STARS

University of Central Florida
STARS

Electronic Theses and Dissertations, 2004-2019

2010

Mitigating Misbehavior In Wireless Networks: A Game Theoretic Approach

Wenjing Wang
University of Central Florida

Part of the Electrical and Electronics Commons

Find similar works at: https://stars.library.ucf.edu/etd

University of Central Florida Libraries http://library.ucf.edu

University of
Central
Florida

STARS
Showcase of Text, Archives, Research & Scholarship

MITIGATING MISBEHAVIOR IN WIRELESS NETWORKS: A GAME THEORETIC APPROACH

by

WENJING WANG

B.S.E.E. University of Science and Technology of China, 2005
M.S.E.E. University of Central Florida, 2007

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the School of Electrical Engineering and Computer Science
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Spring Term
2010

Major Professor: Mainak Chatterjee

ABSTRACT

In a distributed wireless system, multiple network nodes behave cooperatively towards a common goal. Though such assumptions on cooperation are desirable (e.g., controlling the transmit power level, reducing interference for each other, revealing private information, adhering to network policies) for analyzing and modeling, certain nodes belonging to a real-world system have often shown to deviate. These nodes, known as misbehaving nodes, bring more challenges to the design of the wireless network because the unreliable channel makes the actions of the nodes hidden from each other.

In this dissertation, we analyze two types of misbehavior, namely, selfish noncooperation and malicious attacking. We apply game theoretic techniques to model the interactions among the nodes in the network. First, we consider a homogeneous unreliable channel and analyze the necessary and sufficient conditions to enforce cooperative packet forwarding among a node pair. We formulate an anti-collusion game and derive the conditions that achieve full cooperation when the non-cooperative nodes collude. In addition, we consider multi-hop communication with a heterogeneous channel model. We refine our game model as a hidden action game with imperfect private monitoring. A state machine based strategy is proposed to reach Nash Equilibrium. The strategy attains cooperative packet forwarding with heterogeneous channel and requires only partial and imperfect information. Further-

more, it also enforces cooperation in multi-hop packet forwarding. To tackle the malicious attacks, we use Bayesian game analysis to show the existence of equilibrium in the detection game and argue that it might not be profitable to isolate the malicious nodes upon detection. We propose the concept of "coexistence with malicious nodes" by proving the co-existence equilibrium and derive the conditions that achieve the equilibrium.

This research is further accomplished by extensive simulation studies. Simulation results illustrate the properties of the games and the derived equilibria. The results validate our design philosophy and clearly indicate that the proposed game theoretic solutions can be effectively used to enforce cooperation and mitigate attacks.

Dedicated to,

My parents

and

My academic advisor

Dr. Mainak Chatterjee

ACKNOWLEDGMENTS

I would like to express my sincere appreciation and gratitude to Prof. Mainak Chatterjee for bringing me to the beautiful city of Orlando and guiding me throughout my Ph.D. program. It has been very enjoyable to work with him. I thank Prof. Necati Catbas, Prof. Ratan K. Guha, Prof. Lei Wei and Prof. Cliff C. Zou for serving as members of my dissertation committee. Their suggestions and advices have helped me immensely to prepare the dissertation. I thank Dr. Kevin A. Kwiat of Air Force Research Laboratory for his support on our research projects and insightful discussions over the years. Last but not least, I thank my friends, my roommates and labmates. Their company presents me a cherished memory for life.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

In a distributed wireless system where multiple network entities (also called nodes) work towards individual or common goals, cooperative behavior among the nodes (such as controlling the transmit power level, reducing interference for each other, revealing private information, adhering to network policies) is highly desired for increasing system capacity. Though this desirable property makes it easy to analyze a system due to state space reduction; in reality, this assumption might be too strong. For example, there might be nodes in the network which might act in a selfish and/or malicious manner. These nodes, which are also known as misbehaving nodes, bring more challenges to the design of the wireless network.

1.1   Misbehavior in Wireless Networks

The research of mitigating misbehavior in wireless network is motivated from the following example where the network services are disrupted by nodes' misbehavior. We consider a wireless network of mobile devices (nodes) operating in an area without any network infrastructure support, i.e., in ad hoc mode. When transferring packets, the nodes *rely* on each other for forwarding packets. Thus, it is very important that all the nodes in the network act in a cooperative manner. However, due to limited resources (e.g., energy supply,

computing power) that each node has, the notion of cooperation might not be rational. As a result, nodes may prefer not to participate in packet forwarding or even worse, they can, individually or in groups, resist cooperating with the rest of the network. Hence, noncooperation is a type of misbehavior; the network might become disconnected when some nodes do not forward packets cooperatively. Therefore, an important question to ask is how to stimulate or enforce cooperation among the nodes to ensure the proper functioning of the network.

There are two aspects to this question: i) if the nodes are *rational* and *self-interested*, and only care about maximizing their own benefit, how do we design incentives so that the nodes are willing to be cooperative and ii) if the nodes do not want to cooperate, how do we punish them so that the punishment enforces them to cooperate in the future? To address these issues, we need to analyze what *strategies* nodes adopt and what *actions* they take when they get the packets to be forwarded. Moreover, in wireless network, the wireless channel is highly unreliable due to noise, multipath fading, interference, etc. A node's action in packet forwarding may not be accurately observed by others, or in other words, its action is hidden from the rest of the network. Thus, the question becomes even more complicated when the unreliable channel is considered.

This example can be further challenging when some malicious nodes exist. Unlike the uncooperative nodes, the malicious nodes launch attacks in the network. In the context of packet forwarding, the attacks can be: intentionally dropping packets, altering the contents maliciously, and etc. The objective of such malicious nodes is to cause harm and bring

2

disorder to the network; their goal is to maximize the damage before they are detected and isolated.

In order to minimize the impact of the malicious nodes, detection mechanisms need to be in place. Thus, a regular node should monitor its surroundings and distinguish a malicious node from a regular one. However, the detection process has challenges. First, monitoring can be costly. To identify the malice, a regular node has to listen to the channel and/or process the information sent by the nodes being monitored. Listening and processing consume resources and hence, an "always on" monitoring scheme is not efficient even if plausible. Second, the malicious node can disguise itself. To reduce the probability of being detected, a malicious can behave like a regular node and choose longer intervals between attacks. Third, the randomness and unreliability of the wireless channel bring more uncertainty to the monitoring and detection process.

In spite of the above challenges, mechanisms to detect malicious nodes can always be designed. However, the important question is 'what should the regular node do upon detecting a malicious node?' Though the reasonable response would be to immediately isolate the malicious node, there might be situations where malicious nodes can be kept and made use of. The most straightforward reason for the coexistence is that a malicious node has no idea whether it has been identified or not, and it will continue to operate like a regular node to avoid detection. During this time, i.e., when the malicious node cooperates in disguise, it can be exploited for normal network operations. This "involuntary" help from the malicious node may be valuable, especially when the network resource is limited. As a matter of fact,

from the perspective of the malicious nodes, coexistence gives them a longer lifetime in the network and the opportunity to launch future attacks. As far as the regular nodes are concerned, they have a criteria to evaluate the benefit from the malicious nodes. The criteria also determine when to terminate the coexistence and isolate the malicious nodes.

To make the process of detection even more difficult, the malicious nodes do not act passively and wait to be detected. Instead, they also study the interaction they have with the rest of the network and adjust their subsequent actions accordingly. It is also possible that a malicious node is wise enough to learn and predict the actions of the regular nodes to assist itself in decision making. The options available to the malicious nodes complicate the solution space and most traditional control theoretic approaches fail to find the equilibrium strategies for both the regular and malicious nodes. In particular, these problems fall more appropriately in the domain of static and dynamic distributed games and thus the application of game theory is an elegant way to tackle such problems. It is important that solution concepts from game theory are used to guide the protocol design process such that nodes working in a distributed manner can co-exist, even with different intents.

1.2 Game Theory and Wireless Network Design

As far as a node in a wireless network is concerned, its action is accompanied with a cost or utility, e.g., nodes consume energy in monitoring or forwarding others' data. It is very reasonable and intuitive that the nodes are rational (self interested) and the actions of a node,

4

in response to others', are aimed at maximizing its utility. In addition, the nodes adapt their behavior by learning their utility for each potential action through feedback, which is defined by the overall objective function of the network. In this way, nodes dynamically react to changing network conditions, energy budgets, and external stimuli.

Concepts from game theory [16, 38] make perfect sense when dealing with nodes that are interested in net earnings (*utility*, *payoffs*) for the tasks they perform while interacting with others – be it cooperatively, maliciously or otherwise. In such a distributive environment where nodes make their own decisions, the utility obtained by a node not only depends on what it does but also on what others do. Given a set of rational nodes in a wireless network, the decision whether to cooperate in the process of packet forwarding or how to respond to others' actions can be best analyzed using non-cooperative game theory. Moreover, the underlying unreliable channel makes the nodes' actions hidden from each other. This essentially translates to an imperfect information game. When malicious attacks exist, the regular nodes need to detect the malicious ones through a series of interactions, which can be captured by Bayesian games. Often times, the same game is played for a number of repetitions (as in the case with packet forwarding), and the observed history may influence the nodes' future actions. Furthermore, when the nodes can learn from the results of the previously played games, as the game repeats, the population of the players taking the same strategy evolves and it is interesting to find a prevailing strategy.

An important notion in game theory is the *equilibrium*. It characterizes a steady state that all the players are satisfied with the payoffs and willing to adhere to current strategies.

Given different modeling of the games, equilibrium can be characterized with various properties, e.g., Nash Equilibrium and its refinement Sequential Equilibrium. To mitigate the misbehavior in wireless network, we are interested in obtaining certain equilibria such that adhering to the equilibrium strategies leads to the suppression of the misbehavior. However, the desired equilibria are unique when we take different network settings into account. For example, the equilibrium strategy under homogeneous lossy channel differs from that under heterogeneous lossy channel. While the definitions of various games and equilibria are defined in the next chapter, we will give more exemplified explanation when we introduce the modeling of our games.

1.3   Contributions of this Work

Our main focus in this dissertation is to provide a game theoretic analysis on how to mitigate the aforementioned misbehavior in the presence of unreliable channels. The interaction among the nodes in the wireless network is presented by the packet forwarding process which is further abstracted as a two player game. The misbehavior of the nodes can be categorized as two types, namely *uncooperative* and *malicious*. For the former category, we attempt to obtain a condition, under which cooperation can be enforced. In the latter category, the focus is the detection of the malicious node and the strategies after the detection. In particular, this research includes the following three aspects: i) cooperation enforcement with

homogeneous unreliable channel, ii) cooperation enforcement with heterogeneous unreliable channel, and iii) detection and co-existence with malicious nodes.

1.3.1 Cooperation Enforcement with Homogeneous Unreliable Channel

We begin with the credit exchange system, in which both packet purse model and packet trade model [10] are investigated. We show that in the former model, dominant strategy exists while the latter one fails to give enough incentives to foster cooperation. Given certain incentives, we solve the forwarding game under the general unreliable channel and derive the probability of packet forwarding that leads to an equilibrium. Furthermore, we extend our analysis to repeated games; we take several different strategy profiles and find the conditions under which cooperation leads to subgame perfect Nash Equilibrium. Results show that proper incentives leading to cooperation are related to the belief of the nodes' continuous participation in the game. Besides incentives, a reputation based strategy which generates actions based on the observation of opponents' history is also analyzed. It is found that achieving cooperation with such history dependent strategy does not require any incentives, even when the observation is not accurate due to the unreliable channel. To address the prevalence of cooperation, we focus on the resistance on collusion using both repeated games and evolutionary games. Our findings indicate a subgame perfect cooperation enforcement strategy ensures cooperation as a prevailing action if it is evolutionary stable or the initial non-cooperative population is bounded.

The main contributions in this part can be itemized as follows.

- We evaluate the credit exchange system under the unreliable channel and analyze on several well-known strategy profiles in which incentives lead to subgame perfect Nash Equilibrium. Our approaches are general in nature and can be applied to different strategy profiles and/or payoff matrices.

- We present a rigorous proof on the subgame perfect of a reputation based strategy (i.e., CORE [34, 35]). We show that such history based strategy does not require any incentives, and full cooperation is the subgame perfect equilibrium regardless of the channel.

- We adopt evolutionary game theory in capturing the population dynamics. Analysis indicates that if nodes are patient enough in the game and value future payoffs, collusion resistance and cooperation enforcement are equivalent.

- We study the convergence of the cooperation enforcement through simulation. In particular, we show cooperation can be enforced within the entire population when cooperative and collusion strategies coexist. The rate the population convergence is affected by the initial population share, channel unreliability, and the payoff matrix.

1.3.2 Cooperation Enforcement with Heterogeneous Unreliable Channel

The problems solved in the previous section require a revision when the heterogeneous unreliable channel is assumed. The reason is that under heterogeneous unreliable channel, every node in the network has different and private observations. This part of the work is motivated by the state-of-the-art advances in game theory on repeated games under private monitoring and strategies [7, 20, 21]. We re-model the packet forwarding game considering noise and show that although nodes' actions are hidden due to the channel, they can nevertheless monitor their own payoffs. Based on the private observation of their payoffs, we construct a forwarding approach using a two-state machine. We demonstrate that, through carefully designing the state transition parameters, *sequential equilibria* can be achieved to enforce cooperation. Furthermore, we extend our results to a multi-hop wireless network and propose a multi-hop packet forwarding strategy to attain the same equilibria. Simulation results reveal that the network is able to achieve better throughput when the proposed strategies are adopted.

The highlights in this part are as follows.

- We model the packet forwarding process with channel noise as a hidden action game with imperfect monitoring and propose a strategy profile to the game. The strategy is shown to give a sequential equilibrium solution. Extensive simulations show

that the cooperation enforcement strategy is more efficient (Pareto superior) over non-cooperative ones.

- A multi-hop packet forwarding strategy based on the state machine approach is provided in a general multi-hop wireless network. Our simulation results indicate that the performance in terms of network throughput is very close to a fully cooperative network.

1.3.3 Detection and Co-existence with Malicious Nodes

When malicious nodes exist in the network, the modeling and analysis are focused on the interactions between a malicious node and a regular node. In particular, we formalize the interactions into two cascaded games. The first game, namely *malicious node detection game*, is a Bayesian game with imperfect information. The information is hidden because the malicious node can disguise as a regular node and the actions are hidden due to the noise and imperfect observation. The second game, called *post-detection game*, is played when the regular node knows confidently that its opponent is a malicious node. In the latter game, the regular node observes and evaluates the actions of the malicious node, and decides whether to keep it or isolate it. For both games, we show the existence of equilibria and derive the conditions that achieve them. To address the possible countermeasures the malicious node might take, we propose a nested belief model. In this model, the malicious node learns from its private observations and predicts if the regular node has accumulated enough information

to make the detection. Associated with the belief, we show that a Markov Perfect Bayes-Nash Equilibrium emerges. We also provide simulation study to support the efficiency and other properties of the equilibria.

The main findings can be categorized into three aspects.

- We model the malicious node detection game under unreliable channels as a Bayesian game with imperfect monitoring and show a mixed strategy perfect Bayesian Nash Equilibrium is attainable. The strategy profile is also shown to give a sequential equilibrium solution. Results show how the equilibrium strategy profiles are affected by parameters like channel noise, successful attack rate, successful detection rate, attack gain, detection gain, and false alarm rate.

- We propose the notion of coexistence after detection in order to utilize the malicious node. A coexistence index is designed to evaluate the helpfulness of a malicious node. We derive the conditions under which a subgame perfect Nash Equilibrium is achieved. Through simulation, we also show how the malicious node can be used to improve the network throughput and extend network lifetime.

- We introduce a novel belief about belief model employed by the malicious node. A Markov Perfect Bayes-Nash Equilibrium is induced when both nodes constantly update their beliefs. This equilibrium is shown to delay the detection of the malicious node and help the malicious node actively adjust its strategy to avoid detection. This model also helps to integrate the detection and post-detection games with effective transition.

1.4   Related Work

Game theory [16, 38] has been successfully applied to solve various problems in wireless networks including cooperation enforcement [12, 13, 14, 18, 35, 36, 41], routing protocols [17, 37, 45, 52] and other system design issues [4, 26, 27, 30, 31, 50].

As far as cooperation enforcement in wireless networks are concerned, mechanisms have been devised that either stimulate nodes to forward each others' packets [8, 10, 12] or punish nodes for misbehaving [5, 9, 32, 33, 39]. Usually, selfish nodes need to be identified and isolated by mechanisms like Watchdog [32] or Pathrater [33].

Majority of the proposed methods can be generally categorized into two types: incentive based [11, 13, 41, 51] and reputation based [17, 34, 35]. Most incentive based protocols assume the network with rational nodes/agents and adopt the concept of virtual currency (e.g. "nuglets") [10] which is a method to reward nodes participating in forwarding packets. It has been well established that pricing schemes (in terms of reward and penalty) [3, 13], and the security of payment system [11, 12, 51] are closely associated with the incentive based approaches. On the contrary, in a reputation based system, a node's behavior is monitored and measured by its neighbors. Based on the observed past behaviors, a node receives certain level of services or gets isolated for being non-cooperative [9, 32, 33]. An example of reputation based scheme is CORE [34], where each node maintains a reputation table for the other nodes. The reputation value is updated based on the node's own observations and the information provided by the other nodes.

