Optimal Strategies in Jamming Resistant Uncoordinated Frequency Hopping Systems

by

Bingwen Zhang

A Thesis
Submitted to the Faculty
of the
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements for the
Degree of Master of Science
in
Electrical and Computer Engineering
by

____

May 2013

APPROVED:

____

Lifeng Lai, Assistant Professor

____

Donald R. Brown III, Associate Professor

____

Alexander Wyglinski, Associate Professor

Abstract

Uncoordinated frequency hopping (UFH) has recently emerged as an effective mechanism to defend against jamming attacks. Existing research focuses on the optimal design of the hopping pattern, which implicitly assumes that the strategy of the attacker is fixed. In practice, the attacker might adjust its strategy to maximize its damage on the communication system. In this thesis, we study the design of optimal hopping pattern (the defense strategy) as long as the optimal jamming pattern (the attack strategy). In particular, we model the dynamic between the legitimate users and the attacker as a zero sum game, and study the property of this game. We show that when the legitimate users and the jammer can access only one channel at any time, the game has a unique Nash equilibrium. In the Nash equilibrium, the legitimate users and Eve will access or jam only a subset of channels that have good channel quality. Furthermore, the better the channel, the larger the probability that Eve will jam the channel and the smaller the probability the legitimate users will access this channel. We further extend the study to multiple access multiple jamming case and characterize the Nash equilibrium. We also give numerical results to illustrate the analytical results derived in this thesis.

Acknowledgements

First and foremost, I shall greatly thank my research advisor, Dr. Lifeng Lai. He is not only a respectable and responsible person, but also provides valuable guidance and support to my research. Besides, I am grateful to him for recommending me as his PhD student. I hope I can have a very pleasant collaboration with him on my PhD life.

Thanks to my committee members, Dr. Donald R. Brown III and Dr. Alexander Wyglinski for sharing their time on my thesis and presentation.

Thanks to my senior alumnus Jun Geng, my senior alumnus Heng Zhou and Ain Ul Aisha. They give me a lot of help on my research.

Thanks to my family. My mother Ziping Zhang and my father Zhenpeng Zhang, the most important persons for me, give me life, love and whatever I want unconditionally.

The work was supported by the National Science Foundation CAREER Award under grant CCF-1318980.

Contents

List of Figures

Chapter 1

Introduction

In this chapter, we first introduce the concept, consequences and categories of jamming attacks in Section 1.1. The conventional anti-jamming method is introduced in Section 1.2. The concept of uncoordinated frequency hopping (UFH) is introduced in Section 1.3. The related work about UFH is shown and discussed in Section 1.4. In Section 1.5, we summarize the main contributions of this thesis.

1.1 Jamming

Wireless technology is becoming more and more popular [1] and is widely used by companies and individuals for important communications, such as mobile e-commerce transactions, email, and corporate data transmissions [2]. As the result, security issues become more and more important for wireless networks. This is not a trivial problem because wireless devices, including smart cellular phones and personal digital assistants (PDAs) with Internet access, were not originally designed with security as a top priority [2].

Most of wireless network security problems can be mitigated or fully addressed by changing wireless network security architectures or using more advanced cryptographic methods [3]. However, there are still some threats that can not be addressed by these methods. Jamming is an important class of such threats [3].

Due to the openness of the wireless medium, attackers can easily implement jamming attacks to inject signals into the medium. Attackers can easily observe communications between legitimate users, and then make the transmission in wireless networks fail by injecting false messages. The attackers can implement different kinds of jamming attacks [4]:

1. Constant jammer: The constant jammer continually emits a radio signal.

2. Deceptive jammer: The deceptive jammer constantly injects regular packets to the channel. So legitimate users will be deceived into believing the jammer is also a legitimate user in transmitting state.

3. Random jammer: The random jammer alternates between sleeping and jamming.

4. Reactive jammer: The reactive jammer only begins jamming when the jamming detects activity in the channel.

Reactive jamming is the most important threat among the four jammers [5]. The reason is that, while destroying the packets, the attacker minimizes its risk of being detected [5]. In frequency hopping, reactive jammer cannot complete the detection process if the hopping rate is high enough [6]. So it is can be seen that to mitigate jamming, the spread spectrum techniques are usually adopted [7].

1.2 Spread Spectrum Techniques

Spread spectrum techniques are conventional anti-jamming methods [8]. The spread spectrum signals usually have the characteristic that the bandwidth is much larger than the information rate which can be seen as redundancy. This kind of redundancy is added to the signal due to the signal is required to overcome severe interference in the process of transmission in the channel. The redundancy of the spread spectrum signal can be characterize by bandwidth expansion factor which is usually much larger than one [7]. To introduce redundancy to signal, we know that coding is an efficient method [7]. So how to code the signal to make it spread spectrum is the first key element in designing the spread spectrum systems [7].

In the security aspect, in order to avoid the attacker to demodulate the spread spectrum signals, pseudorandomness is needed [7]. The pseudorandomness of the spread spectrum signals makes the signals seem to be random noise to the attacker thus making it very difficult for the attacker to demodulate the signals [7]. This characteristic is actually related to the purpose or application of these spread spectrum signals [7].

In [7], the authors list the main purposes of the spread spectrum signals:

1. To combat the effects of interference due to jamming, interference caused by other users of the channel and self-interference due to multipath propagation.

2. To hide a signal by transmitting it at low power, thus making it difficult for an attacker to detect the signal in the presence of background noise.

3. To achieve message privacy in the presence of attackers.

4. To obtain accurate range (time delay) and range rate (velocity) measurements in radar and navigation (this purpose is not directly related to communications).

In combating the effects of interference of intentional jamming, the knowledge of the jammer is important [7]. If the jammer knows the characteristic of the transmitting signal, it is easy for the jammer to mimic this signal transmitted by the transmitter and confuse the receiver [7]. To prevent this to happen, the transmitter introduces the randomness (actually pseudorandomness) to the signal which is unpredictable for the jammer while known to the receiver. So the only way for the jammer to do jamming is to transmit an interfering signal without any prior knowledge about the pseudorandom pattern [7].

Frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), time-hopping spread spectrum (THSS), chirp spread spectrum (CSS), and combinations of these techniques are forms of spread spectrum [7]. Each of these techniques employs pseudorandom number sequences created using pseudorandom number generators to determine and control the spreading pattern of the signal across the allocated bandwidth [7].

Figure 1.1 shows the traditional frequency hopping (FH) which relies on secrets shared between the transmitter and receiver. The shared secret then determines the hopping pattern in FH. A third party who does not know the secret codes cannot predict the transmission [9]. Then the probability of the transmission being jammed is reduced [9]. But the prerequisite is a secret must be shared by the transmitter and the receiver [9].

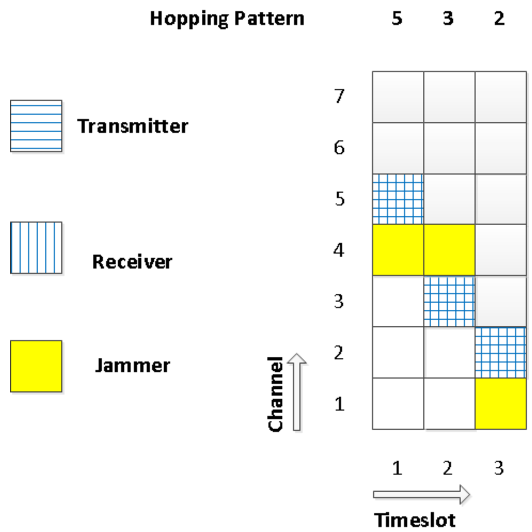

Figure 1.1: Frequency hopping.

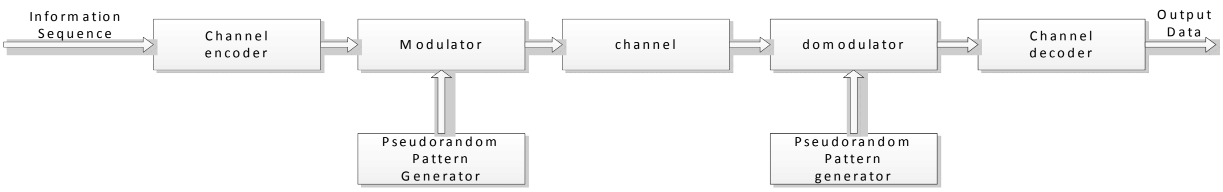

Figure 1.2: Model of spread spectrum system.

Figure 1.2 shows the model of spread spectrum. Notice that we should have two identical pseudorandom pattern generators, one at each side. In practice, we require the transmitter and receiver have the same pattern and we should have the pseudorandom pattern generator perfectly synchronized [7]. The problem arises that if two nodes which have not communicated before but want to communicate in the presence of jammer, the pseudorandom pattern cannot be known by the other side [9]. If we want the pattern to be pre-stored in each node in the network, scalability is a big issue [9]. If the network has N nodes, then for each of them to communicate with other nodes, $N-1$ pairs of pre-shared secrets are needed for each node. The total number of pre-shared secrets in this network is $\frac{N(N-1)}{2}$. If N is large, it is challenging to pre-distribute and further store $N-1$ pairs of secrets for each node. In this context, the uncoordinated frequency hopping discussed below is proposed in [9] to solve this problem.

1.3 Uncoordinated Frequency Hopping(UFH)

The uncoordinated frequency hopping (UFH) to solve the problem described above is originally proposed in [9], which can break the circular dependence of conventional spread spectrum methods.

Figure 1.3 describes the circular dependence problem. In particular, if two devices do not share any secret keys or codes and want to execute a key establishment protocol in the presence of a jammer, they have to use a jamming-resistant communication [9]. However, known anti-jamming techniques such as frequency hopping and direct-sequence spread spectrum rely on secret (spreading) codes that are shared between the communication partners prior to the start of their communication [9]. This creates the circular dependence.

Figure 1.4 illustrates the high level idea of UFH. In UFH, the transmitter and receiver hop randomly between channels in an uncoordinated manner. The transmission is successful when they are in the same channel and the jammer is not in that channel. Figure 1.4 shows 3 different scenarios of UFH:

1. In timeslot 1, both transmitter and receiver are in channel 5, while Eve is not in channel 5. The transmission is successful.

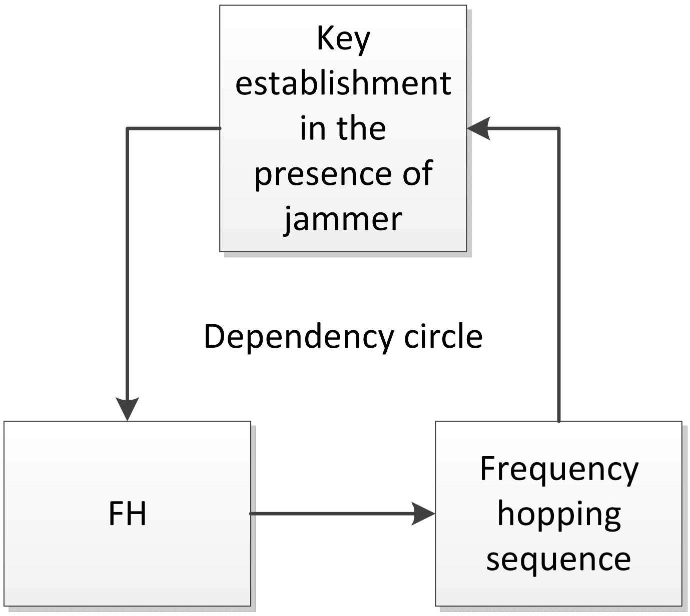

Figure 1.3: Circular dependence.

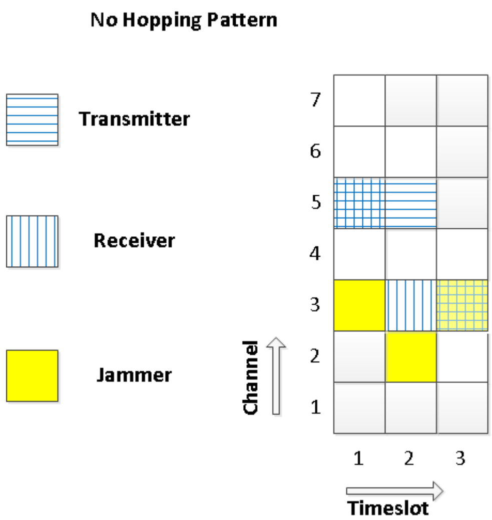

Figure 1.4: Uncoordinated frequency hopping.

2. In timeslot 2, the transmitter and receiver are not in the same channel. The transmission is failed.

3. In timeslot 3, both transmitter and receiver are in channel 3, while Eve is also in channel 3. This transmission is jammed, so it is failed.

Thus UFH breaks the circular dependence by not relying on the hopping pattern [9] and by establishing a secret key when the transmission is successful. In [9], it is shown that UFH scheme can be as resistant to jamming as coordinated frequency hopping. The authors assume the legitimate communication nodes have the ability to store a few megabytes of data and can perform elliptic curve cryptography (ECC) based public key cryptography. The attacker in this model is computationally bounded and also energy constrained. The goal of the attacker is to interfere the communication of the legitimate nodes by inserting messages, modifying messages or jamming messages. In their scheme, a message M which is going to be sent by transmitter is split into l fragments M_1, M_2,..., M_l. And the behavior of transmitting fragment M_j does not relate to any channel and does not relate to the fragments sent before. The authors call this scheme randomized. At the receiver side, the fragments of message M should be reassembled. This process is to avoid the jamming attack. In this paper, the authors assume that the receiver switches channel less often than the transmitter, thus reducing the number of partially received fragments. The scheme of avoiding inserting messages and modifying messages is also designed using Hash link. For each fragment M_i, some additional messages are added to M_i to form a packet $m_i = id|i|M_i|h(m_{i+1})$. id is the message identifier, i is the fragment number, M_i is the fragment of the message, and $h(m_{i+1})$ is the hash value of the next packet. For the last packet, $m_l = id|l|M_l|h(M_1)$, so it forms an unbreakable hash link in the fragments of messages. This ensures the attacker cannot perform effective inserting or modifying attack. The hash-linked packets are transmitted with a high number of repetition. The transmission is successful when the transmitter receives the reply that the reassembling is successful and then the transmission is finished. The transmission can also be finished unsuccessfully with the number of repetitions has exceeded an threshold value. When the packets are received, the receiver starts to compute the packets into a whole message. First, the receiver link the packets according to the fragment number. Second, the receiver computes the hash value of the $i+1$th packet $h(m_{i+1})$ and compares it with the hash value part in the previous packet. When all the packets are linked successfully, the receiver sends the reply message. For the security analysis, given two consecutive packets $m_{i-1} = id|i-1|M_{i-1}|h(m_i)$ and $m_i = id|i|M_i|h(m_{i+1})$ where $2 < i < l$, the attacker need to forge a $m_i^{'}$. So the attacker needs to find $h_i = h(id|i|M_i|h_{i+1}) = h(id|i|M_i^{'}|h_{i+1}^{'})$. But this means to find a collision of hash function $h(\cdot)$, so this is impossible for the computationally bounded attacker to find a collision of hash function. The process that last packet in chain linking to the first packet avoids inserting additional chain heads. The attacker needs to forge a $m_1^{'} = id|1|M_1^{'}|h_2$ for $m_1 = id|1|M_1|h_2$. So $h(M_1) = h(M_1^{'})$, which also means finding a collision for $h(\cdot)$. This UFH scheme for key establishment works like this: first, the transmitter and receiver use a key establishment protocol to generate a key and use the UFH scheme to communicate to agree on a key; second, the transmitter and receiver use this key to find the hopping sequence. In this model, the authors show that for all attacker types, jamming is the best strategy for the attacker. The authors also state that there is no prior work that focuses on circular dependence of anti-jamming establishment and they have not been able to find a scheme to transfer arbitrary length messages without a pre-shared key.

Comparing to FH, UFH does not need shared secrets and synchronization. However, UFH suffers from low throughput [6], as the transmitter and receiver are uncoordinated and hence most of them they are operating at the same channel.

1.4 Existing Schemes to Improve Efficiency

As discussed above, since the hopping in UFH is uncoordinated, UFH often achieves a low efficiency [6]. To alleviate this problem, there have been some recent works attempting to increase the throughput of UFH. They mainly focus on two aspects: learning based approach and cooperative broadcasting approach, which will be discussed in Section 1.4.1 and Section 1.4.2 respectively. Section 1.4.3 will discuss some other research related to UFH.

1.4.1 Learing Based Approach

In [6], the authors develop an almost optimal and adaptive UFH-based anti-jamming scheme and give the thorough quantitative performance analysis for this type of schemes. The UFH-based anti-jamming communication is formulated as a non-stochastic Multi-armed Bandit Problem and online adaptive UFH algorithm against oblivious and adaptive jammer is proposed. The authors show that the performance difference between their algorithm and the optimal one is no more than $O(k_r\sqrt{Tn\ln n})$ in T timeslots, where k_r is the number of frequencies the receiver can receive simultaneously and n is the total number of orthogonal frequencies. A thorough quantitative performance under various strategies of the sender, the receiver and the jammer is made. The authors also analyze the parameter selection to achieve the optimality. In the model of this paper, each node can transmit and receive over k_s and k_r channels respectively, where $k_s \leq n$ and $k_r \leq n$. It is also assumed that the three parties, i.e., the transmitter, the receiver and the jammer have no prior knowledge of others' strategy. The authors do not consider message authentication and privacy in this model because this can be achieved on the application layer. The authors assume the jammer can jam k_j channels in one timeslot. The authors divide the jammers into two categories: oblivious jammer and adaptive jammer. The oblivious jammer selects the jamming strategy independent of the past channel status he has observed. The adaptive jammer can adaptively change his jamming strategy based on his past experiences and observations. In this paper, the authors do not assume the channel quality can be estimated and known before or during transmission. So the algorithm proposed is trying to do online learning the strategy of jammer and use the strategy of jammer to achieve optimality.

In [10], the authors consider power control jointly with UFH problem. The proposed approach in this paper utilizes online learning theory to determine both the hopping channels and the transmitting powers based on the history of channel status. The sender in this model has a power limited budget. Using the proposed approach, the transmitter can choose both transmission power of each channel and which channel to transmit simultaneously.

In [11], the authors discuss primary user emulation (PUE) attack to fight over channels with the secondary user in cognitive radio systems. In this scenario, there are two parties instead of three parties in the UFH model. The authors model the PUE and random hopping as a zerosum game between the attacker and secondary user. The Nash equilibrium of this model is found. One important assumption here is that the channel statistics are known. In this paper, available probability of each channel is known.

In [12], the authors change known channel statistics model into unknown channel statistics model. In this model, the secondary users need to face the challenge that how to address the uncertainties in the channel statistics and the attacker's policy. The authors adopt adversarial bandit algorithm which is significantly modified in the context of blind dogfight in spectrum. This is actually a way to learn the optimal defense strategy using past experience and adaptively change the strategy to the channel dynamics and attack strategy. This key idea is similar as [6] which focuses on a different problem.

The learning based approach implicitly assumes that the strategy of the jammer is fixed. What if the attacker is also intelligent so that the attacker can implement learning method to learn the strategy of the legitimate users and adjust its own strategy? For intelligent attackers, we can not use learning based approach and optimize the throughput using the learned strategy of the attacker since the strategy of the jammer is no longer fixed. This motivates us to think about the UFH problem with intelligent jammers.

1.4.2 Cooperative Broadcasting Approach

In [13], [14], [15], [16], [17] , [18] and [19], a collaborative UFH-based broadcast (CUB) scheme to achieve a higher communication efficiency is proposed and the main idea is to allow nodes that already receive the message to help broadcast. The authors show that their CUB scheme can achieve higher communication efficiency and is more resistant to jamming attack than existing jamming resistant broadcast scheme. In this paper, the authors assume a source node intends to transmit a message to N nodes. The analysis is mainly focused on single hop. The message is split into M fragments of equal length, and each of them is transmitted during one time slot (frequency hop). The CUB scheme is an extension of previous pair-wise UFH schemes. The authors name the straightforward extension of UFH in the broadcast scenario without cooperation as UFH-based Broadcast (NUB). In NUB, each node selects one of C channels in each time slot to receive a packet, and repeat this until the whole broadcast message is received. NUB does not have relay nodes in the broadcast process and in this paper it is shown that NUB takes longer time than pairwise transmission to a single receiver. The authors mainly focus on jamming attack and assume the computation and transmission capability of the attacker is bounded. The time slot is t_p, and the jamming attack needs $t_{\bar{p}}$ to successfully jam a packet, and it takes t_s time to sense a channel. The authors categorize the jamming attacks into responsive attacks and nonresponsive attacks, based on whether the jammer senses the transmission before implementing jamming attacks. For responsive attacks, it is assumed that C_J channels can be blocked simultaneously and t_J time is needed to switch those channels. In one time slot, the number of channels can be jammed is $n_J C_J$ and $n_J = \frac{t_p}{t_{\bar{p}}+t_J}$. For nonresponsive attacks, it is assumed that C_s channels can be sensed simultaneously. In one time slot, the number of channels can be sensed is $n_s C_s$ and $n_s = \frac{t_p - t_{\bar{p}} - t_J}{t_s}$. The authors assume the attacker can implement responsive and nonresponsive attacks simultaneously, which is a worst case, and they call it responsive-sweep strategy. In this worst case, the attacker can jam $n_s C_s + n_J C_J$ channels in one time slot, and each time slot is jammed with probability $\frac{n_s C_s + n_J C_J}{C}$. The authors propose three relay channel selection strategies: Random Relay Channel selection (RRC), Sweep Relay Channel selection (SwRC), and Static Relay Channel selection (StRC). In RRC, each relay node selects randomly and independently one channel in all C channels to transmit a packet. But RRC often results in collision, which is two relay nodes select one same channel. SwRC is an idealized version of RRC. In SwRC, the first node selects one channel in all C channels, and the second node selects one channel in the left $C-1$ channels and so on. SwRC avoids collision but it requires a lot of information exchange between relay nodes. In StRC, the selection of channels is no longer random, the channels in broadcast process is fixed and nonoverlapping. The authors assume the nodes have unique IDs and a suitable algorithm can make the probability of channel collision is negligible. The authors mainly adopt a Random Receiving Channel Selection (RRxC) scheme which means the receiver hops randomly among the C channels. Specially, for StRC, the authors design an Adaptive Receiving Channel selection (ARxC) strategy. As the StRC, each node in ARxC is assumed to know the relay channel list. If all the relay channels in the channel list are jammed, the strategy is switched to RRxC. In CUB, the authors design the control scheme of transmission duration, the transmitter (source node or relay node) stops transmitting when a ACK signal is received or a maximum transmission duration is reached. The authors also analyze the cooperation gain of RRC and StRC strategy. Simulations also indicate a significant improvement of performance of CUB compared to noncollaborative UFH-based broadcast scheme.

[20] investigates efficient Media Access Control (MAC) strategies for the UFH-based collaborative broadcast. To minimize the broadcast delay and to significantly reduce energy cost, the closed-form expression of channel access probabilities is given. This paper is based on [14]. The authors mainly consider two issues: broadcast delay and total energy cost. The authors divide the synchronization among the relays and source into two categories. The first category is perfect synchronization relays, all transmitters are synchronized both in time and transmission content. The second category is asynchronous relays, which is more realistic one, where two or more transmission over the same channel fail. The broadcast delay is the time from the beginning of the transmission to the message is successfully received by the receiver. The energy consumption is all the energy consumed in this process. The authors give the minimal delay strategy and energy efficient strategy. The authors show that if broadcast delay is the main concern, the relays should aggressively access the wireless media. As the network grows, to reduce energy consumption, the channel access probability should be gradually reduced.

[21] addresses the problem of anti-jamming broadcast communication among nodes that do not share secret keys. This paper is based on [9]. Three instances of Uncoordinated Spread Spectrum (USS) are presented: Uncoordinated Frequency Hopping (UFH), Uncoordinated DSSS (UDSSS) and hybrid UFH-UDSSS. UFH randomizes the selection of the frequency channels and UDSSS randomizes the selection of the spreading codes. The feasibility and practicability of the schemes proposed was demonstrated by a USRP/GNU Radio based prototype implementation.

Cooperative broadcasting approach does not focus on improving the throughput of one hop in UFH. If the throughput of one hop can be increased by choosing appropriate strategy, the total throughput of cooperative broadcasting can be increased automatically. As the result, we mainly focus on optimizing the throughput of one hop in UFH.

1.4.3 Other Research about UFH

In [22], the authors propose a new USD-FH scheme for Diffie-Hellman (DH) key establishment using UFH before the FH communication starts. This is based on [9], and tries to design a more efficient scheme. The advantage of this scheme over others is that it does have to split the DH message into multiple packets. The basic idea of USD-FH is to transmit each DH key establishment message using a one time pseudorandom hopping pattern, and before the actual message transmission, the seed of the pseudorandom pattern is disclosed. For energy bounded jammer, it is very difficult to jam all the channels, so there is always a chance that the receiver gets the seed of the pseudorandom hopping pattern while the jammer does not. Since the jammer cannot jam the message transmitted using pseudorandom hopping pattern, so the receiver can receive the DH message correctly. This paper uses UFH to establish key before FH communication.

[23] mainly talks about the coordination between a secondary transmitter and a secondary receiver in order to use the same spectrum white space. This is similar to the synchronization between the transmitter and receiver in UFH. The authors build a new transmission scheme within a framework of frequency-hopping spread spectrum (FHSS) transmission with M-ary frequency-shift keying (M-FSK) modulation. When the white space detection error is large, which happens more often during the beginning stage of the secondary user transmission, the spreading gain is increased to reduce the interference to the primary user. When the white space error detection is small enough, which happens more often after beginning stage of transmission, the white space in spectrum is known, the spreading gain is decreased to increase the data rate of the secondary users. The purpose of using FHSS is to avoid interference and to improve security.

In [24], the authors propose an approximation for the channel capacity of M-frequency T-user multiple access channel.

In [25], the authors propose a detection scheme for uncoordinated narrow-band FH systems. The detection scheme can detect the existence and the number of the narrow-band signals colliding with the desired signal.

These papers are mainly focus on designing the UFH scheme in different specific scenarios. In this thesis, the original model proposed in [9] is used which will lead to more general results.

1.5 Summary of Thesis

In this thesis, the goal is to optimize the throughput of UFH **assuming that the attacker is intelligent**. Since the jammer is intelligent, it will also adapt its attack strategy. Hence, when we design our optimal hopping strategy, we need to take the dynamics of the attacker into consideration. In this thesis, we model the interaction of the legitimate users and the jammer in UFH as a *zero-sum game*, and study the optimal hopping strategy of the legitimate users and correspondingly the optimal attack strategy of the jammer using game theory [26]. In this thesis, we use the name “Alice” to denote the transmitter, “Bob” to denote the receiver and “Eve” to denote the jammer.

