ and $\text{SNR}_2(\alpha_1(n), \alpha_2(n)) \leq \text{SNR}_2$. Iteratively, we derive nonincreasing sequences $\alpha_1(n), \alpha_2(n)$ with $\text{SNR}_1(\alpha_1(n), \alpha_2(n)) \longrightarrow \text{SNR}_1$ and $\text{SNR}_2(\alpha_1(n), \alpha_2(n)) \longrightarrow \text{SNR}_2$. Since SNR_i, $i = 1, 2$ is not unlimited, both of the sequences are considered to be lowerbounded. Then, there must exist the

constants [32]

$$\inf_n \alpha_1(n) = \lim_{n\to\infty} \alpha_1(n) = \alpha_1^*,\ \mathrm{SNR}_1(\alpha_1^*, \alpha_2^*) = \mathrm{SNR}_1, \tag{3.36}$$

$$\inf_n \alpha_2(n) = \lim_{n\to\infty} \alpha_2(n) = \alpha_2^*,\ \mathrm{SNR}_2(\alpha_1^*, \alpha_2^*) = \mathrm{SNR}_2. \tag{3.37}$$

Therefore, based on the previous iterative numerical analysis, we proved that there should be a pair of (α_1^*, α_2^*) at the Nash equilibrium and the optimal power policies (μ_1^*, μ_2^*)can be reached.

From the above analysis, we proved the existence of the Nash equilibrium. Furthermore, we can even deliver a conclusion of the existence of admissible Nash equilibrium in this game by using the concept of admissible Nash equilibrium.

Definition 2 *If no other Nash equilibrium strategy (μ_1', μ_2') satisfying that $\mathbf{C}_1(\mu_1', \mu_2') \geq \mathbf{C}_1(\mu_1^*, \mu_2^*)$, $\mathbf{C}_2(\mu_1', \mu_2') \geq \mathbf{C}_2(\mu_1^*, \mu_2^*)$ exists, and at least one of the equalities is strict, a Nash equilibrium strategy pair (μ_1^*, μ_2^*) is admissible.*

We have the following result.

Proposition 3 *A unique admissible Nash equilibrium always exists.*

Proof: In this problem, we assume (μ_1^*, μ_2^*) and (μ_1', μ_2') are the two power allocation policy pairs at the Nash equilibrium. Correspondingly, their related threshold values are (α_1^*, α_2^*) and (α_1', α_2'). They are also the solutions to the equations (3.34) and (3.35). With the consideration of monotonic properties of SNR_i, $i = 1, 2$ on α_i, $i = 1, 2$, we can find out that $\alpha_1^* = \alpha_1'$ iff $\alpha_2^* = \alpha_2'$, $\alpha_1^* > \alpha_1'$ iff $\alpha_2^* > \alpha_2'$, and $\alpha_1^* < \alpha_1'$ iff $\alpha_2^* < \alpha_2'$. Thus, under this condition, the threshold values must have a strict order. We assume that $\alpha_1^* > \alpha_1'$, $\alpha_2^* > \alpha_2'$. Then, we can demonstrate that $\mathbf{C}_1(\mu_1^*, \mu_2^*) > \mathbf{C}_1(\mu_1', \mu_2')$ and $\mathbf{C}_2(\mu_1^*, \mu_2^*) > \mathbf{C}_2(\mu_1', \mu_2')$

by considering the corresponding unique power policies (μ_1^*, μ_2^*) and (μ_1', μ_2'). When we consider the channel state division previously, we find out that if we decrease the threshold values, the area for $\mathbf{Z}_3$ will extend. According to (3.29), μ_1, μ_2 will increase as well in this case. Therefore, it means both users have to take more power to transmit data in the interference channel. It causes that both user see increased interference from the other user, so that $\mathbf{C}_1(\mu_1^*, \mu_2^*) > \mathbf{C}_1(\mu_1', \mu_2')$ and $\mathbf{C}_2(\mu_1^*, \mu_2^*) > \mathbf{C}_2(\mu_1', \mu_2')$.□

In the example, we choose $\text{SNR}_1 = -12.21$ dB, $\text{SNR}_2 = -16.98$ dB, $\beta_1 = 2, \beta_2 = 3$. At the Nash Equilibrium, $\alpha_1 = 0.7857, \alpha_2 = 1.0971$. $\mathbf{C}_1 = 0.1163$ bps/Hz, $\mathbf{C}_2 = 0.0501$ bps/Hz.

In Fig. 3.4, we have the plot that describes the transmission rates of the users as a function of node 1's normalized QoS exponent β_1. In previous discussion, β_i represents the normalized QoS constraint. Larger β_i indicates more strict QoS constraints which will cause the transmission rate of the related node decrease. In the figure, it is obvious that the transmission rate of node 1 decreases as β_1 increases. This illustrates that as the buffer constraint becomes more strict, the transmission rate will decrease. However, the rate of node 2 does not have much significant changes. This tells us that sacrificing one user's rate does not necessarily benefit the other user as long as both user's have complete information. In Fig. 3.5, we plot the transmission rate of the two users as SNR_1 increases while SNR_2 is kept fixed. If SNR_i increases, it means the related node allocate more power to transmit data. With more power consumed, the transmission rate should increases in this situation. It is clear that transmission rate of node 1 in Fig. 3.5 increases as SNR_1 increases. The transmission rate of node 2 does not change much. It illustrates that the transmission rate of node 2 is not affected by node 1 either.

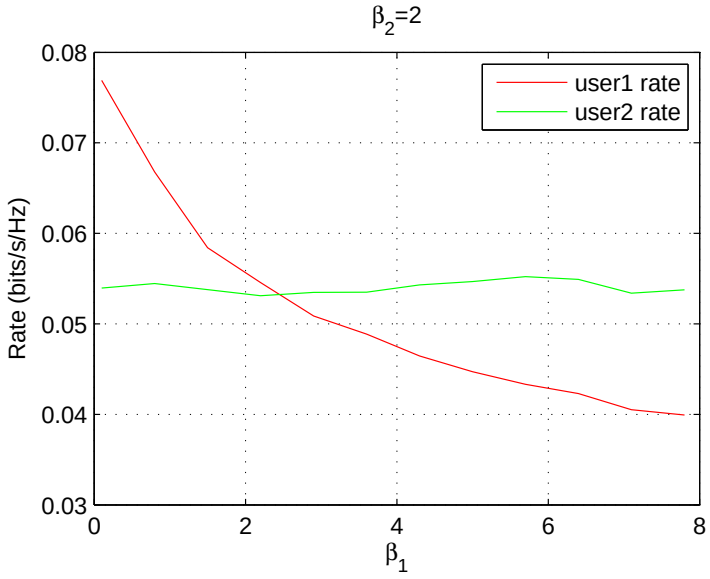

Figure 3.4: The rate of the two users as a function of β_1. $SNR_1 = SNR_2 = 0.02$ $\beta_2 = 2$