Meanwhile, there have been some interesting developments that use game theory to analyze how cooperation can be achieved [14, 35, 41, 52]. In [14], Félegyházi et al. formally define the packet forwarding game in ad hoc networks and derive the conditions under which cooperation yields Nash Equilibrium. Michiardi et al. apply game theory in [35] to analyze several strategies in the repeated prisoner's dilemma. They also show that in order to foster the coalition among cooperative nodes, enough incentives should be granted. Zhong et al. [52] show that there is no dominant strategy solution in a forwarding subgame and cryptographic techniques can be employed for the required tamper-proof hardware support. A more general framework on cooperation in ad hoc networks is presented in [41], where Srinivasan et al. focus on the energy efficiency through cooperation.

However, the aforementioned efforts are not sufficient to completely understand and model cooperation in wireless network in the presence of noise. The noisy nature of the wireless channels makes the analysis very challenging. More recent work [17, 18, 37, 47, 49] have called attention to the effect of noise that makes the observation *imperfect*. In [17], Jaramillo et al. propose a distributed reputation monitoring based strategy to enforce cooperation when the channel is not loss free. Their strategy is proved to be subgame perfect even if the channel estimation is not accurate. Studies on several cooperation enforcement schemes when channel collision exists are presented in [37, 47], where non-cooperative game theory is used. In [49], statistical methods are used to filter noise from observation so that attacks can be identified. Ji et al. [18] calculate the belief of nodes on others' actions and propose a belief-based multi-node multi-hop packet forwarding scheme. Li et al. [26]

further generalize noise and imperfect monitoring as hidden information and hidden action games, and study truthful routing issues from a mechanism design perspective. Related investigations are also shown by Feldman *et al.* in [15].

In spite of these developments, cooperation enforcement in wireless networks with noisy channel has not been generalized. As a matter of fact, although our work is inspired by [17, 18], our modeling and methodology is quite different from existing work and should not be considered as a simple variant. In [17], the implicit assumption is that the channels and environment are identical around the receiver and the observer; however, in our model, the channels are assumed to be heterogeneous. Sometimes, the theories and calculations are too complex [18]. Furthermore, the difficulties in hidden action game with imperfect private monitoring games are generally two-fold. First, when the noisy channel makes action history unknown to the public, the games do not possess the recursive structure on the equilibrium [1]. Second, players (nodes) are not sure about what the opponents are going to do because they cannot perfectly monitor their actions. In this case, a player must take the best strategy based on her belief about her opponents' actions at every move, which is the essence of the strategies proposed in [18]. However, the drawback of the belief updating strategies is that the calculations on updating the beliefs are usually extremely complex. Nonetheless, in this dissertation, our proposed methods overcome such shortcomings.

Recently, much work has been done that investigates the interactions between the regular and malicious nodes using game theory. Kodialam *et. al.* formally propose a game theoretic framework to model how a service provider detects an intruder [23]. However, their

assumptions of zero-sum game and complete, perfect knowledge have limitations. Agah *et.* *al.* study the non-zero-sum intrusion detection game in [2]; their results infer the optimal strategies in one-stage static game with complete information. In [29], Liu *et. al.* propose a Bayesian hybrid detection approach to detect intrusion in wireless ad hoc networks. They design an energy efficient detection procedure while improving the overall detection power. The intrusion detection game with networked devices are investigated in [54], where Zhu *et. al.* introduce an N-person non-cooperative game to study incentive compatibility of the collaborative detection. [28] models the intention and strategies of a malicious attacker through an incentive-based approach. The importance of the topology on the payoffs of the malicious nodes are investigated in [42]. An interesting flee option for the malicious node is proposed in [25]. In that analysis, a malicious decides to flee when it believes it is too risky to stay in the network. While the approach focuses on how the flee action affects the result of the game, it does not consider the noise in observation.

1.5   The Structure of this Dissertation

The rest of the dissertation is organized as follows. In Chapter 2, we introduce the game theoretic definitions and preliminaries. In Chapter 3, we focus on the cooperation enforcement with homogeneous unreliable channel and anti-collusion games. The findings are presented in terms of the conditions for subgame perfect equilibrium and evolutionary stability. Chapter 4 extends the research to consider heterogeneous unreliable channel and shows a state

machine based solution to achieve sequential equilibrium. A multi-hop cooperative packet forwarding strategy is also presented. Chapter 5 further explores the misbehavior of maliciousness by constructing a malicious node detection game. The solutions in this chapter show a co-exist equilibrium that malice can be exploited and taken advantage of. The last chapter summarizes this research and concludes the dissertation.

CHAPTER 2
GAME THEORETIC DEFINITIONS AND PRELIMINARIES

Game theory offers power tools in modeling and analyzing conflicts and cooperation among multiple players in a system with regard to strategic decision making. As a branch of applied mathematics, it is widely applied to areas of politics, biology, engineering and more. In Section 1.4, we have shown some applications of game theory in wireless communication and networking. In this chapter, we formally review some of the fundamental definitions and concepts in game theory [16, 38, 43] that will be used and applied throughout this dissertation.

2.1   Game, strategy, and equilibrium

A game consists of players, the possible actions of the players, and consequences of the actions. Formally, the word "game" is defined as:

Definition 2.1. *A **game** Γ is a triple $(I, S, \boldsymbol{u})$, where*

- *$I = 1, 2, ..., n$ denotes a set of players.*

- *$S = \times_{i \in I} S_i$ is a space of strategy profiles. It is the Cartesian product of strategy profile S_i for each of the player i.*

- **$\boldsymbol{u}$** is a vector of von Neumann-Morgenstern utility functions defined over S. For a particular strategy profile $\boldsymbol{s}$, $\boldsymbol{u(s)} = (u_1(\boldsymbol{s}), u_2(\boldsymbol{s}), ... u_i(\boldsymbol{s}))$ is called a payoff vector consists of individual payoffs $u_i(\boldsymbol{s})$.

The most fundamental assumption in game theory is that all players in the game are *rational*. A rational player chooses actions to maximize her payoffs. In the case the game is not deterministic, the player chooses to maximize her expected utility (payoffs). The idea of maximizing the expected payoff was justified by the seminal work of von Neumann and Morgenstern in 1944 [44]; it is characterize the probabilistic distribution of the payoffs. As the expected utility is governed by the utility functions, a game essentially describes the actions the players can take, which are mapped to the consequences (i.e., payoffs) of the actions by the utility functions.

Since the game is an interaction among players, the payoff of a player (denoted as i) may be determined not only by her actions, but also the actions of other players'. In this regards, often times, player i is interested in what strategies the rest of the players in the game take. We denote the *deleted strategy profile* $\boldsymbol{s}_{-i} = (s_1, ..., s_{i-1}, s_{i+1}, ..., s_n)$. However, it might happen that in a game, a player's action is superior to others', no matter what the other players do.

Definition 2.2. *A strategy s_i' is a **dominant** strategy for player i if $u_i(s_i', \boldsymbol{s}_{-i}) \geq u_i(s_i, \boldsymbol{s}_{-i})$, for every $\boldsymbol{s}_{-i}$ of the other players' actions. Similarly, a **dominated** strategy s'' is $u_i(s_i'', \boldsymbol{s}_{-i}) \leq u_i(s_i, \boldsymbol{s}_{-i})$. The dominance is strict if the inequality holds.*

A game can be solved by iterated elimination of strictly dominated strategies. However, not every strategy profile has strategic dominance. Even if there is no dominant strategies,

18

a player also has her belief on what strategies other players will take, so that she can pick her response strategies accordingly.

Definition 2.3. *A strategy $s'_i \in S_i$ is a **best response strategy** for player i if and only if $u_i(s'_i, \boldsymbol{s}_{-i}) \geq u_i(s_i, \boldsymbol{s}_{-i}), \ \forall \ s_i \in S_i \backslash s'_i$.*

From the definition above, we can see that if the strategies taken by players are mutual best to each other, no player would like to deviate from the given strategy profile. The unwillingness of deviation is an outcome of the game, and it describes a steady condition that all players reach while playing with each other. To identify the strategy profiles that lead to the steady condition, the concept of Nash Equilibrium is introduced and defined as follows:

Definition 2.4. *The strategy profile s^* is a Nash Equilibrium, if*

$$u_i(s^*) \geq u_i(s_i, s^*_{-i}) \ \text{for every strategy } s_i \text{ of player } i.$$

What Nash Equilibrium suggests is a state, that none of the players would unilaterally change the strategy to increase the utility. Thus Nash Equilibrium brings the game to a steady state, from which the players would not like to deviate as that would not increase their benefits any more.

A classical representation of the Nash Equilibrium is illustrated through the famous example of Prisoner's Dilemma. The matrix in Figure 2.1 shows the payoffs (number of years the prisoner will be sentenced) when an strategy profile is adopted, however, in this example, no communication between the prisoners is assumed.

19

	Prisoner B stays Silent	Prisoner B Defects
Prisoner A stays Silent	(1 year, 1 year)	(10 years, 0 year)
Prisoner A Defects	(0 year, 10 years)	(3 years, 3 years)

Table 2.1: Payoff matrix of Prisoner's Dilemma.

In Prisoner's Dilemma, "Defect" is the dominant strategy for Prisoner A/B, because no matter what strategy his opponent takes, the payoff is strictly better (0 year is better than 1 year, 3 years are better than 10 years). Therefore, (Defect, Defect) is the Nash Equilibrium obtained by iterated elimination.

Another classical Nash Equilibrium example is called the Battle of the sexes [38], as the payoff matrix which is shown in Figure 2.2. In this two-player coordination game, a couple prefers to go an evening event together but has not made a decision on which event they will attend, a Football match or Opera. For the husband, if the wife chooses to go to Opera, his best response strategy is to choose Opera. When the husband chooses Opera, the best response for wife is also Opera. Thus, (Opera, Opera) is a mutual best response strategy and forms a Nash Equilibrium. However, (Football, Football) is also a Nash Equilibrium point based on the "mutually best" criteria.

	Wife chooses Opera	Wife chooses Football
Husband chooses Opera	(1, 4)	(0, 0)
Husband chooses Football	(0, 0)	(4, 1)

Table 2.2: Payoff matrix of the Battle of the sexes.

The above examples show the game with *pure strategies*. A pure strategy provides a complete definition of how a player will play a game. Or in other words, a pure strategy gives deterministic moves of a player for every situation she could face. Apart from pure strategies, a player can also play *mixed strategies*. A mixed strategy is an assignment of a probability to each pure strategy available to the player. The mixed strategy allows the player to choose randomly a pure strategy, and thus create infinite numbers of mixed strategies from the strategy set. The Nash Equilibrium obtained with pure strategies is called *Pure Strategy Nash Equilibrium*, as opposed to the *Mixed Strategy Nash Equilibrium* obtained with mixed strategies.

2.2   Classes of games

When game theory is applied to model the interactions among players, based on how the games are played and what the players know, the game can be categorized into different classes. In this section, we introduce several classes of games that are used in our research.

- **Repeated game**. In most cases, games are played continuously rather than one shot. The theory of repeated game is to capture how a player's actions early on can affect what others choose to do later on.

Definition 2.5. *A repeated game is an extensive form game in which stage game Γ is played finite or infinite number of times. For each player, the set of actions available in any period in Γ is the same, regardless of the time or past actions. The payoffs to the players depend only on the action profiles for Γ in that particular period, and is independent of the time.*

In a repeated game, we consider the rth stage. Since all the players know the history h^r (perfectly or imperfectly), we can view the game starting at rth stage as a subset of the original game, and call it a *subgame*.

Similar to a single stage game, a repeated game can be characterized with the concept of Nash Equilibrium. However, it is refined as Subgame perfect equilibrium.

Definition 2.6. *A repeated game strategy $\bar{s}$ is a* **Subgame-Perfect Nash Equilibrium** *(SPNE) if at each subgame, for all players i*

$$\bar{s}_i \in \arg\max_{\mathbf{s_i} \in \mathbf{S_i}} u_i(s_i, \bar{s}_{-i}).$$

If $\bar{h}$ is the history generated by $\bar{s}$, then $\bar{h}$ is the associated **equilibrium path**.

To analyze the subgame perfect equilibria in repeated games, One-Shot Deviation Property (OSDP) is extensively used. A strategy profile is SPNE if it satisfies the OSDP.

Definition 2.7. *One-Shot Deviation Property: no player can increase her payoff by changing her action at the start of any subgame in which she is the first-mover, given the other player's strategies and the rest of her own strategy.*

- **Perfect information game**. A game is called perfect information game if all players know all moves that have taken place. Formally speaking, any players in a perfect information game has only one element in her information set, where the concept of information set is defined as:

Definition 2.8. *Information Set is a set that, for a particular player, establishes all the possible moves that could have taken place in the game so far, given what that player has observed.*

Perfect information cannot always be guaranteed due to the opacity of the opponents' actions or the inaccuracy of the observation. In the case of imperfect information, a player can only conjecture what the other players have played. Hence, probabilistic analysis might be employed to solve the game.

- **Complete information game**. Complete information game is a situation in which knowledge about every players is available to others. Every player knows the payoffs and strategies available to other players.

Similar to perfect information, complete information may not be achieved all the time. In an incomplete information game, the players would not be able to know the structure or the utility functions of the game. As a consequence, they are not able to predict the effect their actions would have on the other players.

It is worth to mention that complete and perfect information game are two distinct type of games. The perfect information describe the actions inside the game, while the complete information states the knowledge about the game structure and goals of the players. A complete information game can be with imperfect information, for example, in Prisoners' Dilemma, although both prisoners know the penalty of silent and defect, they do not know what action the other prisoner takes. Nonetheless, the incomplete information game can be transformed into a imperfect information game by introducing *nature* as a third player. However, unlike regular players, the third player does not care about her payoffs. In our

modeling of the games, we model the observation inaccuracy due to channel unreliability as imperfect information game, while we treat the malicious node detection process as incomplete information game. Bayesian game analysis is applied to transform the incomplete information game to imperfect information game.

The definitions and terminologies introduced in this chapter serve as the preliminaries of our design of misbehavior mitigation system. In the rest of the dissertation, we will carry these definitions. We will also revisit these definitions when we formally define our games.

CHAPTER 3
COOPERATION ENFORCEMENT WITH HOMOGENEOUS UNRELIABLE CHANNEL

In this chapter, we use game theory to analyze the necessary and sufficient conditions to enforce cooperation, especially when a node cannot perfectly monitor other nodes' behaviors due to the unreliability of the wireless channel. In particular, we deal with *homogeneous unreliable* channel in this chapter. Homogeneous unreliable channel describes the wireless media with the same loss rates for every transmitter receiver pair. In contrast, A *heterogeneous unreliable* channel indicates the channels are lossy, but with different loss/error probabilities.

The discussions are based on the packet forwarding scenario in a multi-hop wireless network. In Section 3.1, we analyze a credit exchange method under a generalized unreliable channel model and show that the packet forwarding probability can be adjusted through proper design of incentives, which in turn can be used to attain the desired Nash Equilibrium. We extend our discussion to repeated games in Section 3.2 where we take several well-known strategy profiles and derive the conditions under which the cooperation can lead to a subgame perfect Nash equilibrium. In particular, we show how the unreliable channel can affect the conditions and how a reputation based strategy leads to subgame perfection even under imperfect monitoring. In Section 3.3, we define the anti-collusion game and further

investigate collusion resistance and cooperation coalition formation using evolutionary game theory. We prove the existence of an upper bound on the population share of the non-cooperative nodes for an evolutionarily non-stable strategy that enforces full cooperation.

3.1 Analysis of Credit Exchange System

The credit exchange system is constructed on the notion that each node gains certain amount of credits after participating in packet forwarding. These credits, for example "nuglets [10]", are transferable and exchanged from one node to another as a payment for packet forwarding. Moreover, the credits themselves are issued by a central authority and without forgery, so that the credit can be used as "virtual currency". As suggested in [10], there can be two types of charging models for credit exchange: *Packet Purse Model (PPM)* and *Packet Trade Model (PTM)*. In PPM, the packet to be forwarded is initialized with a certain amount of credit. Each forwarding node acquires some credits and forwards the packet to next hop. If a packet does not have enough credit, it will be discarded. While, in PTM, the packet does not carry any credit, but is traded for credits among intermediate nodes. Nodes "buy" the packet from its previous hop with some credit and "sell" the packet to the next hop, with some increased amount to cover the forwarding cost. A packet will be dropped if no node wants to buy it. Let us further analyze the node behavior under these models.

3.1.1   Packet Purse Model

We consider a set of nodes along a pre-defined forwarding path, and form a "forwarding game". The strategy profile for each of the nodes is $s = (Forward,\ Discard)$. We define the cost to a node for forwarding a packet is 1. The amount of credit (α) a node charges for forwarding varies according to its instantaneous resource availability, for example, a node with less energy may charge more than a node with more energy remaining. It is obvious, $\alpha \geq 1$ for the nodes to have incentives to forward. In the simplest form of PPM, a node takes the credit and forwards the packet.

Lemma 3.1. *In PPM, the dominant strategy is Discard.*

Proof. For node i, the payoff for forwarding is $\alpha - 1$, and the payoff for dropping is α. Thus, all the nodes will simply take the credit and drop the packet. As a matter of fact, since the first node on the route will drop the packet after acquiring the credits, the packet can never be forwarded beyond one hop. $\qquad\square$

It is clear that PPM cannot be directly applied because the nodes will act selfishly and will have no obligation to forward. Hence, secure PPM (SPPM) was proposed that addressed this issue by implementing some credit validation mechanisms [10]. In SPPM, the credit a node acquires from the packet is not valid unless and until it passes the packet to next hop and receives the validation from the next hop node. We further assume that the transmission of validation is costless, i.e., a rational node will pass validation to its previous hop because it will not gain any benefit not to do so. However, due to channel loss, transmission is subject

to be unsuccessful with probability p_e, $p_e \in (0, 1)$. This loss is applicable to both packet and validation.