The organization and main contributions of the thesis are the following:

- In Chapter 2, the background of the zero-sum game and the Nash equilibrium are introduced.

- In Chapter 3, the zero-sum game model of UFH is introduced. The strategies of the transmitter, the receiver and the attacker are defined. The definition of the Nash equilibrium of our game is also given.

- In Chapter 4, we study the case that all the channels have the same capacity. We fully characterize the Nash equilibrium for this case. In the Nash equilibrium, Alice, Bob and Eve always operate on the same set of channels. We show that Alice, Bob and Eve always access or jam all channels. Alice, Bob and Eve access or jam each channel with an equal probability. The average throughput is a decreasing function of N for $N \geq 2$, where N is the total number of channels.

- In Chapter 5, we study the general channel quality case with $R_1 \leq R_2 \leq ... \leq R_N$, where N is the total number of channels. We fully characterize the Nash equilibrium for this case. In the Nash equilibrium, Alice, Bob and Eve always operate on the same set of channels. Alice, Bob and Eve do not always access or jam all channels.

A new variable k^* is introduced and it is for Alice, Bob and Eve to decide on which channels they should take actions. k^* separates "good" channels and "bad" channels. Alice, Bob and Eve have no motivation to access or jam channels from 1 to $k^* - 1$. When the channel quality is better, Eve jams this channel with a larger probability while Alice and Bob access this channel with a smaller probability. It is simple to verify that $N - k^* + 1 \geq 2$. This implies that Alice and Bob will access at least two channels. Otherwise, if they access only one channel, this channel will be jammed by the attacker with probability 1.

- In Chapter 6, we extend the model into one access multiple jamming case, in which case Alice and Bob can access one channel in one timeslot, while Eve can jam multiple channels in one timeslot. We fully characterize the Nash equilibrium for this case. In the Nash equilibrium, Alice, Bob and Eve always operate on the same set of channels. Alice, Bob and Eve do not always access or jam all channels. k^* is a variable that is for Alice, Bob and Eve to decide on which channels they should take actions. k^* separates "good" channels and "bad" channels. Alice, Bob and Eve have no motivation to access or jam channels from 1 to $k^* - 1$. k^* is determined by the channel capacity and M_j, and it is not related to Alice and Bob. When the channel quality is better, Eve jams this channel with a larger probability while Alice and Bob access this channel with a smaller probability. It is simple to verify that $N - k^* + 1 \geq M_j + 1$, and M_j is the number of channels Eve can jam in one timeslot. This implies that Alice and Bob will access at least $M_j + 1$ channels. Otherwise, if they access only M_j channels, this channel will be jammed by the attacker with probability 1.

- In Chapter 7, we extend the model into multiple access one jamming case, in which case Alice and Bob can access multiple channels in one timeslot, while Eve can jam one channels in one timeslot. In the Nash equilibrium, Alice, Bob and Eve do not always operate on the same set of channels. k^* is a variable that is for Alice, Bob and Eve to decide on which channels they should take actions. k^* separates "good" channels and "bad" channels. Alice, Bob and Eve have no motivation to access or jam channels from 1 to $k^* - 1$. But in some cases, Alice and Bob have to access channels from 1 to k^*-1. k^* is determined by the channel capacity and M_j, and it is not related to Alice and Bob. When the channel quality is better, Eve jams this channel with a larger probability while Alice and Bob access this channel with a smaller probability. It is simple to verify that $N - k^* + 1 \geq 2$. This implies that Alice and Bob will access at least two channels. Otherwise, if they access only one channel, this channel will be jammed by the attacker with probability 1.

- In Chapter 8, we extend the model into multiple access multiple jamming case, in which case Alice and Bob can access multiple channels in one timeslot, and Eve can jam multiple channels in one timeslot. In the Nash equilibrium, Alice, Bob and Eve do not always operate on the same set of channels. k^* is a variable that is for Alice, Bob and Eve to decide on which channels they should take actions. k^* separates "good" channels and "bad" channels. Alice, Bob and Eve have no motivation to access or jam channels from 1 to $k^* - 1$. But in some cases, Alice and Bob have to access channels from 1 to k^*-1. k^* is determined by the channel capacity and M_j, and it is not related to Alice and Bob. When the channel quality is better, Eve jams this channel with a larger probability while Alice and Bob access this channel with a smaller probability. It is simple to verify that $N - k^* + 1 \geq M_j + 1$. This implies that Alice and Bob will access at least $M_j + 1$ channels. Otherwise, if they can access only M_j channels, this channel will be jammed by the attacker with probability 1.

- In Chapter 9, numerical simulations of our optimal strategies are shown. The properties of optimal strategies are shown, and we find that the "waste case" which should be avoided. The comparison between our optimal strategy and the learning approach algorithm is shown.

- In Chapter 10, conclusions of this thesis are given.

Chapter 2

Background

In this chapter, we introduce the background of strategic games, including zero-sum game which will be used to model UFH in this thesis in Section 2.1. In Section 2.2, we introduce and discuss the concept and implications of the Nash equilibrium.

2.1 Zero-sum Game

A strategic game is a model used to model the interaction of a set of decision makers [27]. The concept of strategic game theory is widely used in economics, political science, and psychology, as well as logic and biology [27]. In game theory, the decision makers of a game is referred as players [27]. In a strategic game model, the interactions between players are affected not only by his own actions, but also by the actions taken by other players [27]. There is a clear distinction between a strategic game and a one party optimization problem [28]. The players in a strategic game usually do not have complete control of the result of their actions, which suits the case in UFH with intelligent jammers, but in a one party optimization problem, the result can be completely controlled by his own actions, so in strategic game, we usually cannot get a global optimization result [28].

In strategic games, each player has his own action set [27], which is the set of actions the player can take. The action set can be the same for all players, and can also be different for different players. Each player in a game should has preferences over the action set, which means the player may prefer some actions more than others because those actions can give him more reward. Overall, a strategic game consists of a set of players $\{1, \cdots, N\}$, a action set $\mathcal{Y}_i = \{y_i\}$ for each player and preferences over the action set for each player [27]. And the preference is a function of strategy in the action set, and is usually called the payoff function u_i, which depends not only on his own action but the actions of other players of the game.

From the angle of cooperation, there are two types of games: cooperative games and noncooperative games [27]. In noncooperative games, zero-sum game is one of the most important form. Zero-sum game is usually used to describe the situation when the players are in competitive relationship. Players in zero-sum game do not cooperate and the gain of one player will lead to loss to the other player [28]. As the name of zero-sum game implies, in zero-sum game the sum of total rewards of all the players is identically zero [27]:

$$\sum_{i=1}^{N} u_i(y_1, \cdots, y_N) = 0. \tag{2.1}$$

In some games, the sum of the total reward is not zero, but a nonzero constant [27]. We may refer this kind of games including zero-sum game as "constant-sum" game [27]. One property of zero-sum game which makes it widely used is that, nonzero constant games can be easily transformed to zero-sum games without changing the nature of the games [27]. So when we model a constant-sum game, we always choose zero-sum game for it is the same in nature as nonzero constant-sum game [27].

2.2 Nash equilibrium

As the previous section stated, in strategic games, the global optimization usually cannot be reached due to the partial control to the game of each player [28]. This is due to the fact that the optimal action of one player depends on the actions taken by other players [27]. So when choosing an action a player must take account into the actions taken by other players [27]. So the "belief" of other players is very important. This "belief" may be from the past experience of other players and this experience is sufficient for the player to predict what the opponents will behave [27]. Given the other players' strategies, if the player is rational, he can choose the optimal strategy. Under this circumstance, the optimal strategy of each player given other players' strategies is important at the optimization aspect [27].

In game theory, the Nash equilibrium is a solution concept of a non-cooperative game involving two or more players, in which each player is assumed to know the equilibrium strategies of the other players, and no player has anything to gain by changing only his own strategy unilaterally [27].

Definition 2.2.1. *Let y_i denote the strategy of player i, and y_{-i} denote the set of strategies of players except for player i. u_i is the payoff function of player i. y^* is said to be a Nash equilibrium if for each player i and every strategy y_i taken by the player, y^* is at least as good as the strategy (y_i, y^*_{-i}) in which player i chooses y_i while every other player j chooses y^*_j. That is, for every player i and $\forall\ y_i$,*

$$u_i(y^*) \geq u_i(y_i, y^*_{-i}). \tag{2.2}$$

This definition can be explained this way: if each player has chosen a strategy and no player can benefit by changing his or her strategy while the other players keep theirs unchanged, then the current set of strategy choices and the corresponding payoffs constitute a Nash equilibrium [27]. In the Nash equilibrium, changing one's own strategy unilaterally can not lead to a greater reward [27] for him. Everyone is taking his best strategy while taking into account the decisions of the others [27].

For the UFH problem, if the strategy taken by the legitimate transmitter and receiver is in the Nash equilibrium, from definition it can be concluded that the jammer cannot do better even if he knows the strategy of the legitimate transmitter and receiver. So algorithm of learning the strategy taken by the legitimate transmitter and receiver and then design a optimal strategy will not work in the Nash equilibrium. This also secures the UFH in the sense of data rate.

Chapter 3

Model

In this chapter, we introduce the basic model of our UFH problem. At the same time, the definition of parameters and the Nash equilibrium in our model are given.

We consider a time-slotted wireless system with N channels, each with channel capacity R_i, $i = 1, \cdots, N$. Without loss of generality, we assume $R_1 \leq R_2 \leq ... \leq R_N$. Here, to assist the presentation, we assume that all terminals can access or jam one channel at any given time slot. The more general case in which the terminals can access or jam more than one channel at each time slot will be considered in Chapter 6, Chapter 7 and Chapter 8. In UFH, the transmitter (Alice) and receiver (Bob) hop randomly through these N channels. We use p_i^t and p_i^r to denote the probabilities that Alice and Bob will access channel i at any time slot respectively. Furthermore, we define $\mathbf{p}^t \triangleq [p_1^t, \cdots, p_N^t]$ and $\mathbf{p}^r \triangleq [p_1^r, \cdots, p_N^r]$ with $\sum p_i^t = 1$ and $\sum p_i^r = 1$. The jammer will jam channel i with a probability p_i^j, and similarly we define $\mathbf{p}^j \triangleq [p_1^j, \cdots, p_N^j]$ with $\sum p_i^j = 1$. We assume that if Eve chooses to jam a channel, then the communication between Alice and Bob through that channel will fail. The transmission between Alice and Bob is successful when Alice and Bob use the same channel and at the same time and Eve is not jamming this channel. And we use A, B and E to denote the support set of channels, for channels in the support set, Alice, Bob and Eve will access or jam with non-zero probabilities.

Figure 3.1 shows 3 different scenarios of UFH:

1. In timeslot 1, both transmitter and receiver are in channel 5, while Eve is not in

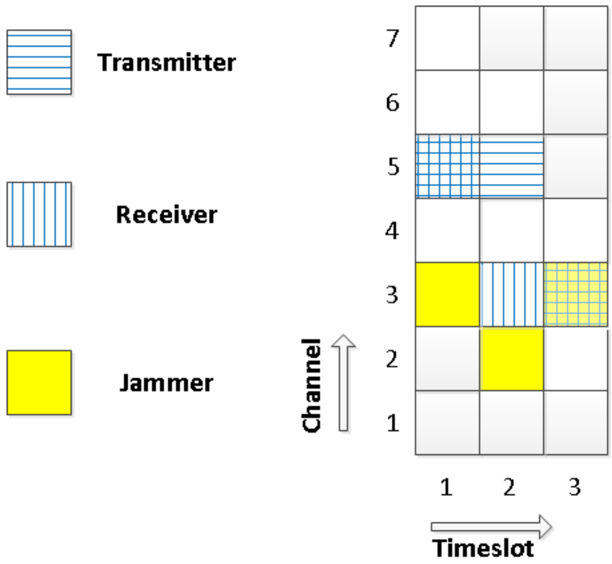

Figure 3.1: System model.

channel 5. The transmission is successful.

2. In timeslot 2, the transmitter and receiver are not in the same channel. The transmission is failed.

3. In timeslot 3, both transmitter and receiver are in channel 3, while Eve is also in channel 3. This transmission is jammed, so the it is failed.

The average throughput of UFH is

$$\bar{R} = \sum_{i=1}^{N} R_i p_i^t p_i^r \left(1 - p_i^j\right). \tag{3.1}$$

Clearly, in UFH, Alice and Bob would like to maximize the average throughput, while Eve would like to minimize it. We model this scenario as a zero-sum game, with Alice and Bob being one party and Eve being the other party. In this game, the strategy of Alice and Bob is to choose $\mathbf{p}^t$ and $\mathbf{p}^r$, and the strategy of Eve is to choose $\mathbf{p}^j$. The reward for Alice and Bob is $\bar{R}$ and the reward for Eve is $-\bar{R}$. A strategy pair $\{(\mathbf{p}^{t*}, \mathbf{p}^{r*}), \mathbf{p}^{j*}\}$ is called a

Nash equilibrium if

$$\bar{R}\left(\mathbf{p}^{t},\mathbf{p}^{r},\mathbf{p}^{j*}\right) \leq \bar{R}\left(\mathbf{p}^{t*},\mathbf{p}^{r*},\mathbf{p}^{j*}\right), \forall \mathbf{p}^{t},\mathbf{p}^{r}, \tag{3.2}$$

$$-\bar{R}\left(\mathbf{p}^{t*},\mathbf{p}^{r*},\mathbf{p}^{j}\right) \leq -\bar{R}\left(\mathbf{p}^{t*},\mathbf{p}^{r*},\mathbf{p}^{j*}\right), \forall \mathbf{p}^{j}. \tag{3.3}$$

This implies that neither party will receive a larger reward by unilaterally deviate from this equilibrium, hence they have no motivation to do so.

Chapter 4

Equal Channel Quality Case

In this chapter, we study the case when all the channels have the same capacity, which is $R_1 = R_2 = ... = R_N$. The Nash equilibrium is given at the beginning of this chapter, and the proof is given in Section 4.1. Remarks are given in Section 4.2.

We can denote

$$R_i = R, \quad \forall i \in \{1, 2, ..., N\}. \tag{4.1}$$

Lemma 4.0.2. *In this case, the Nash Equilibrium is:*

$$p_i^{t*} = p_i^{r*} = p_i^{j*} = \frac{1}{N}, \tag{4.2}$$

for $\forall i \in \{1, 2, ..., N\}$.

This result is intuitive which is illustrated in Figure 4.1, Figure 4.2 and Figure 4.3. Figure 4.1 shows the channel capacity are the same for all channels. Figure 4.2 shows the strategy of Alice and Bob, they access all the channels with equal probability. Figure 4.3 shows the strategy of Eve, she jams all the channels with equal probability.

4.1 Proof

The proof is organized as:

Let A, B and E denote the support set for Alice, Bob and Eve respectively. In Section 4.1.1,we prove $E = \{1, 2, ..., N\}$. In Section 4.1.2, we prove $E \subseteq A$, $E \subseteq B$, $A = B$. So $A = B = E = \{1, 2, ..., N\}$. In Section 4.1.3, we determine the Nash equilibrium.

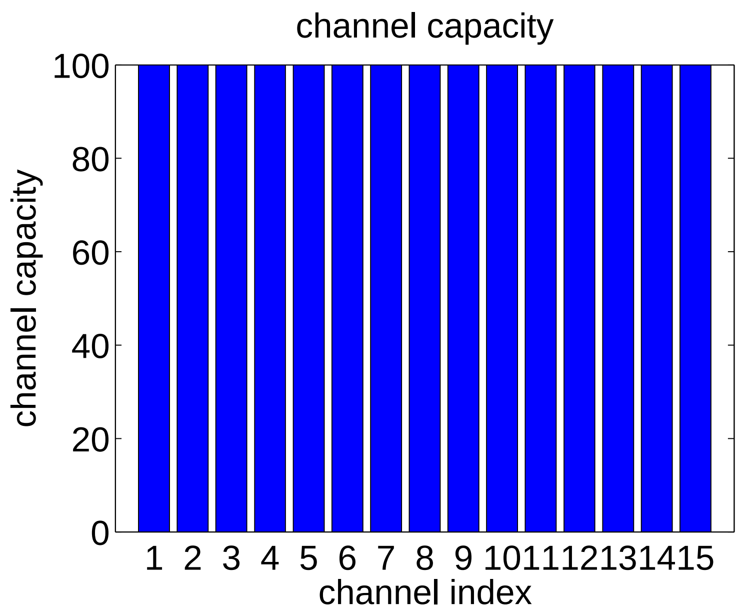

Figure 4.1: Channel Capacity (N=15).

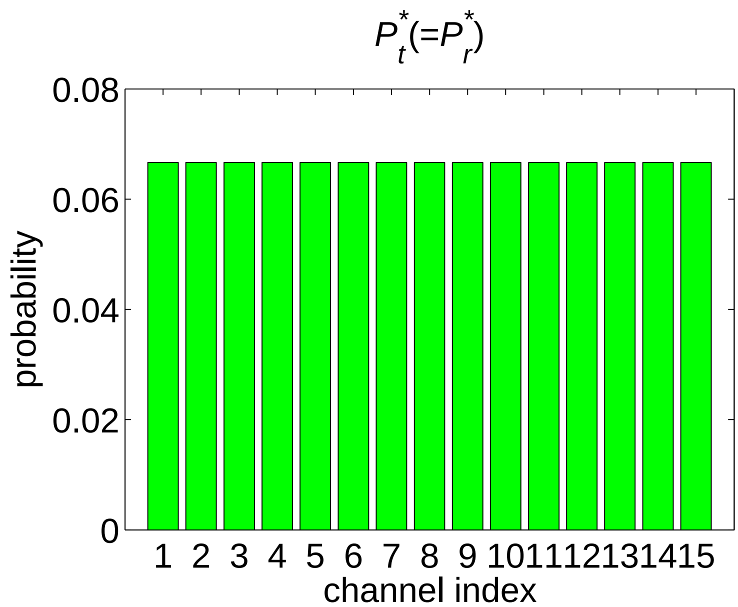

Figure 4.2: $P^{t*}(= P^{r*})$ (N=15).

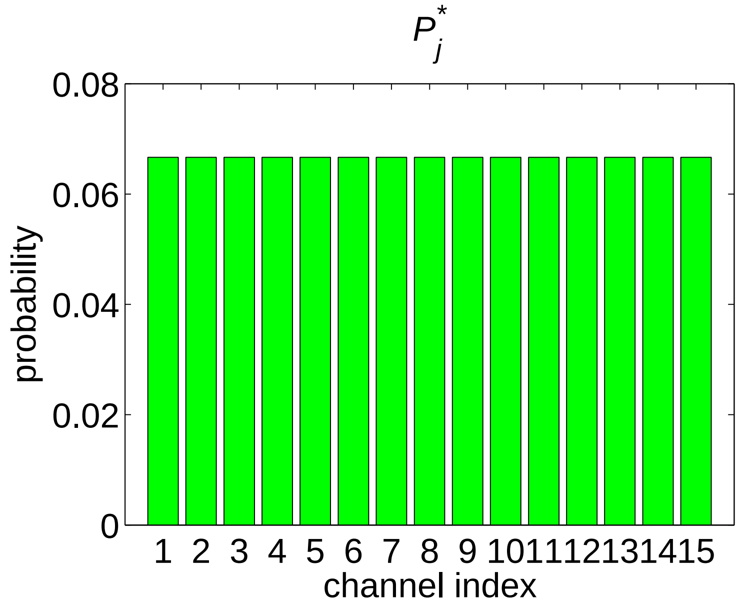

Figure 4.3: P^{j^*} (N=15).

Proof. The reward of Alice and Bob accessing channel i is:

$$R_i \left(1 - p_i^j\right) = R \left(1 - p_i^j\right). \tag{4.3}$$

The reward of Eve jamming channel i is:

$$-\sum_{j=1, j\neq i}^{N} R_j p_j^t p_j^r = S + R_i p_i^t p_i^r, \tag{4.4}$$

where $S = -\sum_{j=1}^{N} R_j p_j^t p_j^r$.

Then we derive the Nash equilibrium step by step.

4.1.1 Prove: $E = \{1, 2, ..., N\}$.

If $E \neq \{1, 2, ..., N\}$, then $\exists i \in \{1, 2, ..., N\}$ s.t. $p_i^{j^*} = 0$.

Case 1: $p_i^{t^*} = p_i^{r^*} = 1$, then it is obvious for Eve to increase his reward by jamming channel i. So this is not a Nash equilibrium.

Case 2: $p_i^{t^*} \neq 1$ and $p_i^{r^*} \neq 1$. Since Eve never jams channel i, so Alice and Bob can always increase their reward by allocating more probability into channel i. But they cannot achieve maximum reward by setting $p_i^{t*} = p_i^{r*} = 1$. So Alice and Bob can always increase their reward by changing their strategy unilaterally. This is not a Nash equilibrium.

From above, we can conclude $E = \{1, 2, ..., N\}$.

4.1.2 Prove: $E \subseteq A$, $E \subseteq B$, $A = B$.

If $E \nsubseteq A$, then Eve is jamming some channel that is never used by the transmitter. So Eve can increase his reward by jamming some other channel. So $E \subseteq A$ [1]. The proof is the same for $E \subseteq B$.

If $A \neq B$, then Alice is transmitting on some channel that is can never used by Bob or Bob is listening on some channel that Alice's message never comes from. This means Alice or Bob is wasting her or his resources. So Alice and Bob can increase their reward by allocating their probability on the same set of channels. Thus, $A = B$.

The above conclusion implies that if all the channel quality are equal, then $A = B = E = \{1, 2, ..., N\}$.

4.1.3 Determine $\mathbf{p}^{t*}$, $\mathbf{p}^{r*}$ and $\mathbf{p}^{j*}$

First we will show that to achieve the Nash equilibrium, $1 - p_i^{j^*} = C_0$ and $p_i^{t*} p_i^{r*} = C_1$, where C_0 and C_1 are constants independent of i.

If $1 - p_i^{j^*} \neq C_0$, then $\exists l_1, l_2 \in \{1, 2, ..., N\}$ s.t.

$$1 - p_{l_1}^{j\ *} = \max\{1 - p_i^{j^*}\}, \tag{4.5}$$

$$1 - p_{l_1}^{j\ *} > 1 - p_{l_2}^{j\ *}, \tag{4.6}$$

where $i \in \{1, 2, ..., N\}$,

$$\bar{R} = R[p_{l_1}^{t\ *} p_{l_1}^{r\ *} \left(1 - p_{l_1}^{j\ *}\right) + p_{l_2}^{t\ *} p_{l_2}^{r\ *} \left(1 - p_{l_2}^{j\ *}\right) + \sum_{\substack{i=1 \\ i \neq l_1 \\ i \neq l_2}}^{N} p_i^{t*} p_i^{r*} \left(1 - p_i^{j^*}\right)]. \tag{4.7}$$

So there exist another strategy of Alice and Bob $\mathbf{p}^{t'}$ and $\mathbf{p}^{r'}$, which satisfy that for $i \neq l_1$

[1] The $\subseteq$ symbol does not mean proper set in this thesis.

and $i \neq l_2$,

$$p_i^{t'} = p_i^{t*}, p_i^{r'} = p_i^{r*}, \tag{4.8}$$

$$p_{l_1}^{t\ '} > p_{l_1}^{t\ *}, p_{l_1}^{r\ '} > p_{l_1}^{r\ *}, \tag{4.9}$$

$$p_{l_2}^{t\ '} < p_{l_2}^{t\ *}, p_{l_2}^{t\ '} < p_{l_2}^{t\ *}. \tag{4.10}$$

This implies

$$p_{l_1}^{t\ '} + p_{l_2}^{t\ '} = p_{l_1}^{t\ *} + p_{l_2}^{t\ *}, \tag{4.11}$$

$$p_{l_1}^{r\ '} + p_{l_2}^{t\ '} = p_{l_1}^{r\ *} + p_{l_2}^{t\ *}. \tag{4.12}$$

We can always find strategy $\mathbf{p}^{t'}$ and $\mathbf{p}^{r'}$ because we have proved $A = B = E = \{1, 2, ..., N\}$, which means the probability of accessing each channel in the game is nonzero. It is obvious that the strategy $\mathbf{p}^{t'}$ and $\mathbf{p}^{r'}$ can increase the reward of Alice and Bob. So Alice and Bob can always increase their reward by moving their probability of accessing channel l_2 into accessing channel l_1. Thus this is not a Nash equilibrium. Then $1 - p_i^{j*} = C_0$. This means that all the p_i^{j*} are all equal, so $p_i^{j*} = \frac{1}{N}$.

Similar to the proof of $1 - p_i^{j*} = C_0$, if $p_i^{t*} p_i^{r*} \neq C_1$, then $\exists l_3, l_4 \in \{1, 2, ..., N\}$ s.t.

$$p_{l_3}^{t\ *} p_{l_3}^{r\ *} = \max p_i^t p_i^r, \tag{4.13}$$

$$p_{l_3}^{t\ *} p_{l_3}^{r\ *} > p_{l_4}^{t\ *} p_{l_4}^{r\ *}. \tag{4.14}$$

So Eve can always increase his reward by moving his probability of jamming channel l_4 into jamming channel l_3. So this is not a Nash equilibrium. Then in the Nash equilibrium $p_i^{t*} p_i^{r*} = C_1$.