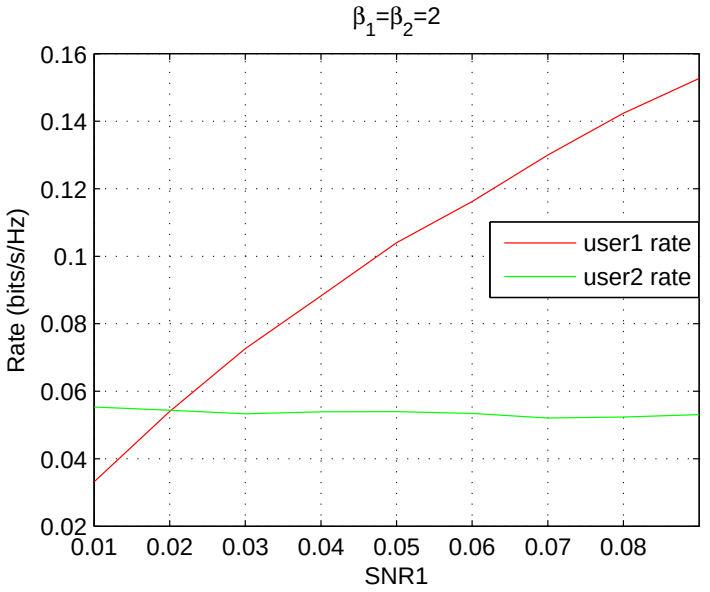

Figure 3.5: The rate of the two users as a function of SNR_1. $SNR_2 = 0.02$ $\beta_1 = \beta_2 = 2$

3.4 Conclusion

In this chapter, we have investigated a two-player non-cooperative game on interference channels under QoS constraints. We formed a 4-node communication scenario. Though a game-theoretic analysis in this situation, optimal power control policies at the Nash equilibrium are provided. We also prove that a unique admissible Nash equilibrium exists in our two-player game. Numerical results and discussions have been provided as well.

Chapter 4

Non-Cooperative Security Games for Wireless Ad Hoc Networks

In this chapter, we are going to perform a game theoretic analysis of security considerations in wireless ad hoc networks. As we introduced before, mobile ad hoc networks belong to one of the categories of wireless ad hoc networks. In mobile ad networks [33][34], such as vehicular networks [35], bluetooth network and delay tolerant networks [36], authentication is a required primitive of the majority of security protocols. Each mobile stored an asymmetric key pair and all messages it sends are signed with the same private key. However, keys are not always secure, it can be detected by external parties so that the locations and trajectory of the mobile nodes can be learned. Hence, when the nodes authenticate themselves to others, they have to avoid revealing privacy-sensitive messages. In this situation, in order to achieve high location information security in wireless ad networks, pseudonym change approach has been used. However, the privacy is not archived if only one node changes its pseudonym because the tracker can still figure out in this situation. Therefore, in this case,

location information security requires help from its neighboring mobile nodes.

Because of the above reasons, the coordination of pseudonym changes has attracted much interest and numerous methods have been proposed [37]. In [38], a base station is used to coordinate pseudonym changes with predefined network architecture. A mix zone strategy is also proposed in [35][39]. With out predefined infrastructure, mix zone strategy defines a certain region for analysis purposes at first. Then, all the mobile nodes in this region will adopt pseudonym change protocol in order to maintain its information security. However, it does not have enough flexibility because the zone location have to be learned before the node goes into the zone. Swing protocol [40] becomes a good candidate to solve this kind of issue. It will predefine a threshold for the node to make pseudonym change decision. If a node's security level is lower than the threshold, the node will change its pseudonym in order to achieve high location security. However, it still lacks flexibility to coordinate the pseudonym change of the network with multiple nodes. In this background, game theory method has been introduced to pseudonym change problem. As we mentioned in the first chapter, game theory can be divided into two categories. One is a cooperative game and the other one is the non-cooperative game. The players in cooperative game are not selfish. They are willing to cooperate with their neighbors to achieve high location security. The players in non-cooperative games are behaving selfishly. They just care about their own privacy level and they are not willing to cooperate when their neighbors try to improve their privacy level. Several papers analyze the problem in the context of cooperate games. But in the real world, every node is acting selfishly. Therefore, non-cooperative game is more realistic. Julien Freudiger is the first one to investigate the game theoretic aspects of location privacy in mobile net-

works [41][42][43]. He also analyzed several cases with non-cooperative game approach. However, its approach has some issue to achieve the privacy with small number of players.

In this case, we propose a game theory based anti-tracking protocol. Each node tries to change its pseudonym based on its own payoff and the prediction of its neighbor. In order to solve the problem for small number of players, we use a bluffing strategy to mess up its own trajectory so that the tracker cannot follow the mobile users. In order to make the protocol work well in the real world, we consider a non-cooperative game scenario and the players do not want their neighbors to know their types.

4.1 Preliminary Work

4.1.1 System Model

For this system, the network that we are focusing on is equipped with WiFi or Bluetooth device [39]. Thus, the users can communicate with each other in a certain range such as the vehicular network or a network communicated by hand-held device directly.

In these networks, we will introduce a trusted third party into the network. It will run an off-line certification authority and load the credentials for all the mobile nodes in the networks. Every node should register with the certification authority that preloads a set of public /private key pairs before it connects with the network. The public key is considered as the ID of each node and can be referred as its pseudonym.

The system that we are considering for this anti-tracking protocol is a dis-

crete time system. At each time step t, the mobile nodes are moving into the network and exchange information immediately after they can connect with each other in the transmission range. The users in this system will also automatically send preamble signal every certain amount of distance or time. The information it sends will include a lot of information such as its authentication information, the time it sends this information, the position and the speed in vehicle network. After sending this signal, it will discover their neighbors. When another node receives this signal, it will control the legitimacy of the sender and then verify the signature of its received message.

The other important part for anti-tracking is the adversary. It will eavesdrop communications between mobile nodes in order to track their locations. The effect of adversary depends on many factors like its coverage range and the location. If the adversary has full coverage of the entire network, it is able to track every mobile node and no node can easily get rid of it. Usually, the adversary collects identifying information and location information from the entire network in order to track the location of mobile nodes. With that location information, the adversary can also run a tracking algorithm to track the trajectory of the mobile nodes in order to get a more accurate result.

4.2 Location Security

In this section, we are going to introduce a location security model which can illustrate the various security levels over time.

4.2.1 Mix Zone and Security Level

There are several methods used for protecting the mobile node's privacy so that the node's location information can be more secure and the node cannot be easily tracked by the adversary. In this section, we are going to discuss the pseudonym change technique. Based on the related work section, there are some limitations for the traditional method. In order to solve these limitations, several strategies will be introduced. In [39], a mix zone is introduced. The mix zone method is described as follows: a number of nodes enter in a fixed area which is named mix zone. In this specific area, the mobile nodes change the pseudonyms simultaneously. Thus, the tracker cannot link the new pseudonym with the old ones. However, it still has an problem regarding the time and location correlation tracking. Therefore, we bring two more strategies to compensate the original mix zone approach. First, mobile nodes can turn off their transceiver making the mix zone a confusing point. Second, mobile nodes can use a bluffing strategy to mess up the trajectory in order to keep the security at a certain level.