Lemma 3.2. *In SPPM, the dominant strategy is Forward if $p_e < \frac{\alpha-1}{2\alpha-1}$, Drop if $p_e > \frac{\alpha-1}{2\alpha-1}$.*

Proof. Since the nodes are rational and they do not obtain any benefit by dropping the validations, they will only adopt pure strategies. The expected payoff of forwarding a packet is $(\alpha - 1)(1 - p_e)^2$, if both the packet transmission and validation feedback are successfully transmitted over the unreliable channel. If a node chooses to drop a packet, it might still get a payoff of $\alpha(1 - p_e)p_e$, should the next hop node be "merciful". In this case, the next hop node believes that the packet had been forwarded but lost due to the channel, and nonetheless passes the validation back and is successfully received. The payoff of *Forward* is strictly greater than the payoff of *Drop* if $p_e < \frac{\alpha-1}{2\alpha-1}$. Else, when $p_e > \frac{\alpha-1}{2\alpha-1}$, the payoff of *Drop* is greater, which means that *Forward* is a dominated strategy and will never be chosen. However, if the next hop node is not "merciful", the payoff for *Discard* is zero. Thus as long as $\alpha > 1$, *Forward* is the dominant strategy. □

From the discussion above, we can see that the validation forces the nodes to forward packets in order to obtain the payoff. However, with a very unreliable channel, a node may still be willing to drop because the lossy channel makes forwarding non-profitable. Thus, in designing the incentives, we make the following claim.

Corollary 3.1. *In SPPM, cooperation is enforced if $\alpha > \frac{1-p_e}{1-2p_e}$.*

3.1.2   Packet Trade Model

		Node $-i$			
		Buy		Discard	
Node i	Buy	$\alpha_i - \bar{\alpha}_i - \alpha_{-i}$	$\alpha_{-i} - \bar{\alpha}_{-i} - \alpha_i$	$-\bar{\alpha}_i - \alpha_{-i}$	$\alpha_{-i} - \bar{\alpha}_{-i}$
	Discard	$\alpha_i - \bar{\alpha}_i$	$-\bar{\alpha}_{-i} - \alpha_i$	$-\bar{\alpha}_i$	$-\bar{\alpha}_{-i}$

Table 3.1: Payoff matrix of two-player forwarding game under PTM.

For the packet trade model, we reconstruct the "forwarding game" as a reciprocal two-player game. Under this game model, any two neighboring nodes have bidirectional network traffic demands [17], i.e., they rely on each other to forward packets. This assumption can be regarded as an abstract scenario when a node is playing the same game versus all the other nodes along the path. We model the two-player forwarding game as both nodes forward packets to each other at the same time, and then, they simultaneously decide whether to *buy* the packet or to *discard* it. We denote two neighboring nodes as i and $-i$. For node i, the price (cost) it pays to buy the packet from its previous node is $\bar{\alpha}_i$, and the price at which it sells to node $-i$ is α_i. These prices are $\bar{\alpha}_{-i}$ and α_{-i} when we consider the node $-i$. The payoff matrix for the nodes is shown in Table 3.1.

In this game, since nodes will obtain benefit by selling packets, $\alpha_x \geq \bar{\alpha}_x > 0;\ x = i, -i$. It is obvious that the strategy *Buy* is strictly dominated by *Discard* for both nodes. Hence, if we assume that both nodes will only adopt pure strategies, the game has the same form as the well-known *Prisoner's Dilemma* game [38], although (*Buy*, *Buy*) is more desired. Thus we have,

Lemma 3.3. *In PTM, the strategies for attaining Nash Equilibrium is (Discard, Discard).*

3.1.3   Hybrid Model

Neither PPM nor PTM provides enough insight for designing proper incentives for cooperation. Thus, we consider a hybrid model which is a combination of PPM and PTM. We still

consider the "forwarding game". We continue to assume that the links are bidirectional, i.e., both nodes forward the packets to each other, and then a decision to forward or discard is made. As shown in Figure 3.1, node N_A relies on node N_B to forward packet to N_C, and N_B relies on N_A to forward packet to N_D. The cost of forwarding is 1, and nodes get α as reward if their packet is forwarded by their counterpart. However, a reward cannot be granted unless packets in both directions are forwarded, otherwise, the node which discards gets no payoff and the other node consumes 1 for forwarding. The payoff matrix is shown in Table 3.2.
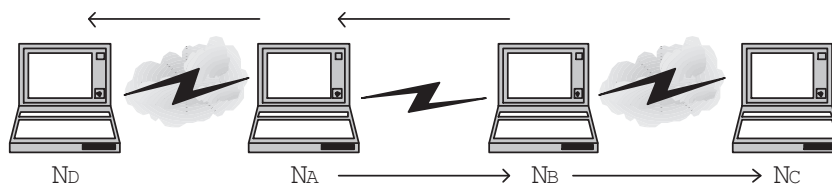
Figure 3.1: Packet forwarding game.

		Node $-i$			
		Forward		Discard	
	Forward	$\alpha - 1$	$\alpha - 1$	-1	0
Node i	Discard	0	-1	0	0

Table 3.2: Payoff matrix of two player forwarding game.

It is shown in [52] that there is no such strategy profile in which forwarding is always the dominant strategy. This also infers that the actions or strategies nodes take are hidden from each other. It is even more obvious when we consider an unreliable channel. When a node drops a packet, it is impossible for others to distinguish whether the dropping was intentional or due to the unreliability of the channel. In this type of game, where the actions

of the nodes are hidden from each other, nodes have enough reason (even if no incentive) to play mixed strategies. Or rather, they are perceived to be playing mixed strategies simply because the perception is not accurate through the unreliable channel.

Let us consider the equilibrium point when mixed strategies are allowed.

Lemma 3.4. *The two-player forwarding game has a mixed strategy Nash Equilibrium when both nodes play Forward with probability $p = \frac{1}{\alpha}$.*

Proof. We denote the probability of *Forward* for node i as p_i, and the probability of *Forward* for node $-i$ as p_{-i}. The expected payoff of node i is $p_i p_{-i}(\alpha - 1) - p_i(1 - p_{-i})$. The best response for node i is *Discard* when $p_{-i} < \frac{1}{\alpha}$, and *Forward*, when $p_{-i} \geq \frac{1}{\alpha}$. For node $-i$, the best response strategy is similar; *Forward*, when $p_i \geq \frac{1}{\alpha}$, and vice verse. The intersection of the two best response strategies is the Nash Equilibrium, where both nodes play *Forward* with probability $p_i = p_{-i} = \frac{1}{\alpha}$. $\square$

Further, we consider the unreliable channel and re-solve the game. The variation the channel brings in is that it is still possible that even node $-i$ plays *Forward*, the credits are lost due to transmission failure, so that it appears to be a *Discard* for node i and hence harm the payoff of node i.

Lemma 3.5. *Under unreliable channel, the two-player forwarding game has a mixed strategy Nash Equilibrium when both nodes play Forward with probability $p = \frac{1}{\alpha(1-p_e)}$.*

Proof. We use the same notations in Lemma 3.4. The expected payoff of node i is $(1 - p_e)[p_i p_{-i}(\alpha - 1)(1 - p_e) - p_i(1 - p_{-i} + p_{-i}p_e)]$. The best response for node i is *Discard* when $p_{-i} < \frac{1}{\alpha(1-p_e)}$, and *Forward*, when $p_{-i} \geq \frac{1}{\alpha(1-p_e)}$. The same reasoning is valid for node $-i$. Thus the equilibrium reaches when both nodes play *Forward* with probability $p = \frac{1}{\alpha(1-p_e)}$. $\square$

Let us further generalize the channel model. We consider a channel with M different states, with channel loss probability $p_e(j)$ for the jth state. We also define a $M \times M$ channel

31

transition probability matrix $\mathcal{A}$, in which $a_{j,k}$ is the probability that channel goes from state j to k. A special case of this model is the widely used two state (Good or Bad) channel model, where channel transfers from one state to another with some probability. The updated problem now can be stated as: Given a user's current channel state j and transition probability matrix $\mathcal{A}$, how do we solve the game as defined in Table 3.2.

To solve this game, we bring the channel as the third player. Unlike node i or $-i$, the channel does not care for a payoff, and the game can be solved with only payoffs of node i or $-i$. If the channel condition goes from j to k, the payoff to node i is $p_i p_{-i}(\alpha - 1)(1 - p_e(k)) - p_i(1 - p_{-i} + p_{-i}p_e(k))$. However, this payoff depends only on probability of $a_{j,k}$. To consider all the channel transition probabilities, node i's payoff with j as the current channel state is

$$u(i) \quad = \quad \sum_{k,k\neq j} a_{j,k}(1 - p_e(k))\Big[p_i p_{-i}(\alpha - 1)(1 - p_e(k)) - p_i(1 - p_{-i} + p_{-i}p_e(k))\Big]. \quad (3.1)$$

The best response for node i is to set p_i as

$$p_i = \frac{1}{\alpha \sum_{k,k\neq j} a_{j,k}(1 - p_e(k))}. \quad (3.2)$$

If both nodes i and $-i$ play the same mixed strategy with *Forward* probability in equation (3.2), it forms a mixed strategy Nash Equilibrium.

Thus, we extend Lemma 3.5 for the generalized channel model as the following Lemma with the discussion above serving as the proof.

Lemma 3.6. *Under a generalized unreliable channel model with channel loss probability $p_e(j)$ for the jth state and probabilities $a_{j,k}$ for the state transitions, the two-player forwarding*

game has a mixed strategy Nash Equilibrium when both nodes play Forward with probability
$p = \frac{1}{\alpha \sum_{k,k \neq j} a_{j,k}(1-p_e(k))}$.

Further, we have

Corollary 3.2. *Under a generalized unreliable channel model, Nash Equilibrium is achieved if incentive α is made equal to $\frac{1}{p \sum_{k,k \neq j} a_{j,k}(1-p_e(k))}$.*

To summarize, we have the the following implications. i) The nodes' strategies are affected by the channel loss probability. We cannot ignore the wireless channel condition when designing credit exchange systems. ii) When nodes' actions are hidden, mixed strategy can lead to a practical Nash Equilibrium. Due to the selfishness of the nodes, pure strategies are mostly impractical. iii) The pricing model used by the nodes should be carefully evaluated to incorporate factors like channel loss and best response strategies.

3.2   The Repeated Game

So far, we have discussed the strategies and payoffs in *one-shot* packet forwarding game (i.e., stage game). In this section, we will analyze the strategies the nodes will adopt in a repeated game, which is the repetitions of the same stage game. We define the repeated packet forwarding game as:

Definition 3.1. *The repeated packet forwarding game G is a two-player repeated game, with a space of strategy profile S, and a vector $\boldsymbol{u}$ of von Neumann-Morgenstern utility functions defined over S. Thus, $G = (\{1,2\}, S, \boldsymbol{u})$ where $S = \times_{i=1}^{2} p_i^{(r)}$, and $p_i^{(r)}$ is the probability in stage r that player i plays **Forward**. $\boldsymbol{u} \equiv < U_1, U_2 >$, and $U_i = \sum_{r \geq t} \delta^{r-t} u_i(r)$ is the discounted payoff of player i from the tth stage.*

The non-negative parameter δ is called the discount factor and $\delta \in (0, 1)$. The discount factor infers the preference of time or patience. A large δ shows a player's patience in the game and good valuation of payoffs she gets in future stages, while a small δ means that the player is more eager for immediate payoffs and has higher probability of leaving the game after each stage.

In the presence of unreliable channel, when a packet transmitted by node $-i$ fails to reach node i, node i cannot instantly distinguish whether node $-i$ intentionally dropped the packet or it was due to channel loss. However, statistically, node i could nonetheless gather information and calculate an observed forwarding probability for node $-i$ in the following way.

Definition 3.2. *The observed forwarding probability of player $-i$ at stage r is*

$$\hat{p}_{-i}^{(r)} = (1 - p_e(k))p_{-i}^{(r)}$$

assuming the channel is at state k.

Definition 3.3. *The observed payoff of player i at stage r is*

$$\hat{u}_i^{(r)} = \sum_{k,k\neq j} a_{j,k}[p_i^{(r)}\hat{p}_{-i}^{(r)}(\alpha - 1) - p_i^{(r)}(1 - \hat{p}_{-i}^{(r)})]$$

$$= \sum_{k,k\neq j} a_{j,k}[(1 - p_e(k))\alpha p_{-i}^{(r)} - 1]p_i^{(r)}.$$

Definition 3.4. *The observed average discounted payoff of player i is*

$$\hat{U}_i = (1 - \delta)\sum_{t\geq 0} \delta^t \hat{u}_i^{(t)}.$$

The $(1 - \delta)$ term is to unify the sum, so that the summation is 1 if there are infinite number of stages.

34

In the remaining part of this section, we present some of the well-known strategies (Last Step Trigger [38], Naive Grim Trigger [38], Grim Trigger [38], and CORE [34, 35]) and analyze their behaviors as well as limitations. In order not to introduce any confusion, we denote $p_{i,S}^{(t)}$ as the probability node i should take to forward packet at t^{th} stage according to the strategy profile $\mathbf{S}$.

3.2.1 Last Step Trigger

Definition 3.5. *The strategy of Last Step Trigger (LST) is defined as*

$$
\begin{aligned}
p_{i,LST}^{(0)} &= 1 \\
p_{i,LST}^{(r)} &= \begin{cases} 1 & \textit{if } \hat{p}_{-i}^{(r-1)} = 1 \\ 0 & \textit{otherwise} \end{cases}
\end{aligned}
$$

From Definition 3.2, we know that it is not possible for $\hat{p}_{-i}^{(r)} = 1$ under channel with $p_e(k) \neq 0$. Thus, both nodes will play *Discard* from the second stage, no matter what they played in the first stage. In other words, there is no non-trivial equilibrium point.

Thus, to show some tolerance towards channel loss, Last Step Trigger strategy sets a threshold value (ρ) for observed forwarding probability.

Definition 3.6. *The strategy of Last Step Trigger with channel loss tolerance is defined as*

$$
\begin{aligned}
p_{i,LST}^{(0)} &= 1 \\
p_{i,LST}^{(r)} &= \begin{cases} 1 & \textit{if } \hat{p}_{-i}^{(r-1)} \geq \rho \\ 0 & \textit{otherwise} \end{cases}
\end{aligned}
$$

where $\hat{p}_{-i}^{(r)}$ is defined in Definition 3.2.

Lemma 3.7. *In repeated packet forwarding game, if both players use LST, the subgame perfect Nash equilibrium (SPNE) is Forward if and only if $p_e(k_r) \leq 1 - \rho$ and forwarding cost conforms to (3.4).*

Proof. We denote $p_e(k_r)$ as the channel loss probability for the rth subgame, and the initial state is k_0. $\alpha_{(r,r+1)}$ is the channel transition probability from rth subgame to the immediate next stage. If $p_e(k_r) \leq 1 - \rho$ in the first stage, $p_i^{(0)} = 1$ and $\hat{p}_{-i}^{(0)} = 1 - p_e(k_{-1})$; the observed payoff for node i is

$$\hat{u}_i^{(0)} = a_{(-1,0)}(\alpha - 1 - \alpha p_e(k_0)).$$

The observed average discounted payoff for node i is

$$\hat{U}_i = (1 - \delta) \sum_{r \geq 0} \delta^r a_{(r-1,r)}(\alpha - 1 - \alpha p_e(k_r)). \tag{3.3}$$

The payoff is the same for node $-i$. If node i unilaterally deviates at the first stage by setting $p_i^{(0)} = 0$, its observed payoff at this stage is 0. In the next stage, $p_i^{(1)} = 1$, $\hat{p}_{-i}^{(1)} = 0$, and

$$\hat{u}_i^{(1)} = -a_{(-1,0)}.$$

Using the same logic, the observed average discounted payoff for node i's deviation is

$$\hat{U}_{i,dev} = (1 - \delta) \sum_{r \geq 0} \delta^{2r+1}(-a_{(2r+1,2r+2)}).$$

Using one-shot deviation property (OSDP: see Definition 2.7), when $\hat{U}_{i,dev} \leq \hat{U}_i$, node i has no incentive to deviate. After some algebraic manipulations, this condition reduces to

$$\alpha \geq \frac{\sum_{r \geq 0}[\delta^r a_{(r-1,r)} - \delta^{2r+1} a_{(2r+1,2r+2)}]}{\sum_{r \geq 0}[\delta^r a_{(r-1,r)}(1 - p_e(k_r))]}. \tag{3.4}$$

If $p_e(k_r) > 1 - \rho$, from second stage, both nodes will get zero payoffs. Thus, no equilibrium point exists. $\qquad \square$

As a special case of Lemma 3.7, if the channel is static, with the same loss probability of p_e, then

$$\hat{U}_i = (1 - \delta) \sum_{r \geq 0} \delta^r(\alpha - 1 - \alpha p_e) = \alpha - 1 - \alpha p_e.$$

$$\hat{U}_{i,dev} = (1 - \delta) \sum_{r \geq 0} \delta^{2r+1}(-1) = \frac{-1}{1 + \delta}.$$

Under OSDP, the restriction on discount factor reduces to

$$\frac{\alpha(1 - p_e)}{\alpha p_e + 1 - \alpha} \leq \delta \leq 1. \tag{3.5}$$

As a matter of fact, what Lemma 3.7 states is a pure strategy SPNE where both nodes adheres to LST and forwards or discard with probability 1, i.e., $p_{i,LST}^{(r)} = p_i^{(r)}$. However, since the channel is unreliable, as long as node i forward packet with probability $p_i^{(r)}$ ($p_{i,LST}^{(r)} = \neq p_i^{(r)}$), such that $\hat{p}_i^{(r)} \geq \rho$, node $-i$ will cooperate in the next stage. Thus, mixed strategy equilibrium analysis can be applied to LST, and when $p_i^{(r)} \geq \frac{\rho}{1-p_e(k)}$, mixed strategy SPNE can be achieved.