Under the Nash equilibrium,

$$\bar{R} = \sum_{i=1}^{N} C_1 \left(1 - \frac{1}{N}\right) = (N-1)\, C_1. \tag{4.15}$$

Since Alice and Bob form one party of the game, so the we can take the pair $(\mathbf{p}^t, \mathbf{p}^r)$ as the strategy of Alice and Bob. So Alice and Bob want maximize $\bar{R}$, that is, to maximize C_1. We build two vectors

$$\vec{A_1} = [\sqrt{p_1^t}, \sqrt{p_2^t}, ..., \sqrt{p_N^t}], \tag{4.16}$$

$$\vec{A_2} = [\sqrt{p_1^r}, \sqrt{p_2^r}, ..., \sqrt{p_N^r}], \tag{4.17}$$

$\vec{A_1}$ and $\vec{A_2}$ are two vector in $\mathbb{R}^N$. Then $|\vec{A_1}| = 1$ and $|\vec{A_2}| = 1$.

$$\vec{A_1} \cdot \vec{A_2} = \sum_{i=1}^{N} \sqrt{p_i^{t*}} \sqrt{p_i^{r*}} = \sum_{i=1}^{N} \sqrt{C_1} = N\sqrt{C_1}, \tag{4.18}$$

so we can convert the problem of maximizing C_1 into maximizing $\vec{A_1} \cdot \vec{A_2}$.

$$\vec{A_1} \cdot \vec{A_2} = |\vec{A_1}||\vec{A_2}| \cos\theta \leq |\vec{A_1}||\vec{A_2}| = 1, \tag{4.19}$$

the equality holds when $\theta = 0$, where θ is the measure of angle between $\vec{A_1}$ and $\vec{A_2}$. So we can maximize C_1 by setting $\theta = 0$. The two vectors $\vec{A_1}$ and $\vec{A_2}$ have the same length, and the same direction, so they are equal. So

$$p_i^{t*} = p_i^{r*} = \sqrt{C_1}, \quad \forall i \in \{1, 2, ..., N\}. \tag{4.20}$$

Then we can determine

$$p_i^{t*} = p_i^{r*} = \frac{1}{N}, \quad \forall i \in \{1, 2, ..., N\}. \tag{4.21}$$

From the proof above, Alice and Bob cannot increase their reward by changing to another strategy unilaterally.

So in the equal channel quality scenario, the Nash Equilibrium is

$$p_i^{t*} = p_i^{r*} = p_i^{j*} = \frac{1}{N}, \tag{4.22}$$

for $\forall i \in \{1, 2, ..., N\}$. □

4.2 Remark

Remark 4.2.1. *Since the Nash equilibrium is obtained, the average throughput is*

$$\bar{R} = R\frac{N-1}{N^2}. \tag{4.23}$$

Remark 4.2.2. *In the Nash equilibrium, Alice, Bob and Eve always operate on the same set of channels. In particular,* $A = B = E = \{1, \cdots, N\}$.

Remark 4.2.3. *Alice, Bob and Eve always access or jam all channels.*

Remark 4.2.4. *Alice, Bob and Eve access or jam each channel with equal probability.*

Remark 4.2.5. $\bar{R}$ *is a decreasing function of* N *for* $N \geq 2$. *Notice* $\bar{R}$ *reach maximum when* $N = 2$.

Chapter 5

General Channel Quality Case

In this chapter, we study the a more general case, $R_1 \leq R_2 \leq ... \leq R_N$. We characterize the Nash equilibrium of the game for this general channel quality case. During the derivation, we also study the properties of the strategies that achieve this equilibrium. The Nash equilibrium is given at the beginning of this chapter, and the proof is given in Section 5.1. Remarks are given in Section 5.2.

Lemma 5.0.6. *The unique Nash equilibrium of this game is*

$$p_i^{t*} = p_i^{r*} = \frac{\frac{1}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}, \tag{5.1}$$

$$p_i^{j*} = 1 - \frac{\frac{N-k^*}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \tag{5.2}$$

for $k^* \leq i \leq N$*, where* $k^* = \min\left\{k | R_k > \frac{N-k}{\sum_{i=k}^{N} \frac{1}{R_i}}\right\}$*, and*

$$p_i^{t*} = p_i^{r*} = p_i^{j*} = 0, \quad \forall i < k^*. \tag{5.3}$$

Figure 5.1, Figure 5.2 and Figure 5.3 give an example to illustrate our results. Figure 5.1 shows the channel capacity. Figure 5.2 shows the strategy of Alice and Bob, we can see that Alice and Bob only access channels from k^* to N, and when the channel quality is better, Alice and Bob access this channel with a smaller probability. Figure 5.3 shows the strategy of Eve, we can see that Eve only jams channels from k^* to N, and when the channel quality is better Eve jams this channel with a larger probability.

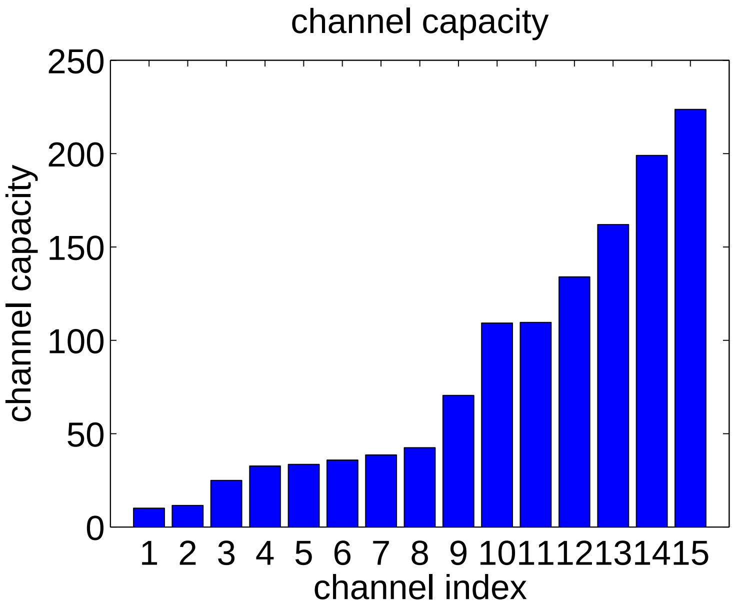

Figure 5.1: Channel Quality ($N = 15$, $k^* = 12$).

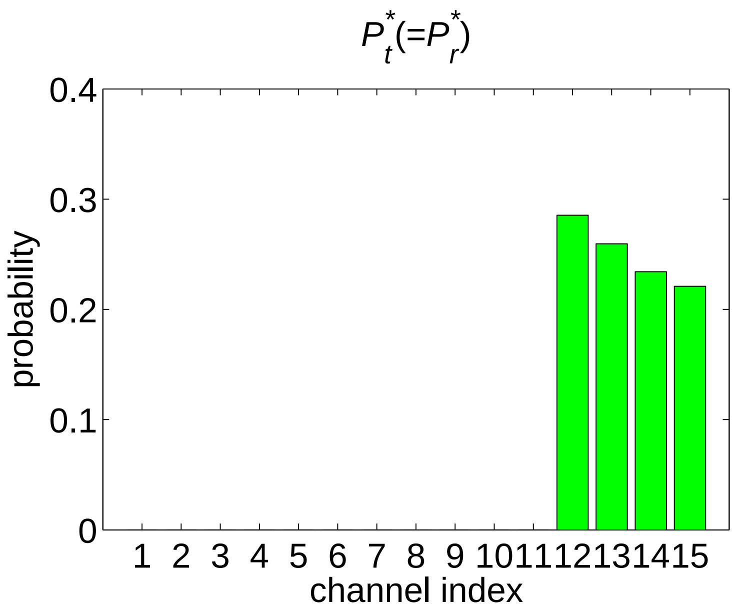

Figure 5.2: $P^{t*}(= P^{r*})$ ($N = 15$, $k^* = 12$).

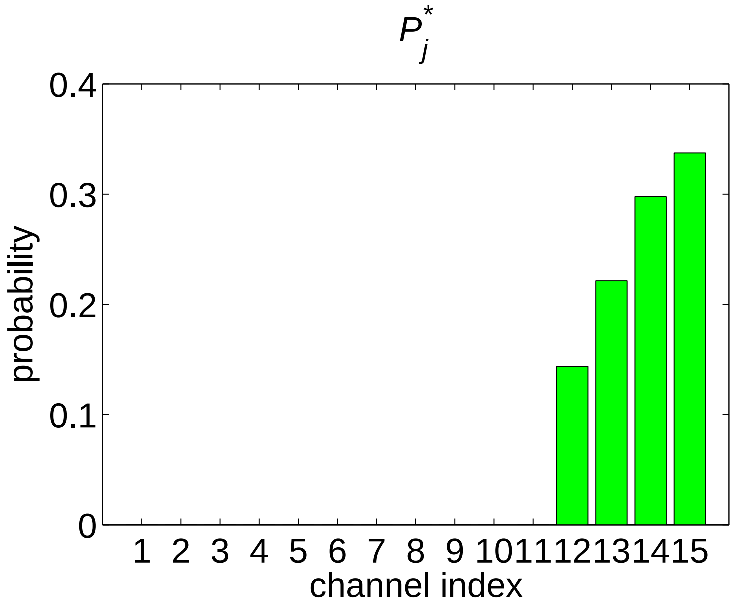

Figure 5.3: P^{j^*} ($N = 15$, $k^* = 12$).

5.1 Proof

Proof. The proof is organized as follows. In Section 5.1.1, we show that in the Nash equilibrium if Eve jams channel k with a non-zero probability, it will jam all channels that have better channel qualities with a non-zero probability. Hence, there exists a number $1 \leq k^* \leq N$, such that the jamming set E has the form $E = \{k^*, k^* + 1, ..., N\}$. In Section 5.1.2, we show that $E \subseteq A$, $E \subseteq B$ and $A = B$. In Section 5.1.3, we show that $A = B = E$ and determine the Nash equilibrium.

Before proceeding to the detailed proof, we have the following facts.

1. The reward of Alice and Bob both accessing channel i is

$$R_i \left(1 - p_i^j\right). \tag{5.4}$$

2. The reward of Eve jamming channel i is

$$-\sum_{j=1, j \neq i}^{N} R_j p_j^t p_j^r = S + R_i p_i^t p_i^r, \tag{5.5}$$

where $S \triangleq -\sum_{j=1}^{N} R_j p_j^t p_j^r$.

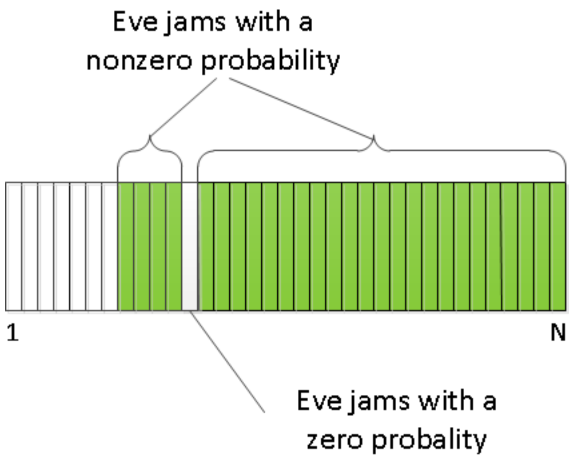

Figure 5.4: Proof for $E = \{k^*, k^* + 1, ..., N\}$.

5.1.1 Prove: if $p_k^{j^*} > 0$, then $p_i^{j^*} > 0$ for all $i > k$. Hence, there exists a number k^* such that E has the form $E = \{k^*, k^* + 1, ..., N\}$.

We will prove this by contradiction. Figure 5.4 shows the idea how to prove this. Suppose this claim is not true, then in the Nash equilibrium strategy of Eve $\mathbf{p}^{j^*}$, there exists some $k_1 > k$ such that $p_{k_1}^{j^*} = 0$ and $p_k^{j^*} > 0$. That is, Eve gives up jamming some channel that is not the worst in her support set. In this case, the reward of Alice and Bob accessing channel k_1 is

$$R_{k_1}\left(1 - p_{k_1}^{j^*}\right) = R_{k_1}. \tag{5.6}$$

Then we have

$$R_{k_1} \geq R_k > R_k\left(1 - p_k^{j^*}\right).$$

We then have the following two cases, each of which will lead to a contradiction.

Case 1: If $p_k^{t^*} = p_k^{r^*} = 0$, that is Alice and Bob never use channel k. Then Eve can increase its reward by reducing the probability of jamming channel k to zero. This contradicts with the definition of the Nash equilibrium.

Case 2: If $p_k^{t^*} > 0$ or $p_k^{r^*} > 0$, then Alice and Bob can increase their rewards by transferring their probability from channel k to channel k_1. This contradicts with the definition of the Nash equilibrium.

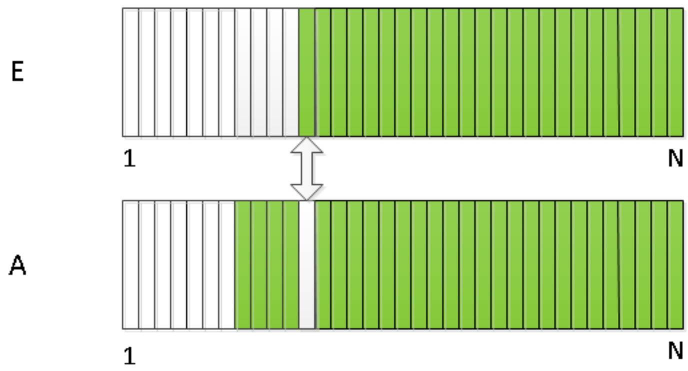

Figure 5.5: Proof for $E \subseteq A$.

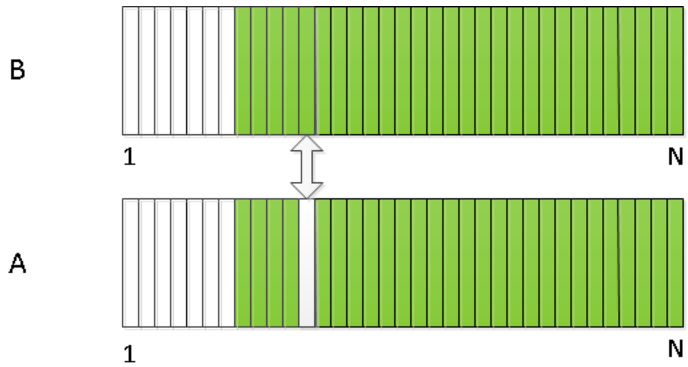

Figure 5.6: Proof for $A = B$.

This completes the proof that in the Nash equilibrium, E must have the form $E = \{k^*, k^* + 1, ..., N\}$ with $1 \leq k^* \leq N$.

5.1.2 Prove: $E \subseteq A$, $E \subseteq B$ and $A = B$

Figure 5.5 and Figure 5.6 show the idea how to prove this. If $E \nsubseteq A$, namely $E \backslash A \neq \phi$, then Eve is jamming some channels that are never used by the transmitter. Here $E \backslash A \triangleq \{k | k \in E \text{ and } k \notin A\}$, and ϕ is the empty set. So Eve can increase his reward by moving jamming probabilities from channels in $E \backslash A$ to channels in A, which contradicts the definition of the Nash equilibrium. Hence, in the Nash equilibrium, we have $E \subseteq A$ [1]. The proof of $E \subseteq B$ is the same. If $A \neq B$, then Alice is transmitting on some channel that

[1]The $\subseteq$ symbol does not mean proper set in this thesis.

is can never used by Bob or Bob is listening on some channel that Alice's message never comes from. This means Alice or Bob is wasting her or his resources. So Alice and Bob can increase their reward by allocating their probability on the same set of channels. Thus, $A = B$.

Now, we show $A = B = \{k_1, k_1 + 1, ..., N\}$ with $k^* - 1 \leq k_1 \leq k^*$. Because we have proved $E \subseteq A$, $E \subseteq B$ and $A = B$, so we have two cases:

Case 1: $A = B = E$, so $k_1 = k^*$.

Case 2: $E \subseteq A$ and $E \neq A$. Since Eve never jams channel 1 to $k^* - 1$, so for channel 1 to $k^* - 1$,

$$\sum_{i=1}^{k^*-1} R_i p_i^t p_i^r \leq R_{k^*-1} \sum_{i=1}^{k^*-1} p_i^t p_i^r \leq R_{k^*-1} \left(\sum_{i=1}^{k^*-1} p_i^t \right) \left(\sum_{i=1}^{k^*-1} p_i^r \right). \tag{5.7}$$

The equality holds when Alice and Bob access channel 1 to $k^* - 2$ with probability zero. So Alice and Bob should put all their probability from channel 1 to $k^* - 2$ into channel $k^* - 1$. Then Alice and Bob should set $k_1 = k^* - 1$. So $A = B = \{k^* - 1, k^*, ..., N\}$.

5.1.3 Determine $\mathbf{p}^{t^*}$, $\mathbf{p}^{r*}$ and $\mathbf{p}^{j*}$

Figure 5.7, Figure 5.8 and Figure 5.9 show the high level idea how to determine $\mathbf{p}^{t*}$, $\mathbf{p}^{r*}$ and $\mathbf{p}^{j*}$. In the Nash equilibrium, in the support set, the reward should be equal to a constant. Intuitively, if this is not true, the other party will find the channel with maximum of the reward and use this channel. Next, the concrete proof is provided.

From the side of Eve, Eve is not going to jam channel $k^* - 1$. So we have

$$R_{k^*-1} p_{k^*-1}^{t^*} p_{k^*-1}^{r^*} \leq R_{k^*} p_{k^*}^{t^*} p_{k^*}^{r^*} = R_{k^*+1} p_{k^*+1}^{t^*} p_{k^*+1}^{r^*} = ... = R_N p_N^{t^*} p_N^{r^*} = C_1, \tag{5.8}$$

where C_1 is a constant.

We have

$$R_{k^*-1} p_{k^*-1}^{t^*} p_{k-1}^{r^*} \leq C_1, \tag{5.9}$$

because if this inequality does not hold, then Eve can increase her reward by jamming channel $k^* - 1$ and thus contradicts with the definition of the Nash equilibrium.

From the side of Alice and Bob, we have

$$R_{k^*-1} = R_{k^*} \left(1 - p_{k^*}^{j^*}\right) = R_{k^*+1} \left(1 - p_{k^*+1}^{j^*}\right) = ... = R_N \left(1 - p_N^{j^*}\right) = C_0, \tag{5.10}$$

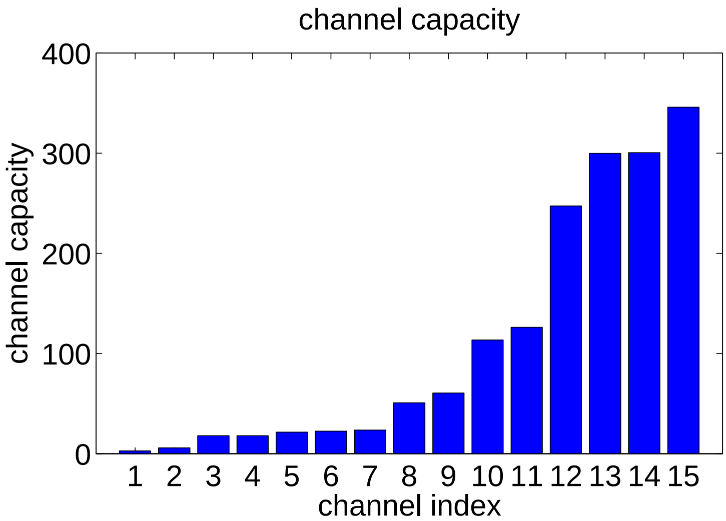

Figure 5.7: Channel capacity.

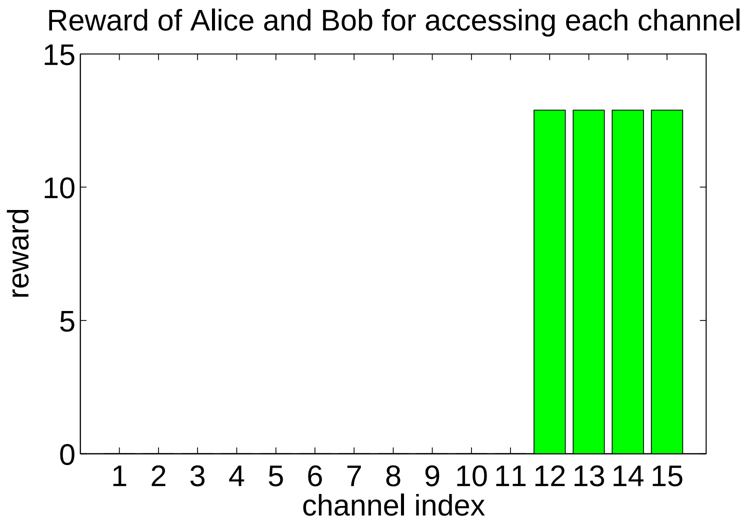

Figure 5.8: Rewards of Alice and Bob for accessing each channel.

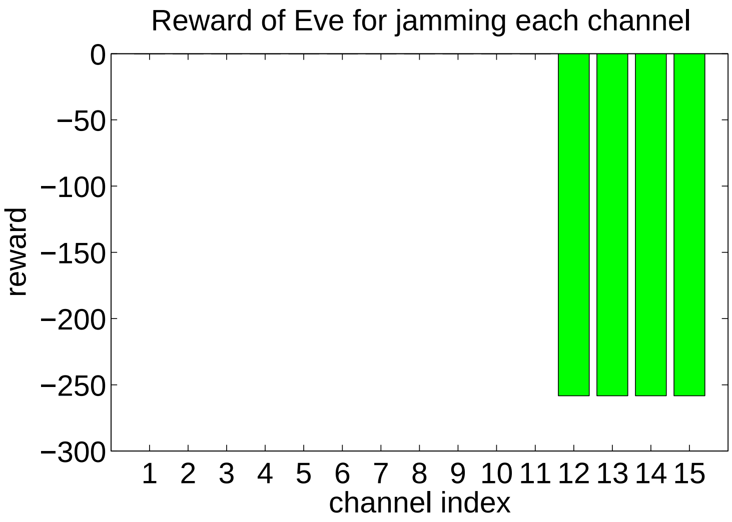

Figure 5.9: Rewards of Eve for accessing each channel.

where C_0 is a constant.

So this implies

$$R_{k^*-1} < R_{k^*} \leq R_{k^*+1} \leq ... \leq R_N. \tag{5.11}$$

We can find $\mathbf{p}^{j^*}$ first. From the discussion above, we know $R_i(1-p_i^{j^*}) = C_0$ for $\forall i \in \{k^*, k^*+1, ..., N\}$. Then we have $p_i^{j^*} = 1 - \frac{C_0}{R_i}$ for $\forall i \in \{k^*, k^*+1, ..., N\}$. Summing $p_i^{j^*}$ from k^* to N, we have

$$\begin{aligned} 1 &= \sum_{l=k^*}^{N} p_l^{j^*} = \sum_{l=k^*}^{N} \left(1 - \frac{C_0}{R_l}\right) \\ &= (N - k^* + 1) - C_0 \sum_{l=k^*}^{N} \frac{1}{R_l}. \end{aligned}$$

From this, we have

$$\begin{aligned} C_0 &= \frac{N-k^*}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \\ p_i^{j^*} &= 1 - \frac{\frac{N-k^*}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}. \end{aligned}$$

So we have $C_0 < R_{k^*} \leq R_{k^*+1} \leq ... \leq R_N$. If R_m satisfies

$$R_m > \frac{N-m}{\sum_{i=m}^{N} \frac{1}{R_i}}, \tag{5.12}$$

then for $m+1$,

$$\begin{aligned} R_m\left(\sum_{i=m}^{N}\frac{1}{R_i}\right) &> N-m, \\ R_m\left(\sum_{i=m+1}^{N}\frac{1}{R_i}\right)+1 &> N-m, \\ R_{m+1}\left(\sum_{i=m+1}^{N}\frac{1}{R_i}\right) &> N-(m+1), \\ R_{m+1} &> \frac{N-(m+1)}{\sum_{i=m+1}^{N}\frac{1}{R_i}}, \end{aligned}$$

$m+1$ also satisfies the inequality. The third inequality use the fact that $R_{m+1} \geq R_m$. By induction, we can conclude that if k is in the set $\left\{k|R_k > \frac{N-k}{\sum_{i=k}^{N}\frac{1}{R_i}}\right\}$, then all the numbers from k to N are also in that set. So for

$$j < \min\left\{k|R_k > \frac{N-k}{\sum_{i=k}^{N}\frac{1}{R_i}}\right\}, \tag{5.13}$$

we have

$$R_j \leq \frac{N-j}{\sum_{i=j}^{N}\frac{1}{R_i}}. \tag{5.14}$$

Next, we show that

$$k^* = k_m \triangleq \min\left\{k|R_k > \frac{N-k}{\sum_{i=k}^{N}\frac{1}{R_i}}\right\}. \tag{5.15}$$

We show this by contradiction. Suppose $k^* = k^{'} \neq k_m$, we have the following two cases:

1. If $k^{'} > k_m$, the reward of Alice and Bob accessing channel $i \geq k^{'}$ is

$$R_i\left(1-p_i^{j^*}\right) = \frac{N-k^{'}}{\sum_{l=k^{'}}^{N}\frac{1}{R_l}}. \tag{5.16}$$

From the discussion above, we know that for $i < k^{'}$, $p_i^{j^*} = 0$. The reward of Alice and Bob accessing channel $k^{'}-1$ is $R_{k^{'}-1}$. We have $k^{'}-1 \geq k_m$, so

$$\begin{aligned} R_{k^{'}-1} &> \frac{N-\left(k^{'}-1\right)}{\sum_{l=k^{'}-1}^{N}\frac{1}{R_l}}, \\ R_{k^{'}-1}\left(\sum_{l=k^{'}}^{N}\frac{1}{R_l}+\frac{1}{R_{k^{'}-1}}\right) &> N-k+1, \\ R_{k^{'}-1} > \frac{N-k^{'}}{\sum_{l=k^{'}}^{N}\frac{1}{R_l}} &= R_{k^{'}}\left(1-p_{k^{'}}^{j}\right). \end{aligned}$$

The right hand side term is the reward of Alice and Bob acessing channel $k^{'}$. So the reward of Alice and Bob accessing channel $k^{'}-1$ is better than accessing channel $k^{'}$. Hence, Alice and Bob has the motivation to deviate from this strategy, which contradicts the definition of Nash equilibrium.

2. If $k^{'} < k_m$, then

$$R_{k'} \leq \frac{N-k^{'}}{\sum_{l=k'}^{N} \frac{1}{R_l}}, \tag{5.17}$$

so

$$p_{k'}^{j} = 1 - \frac{\frac{N-k^{'}}{R_i}}{\sum_{l=k'}^{N} \frac{1}{R_l}} \leq 0.$$

This contradicts with our assumption that $E = \{k^{'}, k^{'}+1, ..., N\}$ which means $p_{k'}^{j} > 0$.

So in the Nash equilibrium,

$$k^* = \min\left\{k | R_k > \frac{N-k}{\sum_{i=k}^{N} \frac{1}{R_i}}\right\}, \tag{5.18}$$

$$p_i^{j*} = 1 - \frac{\frac{N-k^*}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \quad \forall i \in \{k^*, k^*+1, ..., N\}. \tag{5.19}$$

In the following, we characterize $\mathbf{p}^{t^*}$ and $\mathbf{p}^{r^*}$.