Consider a mobile network with n mobile nodes. Like the swing protocol mentioned in [40], once a group of nodes come into the mix zone at time t, one node can initiate the pseudonym change process by broadcasting a trigger message. If mobile node A has complete information of its neighbor, opponents around A will choose its move by estimating type and distance with its neighbor. If the opponents around A are all cooperative, all nodes including A will change pseudonym simultaneously. If the type of nodes around A are defect, A will measure the distance between itself and its neighbor. If the measured distance is less than a specific threshold, A will choose bluffing strategy. If the

measured distance is larger than the threshold, A will shut off its transceiver and consider its next move for a while. During this time, nodes cannot communicate with other nodes. At the end of this time gap, all nodes make their decisions about pseudonym change at the same time. If the node A does not know the type of its opponent, it will change pseudonym by predicting its opponent's type. Then for bluffing strategy, if the total number of players in the mix zone is less than 4, we will measure the distance and mess up the trajectory. The traditional pseudonym change approach does not work quite well for a small number of nodes because its opponents have higher probability to show a defect type and even if its opponent is cooperative, its security level is still pretty low. It makes us have the motivation to pull up the privacy level for a small number of players.

From the adversary's perspective, adversary will notice mobile nodes changing pseudonyms in its covered area, if pseudonym change happens. It will compare the pseudonym before and after the change and then predict the matching with highest match possibility. The location security level of a user i involved in a successful pseudonym change at time T is

$$H_i(T) = -\sum_{d=1}^{n(T)} p_{d|b} log_2(p_{d|b}) \tag{4.1}$$

where H is the security level of user i. T is the time that pseudonym of user i has been changed successfully. $p_{d|b}$ is the probability that a new pseudonym d correspond to an old pseudonym b. $n(T)$ is the number of mobile nodes at time T. Both the number of nodes and the unpredictability of their whereabouts in the mix zone determines the achievable location privacy. If there is only one node i changing pseudonym, the tracker will easily find out so the privacy

level of user i is defined to be $H_i(T) = 0$. If we use the uniform probability distribution for $p_{d|b}$, the entropy will get a maximum value and we can use $log_2(n(T))$ as the security level of mobile node i.

4.2.2 Security Level Loss

In practice, the security level of mobile nodes changes based on location and time. Therefore, we are going to use a model related to location security change feature to analyze our system. In this work, since the security level will change over time, the security loss function $\beta_i(t, T_i^l)$ is introduced, where t is the current time and T_i^l is the time of the last successful pseudonym change of node i. For a given T_i^l, we can have:

$$\beta_i(t, T_i^l) = \begin{cases} \lambda * (t - T_i^l) & \text{for } \; T_i^l \leq t \leq T_i^f \\ H_i(T_i^l) & \text{for } \; T_i^l \leq t \end{cases} \tag{4.2}$$

where λ is the belief of node i about the tracking power of the adversary. λ determines how fast the rate of privacy loss increases. We can find that the maximum value of $\beta_i(t, T_i^l)$ equals the location security level at the time that last pseudonym changes. So with this loss function the user centric security level of node i at time t is:

$$H_i(t) = H_i(T_i^l) - \beta_i(t, T_i^l) \;\; t \geq T_i^l. \tag{4.3}$$

4.3 Anti-Tracking Game

In this section, we discuss the non-cooperative game theoretic aspects of achieving high location security level by changing multiple pseudonyms. The idea of the pseudonym change game is how to make a reasonable decision like pseudonym change or bluffing while considering location security level and cost of related nodes.

The reason for us to build a pseudonym change game is the high cost of requesting new pseudonym. If we use an equation to describe the cost, it can be expressed as $\gamma = \gamma_{acq} + \gamma_{rte} + \gamma_{sil}$ where γ_{acq} is the cost of acquiring new pseudonym, γ_{rte} is the cost of updating routing table and γ_{sil} is the cost of remaining silent. Since every node is considered as a selfish player in a noncooperative game, its own behavior may sabotage the achievable location security.

On the other hand, since the node's behavior is selfish, nodes have incentive to change pseudonym when the value of security level is too low in order to maintain location privacy. Therefore, in this game-theory-based protocol design, we will investigate how a mobile node changes its privacy level dynamically with the consideration of its neighbor nodes' type, its own cost and security level. We will also investigate the requirement for coordinated pseudonym change game. In this game, the goal of nodes is to try to maximize their payoff based on their current location security level and the associated pseudonym change cost.

4.3.1 Game Theory Concept

In this section, we discuss the concept of game theory [18] for our application. As we introduced in chapter 1, game theory is a branch of applied mathematics that is used in the social sciences, most notably in economics, as well as in biology (particularly evolutionary biology and ecology), engineering, political science, international relations, computer science, and philosophy. Game theory attempts to mathematically capture behavior in strategic situations, or games, in which an individual's success in making choices depends on the choices of others. The game we consider in this chapter is a non-cooperative game. It can also be divided into two categories: a complete information game and an incomplete information game.

In a complete information game, a node knows the types of its opponent. A pure strategy for player i is $s_i \in S_i$, where $S_i = \{C, D\}$ is the pure strategy space. A strategy profile $s = \{s_i\}_{i=1}^{n}$ is the players' strategy set. Based on the previous introduction about Nash equilibrium, if two strategies are mutual best responses to each other, no player is willing to deviate from the given strategy as long as they have mutual best responses. The concept of Nash Equilibrium in this game can be defined as

Definition 1 *A strategy profile s^* is a Nash equilibrium if, for each player i:*

$$\varphi_i(s_i^*, s_{-i}^*) \geq \varphi_i(s_i, s_{-i}^*) \quad \forall s_i \in S_i \tag{4.4}$$

In other words, in a NE, none of the players can unilaterally change its strategy to increase its payoff.

In an incomplete information game, a node does not have information about

its opponent's type. Thus, we adopt the concept of Bayesian Nash equilibrium. In this case, since we do not know the type of its opponent, a common probability distribution $f(\theta_i)$ is assigned to player in order to identify the player's type. After the type is assigned to players, the game is transformed from a incomplete information game to a complete information game and all nodes decides their payoff and next move based on their type. For this anti-tracking protocol, since nodes have no idea about their opponent's information, it is the same case as the incomplete information game.

4.3.2 Game Model

Game theory is a very good tool to model the conflict and predict the behavior of participants. In our anti-tracking protocol, we are setting up a pseudonym change game. For this game, we assume the number of every node's opponent is greater than zero because the security level is zero if there is no opponent. We also assume each node has the ability to search its neighbor nodes [44] and find out the number of other nodes in the mix zone. The strategy is another important thing that is used to form a game. In our game, each player has two possible moves: Cooperate and Defect. By cooperating, a mobile node change its pseudonym. By defecting, a mobile node retains its pseudonym. As another important piece to form a game, the payoff function can be built as $\varphi_i(t) = b_i(t) - c_i(t)$, where $b_i(t)$ can be expressed as the location security level of node i at time t, whereas the cost $c_i(t)$ depends on the security level loss function and the updating cost of pseudonym at time t. We provide an example which is shown in the Figs. 4.1 and 4.2 to make the whole game process more clear.

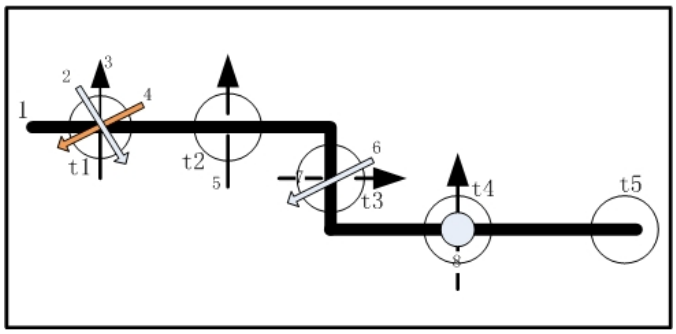

Figure 4.1: 8 players attends the game.