We follow the same procedure as the pure strategy analysis to find the mixed strategy SPNE. When nodes i and $-i$ play *Forward* with probabilities $p_i^{(r)}$ and $p_{-i}^{(r)}$ respectively, the observed average discounted payoff for node i is

$$\hat{U}_i = (1 - \delta) \sum_{r \geq 0} \delta^r a_{(r-1,r)}[(1 - p_e(k_r))\alpha p_{-i}^{(r)} - 1]p_i^{(r)}. \tag{3.6}$$

The observed average discounted payoff for node i under deviation is

$$\hat{U}_{i,dev} = -(1 - \delta) \sum_{r \geq 0} \delta^{2r+1} a_{(2r+1,2r+2)} p_i^{(2r+2)}. \tag{3.7}$$

Therefore, according to OSDP, the condition to attain mixed strategy SPNE is

$$\alpha \geq \frac{\sum_{r \geq 0}[\delta^r a_{(r-1,r)} p_i^{(r)} - \delta^{2r+1} a_{(2r+1,2r+2)} p_i^{(2r+2)}]}{\sum_{r \geq 0}[\delta^r a_{(r-1,r)}(1 - p_e(k_r))]p_{-i}^{(r)} p_i^{(r)}}. \tag{3.8}$$

For the special case of static lossy channel and $p_i^{(r)} = \frac{\rho}{1-p_e(k)}$, the mixed strategy SPNE condition reduces to

$$\frac{\alpha\rho}{1 - \alpha\rho} \leq \delta \leq 1. \tag{3.9}$$
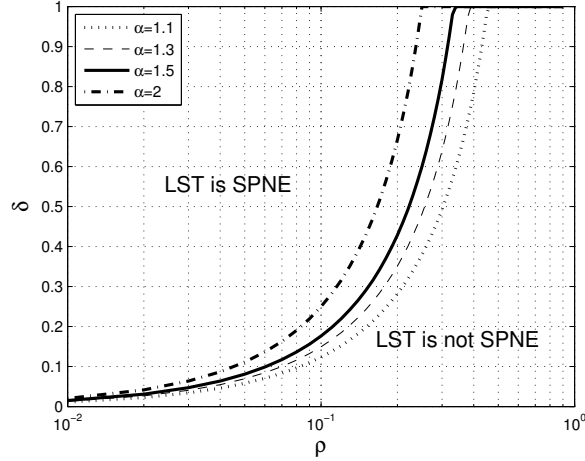
Figure 3.2: Sensitivity of SPNE when LST is adopted.

Figure 3.2 shows the sensitivity of the mixed strategy SPNE obtained with LST. The plots represent the range of δ for a given value of ρ or α. The plots also show the properties of pure strategy SPNE, because when $p_i^{(r)} = 1$, $\rho = 1 - p_e(k)$. It is suggested from the plots that a large α value corresponds to a smaller ρ value, which means large incentives relax the unreliability in the channel.

3.2.2 Naive Grim Trigger

Definition 3.7. *Naive Grim Trigger (NGT) is defined as:*

$$
\begin{aligned}
p_{i,NGT}^{(0)} &= 1 \\
p_{i,NGT}^{(r)} &= \begin{cases} 1 & \text{if } \hat{p}_{-i}^{(r')} \geq \rho \text{ for all } r' < r \\ 0 & \text{otherwise} \end{cases}
\end{aligned}
$$

N-GRIM is an unforgiving strategy. A node is punished if it deviates. If both nodes play *Forward* and $p_e(k_r) \leq 1 - \rho$, the observed average discounted payoff is given by equation (3.3).

38

Let us consider that node i unilaterally deviates at the first stage by setting $p_i^{(0)} = 0$; it gets zero payoff at the first stage. In the second stage, by observing node i's dropping behavior, node $-i$ sets $p_{-i}^{(1)} = 0$, thus the payoff for node i is $\hat{u}_i^{(1)} = a_{(-1,0)}(-1)$. No further payoffs will be gained in future subgames, because both nodes will punish each other for their prior dropping behavior. Under OSDP, N-GRIM attains subgame perfect Nash equilibrium if and only if $(1 - \delta) \sum_{r \geq 0} \delta^r a_{(r-1,r)}(\alpha - 1 - \alpha p_e(k_r)) \geq a_{(0,1)} \times (-1)$, which is equivalent to

$$\alpha \geq \frac{(1 - \delta) \sum_{r \geq 0} \delta^r a_{(r-1,r)} - a_{(0,1)}}{(1 - \delta) \sum_{r \geq 0} \delta^r a_{(r-1,r)} (1 - p_e(k_r))}. \tag{3.10}$$

The mixed strategy SPNE analysis for N-GRIM is similar to what we have done for LST. Equilibrium can be attained when $p_i^{(r)} \geq \frac{\rho}{1 - p_e(k)}$, and the mixed strategy SPNE and its pure strategy counterpart are equivalent when $\rho = 1 - p_e(k)$.

N-GRIM only punishes the nodes if they deviate. Often times, a severe punishment is set up to enforce cooperation between nodes. A Grim Trigger is such a strategy that punishes a node for its own deviation, not just others.

3.2.3 Grim Trigger

Definition 3.8. *Grim Trigger (GRIM) is defined as:*

$$\begin{aligned}
p_{i,GRIM}^{(0)} &= 1 \\
p_{i,GRIM}^{(r)} &= \begin{cases} 1 & \text{if } \hat{p}_{-i}^{(r')}, \hat{p}_i^{(r')} \geq \rho \text{ for all } r' < r \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

Using the same reasoning, if node i unilaterally deviates at the first stage, it does not gain any payoff. Afterwards, according to GRIM, both nodes will play *Discard*. Therefore,

$\hat{U}_{i,dev} = 0$. Thus, the *sufficient condition* for subgame perfect Nash equilibrium under OSDP is $\alpha - 1 - \alpha p_e(k_r) \geq 0$. Hence,

$$\alpha \geq \frac{1}{1 - \rho}. \tag{3.11}$$

In the aforementioned analysis on three trigger strategies, we have shown that pure strategy SPNE is attainable and it can enforce full cooperation. However, the conditions to achieve pure strategy SPNE are associated with the channel loss. Furthermore, because of the channel loss, mixed strategy SPNE is also feasible; nonetheless, mixed strategy SPNE is not desirable because, it does not enforce full cooperation (i.e., $p_i^{(r)} < 1$). In other words, with the trigger strategies, unless the channel loss rates are known, cooperation is hard to achieve.

3.2.4 CORE

CORE is a complex strategy for cooperation enforcement proposed in [34, 35]. It is similar to the well-know Tit-For-Tat (TFT) but different from TFT as it considers the last b stages in the repeated game.

Definition 3.9. *The CORE strategy can be defined as:*

$$
\begin{aligned}
p_{i,CORE}^{(0)} &= 1 \\
p_{i,CORE}^{(r)} &= \begin{cases} 1 & \text{if } \mathcal{B}_{-i} = \frac{1}{b}\sum_{s=r-b}^{r-1}[\hat{p}_{-i}^{(s)}]_{-1}^{1} \geq 0 \\ 0 & \text{otherwise} \end{cases}
\end{aligned}
$$

where the sth stage observed history $h^s = (\hat{p}_i^{(s)}, \hat{p}_{-i}^{(s)})$, and

$$[x]_{-1}^{1} = \begin{cases} 1 & \text{if } x \geq 1 \\ -1 & \text{if } x < 1 \end{cases}$$

Theorem 3.1. *CORE is subgame perfect if and only if*

$$0 \leq \alpha \leq \frac{1}{1 - p_e}.$$

Proof. CORE is a b-stage history strategy because it takes into account what happened in the last b stages. Without loss of generality, let us assume that any history h^n results in $\mathcal{B}_i = m$, where m is uniformly distributed over $[-b, b]$, and m is a discrete integer random variable. For the sake of discussion, we assume $\mathcal{B}_{-i} \geq 0$ and the channel has a loss probability p_e. We focus on node i from the first stage (starting stage). In the proof, we will calculate the expected payoffs for node i considering different values m can take. A certain m value leads to a specific payoff, and it comes with a probability as m changes. We first formalize the expected payoff function, and then derive the probability terms in the function.

Case 1. If node i conforms to CORE, then its payoff at the first stage would be

$$
\begin{aligned}
\hat{u}_i^{(0)} &= \mathbf{P}(m = 0)[(1 - p_e)\hat{u}_i^{forward} + p_e \hat{u}_i^{discard}] \\
&+ \mathbf{P}(m \geq 1)\hat{u}_i^{forward} + \mathbf{P}(m < 0)\hat{u}_i^{discard},
\end{aligned}
\tag{3.12}
$$

where $\mathbf{P}(\cdot)$ means the probability and $\hat{u}_i^{forward}$, $\hat{u}_i^{discard}$ are the observed payoffs of "Forward" and "Discard". From Definition 3.3, we know that

$$
\begin{aligned}
\hat{u}_i^{forward} &= \alpha(1 - p_e) - 1 & (3.13) \\
\hat{u}_i^{discard} &= 0. & (3.14)
\end{aligned}
$$

Consider the next stage, node $-i$ will update $\mathcal{B}_i$ with node i's stage 0 behavior, and we denote the updated $\mathcal{B}_i$ value as m'. Similar to equation (3.12), the observed payoff at this stage is

$$
\begin{aligned}
\hat{u}_i^{(1)} &= \mathbf{P}(m' = 0)[(1 - p_e)\hat{u}_i^{forward} + p_e \hat{u}_i^{discard}] \\
&+ \mathbf{P}(m' \geq 1)\hat{u}_i^{forward} + \mathbf{P}(m' < 0)\hat{u}_i^{discard}.
\end{aligned}
$$

With the process of m to m' taken into consideration, we have the following equations.

$$
\begin{aligned}
\mathbf{P}(m' = 0) &= p_e \mathbf{P}(m = 0) + (1 - p_e)\mathbf{P}(m = -1) & (3.15) \\
\mathbf{P}(m' \geq 1) &= p_e \mathbf{P}(m \geq 2) + (1 - p_e)\mathbf{P}(m \geq 0) & (3.16) \\
\mathbf{P}(m' < 0) &= p_e \mathbf{P}(m \leq 0) + (1 - p_e)\mathbf{P}(m \leq 1) & (3.17)
\end{aligned}
$$

Since the distribution of m is already known, we can obtain the probabilities as

$$
\begin{aligned}
\mathbf{P}(m = x) &= \frac{1}{2b + 1} & (3.18) \\
\mathbf{P}(m \leq x) &= \frac{x + b + 1}{2b + 1} & (3.19)
\end{aligned}
$$

where integer value $x \in [-b, b]$.

Further, let us consider the lth stage. We denote l_p as the random variable of positive scores gained, i.e., the cooperation action is observed successfully by the opponent ($\mathcal{B}_i = \mathcal{B}_i + 1$), l_n as the random variable of negative scores gained, i.e., the cooperation action is not observed by the opponent ($\mathcal{B}_i = \mathcal{B}_i - 1$). Since node i conforms to CORE, and forwards at each stage, any gain in l_n is due to the channel loss. Thus, l_p and l_n are binomially distributed and

$$
\begin{aligned}
\mathbf{P}(l_p = L_P) &= C_l^{L_P}(1 - p_e)^{L_P} p_e^{l-L_P} & (3.20) \\
\mathbf{P}(l_n = L_N) &= C_l^{L_N} p_e^{L_N}(1 - p_e)^{l-L_N}. & (3.21)
\end{aligned}
$$

We denote a random variable $y = \mathcal{B}_i$. From the analysis above, we know $y = m + l_p - l_n$. Similar to $\hat{u}_i^{(0)}$ and $\hat{u}_i^{(1)}$, we can write $\hat{u}_i^{(l)}$ as

$$
\begin{aligned}
\hat{u}_i^{(l)} &= \mathbf{P}(y = 0)[(1 - p_e)\hat{u}_i^{forward} + p_e\hat{u}_i^{discard}] \\
&+ \mathbf{P}(y \geq 1)\hat{u}_i^{forward} + \mathbf{P}(y < 0)\hat{u}_i^{discard}. & (3.22)
\end{aligned}
$$

Hence, the problem relies on obtaining the probability distribution of y. Since $y = m + l_p - (l - l_p) = m + 2l_p - l$ and l is a constant, to get the distribution of y, we first get the distribution of $w = y + l$.

We use the probability generation function (pgf). For discrete random variable x, its pgf is defined as

$$
G_X(z) = E[z^X] = \sum_{x=0}^{\infty} z^x \mathbf{P}(X = x) \tag{3.23}
$$

The pgf for w is

$$
\begin{aligned}
G_W(z) &= E[z^W] = E[z^{M+2L_P}] = E[z^M]E[z^{2L_P}] \\
&= \sum_{n=-b}^{b} z^n \frac{1}{2b+1} [\sum_{n=0}^{l} z^n C_l^n (1 - p_e)^n p_e^{l-n}]^2 \\
&= \frac{z^{-b} - z^{b+1}}{(2b+1)(1-z)} [p_e + (1 - p_e)z]^{2l} & (3.24)
\end{aligned}
$$

Let $f^{(n)}(x) = \frac{\partial^n f(x)}{\partial x^n}$,

$$
\mathbf{P}(w = k) = \frac{G_W^{(k)}(0)}{k!} \tag{3.25}
$$

For the probability terms in equation (3.12),

$$
\mathbf{P}(y = 0) = \mathbf{P}(w = l) = \frac{G_W^{(l)}(0)}{l!} \tag{3.26}
$$

$$\mathbf{P}(y \geq 1) = \mathbf{P}(w \geq l+1) = \sum_{n=l+1}^{b+l} \frac{G_W^{(n)}(0)}{n!} \tag{3.27}$$

$$\mathbf{P}(y < 0) = \mathbf{P}(w < l) = 1 - \frac{G_W^{(l)}(0)}{l!} - \sum_{n=l+1}^{b+l} \frac{G_W^{(n)}(0)}{n!} \tag{3.28}$$

Plugging equations (3.26), (3.27) and (3.28) back to equation (3.22), we can get the observed payoff for node i at l^{th} stage. Further, if node i conforms to CORE, its observed average discounted payoff is given as $\hat{U}_i = (1-\delta)\sum_{t \geq 1} \delta^{t-1} \hat{u}_i^{t-1}$. Algebraic manipulation reduces to

$$\hat{U}_i = (1-\delta)[\alpha(1-p_e)-1]\left\{ \frac{1-p_e+b}{2b+1} + \sum_{r=1}^{\infty} \delta^r \left[(1-p_e)\frac{G_W^{(r)}(0)}{r!} + \sum_{n=r+1}^{b+r} \frac{G_W^{(n)}(0)}{n!} \right] \right\} \tag{3.29}$$

Case 2. If node i does not conform to CORE, and it deviates in the first stage, the payoff at the first stage is

$$\hat{u}_{i,dev}^{(0)} = \mathbf{P}(m \geq 1)\hat{u}_i^{forward} + \mathbf{P}(m \leq 0)\hat{u}_i^{discard}. \tag{3.30}$$

Since the deviation lasts only for one stage, in the next stage, node i will again play CORE. However, $\mathcal{B}_i$ is updated as $= m - 1$, which we denote as m^*. It is not hard to obtain the cumulative distribution function (cdf) of m^* as

$$\mathbf{P}(m^* \leq x) = \begin{cases} 0 & \text{if } x < -b-1 \\ \frac{x+b+2}{2b+1} & \text{if } -b-1 \leq x \leq b-1 \\ 1 & \text{if } x > b-1 \end{cases} \tag{3.31}$$

Using the same notations defined in Case 1, we let $y^* = m^* + l_p - l_n$ and $W^* = y^* + l$. The pgf for W^* is

$$\begin{aligned} G_{W^*}(z) &= \sum_{n=-b-1}^{b-1} z^n \frac{1}{2b+1} [\sum_{n=0}^{l} z^n C_l^n (1-p_e)^n p_e^{l-n}]^2 \\ &= \frac{z^{-b-1} - z^b}{(2b+1)(1-z)} [p_e + (1-p_e)z]^{2l} \end{aligned} \tag{3.32}$$

Similarly, the observed average discounted payoff for node i given it deviation on the first stage is presented in equation (3.33).

$$\hat{U}_{i,dev} = (1-\delta)[\alpha(1-p_e)-1]\left\{ \frac{2b}{2b+1} + \sum_{r=0}^{\infty} \delta^{r+1} \left[(1-p_e)\frac{G_{W^*}^{(r)}(0)}{r!} + \sum_{n=r+1}^{b+r} \frac{G_{W^*}^{(n)}(0)}{n!} \right] \right\} \tag{3.33}$$

43

Under OSDP, CORE is subgame perfect if deviation is not profitable, or $\hat{U}_{i,dev} \leq \hat{U}_i$. We denote $A = (1 - p_e)\frac{G_W^{(r)}(0)}{r!} + \sum_{n=r+1}^{b+r} \frac{G_W^{(n)}(0)}{n!}$, and $B = (1 - p_e)\frac{G_{W*}^{(r)}(0)}{r!} + \sum_{n=r+1}^{b+r} \frac{G_{W*}^{(n)}(0)}{n!}$. Thus,

$$\hat{U}_{i,dev} - \hat{U}_i = (1 - \delta)[\alpha(1 - p_e) - 1][\frac{b + p_e - 1}{2b + 1} + B|_{r=0} + \sum_{r=1}^{\infty} \delta^r(\delta B - A)] \quad (3.34)$$

Since terms A and B are probabilities, $0 \leq A \leq 1$, $0 \leq B \leq 1$, equation (3.34) can be further reduced as

$$\hat{U}_{i,dev} - \hat{U}_i \leq (1 - \delta)[\alpha(1 - p_e) - 1][\frac{b + p_e - 1}{2b + 1} + B|_{r=0} - \delta B|_{r=1}]$$

$$\leq (1 - \delta)[\alpha(1 - p_e) - 1]\frac{b + p_e - 1}{2b + 1} \quad (3.35)$$

Since $b \geq 1$,

$$0 \leq \alpha \leq \frac{1}{1 - p_e}. \quad (3.36)$$

$\square$

Corollary 3.3. *When both nodes adopt CORE, the equilibrium point is $p_i^{(r)} = p_{-i}^{(r)} = 1$, $\forall\ r \geq 0$. Cooperation is hence achieved.*

Remark 1: The theorem suggests that CORE does not enforce cooperation by rewards, but punishment. An incentive based strategy bears the basic constraint that $\alpha > 1$, so that the forwarding is profitable. In CORE, even if the channel is reliable, $\alpha \leq 1$. This property can be further generalized to any strategy where decision is based on past action profiles, especially, when a series of past actions are considered.