First we show that $k_1 = k^*$. If $k_1 = k^* - 1$, then we have

$$R_{k^*-1} = C_0 = \frac{N-k^*}{\sum_{i=k^*}^{N} \frac{1}{R_i}}$$

and

$$R_{k^*} \geq R_{k^*-1}.$$

The total reward of Alice and Bob is

$$\begin{aligned}
\bar{R} &= \sum_{i=k_1}^{N} R_i p_i^t p_i^r (1 - p_i^{j^*}) \\
&= R_{k^*-1} p_{k^*-1}^t p_{k^*-1}^r + C_0 \left(\sum_{i=k^*}^{N} p_i^t p_i^r \right) \\
&= C_0 \left(p_{k^*-1}^t p_{k^*-1}^r + p_{k^*}^t p_{k^*}^r + \sum_{i=k^*+1}^{N} p_i^t p_i^r \right) \\
&\leq C_0 \left[(p_{k^*-1}^t + p_{k^*}^t)(p_{k^*-1}^r + p_{k^*}^r) + \sum_{i=k^*+1}^{N} p_i^t p_i^r \right] \\
&= C_0 \left[{p_{k^*}^t}' {p_{k^*}^r}' + \sum_{i=k^*+1}^{N} p_i^t p_i^r \right],
\end{aligned}$$

and the equality holds when $p_{k^*-1}^t = p_{k^*-1}^r = 0$. So the reward of Alice and Bob will increase if they transfer their effort of accessing channel $k^* - 1$ to accessing channel k^*. So $k_1 = k^* - 1$ is not a Nash equilibrium. So $k_1 = k^*$.

Since $k_1 = k^*$, we can build two vectors $\vec{A_1}$ and $\vec{A_2}$,

$$\begin{aligned}
\vec{A_1} &= [\sqrt{p_1^{t^*}}, \sqrt{p_2^{t^*}}, ..., \sqrt{p_N^{t^*}}], \\
\vec{A_2} &= [\sqrt{p_1^{r^*}}, \sqrt{p_2^{r^*}}, ..., \sqrt{p_N^{r^*}}],
\end{aligned}$$

$\vec{A_1}$ and $\vec{A_2}$ are two vector in $\mathbb{R}^N$. Then $|\vec{A_1}| = 1$ and $|\vec{A_2}| = 1$.

$$\begin{aligned}
\vec{A_1} \cdot \vec{A_2} &= \sum_{i=k^*}^{N} \sqrt{p_i^{t^*} p_i^{r^*}} \\
&= \sum_{i=k^*}^{N} \sqrt{\frac{C_1}{R_i}} \\
&\leq |\vec{A_1}||\vec{A_2}| = 1,
\end{aligned}$$

the equality holds when $\vec{A_1}$ and $\vec{A_2}$ have the same direction. $\vec{A_1}$ and $\vec{A_2}$ also have same length, so they are equal. Then

$$C_1 = \frac{1}{\left(\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}} \right)^2}.$$

So

$$p_i^{t^*} = p_i^{r^*} = \sqrt{\frac{C_1}{R_i}} = \frac{\frac{1}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}.$$

So the Nash equilibrium is

$$p_i^{t*} = p_i^{r*} = \frac{\frac{1}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}},$$
$$p_i^{j*} = 1 - \frac{\frac{N-k^*}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}},$$

for $k^* \leq i \leq N$, where $k^* = \min\{k | R_k > \frac{N-k}{\sum_{i=k}^{N} \frac{1}{R_i}}\}$. □

5.2 Remark

Remark 5.2.1. *Since the Nash equilibrium is obtained, the average throughput is*

$$\bar{R} = \frac{N - k^*}{\left(\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}\right)^2}. \tag{5.20}$$

Remark 5.2.2. *In the Nash equilibrium, Alice, Bob and Eve always operate on the same set of channels. In particular,* $A = B = E = \{k^*, \cdots, N\}$.

Remark 5.2.3. *Alice, Bob and Eve do not always access or jam all channels.* k^* *is a variable that is for Alice, Bob and Eve to decide on which channels they should take actions. Figure 5.10 shows* k^* *separates "good" channels and "bad" channels. Alice, Bob and Eve have no motivation to access or jam channels from 1 to* $k^* - 1$.

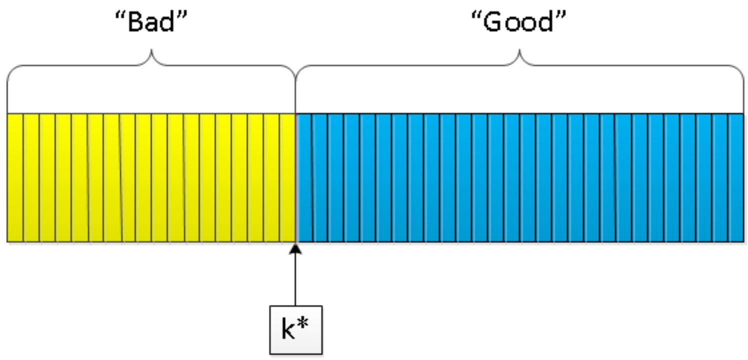

Figure 5.10: k^* separates "good" channels and "bad" channels.

Remark 5.2.4. *When the channel quality is better, Eve jams this channel with a larger probability while Alice and Bob access this channel with a smaller probability.*

Remark 5.2.5. *It is simple to verify that* $N - k^* + 1 \geq 2$. *This implies that Alice and Bob will access at least two channels. Otherwise, if they access only one channel, this channel will be jammed by the attacker with probability 1.*

Chapter 6

One Access Multiple Jamming Case

In this chapter, we assume that Eve can jam more than one channels simultaneously, while Alice and Bob can transmit and receive through only one channel each time. Let M_j denote the number of channels Eve can jam simultaneously, $1 \leq M_j \leq N$. Let Ω_E denote the set of channels Eve jams, where Ω_E has M_j elements. So $p_i^j = \sum_{\substack{\Omega_E \\ i\in\Omega_E}} p_{\Omega_E}^j$.

The Nash equilibrium is given at the beginning of this chapter, and the proof is given in Section 6.1. Remarks about this case are given in Section 6.2.

Lemma 6.0.6. *The Nash Equilibrium in this case is,*

$$p_i^{t*} = p_i^{r*} = \frac{\frac{1}{\sqrt{R_i}}}{\sum_{l=k}^{N} \frac{1}{\sqrt{R_l}}}, \tag{6.1}$$

$$p_i^{j*} = 1 - \frac{\frac{(N-k+1)-M_j}{R_i}}{\sum_{l=k}^{N} \frac{1}{R_l}}, \tag{6.2}$$

for $k^* \leq i \leq N$, *where* $k = \min\left\{k | R_k > \frac{(N-k+1)-M_j}{\sum_{i=k}^{N} \frac{1}{R_i}}\right\}$, *and*

$$p_i^{t*} = p_i^{r*} = p_i^{j*} = 0, \quad \forall i < k^*. \tag{6.3}$$

Figure 6.1, Figure 6.2 and Figure 6.3 give an example to illustrate our results with $M_j = 2$. Figure 6.1 shows the channel capacity. Figure 6.2 shows the strategy of Alice

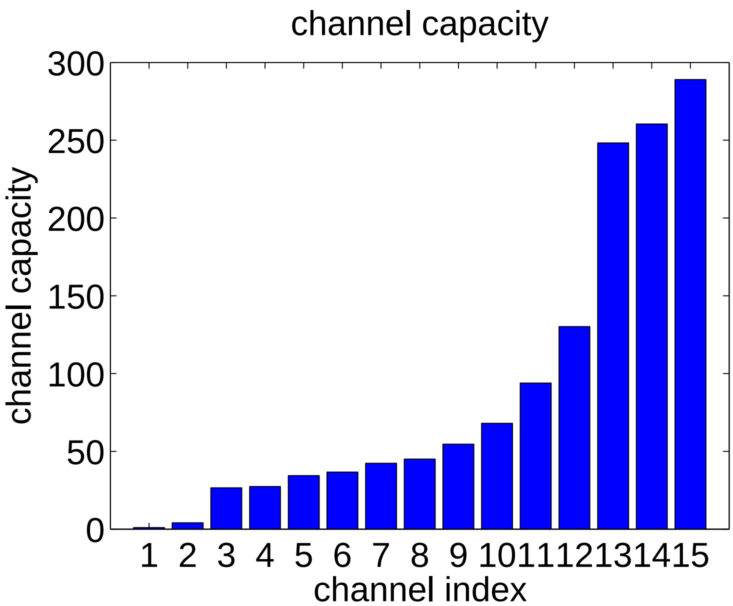

Figure 6.1: Channel Quality ($N = 15$, $k^* = 12$).

and Bob, we can see that Alice and Bob only access channels from k^* to N, and when the channel quality is better, Alice and Bob access this channel with a smaller probability. Figure 6.3 shows the strategy of Eve, we can see that Eve only jams channels from k^* to N, and when the channel quality is better Eve jams this channel with a larger probability.

6.1 Proof

Proof. Similarly, the can prove that $E = \{k^*, k^*+1, ..., N\}$ and $A = B = \{k_1, k_1+1, ..., N\}$, $k-1 \leq k_1 \leq k$. The strategy of Eve in the Nash equilibrium be found, then we can get $A = B = E$. Then we can get the Nash Equilibrium using vector.

The reward of Alice and Bob accessing channel i is

$$R_i \left(1 - \sum_{\substack{\Omega_E \\ i \in \Omega_E}} p^j_{\Omega_E} \right),$$

where $p^j_{\Omega_E}$ is the probability for Eve to choose jamming channel set Ω_E.

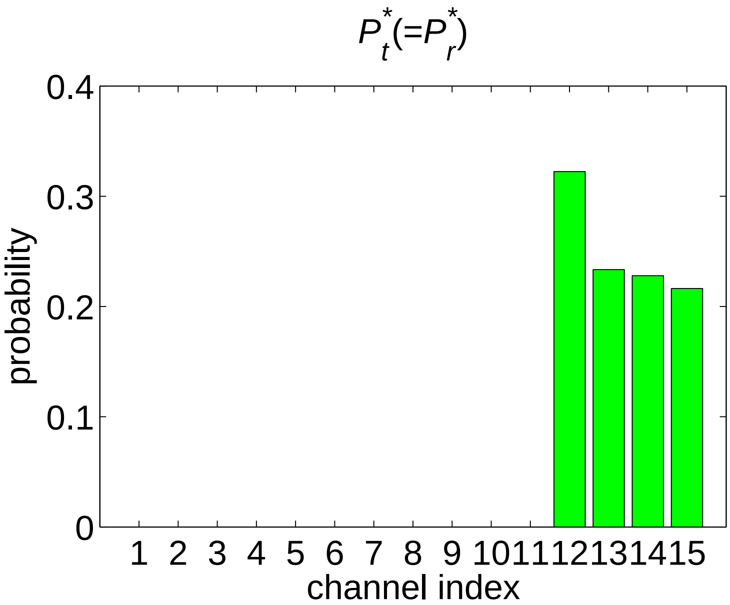

Figure 6.2: $P^{t*}(= P^{r*})$ $(N = 15,\ k^* = 12)$.

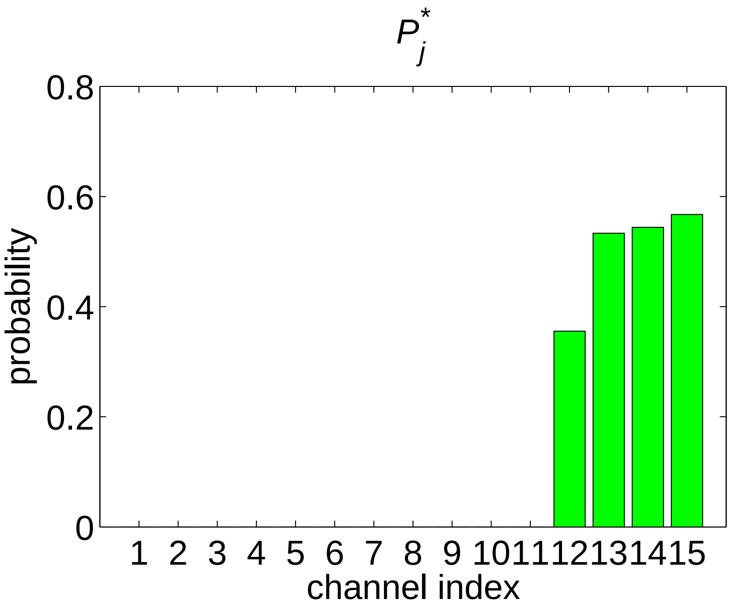

Figure 6.3: P^{j*} $(N = 15,\ k^* = 12)$.

The reward of Eve jamming channel i is

$$\sum_{\substack{\Omega_E \\ i\in\Omega_E}} \left(- \sum_{j\notin\Omega_E} R_j p_j^t p_j^r \right) = \sum_{i\in\Omega_E}^{\Omega_E} \left(S + \sum_{j\in\Omega_E} R_j p_j^t p_j^r \right),$$

where $S = -\sum_j R_j p_j^t p_j^r$.

Similarly, the can prove that $E = \{k^*, k^*+1, ..., N\}$ and $A = B = \{k_1, k_1+1, ..., N\}$, $k^*-1 \le k_1 \le k^*$. To achieve the Nash equilibrium,

$$R_i \left(1 - \sum_{\substack{\Omega_E \\ i\in\Omega_E}} {p_{\Omega_E}^j}^* \right) = C_1, \forall i \ge k^* \tag{6.4}$$

$$\sum_{\substack{\Omega_E \\ i\in\Omega_E}} \left(S + \sum_{j\in\Omega_E} R_j {p_j^t}^* {p_j^r}^* \right) = C_2, \forall i \ge k_1 \tag{6.5}$$

where C_1, C_2 are constants independent of Ω_E.

From

$$R_i \left(1 - \sum_{\substack{\Omega_E \\ i\in\Omega_E}} {p_{\Omega_E}^j}^* \right) = C_1,$$

we have

$$\begin{aligned}
1 - \sum_{\substack{\Omega_E \\ i\in\Omega_E}} {p_{\Omega_E}^j}^* &= \frac{C_1}{R_i}, \\
\sum_{i=k^*}^{N} \left(1 - \sum_{\substack{\Omega_E \\ i\in\Omega_E}} {p_{\Omega_E}^j}^* \right) &= \sum_{i=k^*}^{N} \frac{C_1}{R_i}, \\
(N-k^*+1) - \sum_{i=k^*}^{N} \sum_{\substack{\Omega_E \\ i\in\Omega_E}} {p_{\Omega_E}^j}^* &= C_1 \sum_{i=k^*}^{N} \frac{1}{R_i}, \\
(N-k^*+1) - \frac{\binom{N-k^*}{M_j-1}(N-k^*+1)}{\binom{N-k^*+1}{M_j}} &= C_1 \sum_{i=k^*}^{N} \frac{1}{R_i}, \\
C_1 &= \frac{(N-k^*+1) - M_j}{\sum_{i=k^*}^{N} \frac{1}{R_i}}, \\
{p_i^j}^* = \sum_{\substack{\Omega \\ i\in\Omega}} {p_{\Omega_E}^j}^* &= 1 - \frac{\frac{(N-k^*+1)-M_j}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}.
\end{aligned}$$

Similarly, we can prove

$$k^* = \min\left\{k|R_k > \frac{(N-k+1)-M_j}{\sum_{i=k}^{N}\frac{1}{R_i}}\right\}. \tag{6.6}$$

Obviously, $k^* \leq N - M_j$, that is, Eve has at least $M_j + 1$ channels to jam, then Alice and Bob have at least $M_j + 1$ channels to access.

From

$$\sum_{\substack{\Omega_E \\ i\in\Omega_E}} \left(S + \sum_{j\in\Omega_E} R_j p_j^{t*} p_j^{r*}\right) = C_2,$$

noting S is the same for all different i and

$$|\{\Omega_E | i \in \Omega_E\}| = \binom{N-k_1}{M_j - 1} \tag{6.7}$$

is independent of i, we can rewrite equation 6.7 as

$$\sum_{\substack{\Omega_E \\ i\in\Omega_E}} \sum_{j\in\Omega_E} R_j p_j^{t*} p_j^{r*} = C_3, \tag{6.8}$$

where C_3 is independent of i.

Let us consider two different channels i and j,

$$\begin{aligned}
& \sum_{\substack{\Omega_E \\ i\in\Omega_E}} \sum_{m\in\Omega_E} R_m {p_m^t}^* {p_m^r}^* = \sum_{\substack{\Omega_E \\ j\in\Omega_E}} \sum_{m\in\Omega_E} R_m {p_m^t}^* {p_m^r}^*, \\
& \sum_{\substack{\Omega_E \\ i\in\Omega_E, j\in\Omega_E}} \sum_{m\in\Omega_E} R_m {p_m^t}^* {p_m^r}^* + \sum_{\substack{\Omega_E \\ i\in\Omega_E, j\notin\Omega_E}} \sum_{m\in\Omega_E} R_m {p_m^t}^* {p_m^r}^* \\
= & \sum_{\substack{\Omega_E \\ i\in\Omega_E, j\in\Omega_E}} \sum_{m\in\Omega_E} R_m {p_m^t}^* {p_m^r}^* + \sum_{\substack{\Omega_E \\ i\notin\Omega_E, j\in\Omega_E}} \sum_{m\in\Omega_E} R_m {p_m^t}^* {p_m^r}^*, \\
& \sum_{\substack{\Omega_E \\ i\in\Omega_E, j\notin\Omega_E}} \sum_{m\in\Omega_E} R_m {p_m^t}^* {p_m^r}^* = \sum_{\substack{\Omega_E \\ i\notin\Omega_E, j\in\Omega_E}} \sum_{m\in\Omega_E} R_m {p_m^t}^* {p_m^r}^*, \\
& \sum_{\substack{\Omega_E \\ i\in\Omega_E, j\notin\Omega_E}} \sum_{m\in\Omega_E\backslash\{i\}} R_m {p_m^t}^* {p_m^r}^* + \sum_{\substack{\Omega_E \\ i\in\Omega_E, j\notin\Omega_E}} R_i p_i^{t*} p_i^{r*} \\
= & \sum_{\substack{\Omega_E \\ i\notin\Omega_E, j\in\Omega_E}} \sum_{m\in\Omega_E\backslash\{j\}} R_m {p_m^t}^* {p_m^r}^* + \sum_{\substack{\Omega_E \\ i\notin\Omega_E, j\in\Omega_E}} R_j p_j^{t*} p_j^{r*},
\end{aligned}$$

Notice that

$$\sum_{\substack{\Omega_E \\ i\in\Omega_E, j\notin\Omega_E}} \sum_{m\in\Omega_E\setminus\{i\}} R_m {p_m^t}^* {p_m^r}^* = \sum_{\substack{\Omega_1 \\ i\notin\Omega_1, j\notin\Omega_1}} \sum_{m\in\Omega_1} R_m {p_m^t}^* {p_m^r}^*,$$

$$\sum_{\substack{\Omega_E \\ i\notin\Omega_E, j\in\Omega_E}} \sum_{m\in\Omega_E\setminus\{j\}} R_m {p_m^t}^* {p_m^r}^* = \sum_{\substack{\Omega_1 \\ i\notin\Omega_1, j\notin\Omega_1}} \sum_{m\in\Omega_1} R_m {p_m^t}^* {p_m^r}^*,$$

where Ω_1 is a $M-1$ set. So we have

$$\sum_{\substack{\Omega_E \\ i\in\Omega_E, j\notin\Omega_E}} R_i p_i^{t*} p_i^{r*} = \sum_{\substack{\Omega_E \\ i\notin\Omega_E, j\in\Omega_E}} R_j {p_j^t}^* p_j^{r*},$$

that is

$$|\{\Omega | i\in\Omega, j\notin\Omega\}| R_i p_i^{t*} p_i^{r*} = |\{\Omega | i\notin\Omega, j\in\Omega\}| R_j {p_j^t}^* p_j^{r*}.$$

Because

$$|\{\Omega | i\in\Omega, j\notin\Omega\}| = |\{\Omega | i\notin\Omega, j\in\Omega\}| = \binom{N-k-1}{M_j-2},$$

so we have

$$R_i p_i^{t*} p_i^{r*} = R_j {p_j^t}^* p_j^{r*},$$

thus

$$R_i p_i^{t*} p_i^{r*} = C_4,$$

for all i, where C_4 is a constant independent of i.

Then we transform our problem into this: For Alice and Bob, find the optimal solution of

$$\bar{R} = \sum_{i\in A} R_i p_i^{t*} p_i^{r*} \left(1 - \sum_{\substack{\Omega_E \\ i\in\Omega_E}} {p_{\Omega_E}^j}^*\right), \tag{6.9}$$

$$\sum_{\substack{\Omega_E \\ i\in\Omega_E}} {p_{\Omega_E}^j}^* = 1 - \frac{\frac{(N-k^*+1)-M_j}{R_i}}{\sum_{i=k^*}^N \frac{1}{R_i}}, \tag{6.10}$$

$$R_i p_i^{t*} p_i^{r*} = C_3. \tag{6.11}$$

This problem has been solved in Chapter 5. Using the same method, we can prove $k_1 = k^*$. Then the Nash equilibrium for Alice and Bob is

$$p_i^{t*} = p_i^{r*} = \frac{\frac{1}{\sqrt{R_i}}}{\sum_{l=k^*}^N \frac{1}{\sqrt{R_l}}}, \quad \forall k^* \le i \le N.$$

So for the multiple jamming case, the Nash equilibrium is

$$\begin{aligned} p_i^{t*} &= p_i^{r*} = \frac{\frac{1}{\sqrt{R_i}}}{\sum_{i=k^*}^{N} \frac{1}{\sqrt{R_i}}}, \\ p_i^{j*} &= 1 - \frac{\frac{(N-k^*+1)-M_j}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \end{aligned} \tag{6.12}$$

where $k^* = \min\left\{k|R_k > \frac{(N-k+1)-M_j}{\sum_{i=k}^{N}\frac{1}{R_i}}\right\}$, and

$$p_i^{t*} = p_i^{r*} = p_i^{j*} = 0, \quad \forall i < k^*. \tag{6.13}$$

Notice that Ω_E is a M_j-element set and the element are chosen without replacement in $\{k^*, k^*+1, ..., N\}$. So Ω_E can take $\binom{N-k^*+1}{M_j}$ values. In the Nash equilibrium, we have $(N-k^*+1)$ equations. It can be easily verified that $N-k^*+1 \geq 2$. So $\binom{N-k^*+1}{M_j} > (N-k^*+1)$ for $M_j \geq 2$, which means $p_{\Omega_E}^j$ has infinite number of solutions. So Eve has infinite number of specific strategies in the Nash equilibrium, but these strategies have to satisfy

$$\sum_{\substack{\Omega_E \\ i\in\Omega_E}} p_{\Omega_E}^{j\,*} = 1 - \frac{\frac{(N-k^*+1)-M_j}{R_i}}{\sum_{l=k^*}^{N}\frac{1}{R_l}}.$$

□

6.2 Remark

Remark 6.2.1. *Since the Nash equilibrium is obtained, the average throughput is*

$$\bar{R} = \frac{N-k^*+1-M_j}{\left(\sum_{l=k^*}^{N}\frac{1}{\sqrt{R_l}}\right)^2}. \tag{6.14}$$

Remark 6.2.2. *In the Nash equilibrium, Alice, Bob and Eve always operate on the same set of channels. In particular,* $A = B = E = \{k^*, \cdots, N\}$.

Remark 6.2.3. *Alice, Bob and Eve do not always access or jam all channels.* k^* *is a variable that is for Alice, Bob and Eve to decide on which channels they should take actions. Figure 6.4 shows* k^* *separates "good" channels and "bad" channels. Alice, Bob and Eve have no motivation to access or jam channels from 1 to* k^*-1.

Remark 6.2.4. *k^* is determined by the channel capacity and M_j, and it is not related to Alice and Bob.*

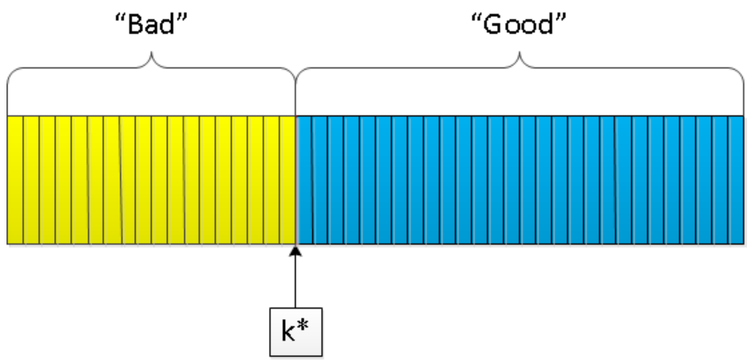

Figure 6.4: k^* separates "good" channels and "bad" channels.

Remark 6.2.5. *When the channel quality is better, Eve jams this channel with a larger probability while Alice and Bob access this channel with a smaller probability.*

Remark 6.2.6. *It is simple to verify that $N - k^* + 1 \geq M_j + 1$. This implies that Alice and Bob will access at least $M_j + 1$ channels. Otherwise, if they access only M_j channels, this channel will be jammed by the attacker with probability 1.*

Remark 6.2.7. *Alice and Bob have a unique Nash equilibrium, while Eve has infinite number of strategies in the Nash equilibrium if $M_j \geq 2$. The Nash equilibrium of Eve is given in the form of marginal distribution.*

Chapter 7

Multiple Access One Jamming Case

In this chapter, we study the case the sender and receiver can access multiple channels in one time slot, but the attacker can only jam one channel at a time. We assume Alice and Bob can access M_t and M_r channels respectively, where $1 \leq M_t \leq N$ and $1 \leq M_r \leq N$. The strategy of Alice and Bob taken in a time slot is denoted by Ω_A and Ω_B. Obviously, Ω_A and Ω_B are subset of A and B , and Ω_A and Ω_B are M_t set and M_r set respectively. Let p_i^t denote $\sum_{\substack{\Omega_A \\ i \in \Omega_A}} p_{\Omega_A}^t$, and p_i^r denote $\sum_{\substack{\Omega_B \\ i \in \Omega_B}} p_{\Omega_B}^r$. S is a subset of $\{1, 2, ..., N\}$, then $R_S \triangleq \sum_{i \in S} R_i$. And without loss of generality, we can assume $M_t \geq M_r$.

The Nash equilibrium is given at the beginning of this chapter, and the proof is given in Section 7.1. Remarks about this case are given in Section 7.2.