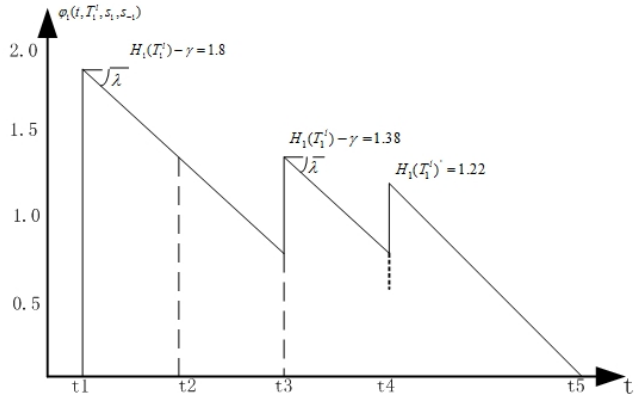

Figure 4.2: change of the payoff of node 1 over time.

Fig. 4.1 is an example of 8 mobile nodes moving on a plane. The Fig. 4.2 shows the updating of the payoff of node 1 over time. The black line in Fig. 4.1 is the trajectory of node 1. At time $t1$, from Fig. 4.1, we see that node 2,3 and 4 meet in a mix zone and cooperate with node 1. In this case, every node will change their pseudonym at time t_1 in the Fig. 4.2 and their payoff function values are updated:$\varphi_i = H_i(T_i^l) - \gamma = log_2(4) - \gamma = 1.8$ and $T_i^l = t_1$. At time t_2, node 1 meets node 5 in the mix zone but node 1 is a defect type player at that time so node 1 does not do anything and the payoff of node 1 keeps decreasing according to the loss function β_1 with slope λ. At time t_3, node 1 meets two cooperative nodes 6 and 7. Therefore, the payoff function value increases again by increasing its security level. At time t_4, the node 1 meets node 8 but node 8 is a defect type player and node 1 is a cooperative type at this time. Hence, we have two cases: one case is that node 1 wastes one pseudonym and the privacy level is dropped by γ. In the other case, the payoff function will be pulled up a little bit by using the bluffing strategy. We will describe this case more specifically in the next section. At time t_5, there is no other node staying in the mix zone so the payoff function goes down to zero.

4.3.3 Bluffing Strategy

Since we already have a general idea about our game model, we start to focus on some specific issue. In the Fig. 4.2, we find that at time t_4, the node 1 will meet a defect type player. It means that if node 1 does not have some special move, it will change its pseudonym without increasing its privacy level. In this case, we propose a bluffing strategy to improve its anti-tracking performance.

The bluffing strategy is an approach that is similar to the path perturbation

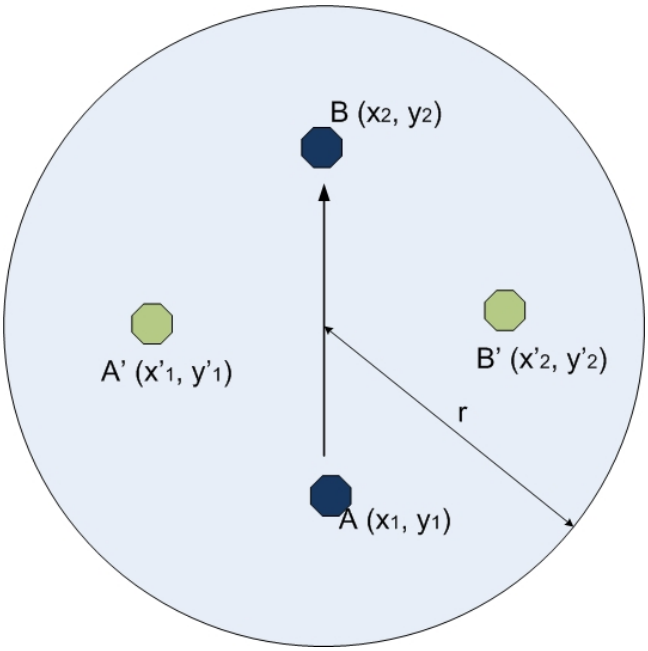

Figure 4.3: Trajectory perturbation region.

[45][46]. It requests the node to measure the distance between itself and its opponent. If the distance $L \leq \epsilon$, where ϵ is a predefined parameter and it is equal to d_1 in the Fig. 4.3, it will recreate a smaller mix zone. And the node do not change the pseudonym. It reports location information as mix zone region but not the actual location of the users. In order to make the tracker hard to follow the trajectory, we can try to generate some noise to mess up the trajectory.

We need to add random variables x′ and y′ to the location information x,y of the node. In order to make the path perturbation reasonable, noise have to be close to the original point and could not be further than r. Thus, we have to make sure $(x - x')^2 + (y - y')^2 < r^2$. The noise available area is shown in the

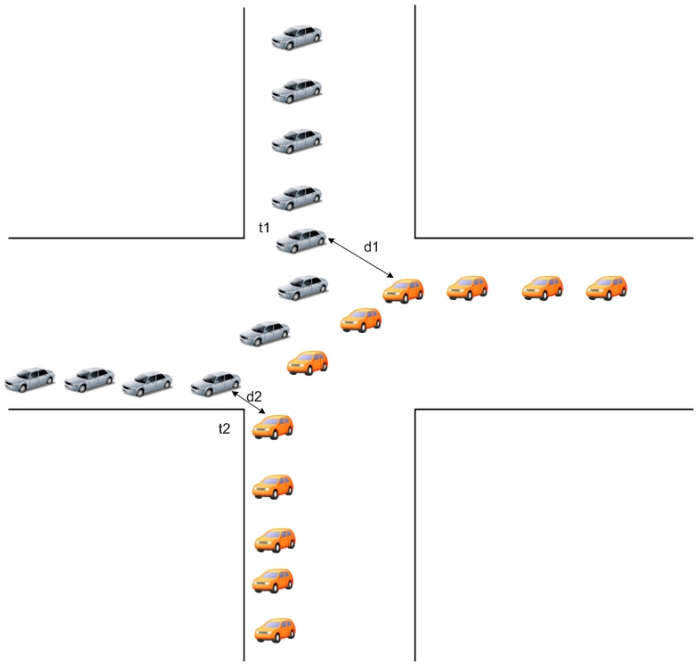

Figure 4.4: Trajectory perturbation example (before).

Fig. 4.3.