Remark 2: CORE can be regarded as a "reputation based" strategy. Nodes gain reputation when forwarding is observed and loose reputation when discarding is observed. Although noise exists (channel is not reliable), CORE can still lead to subgame perfect Nash equilibrium, and hence, full cooperation. Simulation results presented in Section 6.1 also show the effectiveness of CORE under "imperfect monitoring".

44

3.3 Collusion Resistance and Coalition Formation

In this section, we consider how cooperation is enforced. In particular, we address two aspects: i) how to resist collusion among nodes that deviate from the cooperation strategy, and ii) how the population of cooperative nodes grows and cooperation prevails? It is noted that we still focus our analysis on the forwarding game (i.e., single hop forwarding). A good literature of incentive-compatible and strategyproof collusion resistance routing can be found in [26, 45, 46, 53].

3.3.1 Collusion Resistance

Definition 3.10. *Collusion is a group of players working together to maximize their own payoffs regardless of the social optimum. A strategy s^c is a colluding strategy if and only if*

$$\hat{U}_i(s^c, s^c) \geq \hat{U}_i(s^a, s^c),$$

*where s^a is any strategy other than s^c. It is called a **strict colluding strategy** if the inequality holds.*

We consider a pure strategy profile s^* which is subgame perfect and enforce cooperation on the equilibrium point (e.g., CORE). The *anti-collusion game* is a game that played among players adopting colluding strategy s^c and cooperative strategy s^*. The aim of the anti-collusion game is to suppress collusion and achieve cooperation. In the rest of this chapter, we are interested in find the conditions that ensure the outcome of the anti-collusion game is full cooperation.

Let x_c be the population share of a strict colluding pure strategy profile s^c. The following lemma gives an upper bound on x_c.

Lemma 3.8. *A cooperation enforcement strategy s^* is collusion resistant if and only if*

$$x_c < \frac{\hat{U}_i(s^*, s^*) - \hat{U}_i(s^c, s^*)}{\hat{U}_i(s^c, s^c) + \hat{U}_i(s^*, s^*) - \hat{U}_i(s^c, s^*) - \hat{U}_i(s^*, s^c)}. \tag{3.37}$$

Proof. We assume the number of nodes in the game is n. For the group of cooperating nodes, the group's total payoff is

$$\hat{U}^* = n(1 - x_c)\hat{U}_i(s^*, s^*) + nx_c\hat{U}_i(s^*, s^c). \tag{3.38}$$

The total payoff for the group of colluding nodes is

$$\hat{U}^c = n(1 - x_c)\hat{U}_i(s^c, s^*) + nx_c\hat{U}_i(s^c, s^c). \tag{3.39}$$

Collusion resistance requires that $\hat{U}^* > \hat{U}^c$. Therefore,
$x_c[\hat{U}_i(s^*, s^c) - \hat{U}_i(s^*, s^*) + \hat{U}_i(s^c, s^*) - \hat{U}_i(s^c, s^c)] > \hat{U}_i(s^c, s^*) - \hat{U}_i(s^*, s^*)$.
Since subgame perfect Nash equilibrium requires $\hat{U}_i(s^*, s^*) \geq \hat{U}_i(s^c, s^*)$ and strict colluding infers $\hat{U}_i(s^c, s^c) > \hat{U}_i(s^*, s^c)$, we get equation (3.37). □

3.3.2 Coalition Formation

Lemma 3.8 shows that in order to resist collusion, the colluding node population should be kept under a threshold. However, when the games are played over time, the population of different groups (i.e., cooperative or colluding) is highly dynamic. We apply evolutionary game theory [48] in our following analysis to capture the dynamics on population.

Definition 3.11. *Let Δ be a strategy set, when strategies $s_x, s_y \in \Delta$. s_x is an **evolutionarily stable strategy** (ESS) if for every strategy $s_y \neq s_x$ there exists some $\bar{\epsilon}_y \in (0, 1)$ such that*

$$u[s_x, \epsilon s_y + (1 - \epsilon)s_y] > u[s_y, \epsilon s_y + (1 - \epsilon)s_x]$$

for all $\epsilon \in (0, \bar{\epsilon}_y)$.

Proposition 3.1. $\Delta^{ESS} = \{s_x \in \Delta^{NE} : u(s_x, s_y) > u(s_y, s_y), \forall s_y \in \beta(s_x), s_y \neq s_x\}$, *where* Δ^{NE} *denotes the set of Nash Equilibrium strategies, and* $\beta(s_x)$ *is the set of best response strategies against* s_x.

We consider the same s^* and assume it is ESS. We denote x_* as the population share of nodes adopting s^*, i.e., group of cooperative nodes. It is clear $x_* + x_c = 1$.

According to evolution theory, the dynamics for the population of x_* is

$$\dot{x}_* = [u(s^*, s^c) - u(s^c, s^c)]x_* \tag{3.40}$$

Let $\mathbf{M_a}$ represent the payoff matrix when s^* plays s^c.

$$\mathbf{M_a} = \begin{pmatrix} u(s^*, s^*) & u(s^*, s^c) \\ u(s^c, s^*) & u(s^c, s^c) \end{pmatrix}$$

This matrix also holds true for the player plays s^c. Applying $\mathbf{M_a}$ to equation (3.40), we get

$$\begin{aligned} \dot{x}_* &= [(u(s^*, s^*) - u(s^c, s^*))x_*x_c]x_* + [(u(s^*, s^c) - u(s^c, s^c))x_*x_c]x_c \\ &= (a_1x_* - a_2x_c)x_*x_c \end{aligned} \tag{3.41}$$

where $a_1 = u(s^*, s^*) - u(s^c, s^*)$, $a_2 = u(s^c, s^c) - u(s^*, s^c)$.

Lemma 3.9. *The cooperation enforcement strategy* s^* *leads to +1 evolutionarily stable state on population share if and only if* s^* *is ESS or the initial population share* $x_c^0 < a_1/(a_1 + a_2)$.

Proof. For any $x_* < 1$, the +1 state can only be reached if $\dot{x}_* > 0$. Since $x_c, x_* > 0$, it requires $a_1x_* - a_2x_c > 0$. If $a_1a_2 < 0$. The only possibility is $a_1 > 0$, $a_2 < 0$, and indicates s_* is ESS (Proposition 3.1). If $a_1a_2 > 0$. $x_c^0 < \frac{a_1}{a_1+a_2}$. $\square$

It can be noted that in case s^* is not ESS, $x_c^0 = \frac{a_1}{a_1+a_2}$, or $x_*^0 = \frac{a_2}{a_1+a_2}$ are the mixed strategy Nash Equilibrium values. It suggests that when no ESS exists, the strategy with the initial population greater than the equilibrium value prevails.

Summarizing the discussions above, we have the following theorem on a general cooperation enforcement strategy.

Theorem 3.2. *A cooperation enforcement strategy s^* enforces the prevalence of cooperation if and only if it satisfies either of the following two conditions:*

- *s^* is ESS,*
- *$x_c^0 < \min(\frac{\hat{U}_i(s^*,s^*)-\hat{U}_i(s^c,s^*)}{\hat{U}_i(s^c,s^c)+\hat{U}_i(s^*,s^*)-\hat{U}_i(s^c,s^*)-\hat{U}_i(s^*,s^c)}, \frac{a_1}{a_1+a_2})$.*

Remarks: In the second condition, both terms in the minimization function are the same if $\delta = 1$ for the repeated game. It also suggests that when all the players in the game stick to continuous participation, the colluding nodes will be enforced to be cooperative with time. Thus collusion resistant is bona fide cooperation coalition formation. The sensitivity of the convergence of the formation (i.e., $\dot{x}_*$) will be determined by the payoff matrix entries.

3.4   Summary

In this chapter, we address the issue of cooperation enforcement in wireless network under homogeneous unreliable channel. We present a game theoretic approach to analyze how the cooperation can be achieved through Nash equilibrium in the packet forwarding game. We model the unreliable channel as a transition probability matrix and solve the game

for a credit exchange system. We show that in order to sustain equilibrium strategy, an associated forwarding price should be charged. The repeated game analysis is incorporated to solve the stage game that is played again and again. We derive the necessary and sufficient conditions where the forwarding game can reach subgame perfect Nash equilibrium under different strategies. The results show the forwarding cost should be priced with reference to the channel loss rate and discount factor. Four reputation based and history dependent strategies are formally analyzed, and by rigorous proof, we demonstrate such reputation based strategy can enforce cooperation under unreliable channel. Last but not least, we use evolutionary game theory to study how the cooperative population grows and resists collusion. We show that cooperation can be achieved by adopting an evolutionarily stable strategy or restricting the initial population of non-cooperative nodes.

CHAPTER 4
COOPERATION ENFORCEMENT WITH HETEROGENEOUS UNRELIABLE CHANNEL

When we extend our discussions in last chapter to include the case of multi-hop data communication in wireless networks, an important challenge in such scenario is that different nodes will experience heterogeneous channel conditions. In this chapter, we provide a game theoretic solution to enforce cooperation in a multi-hop wireless network in the presence of heterogeneous channel noise. We focus on the packet forwarding process and model it as a hidden action game with imperfect private monitoring in Section 4.1. In Section 4.2, we propose a state machine based strategy to reach Nash Equilibrium. The equilibrium is proved to be a Sequential Equilibrium with carefully designed system parameters. Furthermore, in Section 4.3 we extend our discussion to a general multi-hop wireless network scenario by refining the strategy profiles to handle multi-hop packet forwarding.

4.1   The Packet Forwarding Game under Heterogeneous Noise

We begin our analysis with a review of the classical two-player packet forwarding problem [14, 17]. As shown in Figure 4.1, we consider two data sessions: (i) A_S to A_D through B_S and (ii) B_S to B_D through A_S. If the channel is perfect (loss free), based on the actions

A_S and B_S take, they will obtain different payoffs as listed in Table 4.1. The entries in the matrix, i.e., R, S, T, P, not only determine the payoffs players can obtain, but also indicate the type of the games. For example, in the well-known Prisoner's Dilemma [38], which also characterizes the scenario of packet forwarding, $T > R > P > S$. It is noted that, depending on how the packet system is configured, the values in the matrix might be different. In this research, instead of using a specific payoff matrix like [17], we assume the matrix has a general format as shown in Table 4.1, and later, we will show how the values in the matrix affect the equilibrium properties of our strategy. With the payoff matrix, it is clear that for an action $\boldsymbol{a} = (a_{A_S}, a_{B_S}) = (Forward, Discard)$, the payoff vector would definitely be $\boldsymbol{u} = (u_{A_S}, u_{B_S}) = (S, T)$.
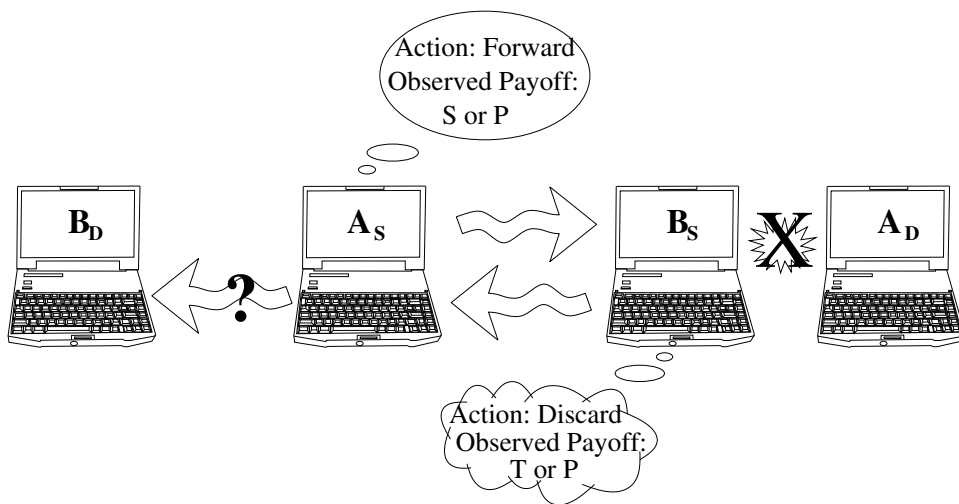

Figure 4.1: Two player packet forwarding game model.

However, when we bring in the channel loss, even if both nodes take the same actions as above, the payoff vector is not likely to remain the same. For node A_S, it forwards B_S's packet to B_D, but the forwarding action might fail due to the channel noise, and B_D does

		Node A_S			
		Forward		Discard	
Node B_S	Forward	R	R	S	T
	Discard	T	S	P	P

Table 4.1: Payoff matrix of two player packet forwarding game. R=Reward, S=Sucker, T=Temptation, P=Penalty.

not receive the packet. Since B_S's payoff is determined by whether B_D receives the packet, from node B_S's perspective, A_S is playing *Discard* even though its action was *Forward*. Thus, the payoff vector now is $\boldsymbol{u} = (P, P)$. Nonetheless, node B_S cannot directly observe A_S's action. This is because what B_S can observe relies only on the channel between it and A_S and this channel is different from that between A_S and B_D due to interference. Also, we do not assume that B_D can, through some mechanism, inform B_S about whether the packet is received or not. Hence, what the nodes can do is to monitor their own payoffs (*realized payoff*), and indirectly, form a *belief* on what others have done. Based on the same payoff matrix in Table 4.1, if the noise is presented as a channel loss probability p_e, we can calculate the probabilities associated with actions and payoffs. In Table 4.2 , we list the probabilities as node i plays the first action and its opponent plays the second action in the action profiles. With these probabilities, we can further calculate the expected payoff of a node. For example, when $\boldsymbol{a} = (Forward, Discard)$, the expected payoff vector is $\boldsymbol{u} = ((1 - p_e)S + p_eP, (1 - p_e)T + p_eP)$.

Let us now formally define the packet forwarding game under noise.

Definition 4.1. *A packet forwarding game (Γ) under noise is a quadruple (I, A, Ω, u), where*

- *$I = 1, 2, ..., n$ denotes the set of nodes.*
- *A is a space of actions (a_i) a node (i) can take.*

		Node i's payoffs			
		R	S	T	P
Actions	(F, F)	$(1-p_e)^2$	$p_e(1-p_e)$	$p_e(1-p_e)$	p_e^2
	(D, F)	0	0	$1-p_e$	p_e
	(F, D)	0	$1-p_e$	0	p_e
	(D, D)	0	0	0	1

Table 4.2: Payoff probabilities for given action profiles.F=Forward, D=Discard.

- Ω *is a space of observed signals. For every action $a_i \in A_i$ node i takes, it observes a signal $\omega_i \in \Omega_i$. Both action a_i and signal ω_i are node i's private information. The probability distribution of private signal $\omega = (\omega_1, ..., \omega_n)$ depends on the action profile $a = (a_1, ..., a_n)$ and the noise in the channel. It is denoted as $p(\omega|a)$.*

- u *presents the realized payoffs. For node i, its expected payoff is given by $g_i(a) = \Sigma_\omega p(\omega|a) u_i(a_i, \omega_i)$.*

Often times, this game is played repeatedly as nodes have a number of packets to be forwarded. From a discounted repeated game [38] perspective, the discounted payoff for node i is $U_i = \Sigma_{t=0}^{\infty} \delta^t g_i(a(t))$, where $a(t)$ is the action taken at time t and $\delta \in (0, 1)$ is the discount factor. The discount factor infers the preference of time or patience. A large δ shows a node's patience in the game and good valuation of payoffs it gets in future stages, while a small δ means that the node is more eager for immediate payoffs and has higher probability of leaving the game after each stage.