Lemma 7.0.8. *The Nash equilibrium in this case is given under three different conditions:*

1. *Case 1:*

If $N - k^* + 1 > M_t$,

$$p_i^{t*} = \frac{\frac{M_t}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}, \tag{7.1}$$

$$p_i^{r*} = \frac{\frac{M_r}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}, \tag{7.2}$$

$$p_i^{j*} = 1 - \frac{\frac{N-k^*}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \tag{7.3}$$

for $k^* \leq i \leq N$,
where $k^* = \min \left\{ k | R_k > \frac{N-k}{\sum_{i=k}^{N} \frac{1}{R_i}} \right\}$, *and*

$$p_i^{t*} = p_i^{r*} = p_i^{j*} = 0, \quad \forall i < k^*. \tag{7.4}$$

2. *Case 2:*

If $M_t \geq N - k^* + 1 > M_r$,

$$p_i^{t*} = 1, \tag{7.5}$$

for $N - M_t + 1 \leq i \leq N$,

$$p_i^{r*} = \frac{\frac{M_r}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}, \tag{7.6}$$

$$p_i^{j*} = 1 - \frac{\frac{N-k^*}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \tag{7.7}$$

for $k^* \leq i \leq N$,
where $k^* = \min \left\{ k | R_k > \frac{N-k}{\sum_{i=k}^{N} \frac{1}{R_i}} \right\}$, *and*

$$p_i^{t*} = 0, \quad \forall i < N - M_t + 1, \tag{7.8}$$

$$p_i^{r*} = p_i^{j*} = 0, \quad \forall i < k^*. \tag{7.9}$$

3. *Case 3:*

If $N - k^* + 1 \leq M_r$,

$$p_i^{t*} = \frac{\frac{M_t}{\sqrt{R_i}}}{\sum_{l=k_t}^{N} \frac{1}{\sqrt{R_l}}}, \quad k_t \leq i \leq N$$

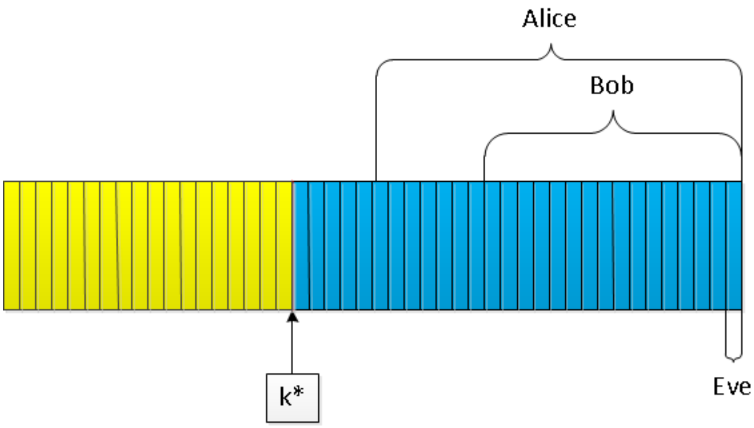

Figure 7.1: Illustration of case 1 in one access multiple jamming case.

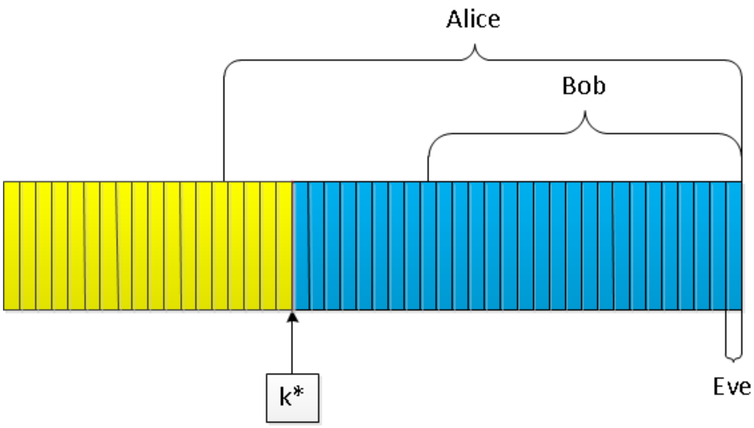

Figure 7.2: Illustration of case 2 in one access multiple jamming case.

$$p_i^{r*} = \frac{\frac{M_r}{\sqrt{R_i}}}{\sum_{l=k_t}^{N} \frac{1}{\sqrt{R_l}}}, \quad k_t \leq i \leq N$$

$$p_i^{j*} = 1 - \frac{\frac{N-k^*}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \quad k^* \leq i \leq N$$

$$where\ k^* = \min\left\{k|R_k > \frac{N-k}{\sum_{i=k}^{N} \frac{1}{R_i}}\right\},\ k_t = \max\left\{k|\frac{\frac{M_t}{\sqrt{R_k}}}{\sum_{i=k}^{N} \frac{1}{\sqrt{R_i}}} \leq 1\right\}.$$

Figure 7.1, Figure 7.2 and Figure 7.3 illustrate the three cases respectively, and notice the brackets denote the number of channels one can access or jam, not the strategy. We can see that case 1 is the case Alice and Bob cannot access all the channels from k^* to N,

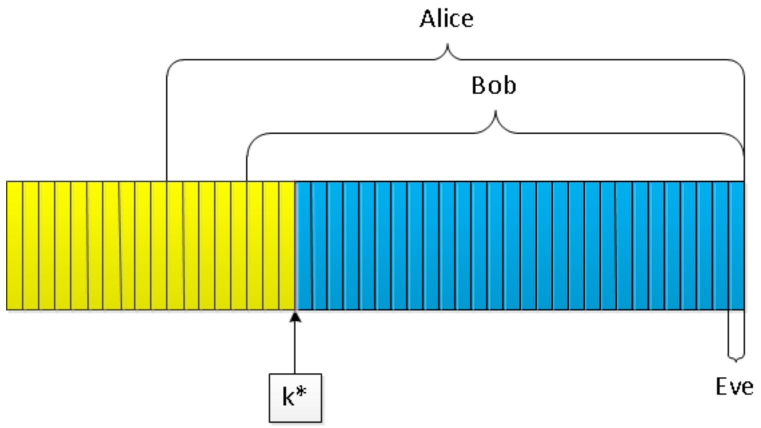

Figure 7.3: Illustration of case 3 in one access multiple jamming case.

case 2 is the case only one of Alice and Bob can access all the channels from k^* to N, and case 3 is the case both Alice and Bob can access all the channels from k^* to N.

- Figure 7.4 shows the channel capacity.

- Figure 7.5 and Figure 7.6 give an example to illustrate case 1 with $M_t = M_r = 2$. Figure 7.5 shows the strategy of Alice and Bob, we can see that Alice and Bob only access channels from k^* to N, and when the channel quality is better, Alice and Bob access this channel with a smaller probability. Figure 7.6 shows the strategy of Eve, we can see that Eve only jams channels from k^* to N, and when the channel quality is better Eve jams this channel with a larger probability.

- Figure 7.7, Figure 7.8 and Figure 7.9 give an example to illustrate case 2 with $M_t = 4$, $M_r = 2$. Figure 7.7 shows the strategy of Alice, we can see that Alice takes constant strategy. Figure 7.8 shows the strategy of Bob, we can see that Bob only access channels from k^* to N, and when the channel quality is better, Bob access this channel with a smaller probability. Figure 7.9 shows the strategy of Eve, we can see that Eve only jams channels from k^* to N, and when the channel quality is better Eve jams this channel with a larger probability.

- Figure 7.10, Figure 7.11 and Figure 7.12 give an example to illustrate case 2 with $M_t = 4$, $M_r = 4$. Figure 7.10 and Figure 7.11 shows the strategy of Alice and Bob,

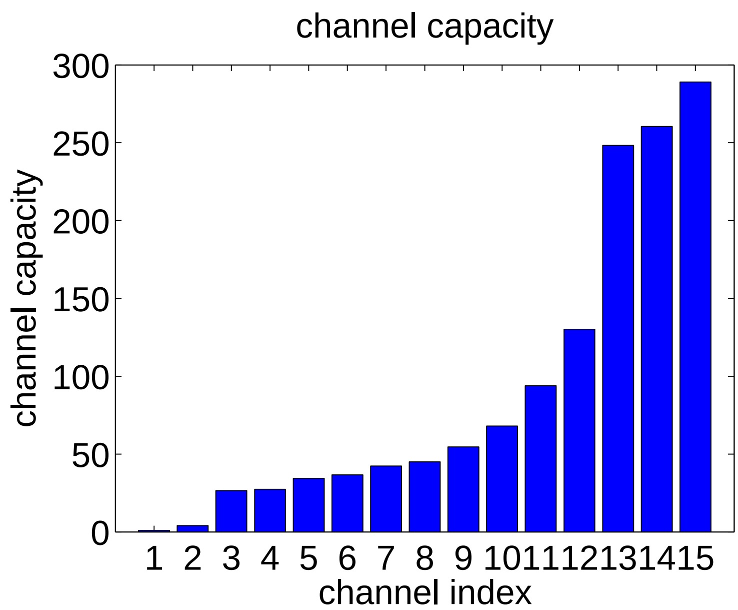

Figure 7.4: Channel Quality ($N = 15$, $k^* = 13$).

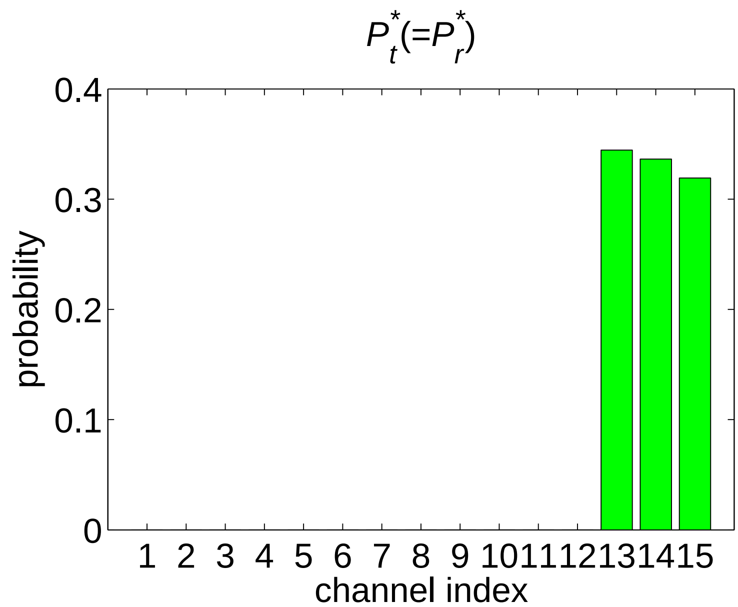

Figure 7.5: Case 1: $P^{t*}(= P^{r*})$ ($N = 15$, $k^* = 13$).

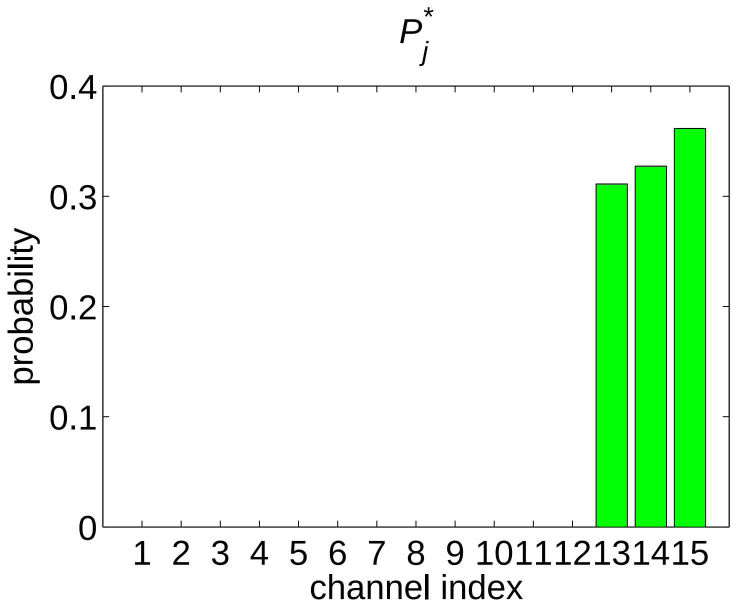

Figure 7.6: Case 1: P^{j*} ($N = 15$, $k^* = 13$).

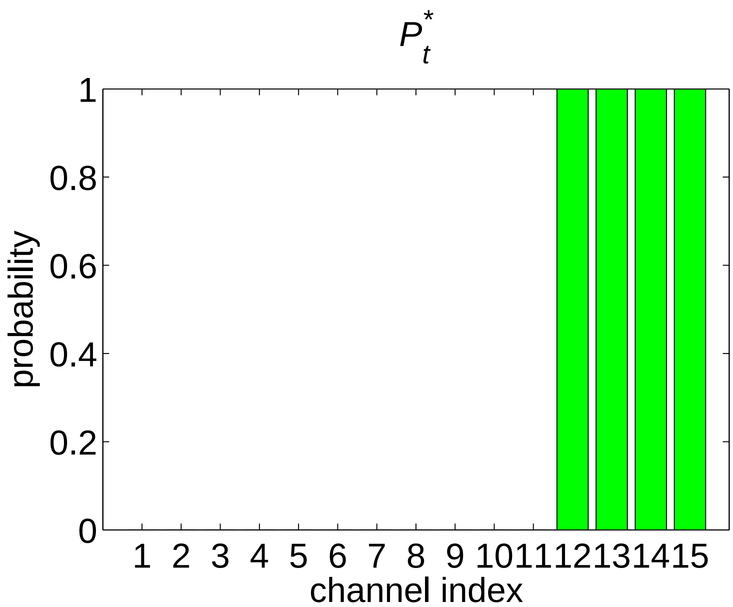

Figure 7.7: Case 2: P^{t*} ($N = 15$, $k^* = 13$).

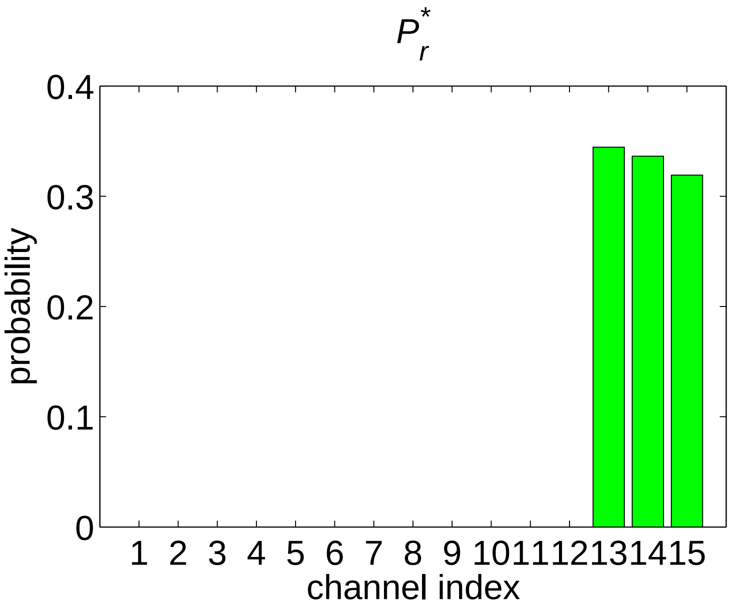

Figure 7.8: Case 2: P^{r*} ($N = 15$, $k^* = 13$).

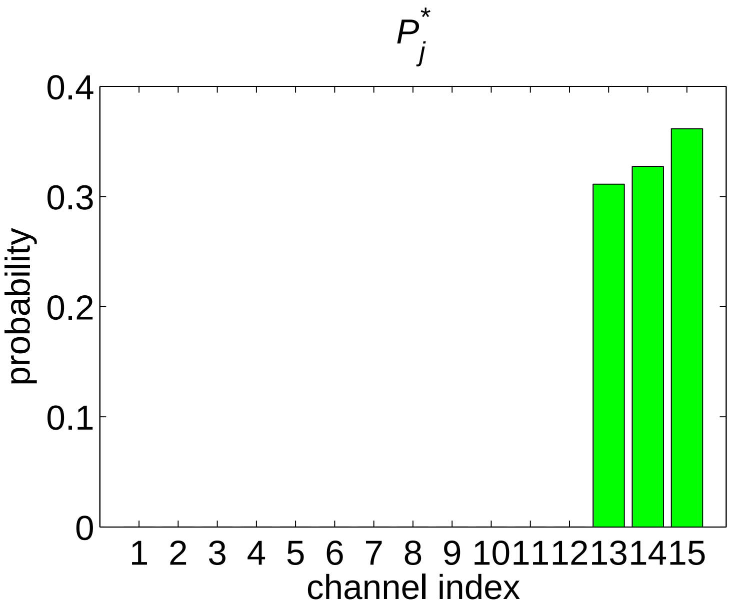

Figure 7.9: Case 2: P^{j*} ($N = 15$, $k^* = 13$).

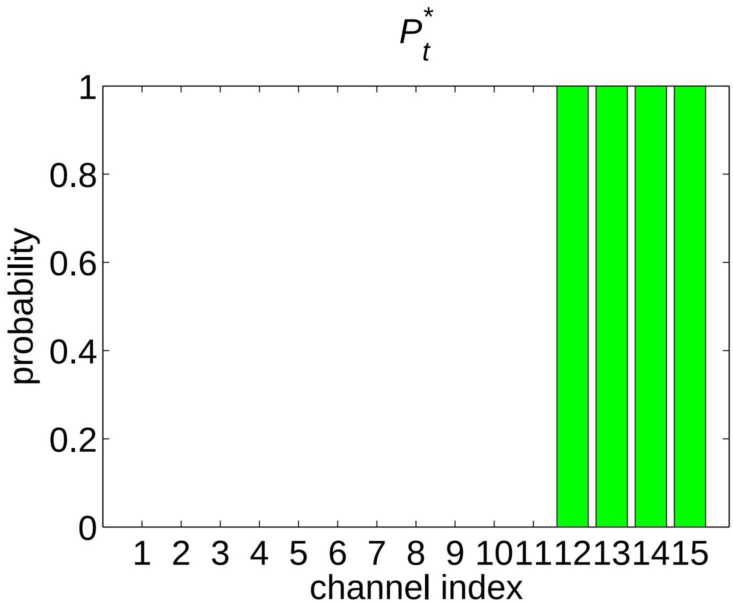

Figure 7.10: Case 3: P^{t*} ($N = 15$, $k^* = 13$).

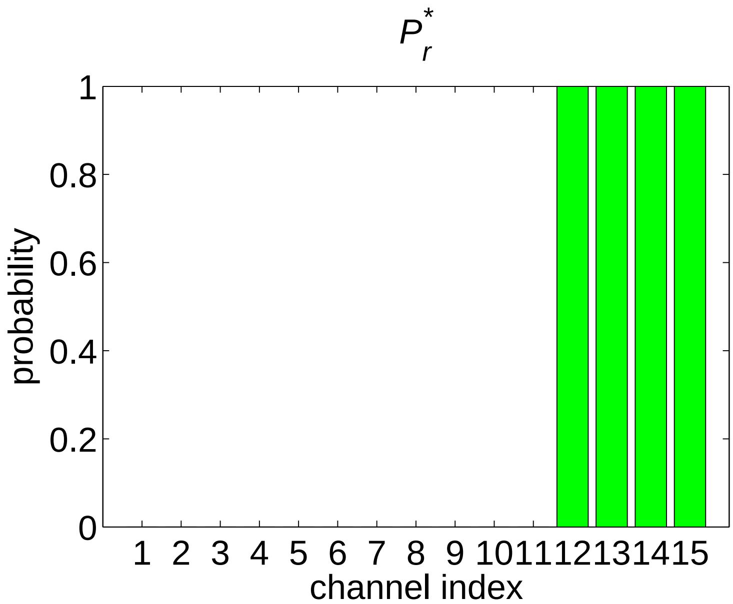

Figure 7.11: Case 3: P^{r*} ($N = 15$, $k^* = 13$).

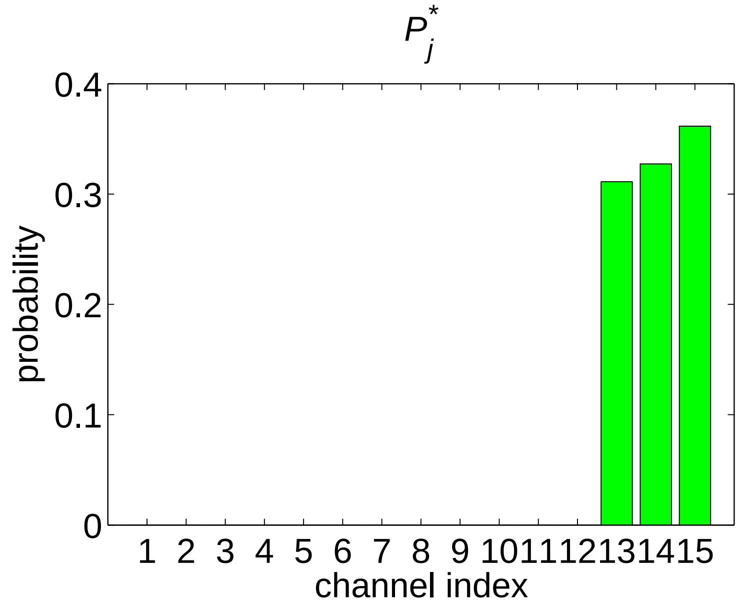

Figure 7.12: Case 3: P^{j^*} ($N = 15$, $k^* = 13$).

we can see that both Alice and Bob take constant strategy. Figure 7.12 shows the strategy of Eve, we can see that Eve only jams channels from k^* to N, and when the channel quality is better Eve jams this channel with a larger probability.

7.1 Proof

Proof. The reward of Alice and Bob accessing channel i is

$$\begin{aligned}
& \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \left(\sum_{m\in\Omega_A\cap\Omega_B} R_{\Omega_A\cap\Omega_B\setminus\{m\}} p_m^j + \sum_{m\notin\Omega_A\cap\Omega_B} R_{m\notin\Omega_A\cap\Omega_B} p_m^j \right) \\
= & \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \left[\sum_{m\in\Omega_A\cap\Omega_B} \left(R_{\Omega_A\cap\Omega_B} - R_m\right) p_m^j + R_{\Omega_A\cap\Omega_B} \left(1 - \sum_{m\in\Omega_A\cap\Omega_B} p_m^j \right) \right] \\
= & \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B} R_m \left(1 - p_m^j\right)
\end{aligned} \tag{7.10}$$

The reward of Eve jamming channel i is

$$
\begin{aligned}
& -\sum_{\Omega_A,\Omega_B} R_{\Omega_A\cap\Omega_B\backslash\{i\}} p^t_{\Omega_A} p^r_{\Omega_B} \\
= & -\sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} R_{\Omega_A\cap\Omega_B\backslash\{i\}} p^t_{\Omega_A} p^r_{\Omega_B} - \sum_{\substack{\Omega_A,\Omega_B \\ i\notin\Omega_A\cap\Omega_B}} R_{\Omega_A\cap\Omega_B} p^t_{\Omega_A} p^r_{\Omega_B} \\
= & -\sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B} - R_i\right) p^t_{\Omega_A} p^r_{\Omega_B} - \sum_{\substack{\Omega_A,\Omega_B \\ i\notin\Omega_A\cap\Omega_B}} R_{\Omega_A\cap\Omega_B} p^t_{\Omega_A} p^r_{\Omega_B} \\
= & -\sum_{\Omega_A,\Omega_B} R_{\Omega_A\cap\Omega_B} p^t_{\Omega_A} p^r_{\Omega_B} + R_i \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} p^t_{\Omega_A} p^r_{\Omega_B}
\end{aligned}
$$

To achieve the Nash equilibrium, in support set E,

$$
-\sum_{\Omega_A,\Omega_B} R_{\Omega_A\cap\Omega_B} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* + R_i \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* = C_0
$$

where C_0 is a constant independent of i, notice

$$
-\sum_{\Omega_A,\Omega_B} R_{\Omega_A\cap\Omega_B} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*
$$

is constant for all i, so

$$
R_i \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega B}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* = C_1, \tag{7.11}
$$

where C_1 is a constant independent of i. And in support set A and B,

$$
\sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B} R_m \left(1 - {p^j_m}^*\right) = C_2, \tag{7.12}
$$

where C_2 is a constant independent of Ω_A and Ω_B.