This strategy focuses on small number of nodes in our game model because it's not possible to have a lot of users staying in a small region. It's also better to choose changing pseudonym with a lot of users because the probability to have a lot of cooperative players is increasing so that it can reach a very high security level compared to its high cost. For complete information game, the node knows its opponent's type and payoff function, it can directly choose bluffing strategy when its opponents are all defect type. For our anti-tracking game, since it's an incomplete information game, the node will use bluffing strategy when the number of its opponents is less than 3. In this case, even if the user successfully change its pseudonym, the privacy level is not quite

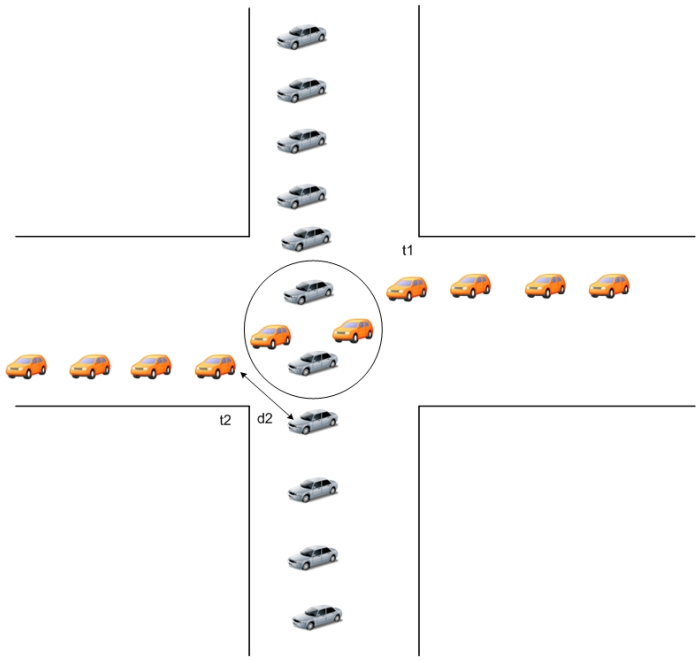

Figure 4.5: Trajectory perturbation example (after).

high. So we choose this strategy to avoid the risk of exposure. After the node chooses to use bluffing strategy, it does not change its pseudonym but it acts like it has already changed its pseudonym by making the tracker follow the other trajectory. The payoff function for this case will not be the original one. If there are n players staying in the smaller mix zone, it means that tracker has $1/n$ chance to guess the right trajectory and find out it did not change its pseudonym. Therefore, the location security level in this case will be the average privacy level $E(H_{i,n}(t))$.

4.3.4 The Payoff Function

In this game model, if more than 3 nodes are willing to change the pseudonym, then each of these three nodes improves its location security level at the cost of a pseudonym change γ. If 3 or less number of nodes are participating in the game, they either use the bluffing strategy or change their pseudonym anyway despite the risk of wasting the pseudonym. Formally, we have: If $(L > \epsilon)\&(s_i = C)\&(n_C(s_{-i}) > 0)$

$$T_i^l = t \tag{4.5}$$

$$w_i(t, T_i^l) = 0 \tag{4.6}$$

$$\varphi_i(t, T_i^l, C, s_i) = max(H_i(T_i^l) - \gamma, \varphi_i^- - \gamma) \tag{4.7}$$

If $(L > \epsilon)\&(s_i = C)\&(n_C(s_{-i}) = 0)$

$$\varphi_i(t, T_i^l, C, s_i) = max(0, \varphi_i^- - \gamma) \tag{4.8}$$

$$w_i(t, T_i^l) = w_i(t, T_i^l) + 1 \tag{4.9}$$

If $(L \leq \epsilon)\&(s_i = C)\&(n_C(s_{-i}) = 0)$

$$\varphi_i(t, T_i^l, C, s_i) = max(\varphi_{i,\epsilon}^- - \gamma_\epsilon, \varphi_i^- - \gamma) \tag{4.10}$$

If $(s_i = D)$

$$\varphi_i(t, T_i^l, C, s_i) = max(0, \varphi_i^-) \tag{4.11}$$

where $\varphi_i^- = H_i(T_i^l) - \beta_i(t, T_i^l) - \gamma w_i(t, T_i^l) - \gamma$ is the payoff function at time t^-, which is the time immediately prior to t. $\varphi_{i,\epsilon}^- = E(H_i(T_i^l)) - \beta_i(t, T_i^l) - \gamma_\epsilon$ is the payoff function for bluffing strategy, where γ_ϵ is the cost of adding noise to its location information.

Based on the previous discussion, we can represent the static pseudonym change game in normal form ($L > \epsilon$) in Table 4.1.

Table 4.1: Pseudonym change game in normal form ($L > \epsilon$).

P_1/P_2	C	D
C	$(H_1(T_1^l) - \gamma, H_2(T_2^l) - \gamma)$	$(\varphi_1^- - \gamma, \varphi_2^-)$
D	$(\varphi_1^-, \varphi_2^- - \gamma)$	$(\varphi_1^-, \varphi_2^-)$

Then we can find out that, for different type of players, we can get different payoff function results. This tells us that the player type prediction is the key to solve this kind of incomplete opponent's information game.

4.4 Player Type Prediction

In this section, the game we are discussing is the incomplete information game. In this case, the players do not know the payoff functions and the types of its opponent. It is very close to the real world practical model. Therefore, our anti-tracking protocol is built based on the incomplete information game.

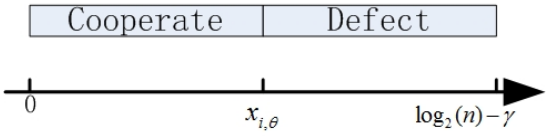

Figure 4.6: Description of the threshold.

4.4.1 Threshold Concept

In a complete information game, a player knows its opponent's type and payoff function so it can decide its own payoff function based on the knowledge of its opponent. In an incomplete information game, a player does not know its opponent's type and payoff function. Therefore, it decides its move based on its belief about their opponent's type. The player's type is defined as: $x_i = H_i - \beta_i - \gamma w_i - \gamma$, which defines the payoff immediately before the game. In order to define the player's type for incomplete information game, we predefine a strategy related threshold [14]. A player behaves defect, if the evaluated type of a player is above a threshold $x_{\theta,i}$, otherwise it cooperates. It can be shown in Fig. 4.6. With this threshold, we can define the probability of cooperation of node i as

$$F(x_{\theta,i}) = P(x \leq x_{\theta,i}) = \int_0^{x_{\theta,i}} f(x_i)dx_i. \tag{4.12}$$

Hence, $1 - F(x_{\theta,i})$ is the probability of defection.

4.4.2 Two Player Game

Let's consider a two-player game analysis as a starting point. In this game, each player computes the probability distribution function $f(x_i)$ in order to decide other node's type. Then, we can use a fixed threshold associated with threshold $x_{\theta,2}$ for player 2, and compute the average payoff to player 1 for cooperative move (C) and defect move (D) based on given type $x_{\theta,1}$.

$$E[\varphi_1(C, s_2)|x_1] = F(x_{\theta,2})(1-\gamma) + (1 - F(x_{\theta,2})) * max(0, (x_1 - \gamma)) \tag{4.13}$$

$$E[\varphi_1(D, s_2)|x_1] = x_1 \tag{4.14}$$

The average payoff for player 2 is similar to the one for player 1.

The key for deciding the players' type is computing the threshold strategy which is also considered as Bayesian Nash Equilibrium by determining the boundary of cooperative and defect activity. Therefore, let's consider the equation $E[\varphi_1(C, s_2^*)|x_{\theta_1}^*] = E[\varphi_1(D, s_2^*)|x_{\theta_1}^*]$ for each player i. By solving this equation we can derive the definition of the Bayesian Nash Equilibrium [43] of two players in incomplete information game.