The above definition differs from most existing game models in the sense that a node cannot directly observe others' actions, rather, it observes through a *private* signal[1] associated with the action profiles played. As a matter fact, existing models can be regarded as a special case when $\omega = a$ for all nodes (all nodes have perfect public observation of others'

---
[1]It is noted that the signal here does not necessarily mean the physical signal in the communication channel, but rather, it refers to all the possible observations a node can make, e.g., the payoffs.

actions), or $\omega_1 = \omega_2 = ... = \omega_n \neq a$ (all nodes have imperfect public observation of others' actions). While the existing models either ignore the noisy nature of the wireless channel or need some sort of communications among nodes to exchange the observations, our model eliminates such pre-assumptions and hence most appropriately abstracts an wireless network scenario.

The outcome of a single stage (static) game can be characterized by the well-known *Nash Equilibrium* [38]. In a Nash equilibrium, no player can unilaterally deviate from the equilibrium strategy to gain more payoff; or in other words, every player is playing the best response to others. When the same game is played repeatedly for finite or infinite number of times, the notion of *subgame* is used so that the game can be viewed as a subset of the original game starting at a certain stage, with a perfectly or imperfectly monitored history. The repeated game can be analyzed by finding the *Subgame-Perfect Nash Equilibrium* (SPNE), which consists of a series of Nash Equilibria at every subgame of the original game [38]. From our modeling of the packet forwarding game, in order for each node to make best response to others' actions that are hidden, it first needs to form a belief on what the others have done. A profile of strategies and beliefs makes an *assessment*. To further refine the SPNE given the assessment, *Sequential Equilibrium* [24] is introduced.

Definition 4.2. *Sequential Equilibrium[2] is an assessment of strategy π and belief μ, which satisfies the following properties:*

- *Strategy Sensibility: When the beliefs are fixed, no player prefers at any point to change her part of strategy in π given the information set, i.e., π maximizes the expected payoffs.*

---

[2] *Please refer to [24] for a more formal definition.*

54

- *Belief Sensibility: Those information sets can be reached with positive probabilities (μ) given π.*

- *Consistency: The assessment should be a limit point of a sequence of the mixed strategies and associated sensible beliefs, i.e., $(\pi, \mu) = \lim_{n \to \infty} (\pi_n, \mu_n)$.*

Thus, in order to enforce cooperation in wireless networks with noisy channel, it is highly desirable that any adopted strategies and their associated beliefs constitute the sequential equilibrium. Also, this sequential equilibrium is attainable by carefully designing the parameters to calculate the beliefs. To further clarify the concept of sequential equilibrium in the packet forwarding game, we assume that although nodes cannot perfectly observe the actions of others, they have beliefs about what the opponents have done. Based on the beliefs, they take corresponding actions in future games. The sequential equilibrium requires that the nodes form their beliefs in such a way (e.g., following Bayesian rules) that the states associated with the beliefs can be reached with positive probabilities. In addition, the consequent actions taken given the beliefs are the best response to the current state. A possible solution to attain the equilibrium is proposed in [18], where one node plays the Grim Trigger strategy and the other one plays the defection strategy, and the beliefs are updated at every stage of the game. However, the belief-based approach requires extensive computations, and moreover, their modeling on the effect of the channel is not thoroughly investigated, as the *Discard* action can never be observed as *Forward*. In this dissertation, our goal is to design a more efficient way to attain sequential equilibrium under the noisy channel. Our approach is different from [18] in both design notion and methodology.

4.2   State Machine Based Forwarding Approach

In this section, we demonstrate how to construct a sequential equilibrium using state machine based forwarding approach. It is noted that a larger space of other cooperation enforcement strategies, as well as the associated equilibria with noisy channels have been analyzed in [37, 47]. For the sake of clarity, we consider the packet forwarding game between two nodes.

First, we define two types of observable signals ω. *Punishment* signal and *Reward* signal. We define that a *Punishment* signal is observed when the node's realized payoff is P, otherwise a *Reward* signal is observed. It is noted that a punishment signal can be observed even if node is playing cooperatively. Table 4.2 can be used to calculate $p(\omega|a)$ given the action profiles. However, the observations are private.

Further, let us consider a strategy with two states, C (Cooperative) and N (Non-Cooperative). The strategy begins with state C and operates with the following transition probabilities.

- When the node is in State C, play *Discard* with a small probability q_C. If *Discard* is taken and *Punishment* is observed, transit to N with probability ρ_C. Stay in C, otherwise.

- When the node is in State N, play *Discard* with a large probability q_N. If *Discard* is taken and *Reward* is observed, transit to C with probability ρ_N. Stay in N, otherwise.

The state machine based forwarding approach is illustrated in Figure 4.2. It is noted that in this approach, there is always uncertainty on which state the opponent node is, and hence the beliefs are updated all the time. In order for this design to reach sequential equilibria, it is important that, with any history, the state machine is a best response to itself, regardless of the beliefs. In other words, the problem is to find whether there is a set of the system parameters (transition probabilities), such that node i does not gain different payoffs by choosing either actions, i.e., *Forward* (F) or *Discard* (D), no matter what state its opponent node $-i$ is in.
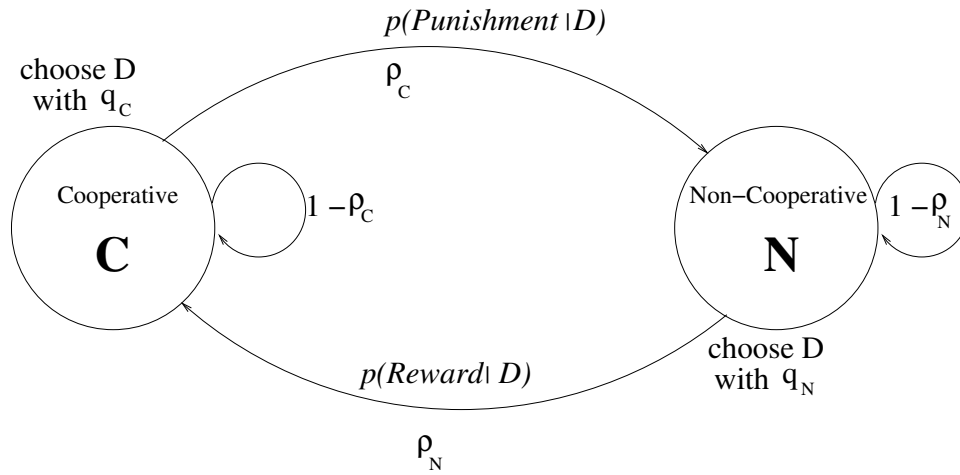

Figure 4.2: Forwarding state machine.

The design problem is hence reduced to finding the system parameters (q_C, q_N, ρ_C, ρ_N) to make the strategy itself a best response to the state machine. We denote V_C and V_N as the average repeated game payoffs for node i when node $-i$ is in state C and N respectively. From Bellman equations [6], we can write the following equations.

When node i plays F,

$$V_C = (1 - \delta)[(1 - q_C)R + q_C S] + \delta[(1 - q_C p_e \rho_C)V_C + q_C p_e \rho_C V_N] \tag{4.1}$$

$$V_N = (1 - \delta)[(1 - q_N)R + q_N S] + \delta\{(1 - p_e)\rho_N q_N V_C + [1 - (1 - p_e)\rho_N q_N]V_N\} \tag{4.2}$$

Similarly, if node i plays D,

$$V_C = (1 - \delta)[(1 - q_C)T + q_C P] + \delta[(1 - q_C \rho_C)V_C + q_C \rho_C V_N] \tag{4.3}$$

$$V_N = (1 - \delta)[(1 - q_N)T + q_N P] + \delta V_N \tag{4.4}$$

For node i to be indifferent between F or D, Equations (4.1) and (4.3) should be equal when node $-i$ is in state C, or Equations (4.2) and (4.4) should be equal when node $-i$ is in state N. Thus, the solutions for above equations represent the equilibria of the state machine. The following theorem provides one of the solutions.

Theorem 4.1. *For the state machine based forwarding approach, there is a sequential equilibrium for large δ, when $p_e < \frac{R-P}{T-P}$ and $T > R$.*

Proof. From Equations (4.1) and (4.3) we have

$$(1 - \delta)[(1 - q_C)(T - R) + p_C(P - S)] = \delta q_C \rho_C (1 - p_e)(V_C - V_N) \tag{4.5}$$

Thus, from Equation (4.1), we can further derive

$$V_C = (1 - q_C)R + q_C S + \frac{p_e}{1 - p_e}[(1 - q_C)(R - T) + q_C(S - P)] \tag{4.6}$$

Similarly, from Equations (4.2) and (4.4) we have

$$(1 - \delta)[(1 - q_N)(T - R) + p_N(P - S)] = \delta q_N \rho_N (1 - p_e)(V_C - V_N) \tag{4.7}$$

and
$$V_N = (1 - q_N)T + q_N P \tag{4.8}$$

From the observation of Equations (4.5)-(4.8), we are left with four variables and two equations, which implies there are two free variables. To find a possible solution to the equations, to begin with, we consider ρ_C as a free variable and set $\rho_C = 1$. The reasoning is as follows. If there is a solution of the above equations with $\rho_C < 1$, we can always decrease q_C in Equation (4.6) to increase V_C. However, this will lead us to further increase ρ_C to balance Equation (4.5). Thus, ρ_C can be increased to 1 but never exceed 1 as it is a probability. The same reasoning can be applied to the other free variable q_N and we let $q_N = 1$. For $q_N < 1$, increasing q_N can lead to a decrease in ρ_N in Equation (4.8) to balance the decreased V_N from Equation (4.7).

The above analysis reduces to

$$V_N = P \tag{4.9}$$

and

$$\rho_N = \frac{q_C(P - S)}{(1 - q_C)(T - R) + q_C(P - S)}. \tag{4.10}$$

It is not hard to see that $\rho_N \in [0, 1]$.

Putting Equations (4.10) and (4.6) back to Equation (4.7), we obtain a quadratic equation of q_C as

$$\{\delta(1 - p_e)[R - S - \frac{p_e}{1 - p_e}(T - R + S - P)]\}q_C^2$$

$$+\{\delta(1 - p_e)[P - R - \frac{p_e}{1 - p_e}(T - R)] + (1 - \delta)$$

$$(P - S - T + R)\}q_C + (1 - \delta)(T - R) = 0 \tag{4.11}$$

One root of Equation (4.11) is easy to get as $q_C = 0$ when $\delta = 1$. To find the relationship between q_C and δ, we check the existence of implicit function (F) around $(q_C, \delta)=(0, 1)$ as

$$\frac{\partial F}{\partial q_C}\Big|_{(q_C,\delta)=(0,1)} = (1 - p_e)[P - R - \frac{p_e}{1 - p_e}(T - R)]. \tag{4.12}$$

Since $p_e < \frac{R-P}{T-P}$, Equation (4.12)$\neq 0$, and thus the Implicit Function Theorem can be applied around $\delta = 1$ such that

$$\frac{dq_C}{d\delta} = -\frac{\frac{\partial F}{\partial \delta}\Big|_{(q_C,\delta)=(0,1)}}{\frac{\partial F}{\partial q_C}\Big|_{(q_C,\delta)=(0,1)}}$$

$$= \frac{T - R}{(1 - p_e)[P - R - \frac{p_e}{1-p_e}(T - R)]}. \tag{4.13}$$

From the assumptions, we know that Equation (4.13)< 0, which essentially states that there exists a value $q_C \in (0, 1)$, for a large enough δ such that $q_C \to 0$ as $\delta \to 1$. Hence, a set of parameters satisfying the system requirement is obtained around $\delta = 1$.

Further, with the set of parameters, the average payoff is updated as

$$\begin{aligned} V_C &= \lim_{q_C \to 0} \{(1-q_C)R + q_C S + \frac{p_e}{1-p_e}[(1-q_C)(R-T) + q_C(S-P)]\} \\ &= R + \frac{p_e}{1-p_e}(R-T) > P. \end{aligned} \qquad (4.14)$$

Thus, state C is always more efficient than state N. In addition, when the nodes are updating their beliefs on the opponent, it will always assume that the opponent has never deviated because no deviation is observable. The consistency requirement is satisfied as neither node tries to update its beliefs about others; instead, the nodes play the best response strategies. Hence, we have proved that the state machine based forwarding approach has a sequential equilibrium for large δ, when $p_e < \frac{R-P}{T-P}$ and $T > R$. $\square$

In the proof, we showed that with the system parameters (state transition probabilities) in $[0,1]$, q_C can be arbitrarily close to 0 as δ goes to 1; and the cooperative state is always strictly Pareto superior to the non-cooperative state. Moreover, the average payoff of the cooperative state is arbitrarily close to $R - \frac{p_e}{1-p_e}(T-R)$.

By further manipulating the constraints in Theorem 4.1, we have the properties as follows.

Corollary 4.1. *In order to reach sequential equilibrium, $R < T < \frac{1-p_e}{p_e}(R-P)$.*

Corollary 4.2. *In a sequential equilibrium, the average payoff of the cooperative state is lower bounded by P and upper bounded by $R - \frac{p_e}{1-p_e}(T-R)$.*

Corollaries 4.1 and 4.2 infer that the values of the elements in the payoff matrix can help to reach the sequential equilibrium, and at the same time pushing the average payoff to the Pareto frontiers. In particular, we can find a small enough ϵ such that $T = R + \epsilon$ to relax the constraint on channel loss in Theorem 4.1.

Corollary 4.3. *If $T = R + \epsilon$, when $\epsilon \to 0^+$, a sequential equilibrium can be reached regardless of the noise in the channel, and the average payoff of the cooperative state $V_C \to R$.*

Proof. Since $T = R + \epsilon$, in Theorem 4.1, in order to reach sequential equilibrium $p_e < \frac{R-P}{T-P} = \frac{T-\epsilon-P}{T-P}$. Also, $\lim_{\epsilon \to 0^+} \frac{T-\epsilon-P}{T-P} = 1$. Since $p_e \in (0,1)$, for $\epsilon \to 0^+$, it essentially relaxes the

constraint on p_e; thus p_e can take any value in (0,1). From Corollary 4.1, $T < \frac{1-p_e}{p_e}(R - P)$, which derives $\frac{p_e}{1-p_e} < \frac{R-P}{R+\epsilon}$. Hence, $V_C(\epsilon) = \lim_{\epsilon \to 0^+} R - \frac{\epsilon(R-P)}{R+\epsilon} = R$. $\qquad\square$

4.3 Multi-hop Packet Forwarding

So far, we have discussed the two-player case of packet forwarding when the observation is imperfect and private. However, in a wireless network, packet forwarding from source to destination usually requires multiple hops. In this section, we model the multi-hop packet forwarding as a multi-player packet forwarding game. We investigate the interactions among the players and analyze the cooperation strategies based on two-player approaches discussed in Section 4.2.

Before we study the cooperation strategies in this scenario, we need to characterize a multi-hop wireless network and model the packet forwarding game, in which multiple nodes participate in a hop-by-hop manner. We consider a network where nodes are mobile within a certain area. The nodes are selfish but not malicious. Each of nodes can be a source of a data session which generates packets and sends them to a specific destination. Thus, the multi-player packet forwarding game can be modeled from the *packet forwarding game under heterogeneous noise.*

Definition 4.3. *The multi-player packet forwarding game is a series of packet forwarding games (as defined in Definition 4.1)* $\Gamma = (I, A, \Omega, u)$ *under noise where for each data session:*

- $I = 1, 2, ..., n$ *denotes a set of nodes that are candidates to form a packet forwarding route from source to destination.*

- $A = (Forward, Drop).$

- Ω *is the space of the observed signals and it is private to the node itself. No private observation exchange is assumed. A node only plays with its immediate neighbors in* I*, and cannot obtain any information beyond one hop.*

- *The payoffs are defined in Table 4.1 for per unit packet forwarded. A data session consists of multiple unit packets and thus the forwarding game is repeated.*

4.3.1   Multi-hop Packet Forwarding Strategy Design

Theorem 4.1 and Corollary 4.3 state that it is possible for the two-player forwarding game to reach a Sequential Equilibrium where cooperation can be enforced. Since a node can only interact with its one hop neighbor, for a route from source node to the destination, it is natural that if the games played at each of the hops reach Sequential Equilibria according to our model, all the nodes are cooperative in the multi-hop forwarding. For each data session, based on whether there is a dedicated route, the multi-hop packet forwarding strategy can be categorized into two types: routing based forwarding and hop-by-hop forwarding.

4.3.1.1   Routing Based Forwarding

In this type of forwarding strategy, a route has to be established before packet forwarding starts. Thus, a route discovery process is involved and the source node knows explicitly the intermediate nodes at the time of route establishment. As the route discovery process can be done in various ways, like Ad hoc On-Demand Distance Vector Routing (AODV) [40] and Dynamic Source Routing (DSR) [19] protocols, a route selection mechanism should be

in place to determine which nodes are chosen to form the route, or in other words, who the players are in the game. The criteria in route selection are diversified. Usually, the aim of the routing protocol and the type of application determine the route selection, e.g., route with least hops, route with least traffic, and etc. With the route established, the packet forwarding games can then be played along the route. For any node possessing a packet, it plays the game with the next hop node on the route following the approaches defined in Figure 4.2 with C as the initial state. If for some reason, the next hop node does not participate in the game any more, the route is broken and a new route needs to be set up and the games will be played with a new set of players. The routing based forwarding strategy can be listed as the following steps:

- Step 1: Routing discovery and selection.