From

$$
R_i \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega B}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* = C_1,
$$

for

$$
p^t_i \triangleq \sum_{i\in\Omega_A} p^t_{\Omega_A}
$$

and

$$
p^r_i \triangleq \sum_{i\in\Omega_B} p^t_{\Omega_B},
$$

then we have

$$\begin{aligned} & R_i \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega B}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* \\ = \; & R_i \left(\sum_{i\in\Omega_A} {p^t_{\Omega_A}}^* \right) \left(\sum_{i\in\Omega_B} {p^r_{\Omega_B}}^* \right) \\ = \; & R_i p_i^{t*} p_i^{r*} \\ = \; & C_1. \end{aligned}$$

From

$$\sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B} R_m \left(1 - {p^j_m}^*\right) = C_2,$$

consider two different channels i and j,

$$\sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B} R_m \left(1 - {p^j_m}^*\right) = \sum_{\substack{\Omega_A,\Omega_B \\ j\in\Omega_A, j\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B} R_m \left(1 - {p^j_m}^*\right),$$

$$\begin{aligned} & \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \left(\sum_{m\in\Omega_A\cap\Omega_B\setminus\{i\}} R_m \left(1 - {p^j_m}^*\right) + R_i \left(1 - p_i^{j*}\right) \right) \\ = & \sum_{\substack{\Omega_A,\Omega_B \\ j\in\Omega_A, j\in\Omega_B}} \left(\sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m \left(1 - {p^j_m}^*\right) + R_j \left(1 - p_j^{j*}\right) \right), \end{aligned}$$

Now we investigate

$$\begin{aligned} & \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{i\}} R_m \left(1 - {p^j_m}^*\right) \\ = & \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B \\ j\in\Omega_A, j\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{i\}} R_m \left(1 - {p^j_m}^*\right) + \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B \\ j\notin\Omega_A, j\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{i\}} R_m \left(1 - {p^j_m}^*\right) \\ & + \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B \\ j\in\Omega_A, j\notin\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{i\}} R_m \left(1 - {p^j_m}^*\right) + \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B \\ j\notin\Omega_A, j\notin\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{i\}} R_m \left(1 - {p^j_m}^*\right), \end{aligned}$$

$$\sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right)$$

$$= \sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\in\Omega_A,i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right) + \sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\notin\Omega_A,i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right)$$
$$+ \sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\in\Omega_A,i\notin\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right) + \sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\notin\Omega_A,i\notin\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right).$$

Let Ω_{A_1} denote a $M_t - 1$ set, so

$$\sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A,i\in\Omega_B\\ j\notin\Omega_A,j\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{i\}} R_m\left(1-{p_m^j}^*\right) = \sum_{\substack{\Omega_{A_1},\Omega_B\\ i\notin\Omega_{A_1},j\in\Omega_B\\ j\notin\Omega_{A_1},i\in\Omega_B}} \sum_{m\in\Omega_{A_1}\cap\Omega_B} R_m\left(1-{p_m^j}^*\right),$$

and

$$\sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\notin\Omega_A,i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right) = \sum_{\substack{\Omega_{A_1},\Omega_B\\ i\notin\Omega_{A_1},j\in\Omega_B\\ j\notin\Omega_{A_1},i\in\Omega_B}} \sum_{m\in\Omega_{A_1}\cap\Omega_B} R_m\left(1-{p_m^j}^*\right).$$

So we have,

$$\sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\notin\Omega_A,i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right) = \sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\notin\Omega_A,i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right).$$

Similarly, we can prove

$$\sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A,i\in\Omega_B\\ j\in\Omega_A,j\notin\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{i\}} R_m\left(1-{p_m^j}^*\right) = \sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\in\Omega_A,i\notin\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right)$$

and

$$\sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\notin\Omega_A,i\notin\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right) = \sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A,j\in\Omega_B\\ i\notin\Omega_A,i\notin\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-{p_m^j}^*\right).$$

Notice

$$
\begin{aligned}
& \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B \\ j\in\Omega_A, j\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{i\}} R_m\left(1-p_m^{j\,*}\right) \\
= & \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B \\ j\in\Omega_A, j\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B} R_m\left(1-p_m^{j\,*}\right) - \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A, i\in\Omega_B \\ j\in\Omega_A, j\in\Omega_B}} R_i\left(1-p_i^{j^*}\right),
\end{aligned}
$$

and

$$
\begin{aligned}
& \sum_{\substack{\Omega_A,\Omega_B \\ j\in\Omega_A, j\in\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B\setminus\{j\}} R_m\left(1-p_m^{j\,*}\right) \\
= & \sum_{\substack{\Omega_A,\Omega_B \\ j\in\Omega_A, j\in\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} \sum_{m\in\Omega_A\cap\Omega_B} R_m\left(1-p_m^{j\,*}\right) - \sum_{\substack{\Omega_A,\Omega_B \\ j\in\Omega_A, j\in\Omega_B \\ i\in\Omega_A, i\in\Omega_B}} R_j\left(1-p_j^{j^*}\right),
\end{aligned}
$$

Hence we have,

$$
\sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B, j\notin\Omega_A\cap\Omega_B}} R_i\left(1-p_i^{j^*}\right) = \sum_{\substack{\Omega_A,\Omega_B \\ j\in\Omega_A\cap\Omega_B, i\notin\Omega_A\cap\Omega_B}} R_j\left(1-p_j^{j^*}\right).
$$

Similar in Chapter 6, $R_i\left(1-p_i^{j^*}\right) = R_j\left(1-p_j^{j^*}\right)$, we have

$$
R_i(1-p_i^{j^*}) = C_3, \quad \forall i \geq k^*.
$$

Similarly, we can give the solution as

$$
p_i^{j^*} \;=\; 1-\frac{\frac{N-k^*}{R_i}}{\sum_{i=k^*}^{N}\frac{1}{R_i}}, \tag{7.13}
$$

for $k^* \leq i \leq N$, where $k^* = \min\left\{k|R_k > \frac{N-k}{\sum_{i=k}^{N}\frac{1}{R_i}}\right\}$.

Now we can notice k^* is determined by the channel quality, but M_t and M_r are determined by users. From discussion in Chapter 5 and Chapter 6, we notice that Alice and Bob have no motivation to access channels from 1 to $k^* - 1$. So we should discuss different cases.

If $N - k^* + 1 > M_t$, from conclusion in Chapter 5 and Chapter 6 we have $k_1 = k^*$, we can simplify our problem as,

$$\begin{aligned} R_i p_i^{t*} p_i^{r*} &= C_1, \forall i \geq k^*, \\ \sum_{i=k^*}^{N} p_i^{t*} &= M_t, \\ \sum_{i=k^*}^{N} p_i^{t*} &= M_r. \end{aligned}$$

Using the same vector method Chapter 5 and Chapter 6, we have

$$\begin{aligned} p_i^{t*} &= \frac{\frac{M_t}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}, \\ p_i^{r*} &= \frac{\frac{M_r}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}, \end{aligned}$$

But there is still one question unanswered: Is $p_i^{t*} < 1$ and $p_i^{r*} < 1$? Now we define we set:

$$\begin{aligned} K_1 &= \left\{ k | R_k > \frac{N-k}{\sum_{i=k}^{N} \frac{1}{R_i}} \right\}, \\ K_2 &= \left\{ k | \sqrt{R_k} > \frac{N-k}{\sum_{i=k}^{N} \frac{1}{\sqrt{R_i}}} \right\}. \end{aligned}$$

For $\forall k \in K_1$,

$$\sum_{i=k}^{N} \frac{R_k}{R_i} > N - k.$$

This is because

$$\frac{R_k}{R_i} \leq 1, \forall i \geq k,$$

so

$$\frac{\sqrt{R_k}}{\sqrt{R_i}} \geq \frac{R_k}{R_i}.$$

Then we have

$$\sum_{i=k}^{N} \frac{\sqrt{R_k}}{\sqrt{R_i}} \geq \sum_{i=k}^{N} \frac{R_k}{R_i} > N - k.$$

So k is also in K_2. So $\min K_1 \geq \min K_2$. So for $k^* = \min\{k | R_k > \frac{N-k}{\sum_{i=k}^{N} \frac{1}{R_i}}\}$,

$$\sqrt{R_{k^*}} > \frac{N - k^*}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}} \geq \frac{M_t}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}.$$

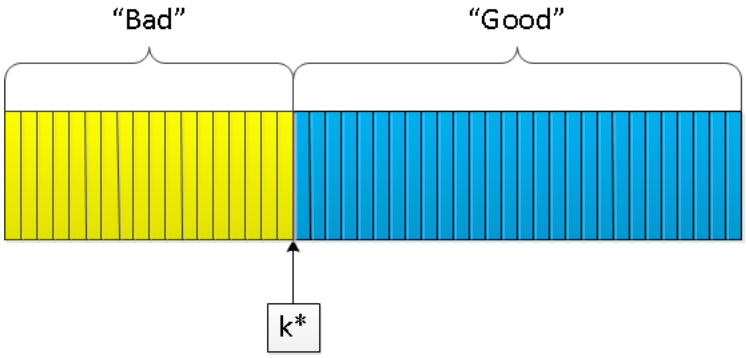

Figure 7.13: k^* separates "good" channels and "bad" channels.

So $p_i^{t*} < 1$. The proof is same for $p_i^{r*} < 1$.

If $M_t \geq N - k^* + 1 > M_r$, Alice can cover all the channel from k^* to N, while Bob cannot. $C_3 = \frac{N-k^*}{\sum_{l=k^*}^{N} \frac{1}{R_l}} \geq R_m$ where $m = 1, 2, ..., k^* - 1$, and we know Alice and Bob have no motivation to access channels except channel k^* to N. So Alice have to constantly access channels from $N - M_t + 1$ to N, and the strategy of Bob keeps random.

If $M_r \geq N - k^* + 1$, both Alice and Bob can cover all the channel from k^* to N. We know Alice and Bob have no motivation to access channels except channel k^* to N, however, both Alice and Bob have to access some other channel to access M_t and M_r channels respectively. So both Alice and Bob will access some channels below k^*. □

7.2 Remark

Remark 7.2.1. *Under the Nash equilibrium in this case, Alice, Bob and Eve do not always operate on the same set of channels.*

Remark 7.2.2. *k^* is a variable that is for Alice, Bob and Eve to decide on which channels they should take actions. Figure 7.13 shows k^* separates "good" channels and "bad" channels. Alice, Bob and Eve have no motivation to access or jam channels from 1 to $k^* - 1$. But in Case 2 and Case 3, Alice and Bob have to access channels from 1 to $k^* - 1$.*

Remark 7.2.3. *k^* is determined by the channel capacity and M_j, and it is not related to Alice and Bob.*

Remark 7.2.4. *When the channel quality is better, Eve jams this channel with a larger probability while Alice and Bob access this channel with a smaller probability.*

Remark 7.2.5. *It is simple to verify that* $N - k^* + 1 \geq 2$. *This implies that Alice and Bob will access at least two channels. Otherwise, if they access only one channel, this channel will be jammed by the attacker with probability 1.*

Remark 7.2.6. *Alice and Bob do not have a unique Nash equilibrium if* $M_t \geq 2$ *and* $M_r \geq 2$, *while Eve has unique strategy under the Nash equilibrium. The Nash equilibrium of Alice and Bob is given in the form of marginal distribution.*

Chapter 8

Multiple Access Multiple Jamming Case

In this chapter, we study the case Alice, Bob and Eve can access or jam more than one channel simultaneously. Alice and Bob can access M_t and M_r channels respectively, while Eve can jam M_j channels, $1 \leq M_t \leq N$, $1 \leq M_r \leq N$ and $1 \leq M_j \leq N$. Let Ω_A, Ω_B and Ω_E denote the set of channels Alice, Bob and Eve access or jam. Ω_A is a M_t set, Ω_B is a M_r set and Ω_E is a M_j set. Let p_i^t denote $\sum_{\substack{\Omega_A \\ i\in\Omega_A}} p_{\Omega_A}^t$, p_i^r denote $\sum_{\substack{\Omega_B \\ i\in\Omega_B}} p_{\Omega_B}^r$ and p_i^j denote $\sum_{\substack{\Omega_E \\ i\in\Omega_E}} p_{\Omega_E}^j$. And without loss of generality, we can assume $M_t \geq M_r$. Figure 8.1 shows an example of multiple access multiple jamming case with $M_t = 2$, $M_r = 2$ and $M_j = 2$.

The Nash equilibrium is given at the beginning of this chapter, and the proof is given in Section 8.1. In the end, some remarks about this case are given in Section 8.2.

Lemma 8.0.7. *The Nash equilirium in this case is given under three different conditions:*

1. *Case 1:*

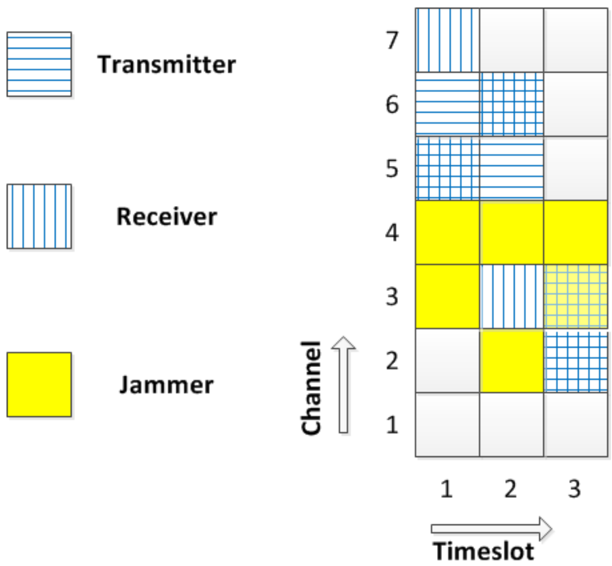

Figure 8.1: Example of multiple access multiple jamming case.

If $N - k^* + 1 > M_t$,

$$p_i^{t*} = \frac{\frac{M_t}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}, \tag{8.1}$$

$$p_i^{r*} = \frac{\frac{M_r}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}, \tag{8.2}$$

$$p_i^{j*} = 1 - \frac{\frac{N-k^*+1-M_j}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \tag{8.3}$$

for $k^* \leq i \leq N$, *where* $k^* = \min\left\{k|R_k > \frac{N-k+1-M_j}{\sum_{i=k}^{N} \frac{1}{R_i}}\right\}$, *and*

$$p_i^{t*} = p_i^{r*} = p_i^{j*} = 0, \quad \forall i < k^*. \tag{8.4}$$

2. *Case 2:*

If $M_t \geq N - k^* + 1 > M_r$,

$$p_i^{t*} = 1, \tag{8.5}$$

for $N - M_t + 1 \le i \le N$,

$$p_i^{r*} = \frac{\frac{M_r}{\sqrt{R_i}}}{\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}}}, \tag{8.6}$$

$$p_i^{j*} = 1 - \frac{\frac{N-k^*+1-M_j}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \tag{8.7}$$

for $k^* \le i \le N$,

where $k^* = \min\left\{k|R_k > \frac{N-k+1-M_j}{\sum_{i=k}^{N}\frac{1}{R_i}}\right\}$, *and*

$$p_i^{r*} = 0, \quad \forall i < N - M_t + 1, \tag{8.8}$$

$$p_i^{r*} = p_i^{j*} = 0, \quad \forall i < k^*. \tag{8.9}$$

3. *Case 3:*

   If $N - k^* + 1 \le M_r$,

$$p_i^{t*} = \frac{\frac{M_t}{\sqrt{R_i}}}{\sum_{l=k_t}^{N} \frac{1}{\sqrt{R_l}}}, \quad k_t \le i \le N$$

$$p_i^{r*} = \frac{\frac{M_r}{\sqrt{R_i}}}{\sum_{l=k_t}^{N} \frac{1}{\sqrt{R_l}}}, \quad k_t \le i \le N$$

$$p_i^{j*} = 1 - \frac{\frac{N-k^*+1-M_j}{R_i}}{\sum_{l=k^*}^{N} \frac{1}{R_l}}, \quad k^* \le i \le N$$

where $k^* = \min\left\{k|R_k > \frac{N-k+1-M_j}{\sum_{i=k}^{N}\frac{1}{R_i}}\right\}$, $k_t = \max\left\{k|\frac{\frac{M_t}{\sqrt{R_k}}}{\sum_{i=k}^{N}\frac{1}{\sqrt{R_i}}} \le 1\right\}$.

Figure 8.2, Figure 8.3 and Figure 8.4 illustrate the three cases respectively, and notice the brackets denote the number of channels one can access or jam, not the strategy. From the figures, we can see that case 1 is the case Alice and Bob cannot access all the channels from k^* to N, case 2 is the case only one of Alice and Bob can access all the channels from k^* to N, and case 3 is the case both Alice and Bob can access all the channels from k^* to N.

- Figure 8.5 shows the channel capacity.

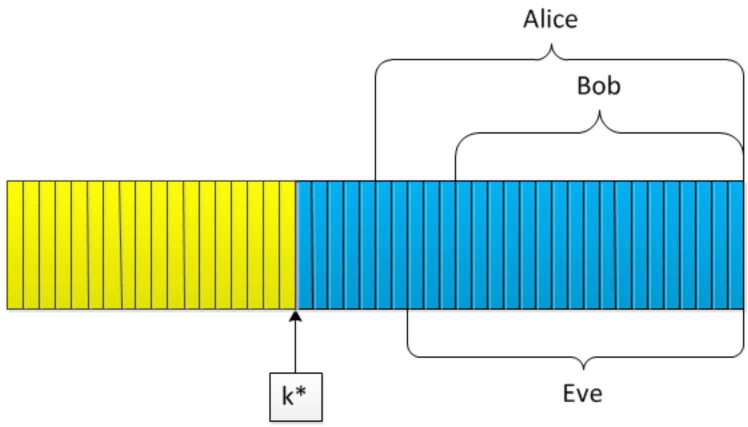

Figure 8.2: Illustration of case 1 in multiple access multiple jamming case.

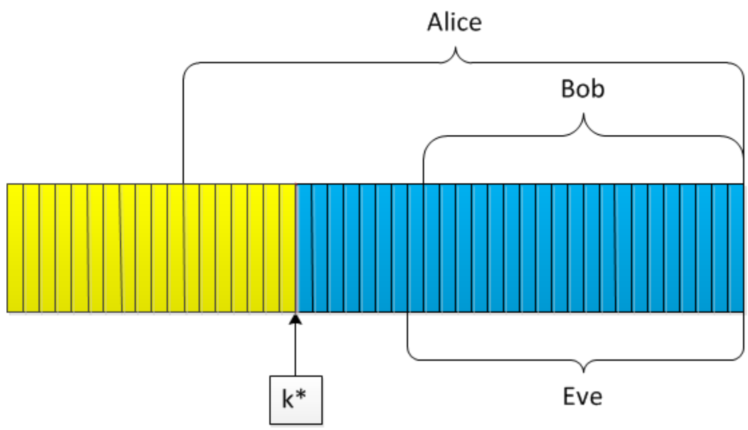

Figure 8.3: Illustration of case 2 in multiple access multiple jamming case.

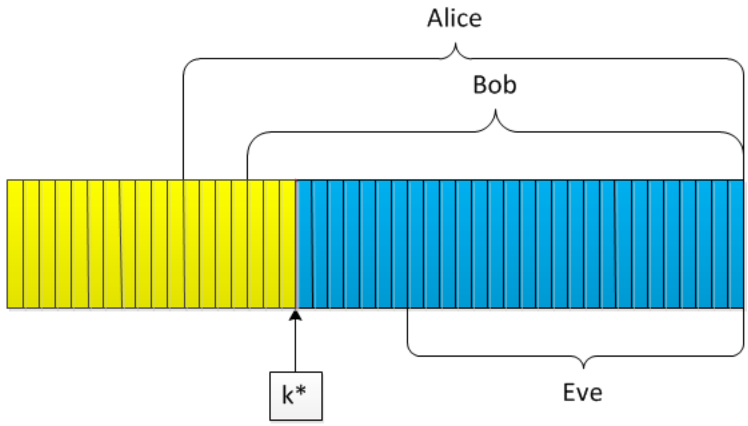

Figure 8.4: Illustration of case 3 in multiple access multiple jamming case.

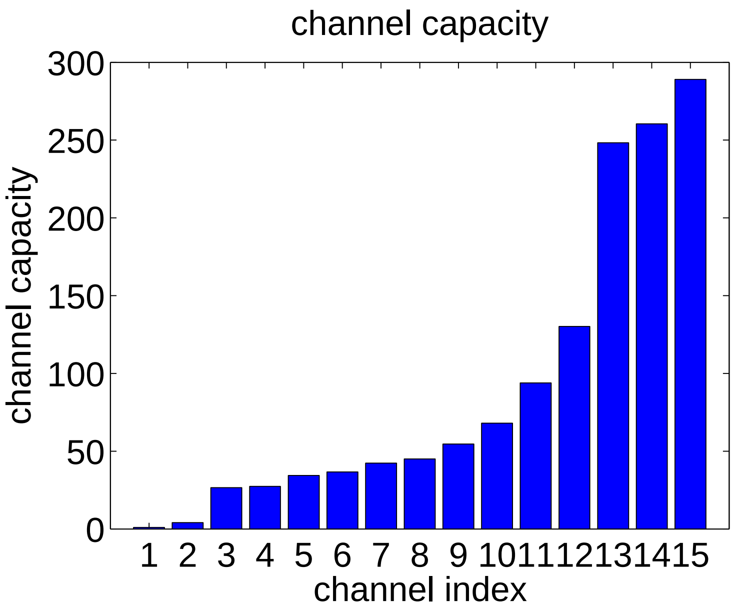

Figure 8.5: Channel Quality ($N = 15$, $k^{*} = 12$).

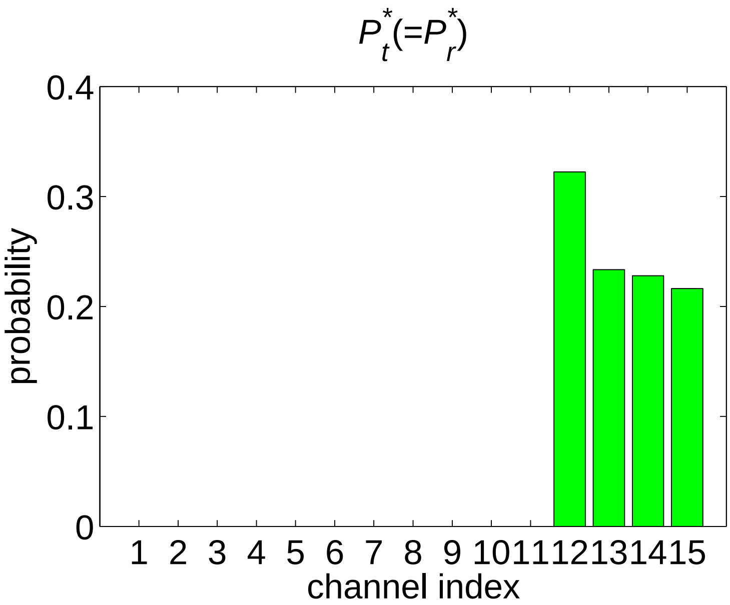

Figure 8.6: Case 1: $P^{t*}(= P^{r*})$ ($N = 15$, $k^* = 12$).

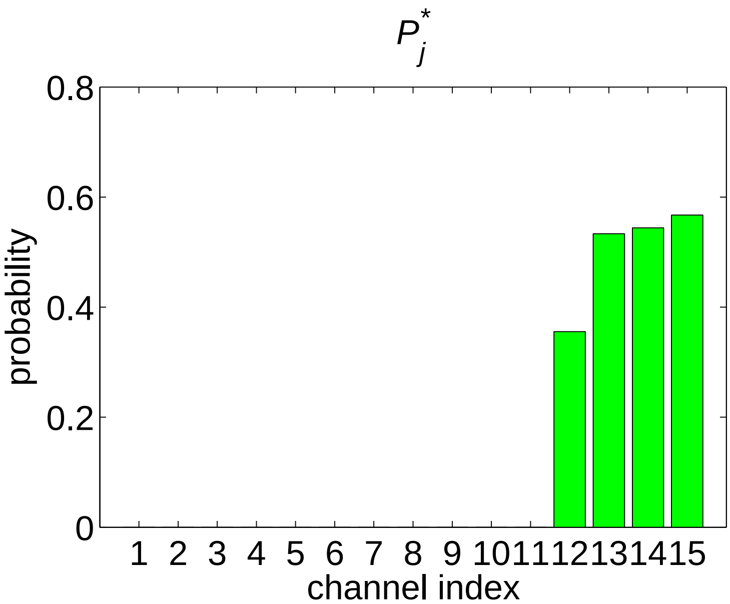

Figure 8.7: Case 1: P^{j*} ($N = 15$, $k^* = 12$).

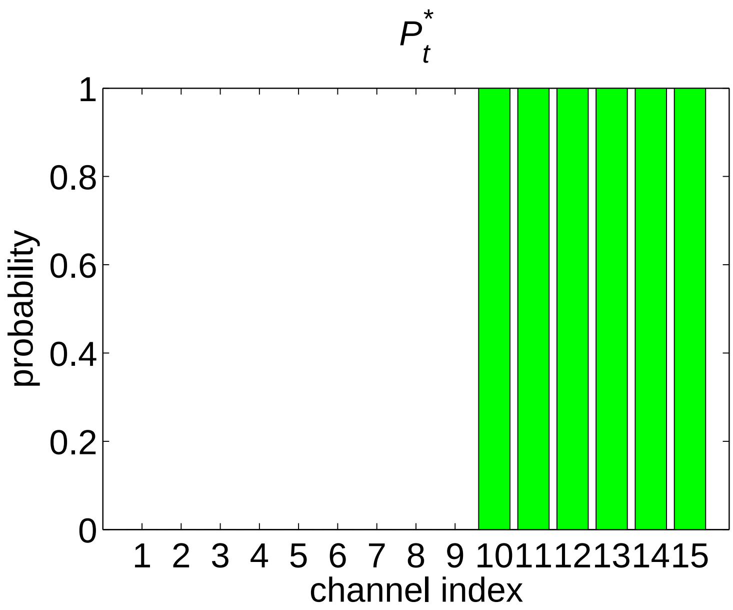

Figure 8.8: Case 2: P^{t*} ($N = 15$, $k^* = 12$).

- Figure 8.6 and Figure 8.7 give an example to illustrate case 1 with $M_t = M_r = 2$ and $M_j = 2$. Figure 8.6 shows the strategy of Alice and Bob, we can see that Alice and Bob only access channels from k^* to N, and when the channel quality is better, Alice and Bob access this channel with a smaller probability. Figure 8.7 shows the strategy of Eve, we can see that Eve only jams channels from k^* to N, and when the channel quality is better Eve jams this channel with a larger probability.

- Figure 8.8, Figure 8.9 and Figure 8.10 give an example to illustrate case 2 with $M_t = 6$, $M_r = 2$ and $M_j = 2$. Figure 8.8 shows the strategy of Alice, we can see that Alice takes constant strategy. Figure 8.9 shows the strategy of Bob, we can see that Bob only access channels from k^* to N, and when the channel quality is better, Bob access this channel with a smaller probability. Figure 8.10 shows the strategy of Eve, we can see that Eve only jams channels from k^* to N, and when the channel quality is better Eve jams this channel with a larger probability.

- Figure 8.11, Figure 8.12 and Figure 8.13 give an example to illustrate case 2 with $M_t = 6$, $M_r = 5$ and $M_j = 2$. Figure 8.11 and Figure 8.12 shows the strategy of Alice

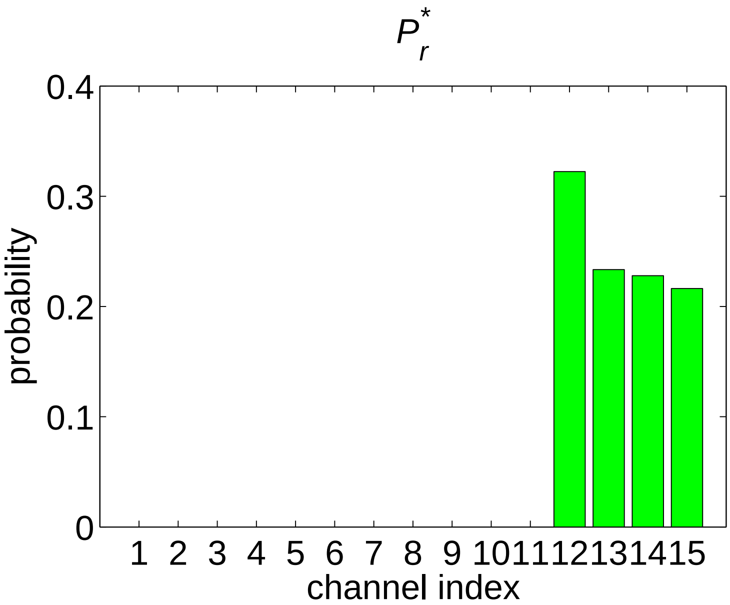

Figure 8.9: Case 2: P^{r*} ($N = 15$, $k^* = 12$).