Lemma 1 *If*

$$\begin{cases} E[\varphi_1(C, s_2^*)|x_{\theta_1}^*] = E[\varphi_1(D, s_2^*)|x_{\theta_1}^*] \\ E[\varphi_2(C, s_1^*)|x_{\theta_2}^*] = E[\varphi_2(D, s_1^*)|x_{\theta_2}^*] \end{cases}, \tag{4.15}$$

a Bayesian Nash equilibrium $s^* = (x_{\theta_1}^*, x_{\theta_2}^*)$ of the 2 player incomplete information pseudonym change game is existed.

Proof 1 *Since we have* $E[\varphi_1(C, s_2^*)|x_{\theta_1}^*] = E[\varphi_1(D, s_2^*)|x_{\theta_1}^*]$*, we can fix user2's strategy and consider player1 as* $x_{\theta,1} \leq x_{\theta_1}^*$*. Hence, we can have* $E[\varphi_1(D, s_2^*)|x_{\theta_1}^*] - E[\varphi_1(D, s_2^*)|x_{\theta,1}] = x_{\theta_1}^* - x_{\theta,1} \geq (1 - F(x_{\theta,2}))(x_{\theta_1}^* - x_{\theta,1}) = E[\varphi_1(C, s_2^*)|x_{\theta_1}^*] - E[\varphi_1(C, s_2^*)|x_{\theta,1}]$*. Based on the above inequality, we can find out that if* $x_{\theta,1} \leq x_{\theta_1}^*$ *the drop in payoff of D is larger than the drop in payoff of C. Therefore, C is the best response. Similarly, we can get that if* $x_{\theta,1} > x_{\theta_1}^*$*, then* $E[\varphi_1(D, s_2^*)|x_{\theta_1}^*] - E[\varphi_1(D, s_2^*)|x_{\theta,1}] \geq E[\varphi_1(C, s_2^*)|x_{\theta,1}] - E[\varphi_1(C, s_2^*)|x_{\theta_1}^*]$*. So the increase in payoff of D is greater than the increase in payoff of C. The best response should be D in this case.*

Theorem 1 *All cooperate and all defect pure strategy Bayesian Nash equilibrium* $s^* = (x_{\theta_1}^*, x_{\theta_2}^*)$ *exists in the 2 player incomplete information pseudonym change game.*

Proof 2 *For all defection BNE which is* $x_{\theta_1}^* = x_{\theta_1}^* = 0$*, we can find out that* $E[\varphi_1(C, s_2^*)|x_{\theta_1}^* = 0] = 0 = E[\varphi_1(D, s_2^*)|x_{\theta_1}^* = 0]$*. Similarly, for all cooperation BNE which is* $x_{\theta_1}^* = x_{\theta_1}^* = 1 - \gamma$*, we have* $F(x_{\theta_1}^*) = F(x_{\theta_2}^*) = 1$*. Then* $E[\varphi_1(C, s_2^*)|x_{\theta_1}^* = 1 - \gamma] = 1 - \gamma = E[\varphi_1(D, s_2^*)|x_{\theta_1}^* = 1 - \gamma]$*. Therefore, we prove that we have all cooperation and all defection BNE.*

Other than all cooperate and all defect BNE, we can also find an intermediate threshold equilibrium under different conditions, where a player will not only show cooperative activity or defect activity at this point.

Let's consider an example to illustrate this incomplete information game. Consider that the distribution on types is uniform. We can have the cumulative probability as $F(x_i) = x_i/(1 - \gamma)$. Looking for an equilibrium with a threshold $x_{\theta,i} \geq \gamma$ and solving equation (4.15), we can obtain $x_{\theta,i} = 1 - (\gamma/F(x_{\theta,-i}))$ and $x_{\theta,i}^2 - x_{\theta,i} + \gamma(1 - \gamma) = 0$. From these two equations, we can get $x_{\theta_i}^* \in \{\gamma, 1 - \gamma\}$. We still assume $\gamma < 0.5$ because it will make the payoff function always larger

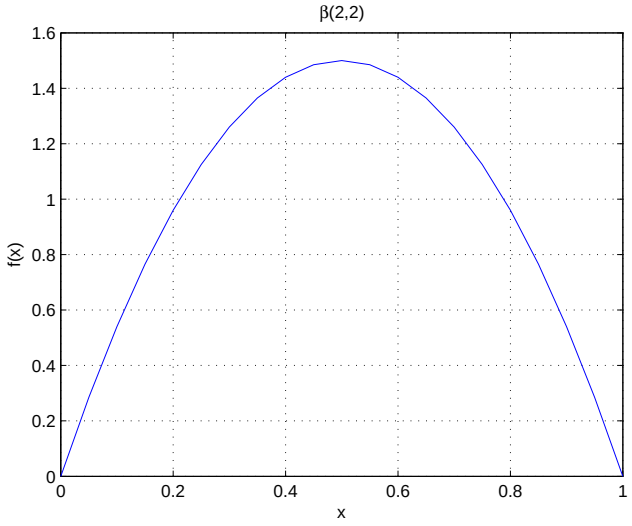

Figure 4.7: pdf of $\beta(2,2)$.

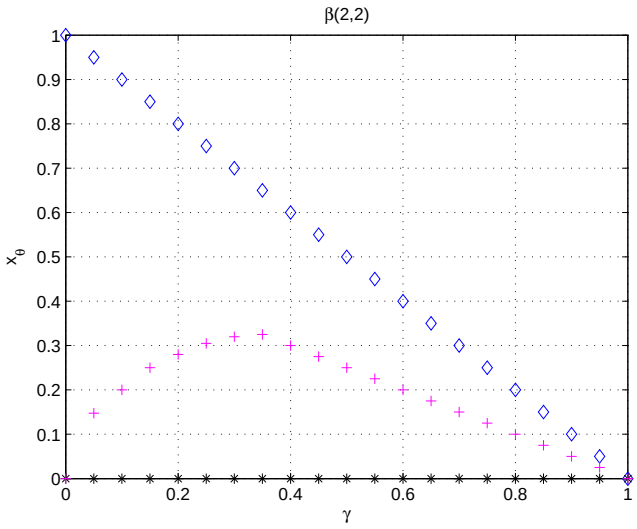

Figure 4.8: BNE based on increasing cost.

than 0 for the two player game. Then if $F(x_{\theta,-i}) \to 1$, the solution $x^*_{\theta_i} = 1-\gamma$ corresponds to an all cooperation BNE. If we take a look at intermediate equilibrium, we can have $E[\varphi_1(C,s_2)|x_1] = F(x_{\theta,2})(1-\gamma) + (1-F(x_{\theta,2})) * 0 = x^*_{\theta_2} = x^*_{\theta_1}$. Hence, we can confirm that C is the best response for $x_{\theta,1} > x^*_{\theta_1}$. D is the best response for $x_{\theta,1} < x^*_{\theta_1}$.

Then we can numerically solve those equations based on different probability distributions such as β distribution. In this case, we can see that the equilibrium changes based on different probability distribution value. If $x \sim \beta(2,2)$, x is symmetric and centralized around 0.5. For this distribution, we can obtain 3 BNE: all cooperate (blue), all defect(black) and intermediate equilibrium(pink curve in the middle) and it is shown in the Fig. 4.8. Let's focus on the intermediate equilibrium which is the solution for threshold. As the cost γ increases, the probability of cooperation $F(x^*_\theta)$ increases as well. It means that the probability for a player to cooperate is increasing when cost is increasing. In other words, if the cost is small, the nodes will become selfish. They do not quite care about the whole cooperation success.