- Step 2: Play two-player packet forwarding game at every hop along the route for each of the data packet to be delivered.

- Step 3: Re-establish a new route if the original route is down and repeat the process from Step 1.

4.3.1.2 Hop-by-Hop Forwarding

In the situation of high mobility, route changes are fast and it is costly to maintain a dedicated route from source to destination. Thus, it is possible that any node possessing the packet determines the next hop relay node as long as the packet can eventually reach

the destination node. A typical hop-by-hop forwarding is the Greedy Perimeter Stateless Routing (GPSR) [22] in which every hop is geographically closer to the destination. While the frequency of updating the next hop differs from one application to another, a node can possibly have several next hop relaying nodes during the same data session. From the game theory perspective, a node might choose to play the same forwarding game with different nodes at different times. The hop-by-hop forwarding strategy simply follows two steps.

- Step 1: Choose or update the selection of next hop relay node.

- Step 2: If a node possesses the packet, play the two-player packet forwarding game for each of the data packet to be delivered.

The advantage of routing based forwarding over hop-by-hop forwarding is that the source nodes have some control on the players in the games. This might be important because the source node can specify which nodes it wants to include in the multi-player packet forwarding game. However, the extra overhead on route discovery and maintenance put routing based forwarding on a less favorable side compared with the lightweight hop-by-hop forwarding.

As indicated in Section 4.2, the difficult of the forwarding game lies in the incapability of identifying the state the opponent node is in, and it is also true for multi-hop packet forwarding games. However, since all nodes are selfish and only interested in maximizing their own payoffs, individual games can be devised so that cooperation strategy means optimal payoffs for all the nodes in the games. We simplify the multi-hop packet forwarding game by decomposing it to multiple two-player packet forwarding games between a node

and its next hop relay node. The following theorem shows how cooperation is enforced in

multi-hop packet forwarding.

Theorem 4.2. *Multi-hop packet forwarding strategies (defined above) lead to a Sequential Equilibrium for the multi-player packet forwarding game.*

Proof. First, we consider the hop-by-hop forwarding strategy. For each sender node j and its next hop relay node k, the game played between them can reach Sequential Equilibrium as suggested in Theorem 4.1. If node j changes its criteria in selecting the next hop, and choose another node, the new node pair will still play the two-player packet forwarding game and hence guarantees a Sequential Equilibrium, as long as δ is close to 1 and the system parameters are set accordingly. Further, when we consider any two consecutive hops, the games played at every hop generate independent equilibria of each other. Thus, when Sequential Equilibrium is achieved at every hop, the hop-by-hop forwarding strategy leads to Sequential Equilibrium for the whole multi-player packet forwarding game.

In the scenario of routing based forwarding strategy, when a route is selected, the players and games to be played at each hop are fixed. Since Sequential Equilibria are attainable at each hop, a route level Sequential Equilibrium on multi-player packet forwarding game is induced. In the case of route selection, if no payoff metrics are involved in the selection decision, reaching the equilibrium solely depends on the games played at each hop. However, if the route with maximum payoff is selected (e.g., VCG [3] and its variant protocols), the sender node has no incentive to switch to another route because any deviation will incur a lower payoff. In this case, the Sequential Equilibrium can be achieved on the route with maximized payoff.

Moreover, when we apply Theorem 4.1 to each of the hops of two-player forwarding game, consistency is maintained and hence the same for the multi-player packet forwarding game. Therefore, multi-hop packet forwarding strategies lead to a Sequential Equilibrium for the multi-player packet forwarding game. $\square$

Furthermore, the corollaries for Theorem 4.1 can be extended for multi-player packet

forwarding game. For example, if we assume a forwarding process of m hops with $p_e(m)$ as

the associated channel loss probabilities, the payoff boundaries for the forwarding with all

cooperative node are $[mP, \ mR - \Sigma_m \frac{p_e(m)}{1-p_e(m)}(T - R)]$, which is also strictly bounded by mR.

4.4   Summary

In this chapter, we investigate strategies that attain cooperation in wireless networks with heterogeneous noisy channel. We consider packet forwarding in unreliable channel as the core problem and abstract it into a game theoretic model. The heterogeneous and unreliable nature of the channel only allow the game to be played with imperfect private information. To solve the game, we propose a state machine based forwarding strategy which brings a Sequential Equilibrium to the game. We also show that through carefully designing the system parameters, the equilibrium points are attainable. To address the packet forwarding problem in a multi-hop wireless network, we model a multi-player packet forwarding game and extend our strategy to the multi-hop case, where Sequential Equilibrium can still be obtained.

CHAPTER 5
COEXISTENCE WITH MALICIOUS NODES

In Chapters 3 and 4, we focused on how to enforce the selfish nodes to cooperate. However, another type of misbehavior in wireless network exists, viz, malicious attacking. In the context of packet forwarding, attacking includes altering the contents of the packets, denial-of-service attacks, malicious packet dropping, and so on. Identification and isolation of malicious nodes in a distributed system is a challenging problem. This problem is even more aggravated in wireless networks because the unreliable channel makes the actions of the nodes hidden from each other. Therefore, a regular node in the network can only construct a belief about a malicious node through monitoring and observation. In this chapter, we use game theory to study the interactions between regular and malicious nodes in a wireless network. In Section 5.1, we model the malicious node detection process as a Bayesian game with imperfect information and show that a mixed strategy perfect Bayesian Nash Equilibrium (also a sequential equilibrium) is attainable. While the equilibrium in the detection game ensures the identification of the malicious nodes, we argue that it might not be profitable to isolate the malicious nodes upon detection. As a matter of fact, malicious nodes can co-exist with regular nodes as long as the destruction they bring is less than the contribution they make. To show how we can utilize the malicious nodes, a post-detection game between

the malicious and regular nodes is formalized in Section 5.2. Solution to this game shows the existence of a subgame perfect Nash Equilibrium and the conditions that achieve the equilibrium. Further, in Section 5.3, we show how a malicious node can construct a nested belief about the belief held by a regular node. By employing the nested belief system, a Markov Perfect Bayes-Nash Equilibrium is reached and the equilibrium postpones the detection of the malicious node.

5.1 Malicious Nodes Detection Game

We consider a wireless network consisting of *Regular* and *Malicious* nodes. By regular node we mean that a node that works towards the common goal of the network. Also, it is rational and its actions are governed by an underlying utility function. On the other hand, a malicious node aims to hamper, disturb, and even attack the network. Although the actions of a malicious node is also determined by certain utility functions, such functions are designed to bring damages to the network.

Despite the two types of nodes, the identity (type) of a malicious node is not directly revealed to others. Instead, the types can only be estimated or conjectured through observing actions. To identify the attacks and malicious nodes in the network, a regular node can monitor the actions of others. However, such monitoring is costly (e.g., consumes the receivers' own resource) and a node cannot afford to monitor all the time. Moreover, the observations might not be accurate because of the noise, e.g., wireless channel loss. Thus,

the regular nodes do not monitor the network all the time and during those times, attacks cannot be identified.

To simplify the analysis, our research focuses on the packet forwarding process. We assume that node i, or the sender node, has a packet to send to node j, or the receiver node. If the sender node is regular, it only takes the action "*Forward*". If the sender node is malicious, it can choose to "*Attack*" with a risk of being identified or "*Forward*" (not attack) to disguise. We further assume that time is divided into slots and nodes take their actions within each slot.

5.1.1 Detection Game Model

To abstract the interactions among the nodes, we consider a two-player non-zero sum game played by the sender node i and the receiver node j. The types of these nodes, θ_i and θ_j, are private information. Since the type of each player is hidden, and the observation is not accurate, it is a Bayesian game with imperfect information [38].

To model the process of detecting the malicious nodes in the network, we apply a special category of Bayesian game called the signaling game. A *signaling game* is played between a sender and a receiver. The sender has a certain type and a set $\mathcal{M}$ of available messages to be sent. Based on its knowledge on its own type, the sender chooses a message from $\mathcal{M}$ and sends it to the receiver. However, the receiver does not know the type of the sender and can only observe the message but not the type. Through observation, the receiver then takes an

action in response to the message it observed. In the malicious node detection game, the sender, node i can be either regular $\theta_i = 0$ or malicious $\theta_i = 1$. The receiver, node j is always a regular node, i.e., $\theta_j = 0$.

The action profiles a_i available to node i are based on its type. For $\theta_i = 0$, $a_i = \{Forward\}$. For $\theta_i = 1$, $a_i \in \{Attack, \ Forward\}$. The receiver node j has the option to monitor if node i is attacking or not, thus $a_j \in \{Monitor, \ Idle\}$.

To further construct the game, we define the following values. Let g_A be the payoff of a malicious node if it successfully attacks. The cost associated with such an attack is c_A. For the receiver node j, the cost of monitoring is c_M and 0 if it is idle. Hence, for the action profile $(a_i, \ a_j) = (Attack, \ Idle)$, the net utility for a successful attacking node i is $g_A - c_A$, the loss for node j is $-g_A$ due to the attack. Similarly, if the action profile is $(a_i, \ a_j) = (Attack, \ Monitor)$, the attacking malicious node i losses $g_A + c_A$, and the net gain for node j is $g_A - c_M$. However, if a malicious node chooses not to attack, the cost to forward a packet is c_F, which is the same cost to a regular sender node. Based on the types of node i and node j, the payoffs matrices are presented in Table 5.2. For quick reference, the notations used in this chapter are tabulated in Table 5.1.

In addition, in our model, we introduce p_e as the channel loss rate. The channel unreliability implies that monitoring can be accurate with probability $1 - p_e$. We also denote γ as the attack success rate for a malicious node.

Node i	(potential) malicious node, attacker
Node j	regular node, monitor
θ_i	type of node i, 1 for malicious, 0 for regular
$u_i,\ u_j$	payoff of node i or j in the stage game
g_A	gain of successfully attack for node i
c_A	cost of any attack for node i
c_F	cost of forward (not attack) for node i
c_M	cost of monitoring for node j
ϕ	the belief of node i being malicious in stage game
γ	attack success rate for node i
p_e	channel error rate
α	false alarm rate for node j
$a_i,\ a_j$	action profile for node i or j
$\hat{a}_i(t)$	node i's action observed by node j in stage t
o_i	node i's observation of its payoffs
$\mu_j(\theta_i)$	belief node j holds about node i's type in the dynamic game
$\mu_i(\mu_j(\theta_i))$	belief node i holds about node j's belief in the dynamic game (used to derive the MPBNE)
$\sigma_i,\ \sigma_j$	node i or j's strategy profile
$p,\ q$	random variable of probability node i attacks or node j monitors in the malicious node detection game
$p^*(t),\ q^*(t)$	random variable of probability node i attacks or node j monitors in the post-detection game
$\tilde{p},\ \tilde{q}$	random variable of probability node i attacks or node j monitors in the malicious node detection game with node i's nested belief model
$\mathcal{C}_i$	coexistence index
μ_j^*	node j's belief about node i's type when node i uses nested belief model
p_{j*i}	node j's belief about node i's attack probability when node i uses nested belief model
p_{M}	the value of node i's attack probability in MPBNE
p_{PBE}	the value of node i's attack probability in PBE
p_{SPNE}	the value of node i's attack probability in SPNE

Table 5.1: Notations used in malicious nodes coexistence analysis.

	Node j			
	Monitor		Idle	
Node i — Attack	$-g_A - c_A$	$g_A - c_M$	$g_A - c_A$	$-g_A$
Forward	$-c_F$	$-c_M$	$-c_F$	0

(a) $\theta_i = 1$, malicious sender

	Node j			
	Monitor		Idle	
Node i Forward	$-c_F$	$-c_M$	$-c_F$	0

(b) $\theta_i = 0$, regular sender

Table 5.2: Payoff matrix of two player malicious node detection game.

5.1.2   Equilibrium Analysis for the Stage Game

We begin our analysis on the malicious node detection game from the extensive form of the static Bayesian game as illustrated in Figure 5.1. We consider the type determination of node i when $\theta_i = 1$ happens with probability ϕ. To solve this game, we are interested in finding the possible *Bayesian Nash Equilibrium* (BNE). In a static Bayesian game, the BNE is the Nash Equilibrium given the beliefs of both nodes. In our case, node i knows for sure that for node j, $\theta_j = 0$, however, node j's belief about node i is that $\theta_i = 1$ with probability ϕ.

First, let us consider pure strategies only. Based on θ_i, the pure strategies available for node i are $\sigma_i = \{(Attack \; if \; \theta_i = 1, Forward \; if \; \theta_i = 0), \; Forward \; \forall \; \theta_i\}$. For node j, the strategy set is $\sigma_j = \{Monitor, \; Idle\}$. To find the BNE, we let σ_i and σ_j play with each other

72
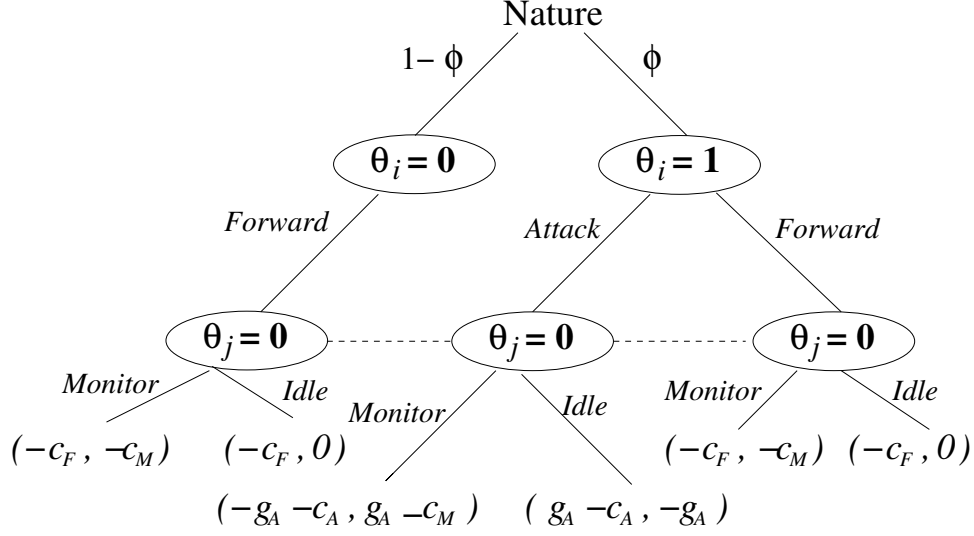
Figure 5.1: Stage malicious node detection game tree.

and derive the conditions under which neither node can increase its utility by unilaterally

changing its strategy.

Lemma 5.1. *In the malicious node detection game, there is a malice belief threshold ϕ_0, such that no pure strategy BNE exists if $\phi > \phi_0$.*

Proof. We start by eliminating a trivial pure strategy pair ($Forward \ \forall \ \theta_i \ Monitor$). From Table 5.25.2(a), we know that for both nodes, they can improve their payoffs by deviating from the strategy pair. We further analyze the following two cases.

Case 1: $\sigma_i = (Attack \ if \ \theta_i = 1, Forward \ if \ \theta_i = 0)$. For node j, if $\sigma_j = Monitor$, the expected payoff is

$$u_j(Monitor) \ = \ \phi(1-p_e)(g_A - c_M) - \phi p_e[\gamma(g_A + c_M) + (1-\gamma)c_M] - (1-\phi)c_M \quad (5.1)$$

where each term represents monitoring the attack successfully, failing to monitor the attack, and node i is regular respectively. If $\sigma_j = Idle$, the expected payoff is

$$u_j(Idle) = -\phi\gamma g_A \quad (5.2)$$

If (5.2)>(5.1), the dominant strategy for node j is *Idle*. Correspondingly, for node i, the best response would be ($Attack \ if \ \theta_i = 1, Forward \ if \ \theta_i = 0$). Thus ($\sigma_i, \ \sigma_j$) = {($Attack \ if \ \theta_i = 1, Forward \ if \ \theta_i = 0$), $Idle$} is a BNE under the condition that $\phi < \frac{c_M}{(1-p_e)(1+\gamma)g_A}$. If (5.2)<(5.1), or $\phi > \frac{c_M}{(1-p_e)(1+\gamma)g_A}$, the dominant strategy for node j is *Monitor*, however, the best response to *Monitor* for node i is $Forward \ \forall \ \theta_i$. Hence ($\sigma_i, \ \sigma_j$) = {($Attack \ if \ \theta_i = 1, Forward \ if \ \theta_i = 0$), $Monitor$} is not a BNE under the condition that $\phi > \frac{c_M}{(1-p_e)(1+\gamma)g_A}$.