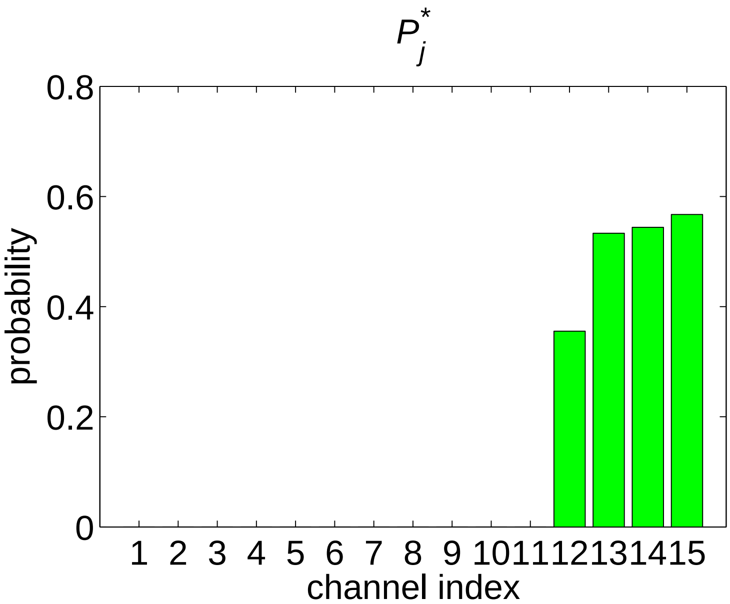

Figure 8.10: Case 2: P^{j*} ($N = 15$, $k^* = 12$).

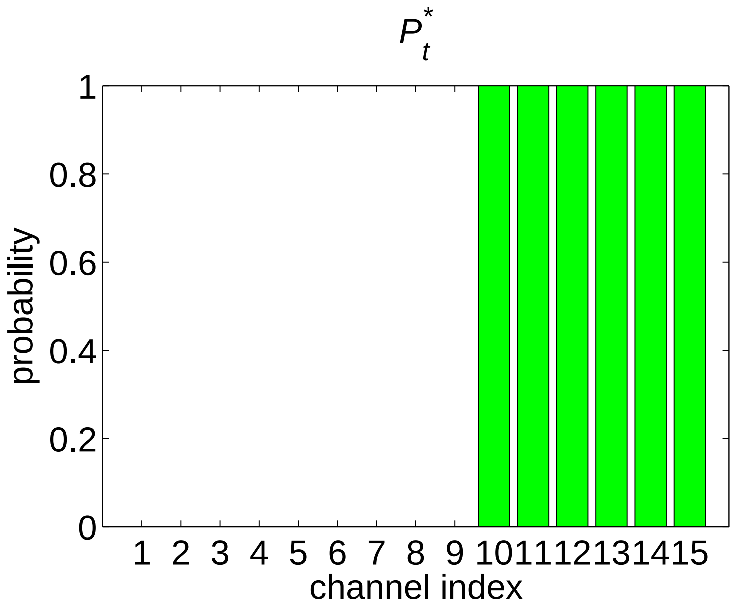

Figure 8.11: Case 3: P^{t*} ($N = 15$, $k^* = 12$).

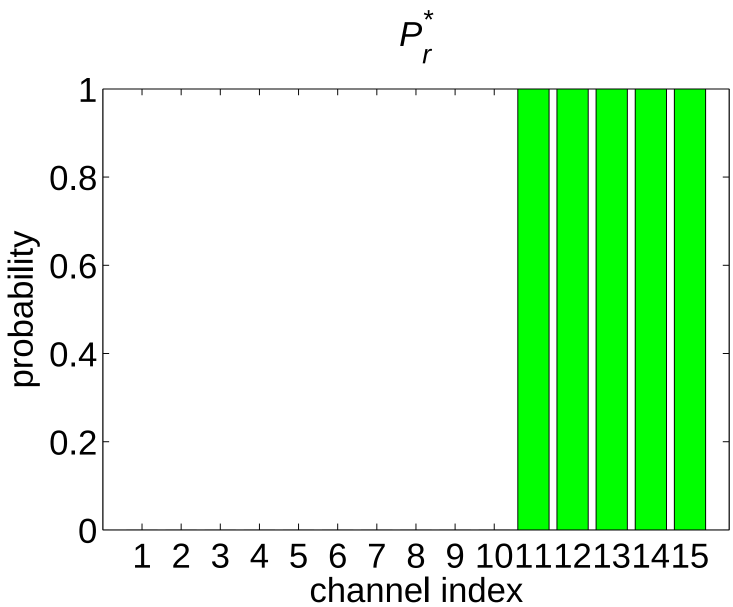

Figure 8.12: Case 3: P^{r*} ($N = 15$, $k^* = 12$).

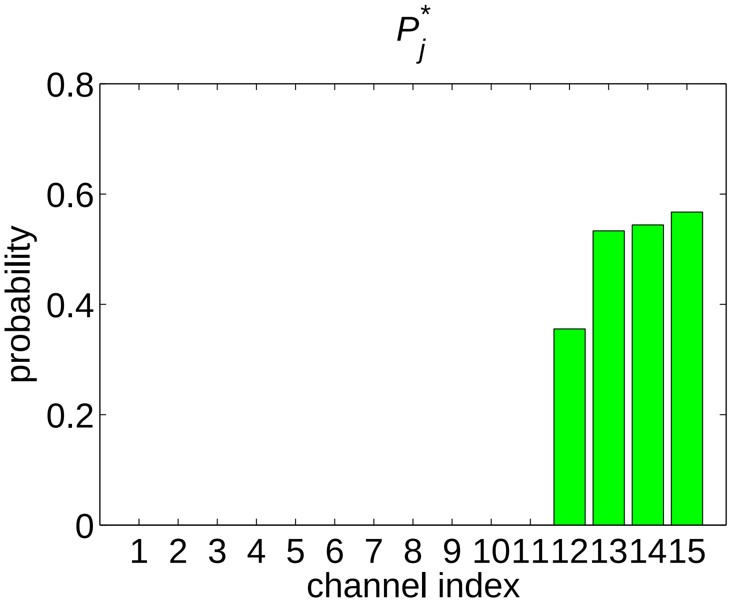

Figure 8.13: Case 3: P^{j*} ($N = 15$, $k^* = 12$).

and Bob, we can see that both Alice and Bob take constant strategy. Figure 8.13 shows the strategy of Eve, we can see that Eve only jams channels from k^* to N, and when the channel quality is better Eve jams this channel with a larger probability.

8.1 Proof

Proof. The organization of proof is the same as Chapter 7.

The reward of Alice and Bob access channel i is:

$$
\begin{aligned}
& \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} \sum_{\Omega_E} R_{\Omega_A\cap\Omega_B\setminus\Omega_E} p^j_{\Omega_E} \\
= & \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} \left(\sum_{\substack{\Omega_E \\ \Omega_E\cap\Omega_A\cap\Omega_B=\emptyset}} R_{\Omega_A\cap\Omega_B} p^j_{\Omega_E} + \sum_{\substack{\Omega_E \\ \Omega_E\cap\Omega_A\cap\Omega_B\neq\emptyset}} R_{\Omega_A\cap\Omega_B\setminus\Omega_E} p^j_{\Omega_E} \right) \\
= & \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} \left[R_{\Omega_A\cap\Omega_B} \left(1 - \sum_{\substack{\Omega_E \\ \Omega_E\cap\Omega_A\cap\Omega_B\neq\emptyset}} p^j_{\Omega_E} \right) + \sum_{\substack{\Omega_E \\ \Omega_E\cap\Omega_A\cap\Omega_B\neq\emptyset}} \left(R_{\Omega_A\cap\Omega_B} - R_{\Omega_A\cap\Omega_B\cap\Omega_E} \right) p^j_{\Omega_E} \right] \\
= & \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B} - \sum_{\substack{\Omega_E \\ \Omega_E\cap\Omega_A\cap\Omega_B\neq\emptyset}} R_{\Omega_E\cap\Omega_A\cap\Omega_B} p^j_{\Omega_E} \right)
\end{aligned}
$$

In the Nash equilibrium,

$$
\sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B} - \sum_{\substack{\Omega_E \\ \Omega_E\cap\Omega_A\cap\Omega_B\neq\emptyset}} R_{\Omega_E\cap\Omega_A\cap\Omega_B} {p^j_{\Omega_E}}^* \right) = C_0,
$$

where C_0 is a constant independent of i. So we have

$$
\begin{aligned}
& \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B} - \sum_{\substack{\Omega_E \\ \Omega_E\cap\Omega_A\cap\Omega_B\neq\emptyset}} R_{\Omega_E\cap\Omega_A\cap\Omega_B} {p^j_{\Omega_E}}^* \right) \\
= & \sum_{\substack{\Omega_A,\Omega_B \\ j\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B} - \sum_{\substack{\Omega_E \\ \Omega_E\cap\Omega_A\cap\Omega_B\neq\emptyset}} R_{\Omega_E\cap\Omega_A\cap\Omega_B} {p^j_{\Omega_E}}^* \right),
\end{aligned}
$$

where j is a channel index different from i.

$$\sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B} - \sum_{\substack{\Omega_E\\ \Omega_E\cap\Omega_A\cap\Omega_B\neq\emptyset}} R_{\Omega_E\cap\Omega_A\cap\Omega_B} {p^j_{\Omega_E}}^* \right)$$

$$= \sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B}} R_i \left(1 - p_i^{j*}\right) + \sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B\setminus\{i\}} - \sum_{\Omega_E} R_{\Omega_A\cap\Omega_B\setminus\{i\}\cap\Omega_E} {p^j_{\Omega_E}}^* \right)$$

$$= \sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B}} R_i \left(1 - p_i^{j*}\right) + \sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B\\ j\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B\setminus\{i\}} - \sum_{\Omega_E} R_{\Omega_A\cap\Omega_B\setminus\{i\}\cap\Omega_E} {p^j_{\Omega_E}}^* \right)$$

$$+ \sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B\\ j\notin\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B\setminus\{i\}} - \sum_{\Omega_E} R_{\Omega_A\cap\Omega_B\setminus\{i\}\cap\Omega_E} {p^j_{\Omega_E}}^* \right),$$

Notice that

$$\sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B\\ j\notin\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B\setminus\{i\}} - \sum_{\Omega_E} R_{\Omega_A\cap\Omega_B\setminus\{i\}\cap\Omega_E} {p^j_{\Omega_E}}^* \right)$$

$$= \sum_{\substack{\Omega_A,\Omega_B\\ j\in\Omega_A\cap\Omega_B\\ i\notin\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B\setminus\{j\}} - \sum_{\Omega_E} R_{\Omega_A\cap\Omega_B\setminus\{j\}\cap\Omega_E} {p^j_{\Omega_E}}^* \right),$$

and

$$\sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B\\ j\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B\setminus\{i,j\}} - \sum_{\Omega_E} R_{\Omega_A\cap\Omega_B\setminus\{i,j\}\cap\Omega_E} {p^j_{\Omega_E}}^* \right)$$

$$= \sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B\\ j\in\Omega_A\cap\Omega_B}} \left(R_{\Omega_A\cap\Omega_B\setminus\{i,j\}} - \sum_{\Omega_E} R_{\Omega_A\cap\Omega_B\setminus\{i,j\}\cap\Omega_E} {p^j_{\Omega_E}}^* \right),$$

so we have

$$\sum_{\substack{\Omega_A,\Omega_B\\ i\notin\Omega_A\cap\Omega_B\\ j\in\Omega_A\cap\Omega_B}} R_i \left(1 - p_i^{j*}\right) = \sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B\\ j\notin\Omega_A\cap\Omega_B}} R_j \left(1 - p_j^{j*}\right).$$

Because

$$|\{(\Omega_A,\Omega_B)|i\notin\Omega_A\cap\Omega_B, j\in\Omega_A\cap\Omega_B\}| = |\{(\Omega_A,\Omega_B)|i\in\Omega_A\cap\Omega_B, j\notin\Omega_A\cap\Omega_B\}|,$$

so

$$R_i(1-p_i^j) = C_1, \quad \forall i\in A\cap B,$$

where C_1 is a constant independent of i.

The reward of Eve jamming channel i is:

$$\begin{aligned}
&-\sum_{\substack{\Omega_E\\ i\in\Omega_E}}\sum_{\Omega_A,\Omega_B} R_{\Omega_A\cap\Omega_B\backslash\Omega_E} p^t_{\Omega_A} p^r_{\Omega_B}\\
=\;& -\sum_{\substack{\Omega_E\\ i\in\Omega_E}}\left[\sum_{\substack{\Omega_A,\Omega_B\\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} (R_{\Omega_A\cap\Omega_B} - R_{\Omega_A\cap\Omega_B\cap\Omega_E}) p^t_{\Omega_A} p^r_{\Omega_B} + \sum_{\substack{\Omega_A,\Omega_B\\ \Omega_A\cap\Omega_B\cap\Omega_E=\emptyset}} R_{\Omega_A\cap\Omega_B} p^t_{\Omega_A} p^r_{\Omega_B}\right]\\
=\;& -\sum_{\substack{\Omega_E\\ i\in\Omega_E}}\left(\sum_{\Omega_A,\Omega_B} R_{\Omega_A\cap\Omega_B} p^t_{\Omega_A} p^r_{\Omega_B} - \sum_{\substack{\Omega_A,\Omega_B\\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E} p^t_{\Omega_A} p^r_{\Omega_B}\right).
\end{aligned}$$

In the Nash equilibrium,

$$-\sum_{\substack{\Omega_E\\ i\in\Omega_E}}\left(\sum_{\Omega_A,\Omega_B} R_{\Omega_A\cap\Omega_B} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* - \sum_{\substack{\Omega_A,\Omega_B\\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*\right) = C_2,$$

where C_2 is a constant independent of i. Because

$$\sum_{\substack{\Omega_E\\ i\in\Omega_E}}\sum_{\Omega_A,\Omega_B} R_{\Omega_A\cap\Omega_B} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*$$

is the same for all i, so

$$\sum_{\substack{\Omega_E\\ i\in\Omega_E}}\sum_{\substack{\Omega_A,\Omega_B\\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* = C_3, \quad \forall i\in E$$

where C_3 is a constant independent of i. Then,

$$\begin{aligned}
&\sum_{\substack{\Omega_E\\ i\in\Omega_E}}\sum_{\substack{\Omega_A,\Omega_B\\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*\\
=\;& \sum_{\substack{\Omega_E\\ i\in\Omega_E}}\sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B}} R_{\Omega_A\cap\Omega_B\cap\Omega_E} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* + \sum_{\substack{\Omega_E\\ i\in\Omega_E}}\sum_{\substack{\Omega_A,\Omega_B\\ i\notin\Omega_A\cap\Omega_B\\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{\Omega_E \\ i\in\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} R_i {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* + \sum_{\substack{\Omega_E \\ i\in\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} R_{\Omega_A\cap\Omega_B\cap\Omega_E\setminus\{i\}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* \\
&\quad + \sum_{\substack{\Omega_E \\ i\in\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ i\notin\Omega_A\cap\Omega_B \\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E\setminus\{i\}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* \\
&= \sum_{\substack{\Omega_E \\ i\in\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} R_i {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* + \sum_{\substack{\Omega_E \\ i\in\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E\setminus\{i\}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* \\
&= \sum_{\substack{\Omega_E \\ i\in\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} R_i {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* + \sum_{\substack{\Omega_E \\ i\in\Omega_E \\ j\notin\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E\setminus\{i\}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* \\
&\quad + \sum_{\substack{\Omega_E \\ i\in\Omega_E \\ j\in\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E\setminus\{i\}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*
\end{aligned}
$$

Consider a channel j different from i, notice

$$
\sum_{\substack{\Omega_E \\ i\in\Omega_E \\ j\notin\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E\setminus\{i\}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* = \sum_{\substack{\Omega_E \\ j\in\Omega_E \\ i\notin\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E\setminus\{j\}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*,
$$

and we can subtract the common term

$$
\sum_{\substack{\Omega_E \\ i\in\Omega_E \\ j\in\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ \Omega_A\cap\Omega_B\cap\Omega_E\neq\emptyset}} R_{\Omega_A\cap\Omega_B\cap\Omega_E\setminus\{i,j\}} {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*,
$$

then we have

$$
\sum_{\substack{\Omega_E \\ i\in\Omega_E \\ j\notin\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} R_i {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* = \sum_{\substack{\Omega_E \\ i\notin\Omega_E \\ j\in\Omega_E}} \sum_{\substack{\Omega_A,\Omega_B \\ j\in\Omega_A\cap\Omega_B}} R_j {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*.
$$

Because

$$
|\{\Omega_E | i\in\Omega_E, j\notin\Omega_E\}| = |\{\Omega_E | i\notin\Omega_E, j\in\Omega_E\}|,
$$

so

$$
\sum_{\substack{\Omega_A,\Omega_B \\ i\in\Omega_A\cap\Omega_B}} R_i {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* = \sum_{\substack{\Omega_A,\Omega_B \\ j\in\Omega_A\cap\Omega_B}} R_j {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^*.
$$

$$\sum_{\substack{\Omega_A,\Omega_B\\ i\in\Omega_A\cap\Omega_B}} R_i {p^t_{\Omega_A}}^* {p^r_{\Omega_B}}^* = C_4$$

where C_4 is a constant independent of i. And we can rewrite it as

$$R_i p_i^{r*} p_i^{t*} = C_4$$

So far we have

$$\begin{aligned}
R_i(1-p_i^j) &= C_1, \quad \forall i \in A \cap B \\
R_i p_i^r p_i^t &= C_4, \quad \forall i \in E \\
\sum_{i\in A} p_i^{t*} &= M_t, \\
\sum_{i\in B} p_i^{r*} &= M_r, \\
\sum_{i\in E} p_i^{j*} &= M_j,
\end{aligned}$$

where C_1 and C_4 are constant independent of i.

From the discussion in Chapter 6 and Chapter 7, we can give the result same as the lemma. □

8.2 Remark

Remark 8.2.1. *Under the Nash equilibrium in this case, Alice, Bob and Eve do not always operate on the same set of channels.*

Remark 8.2.2. k^* *is a variable that is for Alice, Bob and Eve to decide on which channels they should take actions. Figure 8.14 shows* k^* *separates "good" channels and "bad" channels. Alice, Bob and Eve have no motivation to access or jam channels from 1 to* k^*-1. *But in Case 2 and Case 3, Alice and Bob have to access channels from 1 to* k^*-1.

Remark 8.2.3. k^* *is determined by the channel capacity and* M_j, *and it is not related to Alice and Bob.*

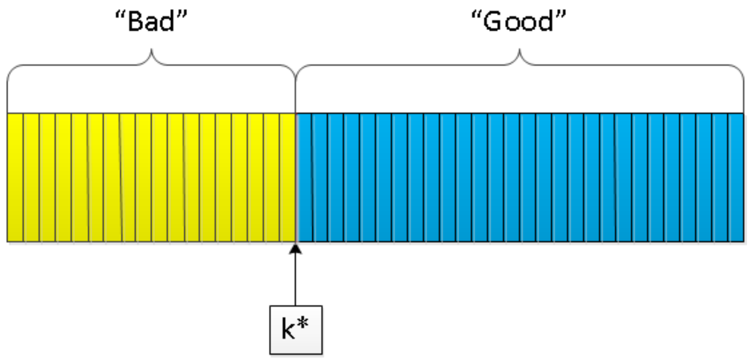

Figure 8.14: k^* separates "good" channels and "bad" channels.

Remark 8.2.4. *When the channel quality is better, Eve jams this channel with a larger probability while Alice and Bob access this channel with a smaller probability.*

Remark 8.2.5. *It is simple to verify that* $N - k^* + 1 \geq M_j + 1$*. This implies that Alice and Bob will access at least* $M_j + 1$ *channels. Otherwise, if they can access only* M_j *channels, this channel will be jammed by the attacker with probability 1.*

Remark 8.2.6. *The Nash equilibrium of Alice, Bob and Eve is given in the form of marginal distribution.*

Chapter 9

Numerical Simulation

In this chapter, we show the numerical simulation results of the Nash equilibrium. In our simulation, the channel quality is independently generated by the same probability density function, we choose exponential distribution. $R_i \sim \exp(100)$, where $i = 1, 2, ..., N$.

9.1 Equal Channel Quality Case

In this section, we show how the average data rate is affected by the total number of channels. From Figure 9.1, we can see that the average data is maximized when $N = 2$. This is because when N becomes larger, the total probability 1 need to be spread among more channels, it becomes harder for Alice and Bob to be in the same channel. We have to keep $N \geq 2$ because this is needed to avoid being jammed with probability 1.

9.2 General Channel Quality Case

First we set $N = 10$ and $E(R_i) = 100$ to make numerical analysis about $\bar{R}$. So R_i are i.i.d. From $\bar{R} = \frac{N-k^*}{(\sum_{l=k^*}^{N} \frac{1}{\sqrt{R_l}})^2}$, we can see that this is an order statistic problem. In this problem, $\bar{R}$ depends on another random variable k^*, which also depends on the distribution of R. The involvement of k^* makes the theoretical analysis complex. The following analysis here is numerical and we show that for a not so large N the distribution of R can be approximated by Gamma distribution. Each simulation runs 10^5 times.

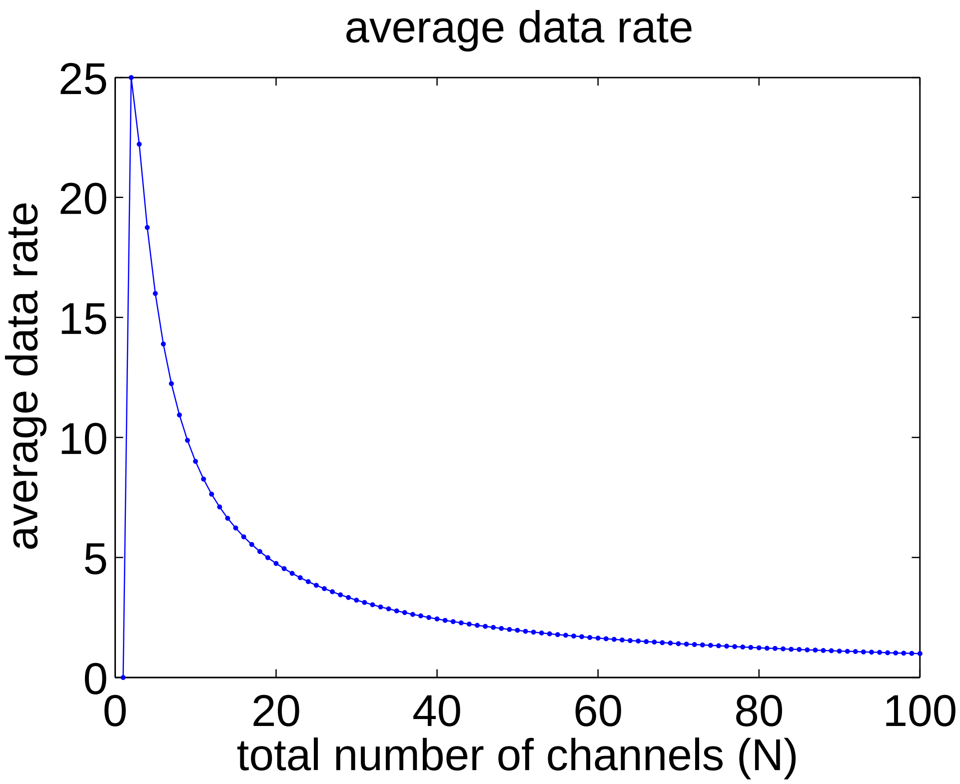

Figure 9.1: Average data rate vs. Total number of channels.

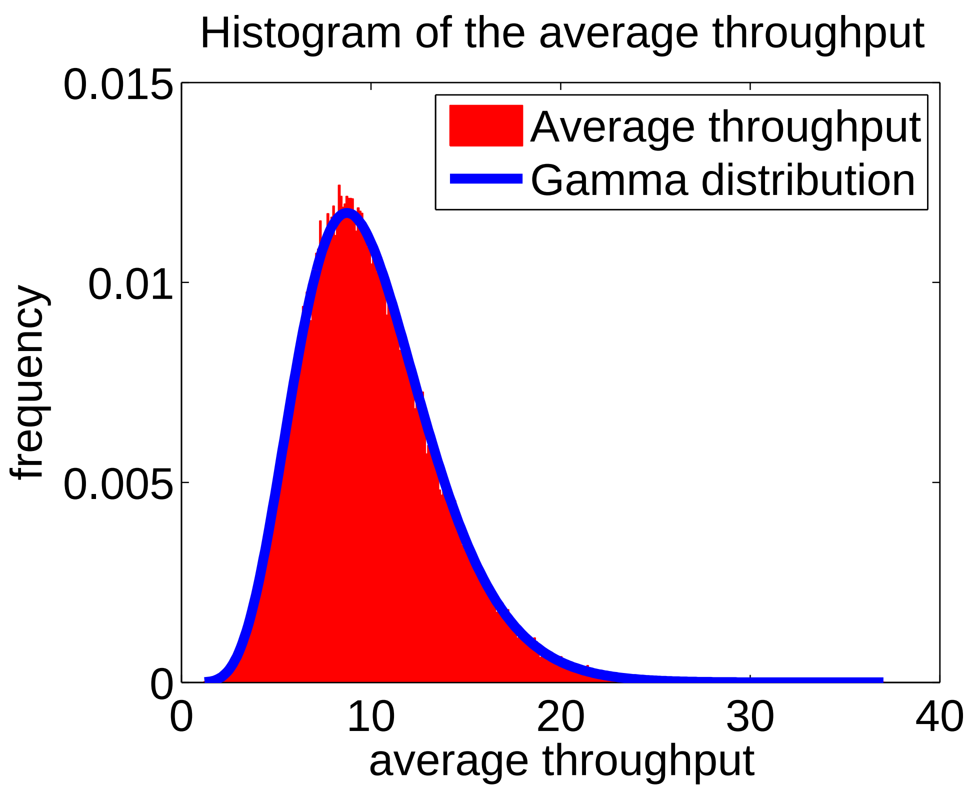

Figure 9.2: Distribution of $\bar{R}$, $N = 10$.