4.4.3 n Players Game

In this case, we change the number of game players from 2 to N. The idea is still trying to compute the average payoff function. Let $P(K=k)$ be the probability that k nodes cooperate. We can get the following average payoff function as:

$$E[\varphi_i(C,s_{-i})] = \sum_{k=0}^{n-1} P(K=k)\varphi_i(C,s_{-i}) \tag{4.16}$$

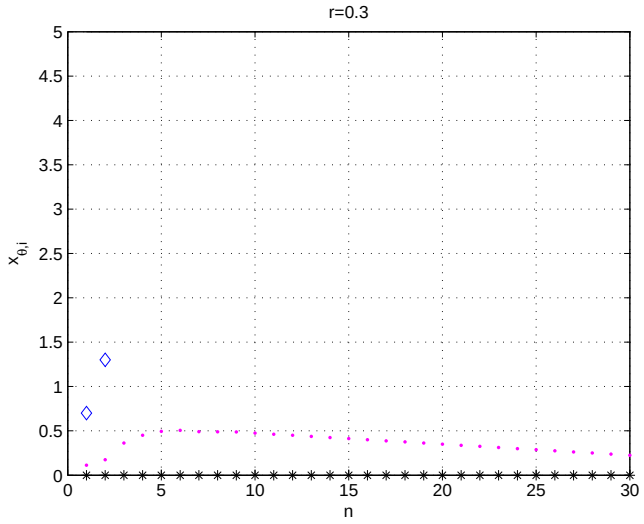

Figure 4.9: BNE based on increasing number of users ($\gamma = 0.3$).

$$E[\varphi_i(D, s_{-i})] = \varphi_i^- \tag{4.17}$$

where φ_i^- is the payoff function immediately before the pseudonym change happens. Similar to the two player game, a BNE can be obtained as the solution to the following system of **n** non-linear equations for the **n** variables $x_{\theta,i}$:

$$\sum_{k=0}^{n-1} P(K = k)\varphi_i(C, s_{-i}) = \varphi_i^-, \quad i = 1, 2, ..., n \tag{4.18}$$

where $P(K = k) = C_n^k p^k (1-p)^{n-k}$ and $p_i = F(x_{\theta,i})$. If $p \to 0$, then $x_{\theta,i}^* = 0$, $P(K > 0) = 0$ and $P(K = 0) = 1$. This means that the all defect equilibrium exists. If $p \to 1$, then $x_{\theta,i}^* = 1$, $P(K < n-1) = 0$ and $P(K = n-1) = 1$. This means that all cooperation equilibrium exists when $log_2(n) - \gamma > \varphi_i^-$ for all node i.

For intermediate values of p, we still numerically calculate the result. It is also shown in the Figs. 4.9 and 4.10. We still use β function to evaluate

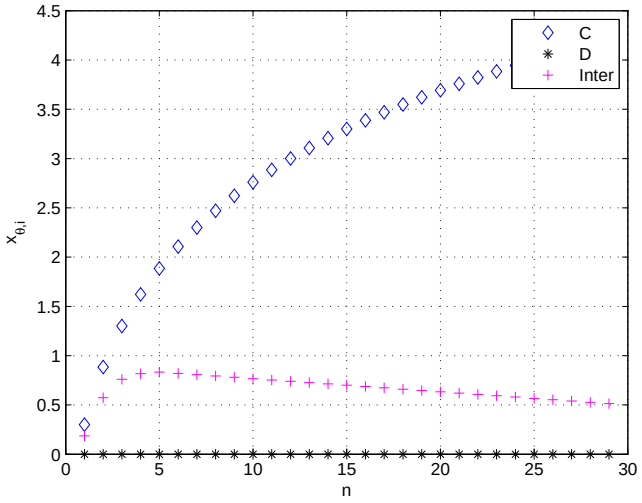

Figure 4.10: BNE based on increasing number of users ($\gamma = 0.7$).

the BNE. For $\gamma = 0.3$, with a large number of players $\mathbf{n}$, intermediate BNE decreases, meaning that players cooperate with less possibility. It also shows that all cooperate BNE disappears when the number of players increases. With cost $\gamma = 0.7$, we can find out all cooperation equilibrium lasts longer when γ increases. It looks like when the cost increases, the nodes have incentive to cooperate with others. With lower cost, the larger $\mathbf{n}$ makes the nodes not cooperate.

4.5 Anti-Tracking Protocol

As we discussed before, mobile nodes can execute pseudonym change using swing protocol. Therefore, our anti-tracking protocol is also built on this swing protocol but we need to consider more details. In the swing protocol, the decision of mobile nodes depends on their privacy level compared to a fixed threshold. In our case, the cost and probability of its opponent's type have

been considered. Hence, it changes from fix decision game to a dynamic non cooperation game. We can develop much more realistic protocol than swing protocol.

For a vehicle network, the car in the network has different speed and direction. It is a small challenge to coordinate all the mobile nodes. Therefore, we assume the mobile nodes will move into the mix zone with a speed range so that the car did not leave the zone so quickly without finishing the whole process.

We assume that the node knows the probability distribution $f(x)$, number of its opponents and its location privacy level φ_i^-

1: if (the speed is in the speed range) & (at least one neighbor) then

2: Broadcast initiation information to ask for changing pseudonym.

3: Go to 6

4: else

5: if (received initiation information) then

6: n=estimate(n)

7: calculate the BNE threshold $x^*_{\theta,i}$ as a solution of

7: $\sum_{k=0}^{n-1} P(K=k)\varphi_i(C, s_{-i}) = \varphi_i^-$ where $P(K=k) = C_n^k p^k (1-p)^{n-k}$ and $p_i = F(x_{\theta,i})$

8: if ($\varphi_i^- \leq x^*_{\theta,i}$) then

9: play Cooperation

10: if (distance $L < \epsilon$ & $n < 4$)then

11: keep pseudonym, adding noise, reporting the zone location and update φ_i^-

12: else if(distance $L > \epsilon$)

13: change pseudonym, keep speed in the range

14: else

14: change pseudonym, keep speed in the range

15: else

16: play Defect

17: else

18: keep pseudonym

4.6 Conclusion

We have considered a selfish environment in a vehicular network. In order to get rid of the tracker, the mobile node changes its pseudonym. In this case, every node changes its pseudonym by evaluating its own payoff function and predicting its opponent's type. We propose an anti-tracking protocol based on a game-theoretic model. The game can be analyzed based on opponent's complete information and opponent's incomplete information. In our case, the opponent's incomplete information game is more realistic. Hence, we first analyze 2 player case to get the BNE and then expand this conclusion to multiple-user situation. We use bluffing strategy to improve the low location security level issues for small number of mobile nodes. We analyze the equilibrium and find that when the cost increases the mobile nodes cooperate more. If the cost is very small, the larger number of nodes will encourage nodes not to cooperate. In the future work, we can consider the place and coverage range of the adversary into this game and make the game more realistic. We can also use a Kalman filter tracking algorithm to test if our anti-tracking protocol works well.