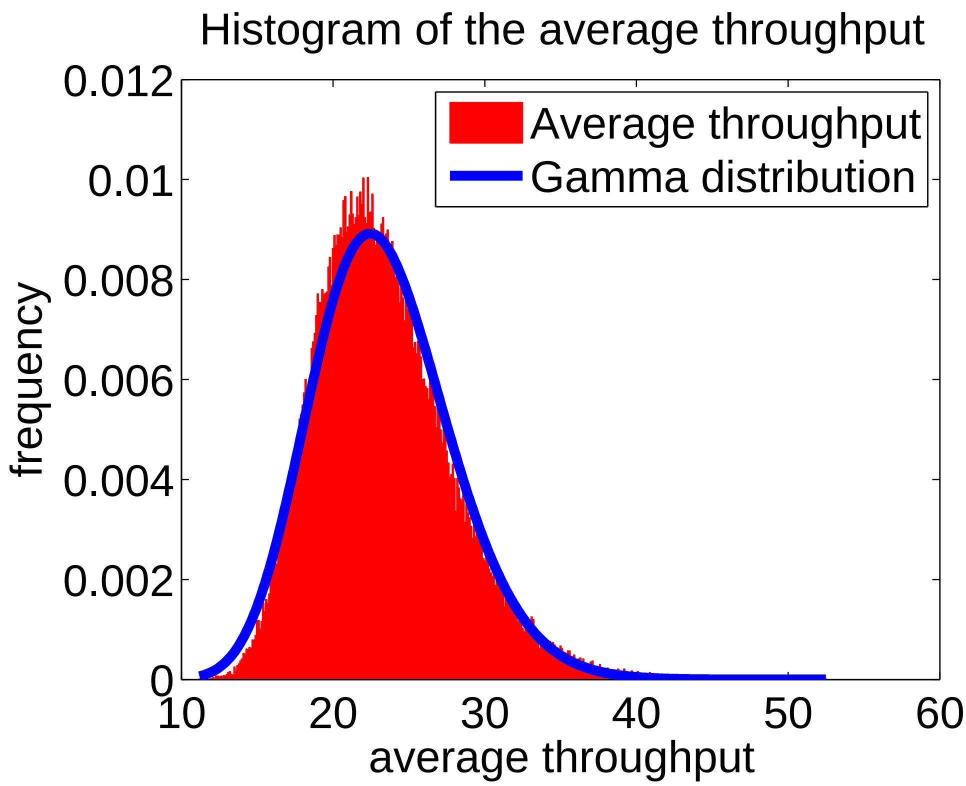

Figure 9.3: Distribution of $\bar{R}$, $N = 1000$.

From Figure 9.2, we can see the distribution of $\bar{R}$ can be approximated by Gamma distribution when $N = 10$.

We set N to $N = 1000$. From Figure 9.3 we can see the approximation of Gamma distribution is not as good as $N = 10$ but it is still acceptable.

9.3 One Access Multiple Jamming Case

In this numerical examples, we illustrate the case of one access multiple jamming case. We set the total number of channels to $N = 100$. The data we use in this and next section are the same set of R. In this case, Eve has infinite numbers of the Nash equilibrium, but they all achieve the same performance, so we just choose one solution which assumes jamming each of the channels are all independent. From Figure 9.4, we can see that with the number of channels Eve can jam increasing, the average throughput is decreasing. Notice

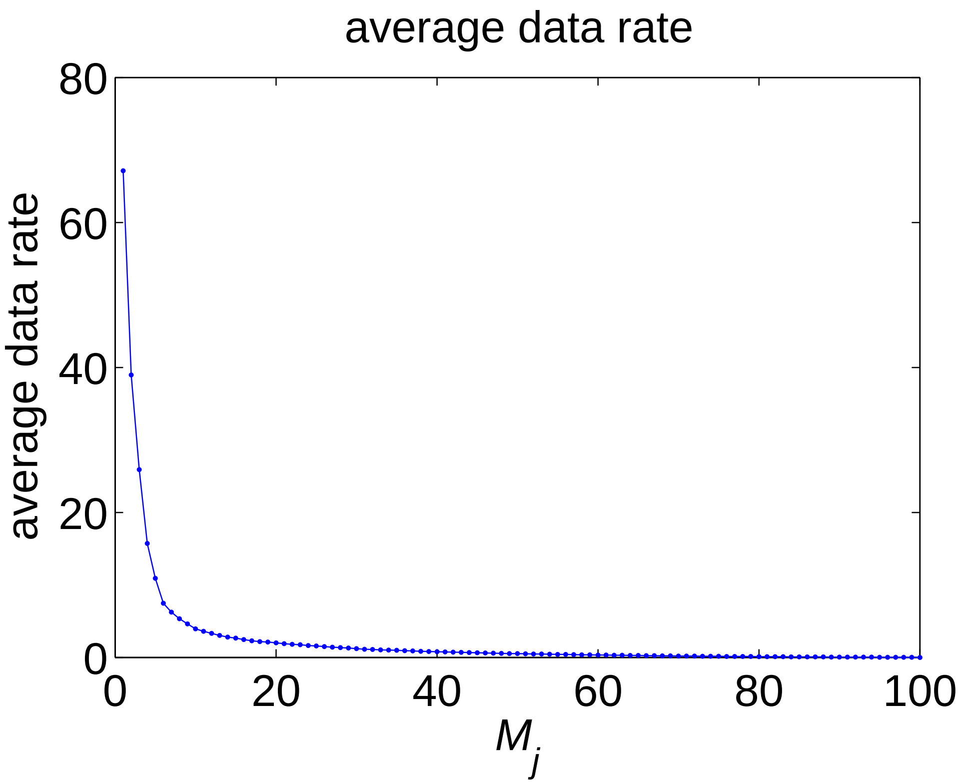

Figure 9.4: $\bar{R}$ affected by M_j.

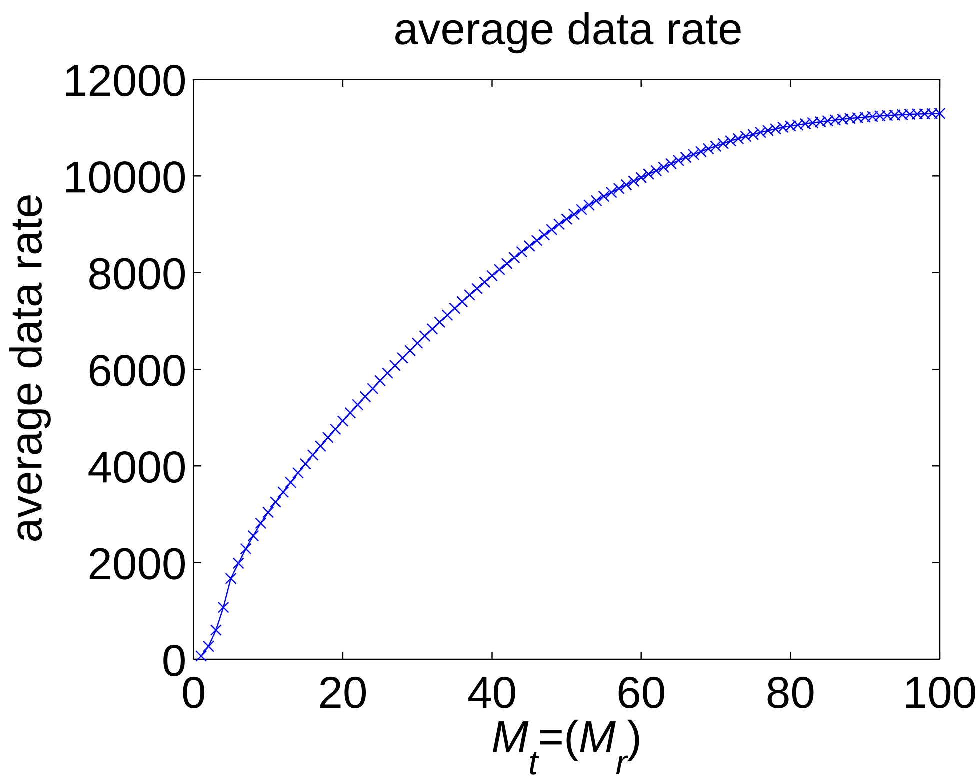

Figure 9.5: $\bar{R}$ affected by M_t.

that Eve can increase her reward by jamming more channels, but if the number of channels is already larger than a threshold, for example $M_j > 20$ in our simulation, her effort may not worth the money to buy a more powerful device. This is because the channel becomes very bad when their rank in the whole channels becomes low.

9.4 Multiple Access One Jamming Case

The simulation result shows that with the number of channels Alice and Bob can access increased, the average throughput is increased. $N = 100$ in this section.

From Figure 9.5, we can see the curve is not so steep as the performance of multiple jamming. But we can still see that if the number of channels is already larger than a threshold, their reward increased per channel becomes small due to the channel becomes worse with channel index decreases. If we increase M from 1 to 20, $\bar{R}$ is increased by more

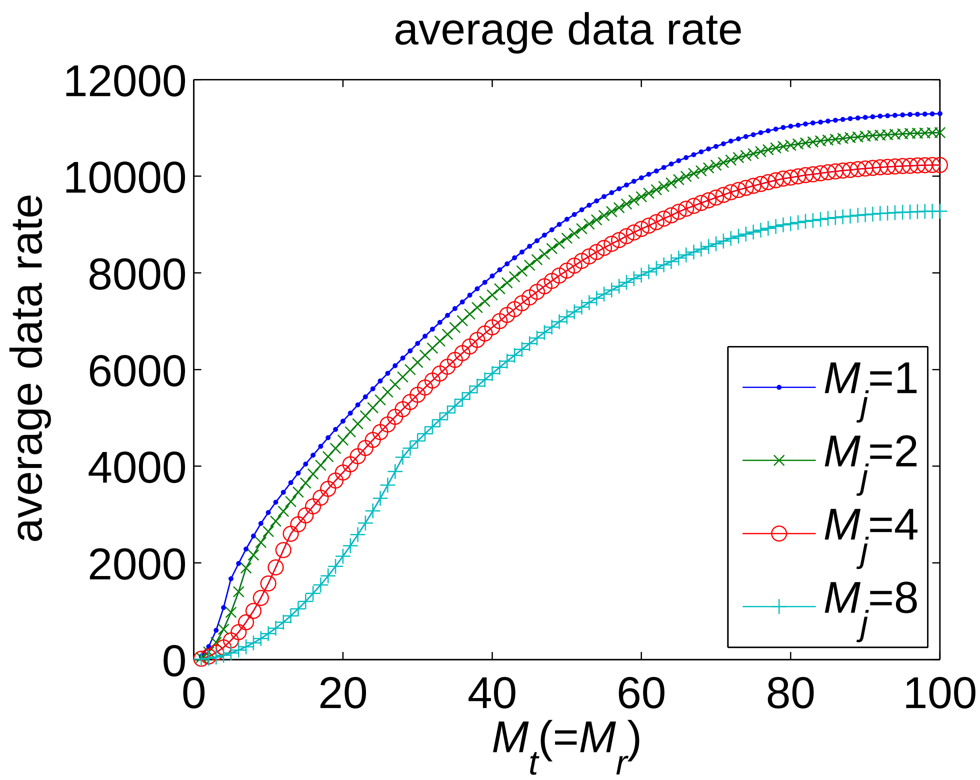

Figure 9.6: $\bar{R}$ affected by M_t under different M_j.

than 2000, but if we increase M from 80 to 100, $\bar{R}$ is increased by about 1400.

9.5 Multiple Access Multiple Jamming Case

Multiple access multiple jamming case is similar to the multiple access one jamming case in nature. The difference is that in this case Eve can jam two or more channels. What we concern is just the average data rate of Alice and Bob, so we investigate this by setting different values of M_j.

From Figure 9.6, we can see that with M_j increasing, the average data rate is decreasing, this is similar to one access multiple jamming case.

Figure 9.7 shows that with $M_t(= M_r)$ increasing, the average data rate is increasing, this is similar to multiple access one jamming case.

Now we investigate the "waste case" by setting $M = M_t - M_r$. In multiple access case,

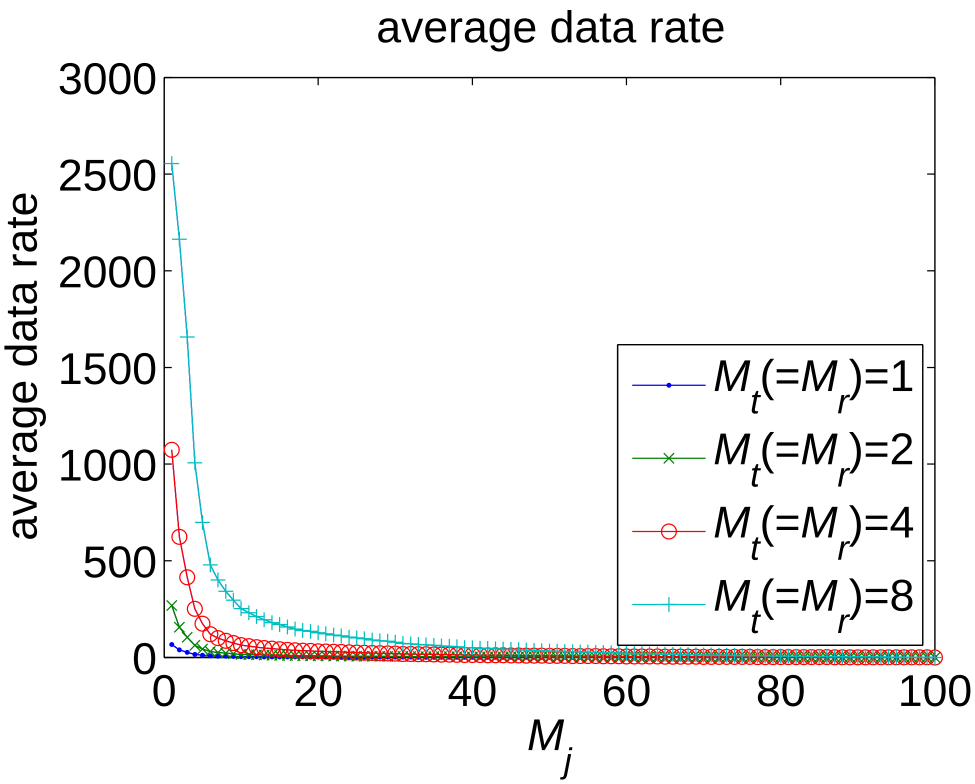

Figure 9.7: $\bar{R}$ affected by M_j under different $M_t(= M_r)$.

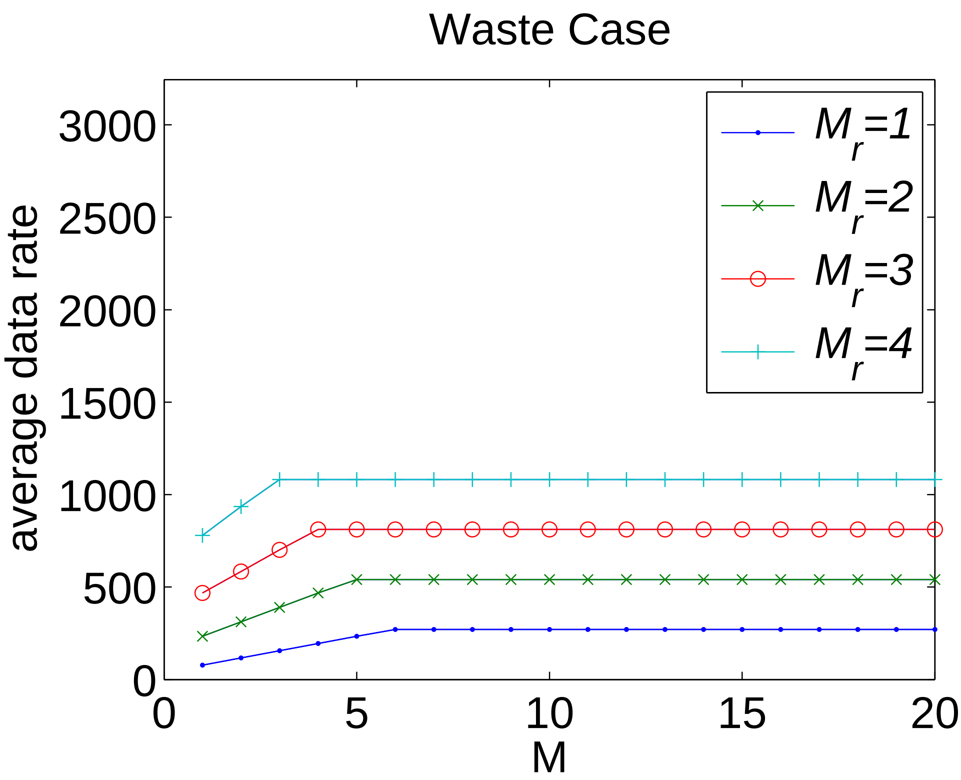

Figure 9.8: $\bar{R}$ affected by M under different $M = M_t - M_r$, $Mr = 2$.

when Alice can access more channel than Bob, Alice will have the chance to waste energy as analyzed before. We can call this case “waste case”.

In Figure 9.8, we can see if M_t and M_r is large enough, the performance of different M is the same, so there is no motivation to use a large M due to the concern of power and device cost.

In Figure 9.9, we compare the performance under the Nash equilibrium in our model and the performance in learning based approach. We use the algorithm proposed in [6]. We can see that our strategy performs better in two aspects: First, throughput of our strategy is higher, because in the learning based algorithm, the authors always leave some probability for “bad” channels; Second, our strategy do not need time to reach the maximum.

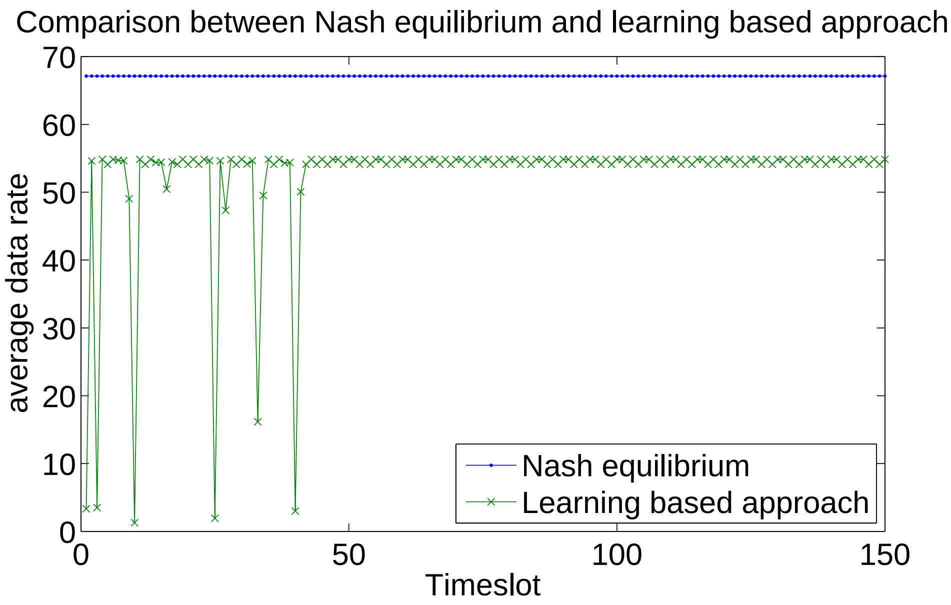

Figure 9.9: $\bar{R}$ under the Nash equilibrium in our model and learning based approach.

Chapter 10

Conclusion

The uncoordinated frequency hopping has been modeled as a zero-sum game between the legitimate users and the attack. In the general channel quality case, we have obtained the unique Nash equilibrium. For the case when the legitimate users or the attacker can access or jam more than one channels, following similar steps in general channel quality case, we have obtained the Nash equilibrium. In general, for better channels, it is more probable for Eve to jam, while it is less probable for Alice and Bob to access. But there are also some channel are not good enough so that none of Alice, Bob or Eve will access or jam these channels. To determine which channels to access or jam, k^* is an important variable to separate good channels and bad channels.

Using numerical simulation, we have shown the performance of UFH under the Nash equilibrium. In general, if Alice and Bob have the ability to access more channels, the average data rate will become larger, while if Eve has the ability to jam more channels, the average data rate will become smaller. However, there is a special case called “waste case” which needs more attention. In the “waste case”, Alice is wasting power to access some channels that is never accessed by Bob. And we also show that our strategy outperforms the learning based strategy.

Bibliography

[1] David Tse and Pramod Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[2] Sandra Kay Miller. Facing the challenge of wireless security. *Computer*, 34(7):16–18, July 2001.

[3] Marco Di Renzo and Merouane Debbah. Wireless physical-layer security: The challenges ahead. In *International Conference on Advanced Technologies for Communications*, pages 313–316, Haiphong, Vietnam, Oct. 2009.

[4] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *MobiHoc05*, pages 1–12, UrbanaChampaign,Illinois, USA, May 2005.

[5] Matthias Wihelm, Ivan Martinovic, Jens B. Schmitt, and Vincent Lenders. Reactive jamming in wireless networks-how realistic is the threat? In *Proc. ACM Conference on Wireless Network Security*, pages 47–52, Hamburg, Germany, Jan. 2011.

[6] Qian Wang, Ping Xu, Kui Ren, and Xiangyang Li. Towards optimal adaptive UFH-based anti-jamming wireless communication. *IEEE Journal on Selected Areas in Communications*, 1(30):16–30, Jan. 2012.

[7] John G. Proakis and Masoud Salehi. *Digital Communications*. McGraw-Hill, fifth edition edition, 2008.

[8] Harish Laxmichand Sharma, Atul R. Deshmukh, and N. G. Bawane. Spread spectrum pattern & PN sequence retrieval in wireless ad hoc network: Design approach. In *Second*

International Conference on Emerging Applications of Information Technology, pages 391–394, Kolkata, West Bengal, India, Feb. 2011.

[9] Mario Strasser, Christina Pöpper, Srdjan Čapkun, and Mario Čagalj. Jamming-resistant key establishment using uncoordinated frequency hopping. In *Proc. IEEE Intl. Symposium on Security and Privacy*, pages 64–78, Oakland, California, USA, May 2008.

[10] Kaihe Xu, Qian Wang, and Kui Ren. Joint UFH and power control for effective wireless anti-jamming communication. In *Proc. IEEE Conf. Computer Communications (Infocom)*, pages 738–746, Orlando, FL, USA, Mar. 2012.

[11] Husheng Li and Zhu Han. Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part I: Known channel statistics. *IEEE Trans. Wireless Commun.*, 9(11):3566–3577, Nov. 2010.

[12] Husheng Li and Zhu Han. Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part II: Unknown channel statistics. *IEEE Trans. Wireless Commun.*, 10(1):274–283, Jan. 2011.

[13] Chengzhi Li, Huaiyu Dai, Liang Xiao, and Peng Ning. Analysis and optimization on jamming-resistant collaborative broadcast in large-scale networks. In *Proc. Asilomar Conf. on Signals, Systems and Computers*, pages 1860–1863, Asilomar Grounds, Pacific Grove, California, USA, Nov. 2010.

[14] Liang Xiao, Huaiyu Dai, and Peng Ning. Jamming-resistant collaborative broading using uncoordinated frequency hopping. *IEEE Trans. Inform. Forensics and Security*, 7(1):297–309, Feb. 2011.

[15] Qian Wang, Ping Xu, Kui Ren, and Xiangyang Li. Delay-bounded adaptive UFH-based anti-jamming wireless communication. In *Proc. IEEE Conf. Computer Communications (Infocom)*, pages 1413–1421, Shanghai, China, Apr. 2011.

[16] Liang Xiao, Huaiyu Dai, and Peng Ning. Jamming-resistant collaborative broadcast

in wireless networks, Part I: Single-hop networks. In *Proc. IEEE Global Telecommunications Conf.*, pages 1–6, Houston, Texas, USA, Dec. 2011.

[17] Liang Xiao, Huaiyu Dai, and Peng Ning. Jamming-resistant collaborative broadcast in wireless networks, Part II: Multihop networks. In *Proc. IEEE Global Telecommunications Conf.*, pages 1–6, Houston, Texas, USA, Dec. 2011.

[18] Liang Xiao, Huaiyu Dai, and Peng Ning. Jamming-resistant collaborative broadcast using uncoordinated frequency hopping. *IEEE Trans. Inform. Forensics and Security*, 7(1):297–309, Feb. 2012.

[19] Chengzhi Li, Huaiyu Dai, Liang Xiao, and Peng Ning. Communication efficiency of anti-jamming broadcast in large-scale multi-channel wireless networks. *IEEE Trans. Signal Processing*, 60(10):5281–5292, Oct. 2012.

[20] Liang Xiao, Huaiyu Dai, and Peng Ning. MAC design of uncoordinated FH-based collaborative broadcast. *IEEE Wireless Communications Letters*, 1(3):261–264, June 2012.

[21] Christina Pöpper, Mario Strasser, and Srdjan Čapkun. Anti-jamming broadcast communication using uncoordinated spread spectrum techniques. *IEEE Journal on Selected Areas in Communications*, 5(28):703–715, June 2011.

[22] An Liu, Peng Ning, Huaiyu Dai, and Yao Liu. USD-FH: Jamming-resistant wireless communication using frequency hopping with uncoordinated seed disclosure. In *Mobile Adhoc and Sensor Systems (MASS), 2010 IEEE 7th International Conference on*, pages 41–50, San Francisco, CA, USA, Nov. 2010.

[23] Xiaohua(Edward) Li and Juite Hwu. A frequency hopping spread spectrum transmission scheme for uncoordinated cognitive radios. In *Proc. IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing*, pages 2345–2348, Taipei, Taiwan, Apr. 2009.

[24] Peter Gober, Stefan Coetzee, and A. J. Han Vinck. A new approach to uncoordinated frequency hopping multiple-access communication. In *Proc. IEEE Intl. Symposium on Inform. Theory*, page 403, Cambridge, MA, USA, Aug. 1998.

[25] Yi-Chen Chen and Kwang-Cheng Chen. FFH-BFSK multiuser detection in uncoordinated narrow-band FH systems. In *Proc. IEEE Global Telecommunications Conf.*, pages 272–276, Dallas, Texas, USA, Dec. 2004.

[26] Bingwen Zhang and Lifeng Lai. Optimal strategies in jamming resistant uncoordinated frequency hopping systems. In *Proc. Conf. on Information Science and Systems*, Baltimore, MD, USA, Mar. 2013.

[27] Martin J. Osborne. *An introduction to game theory.* Oxford University Press, first edition edition, 2002.

[28] Tamer Basar and Geert Jan Olsder. *Dynamic Noncooperative Game Theory.* Society for Industry and Applied Mathematics, Philadelphia, second edition edition, 1998.