Bibliography

[1] C. K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*. Prentice Hall, 2001. 1.1

[2] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005. 1.1, 1.2

[3] Y. Yi, M. Gerla, and T. Kwon, "Efficient flooding in ad hoc networks using on-demand (passive) cluster formation," in *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2002. 1.1

[4] C. Ho, K. Obraczka, G. Tsudik, and K. Viswanath, "Flooding for reliable multicast in multi-hop ad hoc networks," in *Proceedings of the International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communication (DIALM)*, 1999. 1.1

[5] S. A., G. D.L., and L. J.N, "Cooperative communications in mobile ad hoc networks," *IEEE Signal Processing Magazine*, 2006. 1.1

[6] I. Stojmenovic, *Handbook of Wireless Networks and Mobile Computing*. Wiley-Interscience Publication, 2002. 1.1

[7] T. Kosch, C. Adler, S. Eichler, C. Schroth, and M. Strassberger, "The scalability problem of vehicular ad hoc networks and how to solve it," *Wireless Communications, IEEE*, vol. 13(5), 2006. 1.1

[8] K. Saravanan, A. Thangavelu, and K. Rameshbabu, "A middleware architectural framework for vehicular safety over vanet (invanet)," in *Networks and Communications. NETCOM '09*, 2009. 1.1

[9] S. Lim, W.-C. Lee, G. Cao, and C. Das, "Performance comparison of cache invalidation strategies for internet-based mobile ad hoc networks," in *Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference*, 2004. 1.1

[10] S. Chen, L. P, D.-W. Huang, and S.-R. Yang, "A study on distributed/centralized scheduling for wireless mesh network," in *Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing*, 2006. 1.1

[11] R. Yates, "A framework for uplink power control in cellular radio systems," *Selected Areas in Communications, IEEE Journal*, vol. 13(7), 1995. 1.2

[12] L. Zhou and Z. Haas, "Securing ad hoc networks," *Network, IEEE*, vol. 13(6), 1999. 1.2

[13] K. Leyton-Brown and Y. Shoham, *Essentials of Game Theory: A Concise, Multidisciplinary Introduction*. Morgan and Claypool Publishers series, 2008. 2.1, 2.1.1, 2.1.2

[14] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991. 2.1, 4.4.1

[15] M. J. Osborne, *An introduction to game theory*. Oxford University Press, 2004. 2.1

[16] Y. Xiao, X. Shan, and Y. Ren, "Game theory models for ieee 802.11 dcf in wireless ad hoc networks," *Communications Magazine, IEEE*, vol. 43(3), 2005. 2.1

[17] T. Driessen, *Cooperative Games, Solutions and Applications*. Kluwer Academic Publishers, 1988. 2.1.1

[18] J. Nash, "Non-cooperative games," *Annals of Mathematics*, vol. 54(2), 1951. 2.1.2, 4.3.1

[19] V. N. Srivastava, J. Mackenzie, A. Menon, R. Dasilva, L. Hicks, J. Reed, J. Gilles, and R.P., "Using game theory to analyze wireless ad hoc networks," *Communications Surveys and Tutorials, IEEE*, vol. 7(4), 2005. 2.2

[20] A. Urpi, M. Bonuccelli, and S. Giordano, "Modeling cooperation in mobile ad hoc networks: a formal description of selfishness," in *Proc. of the 1st Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, 2003. 2.2

[21] M. Felegyhazi, J.-P. Hubaux, and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," in *Mobile Computing, IEEE Transactions*, 2006. 2.2

[22] P. Michiardi and R. Molva, "A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile ad hoc networks," in *Proc. of the 1st Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, 2003. 2.2

[23] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in self-organizing ad hoc networks," *ACM Journal on Mobile Networks and Applications(MONET)*, vol. 8(5), 2003. 2.2

[24] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," in *Proc. of the 1st Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, 2003. 2.2

[25] P. Michiardi and R. Molva, "Analysis of coalition formation and cooperation strategies in mobile ad hoc networks," *Journal of Ad Hoc Networks*, vol. 3(2), 2005. 2.2

[26] W. Yu, G. Ginis, and J. M. Cioffi, "Distributed multiuser power control for digital subscriber lines," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 20(5), 2002. 3

[27] L. Lai and H. E. Gamal, "The water-filling game in fading multiple-access channels," *IEEE Trans. Inform. Theory*, vol. 54(5), 2008. 3, 3.3

[28] D. Qiao, M. Gursoy, and S. Velipasalar, "A noncooperative power control game in multiple-access fading channels with qos constraints," in *Wireless Communications and Networking Conference (WCNC)*, 2010. 3

[29] D. Tse and S. Hanly, "Multi-access fading channels–part i: Polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Trans. Inform. Theory*, vol. 44(7), 1998. 3.1

[30] D. Wu and R. Negi, "Effective capacity: a wireless link model for support of quality of service," *IEEE Trans. Wireless Communication*, vol. 2(4), 2003. 3.2

[31] J. Tang and X. Zhang, "Quality-of-service driven power and rate adaptation for multichannel communications over wireless links," *IEEE Trans Wireless Commun*, vol. 6(12), 2007. 3.2, 3.3

[32] W. Rudin, *Principles of Mathmatical Analysis. 3rd Ed*. McGraw-Hill Science/Engineering/Math, 1977. 3.3

[33] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing IEEE*, 2003. 4

[34] H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine, 46(6)*, 2008. 4

[35] T. H. L. Buttyan and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *ESAS'07 Proceedings of the 4th European conference on Security and privacy in ad-hoc and sensor networks*, 2007. 4

[36] K. Fall, "A delay-tolerant network architecture for challenged internets," in *In SIGCOMM.*, 2003. 4

[37] R. W. Cooper, *Coordination Games*. The press syndicate of the university of cambridge, UK, 1998. 4

[38] . L. Huang, K. Matsuura, H. Yamane, and K. Sezako, "Towards modeling wireless location privacy," in *In PET.*, 2005. 4

[39] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Proceedings of the Second IEEE Annual Conference*, 2004. 4, 4.1.1, 4.2.1

[40] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: User centric approaches towards maximizing location privacy," in *In WPES.*, 2006. 4, 4.2.1

[41] J. Freudiger, M. Raya, and J. Hubaux, "Self-organized anonymous authentication in mobile networks," in *In SECURECOMM.*, 2009. 4

[42] J. Freudiger, R. Shokri, and J. Hubaux, "On the optimal placement of mix zones," in *In PETS.*, 2009. 4

[43] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: a game-theoretic analysis," in *Conference on Computer and Communications Security.*, 2009. 4, 4.4.2

[44] S. Vasudevan, J. Kurose, and D. Towsley, "On neighbor discovery in wireless networks with directional antennas," in *In Infocom.*, 2005. 4.3.2

[45] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in *In SECURECOMM.*, 2005. 4.3.3

[46] Z. Le, Y. Ouyang, G. Chen, and F. Makedon, "Dynamic mix zone: location data sanitizing in assisted environments," *UNIVERSAL ACCESS IN THE INFORMATION SOCIETY*, vol. 10(2), pp. 195–205, 2004. 4.3.3

[47] Y. V. S.F. Cheng, D.M. Reeves and W. Wellman, "Notes on equilibria in symmetric games," University of Michigan Artificial Intelligence Lab, Tech. Rep., 2004.

[48] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J. Hubaux, "Mix zones for location privacy in vehicular networks," in *In WiN-ITS.*, 2007.

[49] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Wireless Communications and Networking Conference.*, 2005.

[50] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets," in *In ESAS.*, 2006.