Case 2: $(\sigma_i, \sigma_j) = \{(Forward \ \forall \ \theta_i, \ Idle\}.$ If node j chooses not to monitor, the best response for node i is to *Attack* if $\theta_i = 1$. This will lead to the previous case when $\phi < \frac{c_M}{(1-p_e)(1+\gamma)g_A}$. Therefore, there is no BNE if $(\sigma_i, \sigma_j) = \{(Forward \ \forall \ \theta_i, \ Idle\}.$

To sum up, the pure strategy BNE exists if and only if $\phi < \frac{c_M}{(1-p_e)(1+\gamma)g_A}$. The equilibrium strategy profile is $(\sigma_i, \sigma_j) = \{(Attack \ if \ \theta_i = 1, Forward \ if \ \theta_i = 0), \ Idle\}.$ In other words, we can find $\phi_0 = \frac{c_M}{(1-p_e)(1+\gamma)g_A}$, such that no pure strategy BNE exists if $\phi > \phi_0$. □

Although pure strategy BNE exists, it is not practical because the equilibrium requires node j to be *Idle* at all times, and hence the malicious nodes cannot be detected. It is also called Pooling Equilibrium [38] in which the receiver has no clue about sender's type. Therefore, it is desirable to seek a mixed-strategy BNE, and obviously, such BNE exists when $\phi > \phi_0$.

Let us denote p as the probability with which node i of type $\theta_i = 1$ plays *Attack* and q as the probability with which node j plays *Monitor*. To find the mixed strategy BNE of this game, we need to find the values of p and q such that neither node i nor j can increase payoff by altering the actions. For the mixed strategy played by node i, the payoff of node j playing *Monitor* is

$$
\begin{aligned}
u_j(Monitor) &= \phi p[(1-p_e)\gamma(g_A - c_M) + (1-p_e)(1-\gamma)(g_A - c_M) \\
&\quad - p_e(1-\gamma)c_M - p_e\gamma(g_A + c_M)] - \phi(1-p)c_M - (1-\phi)c_M \\
&= \phi[1 - p_e(1+\gamma)]pg_A - c_M.
\end{aligned}
\tag{5.3}
$$

If node j plays *Idle*,

$$
u_j(Idle) = -\phi\gamma pg_A.
\tag{5.4}
$$

Thus, in the mixed BNE strategy, $u_j(Monitor) = u_j(Idle)$. Thus $p = \frac{c_M}{\phi(1-p_e)(1+\gamma)g_A}$.

Similarly, when node j plays the mixed strategy, the payoff of node i playing *Attack* is

$$
\begin{aligned}
u_i(Attack) &= -(1-p_e)q(g_A + c_A) + \gamma(1-q)(g_A - c_A) \\
&\quad + p_e\gamma q(g_A - c_A) - p_e(1-\gamma)qc_A - (1-\gamma)(1-q)c_A \\
&= (p_e - 1)(1+\gamma)qg_A + \gamma g_A - c_A.
\end{aligned}
\tag{5.5}
$$

When node i plays *Forward*,

$$
u_i(Forward) = -c_F.
\tag{5.6}
$$

Hence, to obtain q, $u_i(Attack) = u_i(Forward)$, and $q = \frac{\gamma g_A - c_A + c_F}{(1-p_e)(1+\gamma)g_A}$.

To sum up the analysis, we state the following lemma.

Lemma 5.2. *The malicious node detection game has a mixed strategy BNE when σ_i, $\sigma_j = \{(Attack\ with\ \frac{c_M}{\phi(1+\gamma)(1-p_e)g_A}\ if\ \theta_i = 1,\ Forward\ if\ \theta_i = 0),\ Monitor\ with\ \frac{\gamma g_A - c_A + c_F}{(1-p_e)(1+\gamma)g_A}\},$ given $\phi > \phi_0$.*

Lemmas 5.1 and 5.2 provide us with the conditions under which BNE can be attained. One of the conditions is the belief of malice threshold ϕ_0. As suggested in Lemma 5.1, this threshold is related to the channel reliability $(1 - p_e)$, attack success rate (γ) and detection gain (g_A/c_M). In the pure strategy BNE, node i always attacks and the belief of node j on node i's malice is very low since the detection gain is usually very large as $p_e, \gamma \in [0, 1]$. However, when the belief grows and eventually exceeds the threshold, the mixed strategy BNE requires node i to be less aggressive in attacking. In other words, the equilibrium implies node i should know about node j's belief when making the decision. When node j

is absolutely sure about node i's type, node i's equilibrium attack probability drops to the value of the belief threshold.

5.1.3 Belief Update and Dynamic Bayesian Games

So far, the analysis on the malicious node detection stage game has shown that the equilibrium is associated with node j's belief on node i's type. However, the difficulty lies in the assignment of the belief as a priori information available to node j. Thus, it is desirable that this belief can be accurately presented and dynamically updated. We apply dynamic Bayesian game theory to discuss how the belief is updated.

We assume that the static malicious node detection game is repeatedly played at every time slot, and we consider the infinite repeated game without discounting (i.e., payoffs in every stage/slot have equal weight). In addition to the notation defined in the stage game, we introduce $\mu_j^{(t)}(\theta_i = \bar{\theta}_i)$ as the belief node j holds about $\theta_i = \bar{\theta}_i$ at the tth stage of the subgame. Since node j is always a regular node, $\mu_i^{(t)}(\theta_j = 0)$ for all $t > 0$. We further define $a_i(t)$ as the action node i plays at t^{th} stage. Node j may monitor node i's actions through the observed signal $\hat{a}_i(t)$. The reasons for the discrepancy between $a_i(t)$ and $\hat{a}_i(t)$ are the observation error caused by the channel unreliability and the false alarm rate (α) caused by the inaccuracy and limitation in the detection of node j.

Based on Bayes' theorem, we construct our belief update rule. If node j is continuously monitoring, its belief on θ_i can be calculated with the belief it holds at the immediate previous

stage and the actions it observed. We write the belief at the $(t+1)^{\text{th}}$ stage as:

$$\mu_j^{(t+1)}(\theta_i) = \frac{\mu_j^{(t)}(\theta_i)P(\hat{a}_i(t)|\theta_i)}{\sum_{\tilde{\theta}_i \in \Theta} \mu_j^{(t)}(\tilde{\theta}_i)P(\hat{a}_i(t)|\tilde{\theta}_i)}, \tag{5.7}$$

where Θ is the space of all possible values θ_i can take; in our case $\Theta = \{0, 1\}$.

For each of the terms in equation (5.7), we have the following equations.

$$P(\hat{a}_i(t) = Attack|\theta_i = 1) = (1 - p_e)p + \alpha(1 - p) \tag{5.8}$$

$$P(\hat{a}_i(t) = Attack|\theta_i = 0) = \alpha \tag{5.9}$$

$$P(\hat{a}_i(t) = Forward|\theta_i = 1) = p_e p + (1 - \alpha)(1 - p) \tag{5.10}$$

$$P(\hat{a}_i(t) = Forward|\theta_i = 0) = 1 - \alpha. \tag{5.11}$$

Since node j does not monitor node i's actions at every stage, but rather with probability q. When node j is not monitoring, its belief remains the same at the next stage. Thus, Equation (5.7) is revised as:

$$\mu_j^{(t+1)}(\theta_i) = q\frac{\mu_j^{(t)}(\theta_i)P(\hat{a}_i(t)|\theta_i)}{\sum_{\tilde{\theta}_i \in \Theta} \mu_j^{(t)}(\tilde{\theta}_i)P(\hat{a}_i(t)|\tilde{\theta}_i)} + (1 - q)\mu_k^{(t)}(\theta_i). \tag{5.12}$$

The concept of *belief system* is hence introduced to describe the aforementioned belief building and updating process. A belief system is a function that assigns each information set[1] a probability distribution over the histories (i.e., past moves and states) in that information set [38]. Although in our discussions above, we did not explicitly state how history is

---

[1] An information set is a set of all the possible moves that could have taken place in the game so far, for a particular player, given what that player has observed. In an imperfect information game, an information set contains all possible states in the history, e.g., in Figure 5.1, the dotted lines show the information set available to node j.

accounted for in equations (5.7) and (5.12), it is easy to observe that every updated belief is determined by the actions node j observes in the current stage and the belief it holds. The beliefs are further determined by the actions in the previous stages and it can be backtracked to the initial belief and the subsequent actions. Thus, the current belief and observed action can fully represent the histories in the information sets, and those information sets can be reached with positive probabilities if the strategies are carefully designed.

With the belief system, the games are played in a sequential manner. As the game evolves, neither nodes can stick to the very same strategy at every stage to yield the most payoffs. Thus, the best response strategies are dependent on the current beliefs held by the nodes. Perfect Bayesian Equilibrium (PBE) can be applied to characterize the aforementioned dependency. In PBE, the belief system is updated by Bayes' rule. PBE also demands the optimality of subsequent play given the belief. Next, we show how to construct a PBE in the dynamic malicious node detection game.

We first show the existence of a mixed strategy equilibrium and then argue the infeasibility of the pure strategy equilibrium. Consider an arbitrary stage k of the game; we denote $p^{(k)}$ as the probability node i of type $\theta_i = 1$ plays *Attack*, $q^{(k)}$ as the probability node j plays *Monitor*. In the equilibrium, $u_i^{(k)}(Attack) = u_i^{(k)}(Forward)$ and $u_j^{(k)}(Monitor) = u_j^{(k)}(Idle)$.

In particular,

$$u_i^{(k)}(a_i^{(k)} = Attack | a_j^{(k)} = Monitor) = -(1 - p_e)q^{(k)}(g_A + c_A) + \gamma(1 - q^{(k)})(g_A - c_A)$$

$$+\gamma q^{(k)} p_e(g_A - c_A) - p_e(1 - \gamma)q^{(k)} c_A - (1 - \gamma)(1 - q^{(k)})c_A \tag{5.13}$$

$$u_i^{(k)}(a_i^{(k)} = Forward | a_j^{(k)} = Monitor) = -c_F. \tag{5.14}$$

$$u_j^{(k)}(a_j^{(k)} = Monitor | a_i^{(k)} = Attack) = \mu_j^{(k)}(\theta_i = 1)p^{(k)}[(1 - p_e)\gamma(g_A - c_M)$$

$$+(1 - p_e)(1 - \gamma)(g_A - c_M) - p_e(1 - \gamma)c_M - p_e\gamma(g_A + c_M)] - \mu_j^{(k)}(\theta_i = 1)(1 - p^{(k)})c_M$$

$$-\mu_j^{(k)}(\theta_i = 0)c_M \tag{5.15}$$

$$u_j^{(k)}(a_j^{(k)} = Idle | a_i^{(k)} = Attack) = -\mu_j^{(k)}(\theta_i = 1)\gamma p^{(k)} g_A. \tag{5.16}$$

The solutions to the above equations are

$$p^{(k)} = \frac{c_M}{\mu_j^{(k)}(\theta_i = 1)(1 - p_e)(1 + \gamma)g_A} \tag{5.17}$$

$$q^{(k)} = \frac{\gamma g_A - c_A + c_F}{(1 - p_e)(1 + \gamma)g_A}. \tag{5.18}$$

What $p^{(k)}$ and $q^{(k)}$ suggest is an equilibrium profile $(\sigma_i^{(k)}, \sigma_j^{(k)})$. This profile shows the sequential rationality [16, 38], that is, each node's strategy is optimal whenever it has to move, given its belief and the other node's strategy. In other words, for any alternative strategies $\sigma_i'^{(k)}$ and $\sigma_j'^{(k)}$,

$$u_i^{(k)}((\sigma_i^{(k)}, \sigma_j^{(k)}) | \theta_i, a_i(t), \mu_j^{(k)}(\theta_i)) \geq u_i^{(k)}((\sigma_i'^{(k)}, \sigma_j^{(k)}) | \theta_i, a_i(t), \mu_j^{(k)}(\theta_i)) \tag{5.19}$$

$$u_j^{(k)}((\sigma_i^{(k)}, \sigma_j^{(k)}) | \theta_i, \hat{a}_i(t), \mu_j^{(k)}(\theta_i)) \geq u_j^{(k)}((\sigma_i^{(k)}, \sigma_j'^{(k)}) | \theta_i, \hat{a}_i(t), \mu_j^{(k)}(\theta_i)) \tag{5.20}$$

Besides sequential rationality, a PBE also demands that the belief system satisfies the Bayesian conditions [16].

Definition 5.1. *([16], pp. 331-332) The Bayesian conditions defined for PBE are*

B(i): Posterior beliefs are independent. For history $h^{(k)}$, $\mu_i(\theta_{-i}|\theta_i, h^{(k)}) = \prod_{j \neq i} \mu_i(\theta_j|h^{(k)})$.

B(ii): Bayes' rule is used to update beliefs whenever possible.

B(iii): Nodes do not signal what they do not know.

B(iv): Posterior beliefs are consistent for all nodes with a common joint distribution on θ given $h^{(k)}$.

Our proposed belief system satisfies the Bayesian conditions. B(i) is satisfied because $\theta_j = 0$ all the time. Equation (5.7) is derived from Bayes' rule, and hence B(ii) is also satisfied. B(iii) is fulfilled because node i's signal is determined by its action and if $a_i(k) = \hat{a}_i(k)$, $\mu_j(\theta_i|a_i(k), h_j^{(k)}) = \mu_j(\theta_i|\hat{a}_i(k), h_j^{(k)})$. B(iv) is trivial in our game because no third player exists.

The analysis on Bayesian conditions and sequential rationality serves as the proof of the following theorem.

Theorem 5.1. *The dynamic malicious node detection game has a perfect Bayesian equilibrium that can be attained with strategy profile $(\sigma_i^{(k)},\ \sigma_j^{(k)}) = (p^{(k)}, q^{(k)})$.*

Remark 1: The infeasibility of pure strategy PBE is proved as follows: If node i attacks, the best response for node j is *Monitor*, which makes node i non-profitable to play *Attack*. If node i plays *Forward*, $p^{(k)} = 0$, the best response for node j is *Idle* (i.e., $q^{(k)} = 0$). However, the sequential rationality requires $q^{(k)} \geq \frac{g_A \gamma - c_A + c_F}{g_A(1 - p_e)(1 + \gamma)}$, which leads to a contradiction. Therefore, no pure strategy PBE exists in the dynamic malicious node detection game. It is noted that the infeasibility of the pure strategy PBE in the dynamic settings should not be confused with the existence of a pure strategy BNE in a static game because the pure strategy BNE in a static game is always an artifact.

Remark 2: The proved PBE can be further refined to *Sequential Equilibrium* [24]. In the sequential equilibrium, the Bayesian conditions are extended as *belief sensibility* and *consistency*. The belief sensibility requires the information sets can be reached with positive probabilities (μ) given the strategy profile σ. The consistency demands an assessment (σ, μ) should be a limit point of a sequence of the mixed strategies and associated sensible beliefs, i.e., $(\sigma, \mu) = \lim_{n \to \infty}(\sigma^n, \mu^n)$. In our game, belief sensibility is satisfied because our proposed belief system updates the beliefs according to Bayes' rule and it assigns a positive probability to each of the information set. Theorem 8.2 in [16] states that in incomplete information multi-stage games, if neither player has more than 2 types, Bayesian condition is equivalent to belief consistency requirement. In our game, $\theta_i = 0, 1$, $\theta_j = 0$, and hence consistency is fulfilled. Together with the sequential rationality, the PBE in our game is also a sequential equilibrium. Since every finite extensive-form game has at least one sequential equilibrium, which is a refinement to PBE, it also implies the existence of PBE in our game.

5.2   Post-detection Game and Coexistence

In the previous section, we have discussed how to update node j's belief system based on Bayes' rule. It is natural that through observation, although imperfect at every stage game, node j can accumulate a better estimation about θ_i. Eventually, after repeated monitoring, there will be a stage at which node j can predict with confidence whether node i is regular or malicious.

5.2.1　Post-detection Game Model

Traditionally speaking, after node j has identified node i as a malicious node, it will try to report and isolate node i immediately to prevent future attacks. However, there are also situations where "isolation" may not be a good choice. Let us consider a wireless network which operates on a limited resource budget. In order to prolong the lifetime of the network, every regular node has to be economical towards packet forwarding. Hence, if a malicious node can be used to handle some of the traffic, it is beneficial not to isolate it.

However, there is a trade-off between how much benefit a malicious node can bring and what damage it can do. We denote n_F and n_A as the number of successful forwarding actions and number of attacks taken by a malicious node. Recall the cost of forwarding is c_F and the loss due to an attack to the network is g_A. Thus, for a regular node, if it observes that the total saving due to forwarding $(n_F c_F)$ a malicious node contributes is greater than the total cost due to its attack $(n_A g_A)$, then keeping that node in the network is profitable. It is also worthwhile to mention that although the values of c_F and g_A vary from one application to another, for a given application, the values are constant and measurable.

To further analyze the conditions under which a malicious node can be kept and coexist with the regular ones, we formally define the post detection game. The game has two players: node i and node j, both nodes know the types of their opponent, i.e., node j knows that node i is malicious but has not taken any action to isolate it. Thus, $\theta_i = 1$, $\theta_j = 0$. The actions available for node i is $a_i \in \{Attack,\ Forward\}$, while the actions for node j is

$a_j \in \{Monitor, \ Idle\}$. When node j monitors, it keeps a record of what node i has done since the beginning of the game. It also calculates a coexistence index $\mathcal{C}_i = \hat{n}_F c_F - \hat{n}_A g_A$ for node i, where $\hat{n}_F$ is the observed number of forwarding actions and $\hat{n}_A$ is the observed number of attacks. If $\mathcal{C}_i$ falls under a certain threshold τ, node j will isolate node i and terminate the post-detection game because keeping node i is no longer beneficial. If $\mathcal{C}_i \geq \tau$, the game will be played in a repeated manner. The payoff matrix for the post-detection game is the same as the detection game for $\theta_i = 1$ as was shown in Table 5.25.2(a).

5.2.2   Searching for a Coexistence Equilibrium

Let us explore the strategies that both nodes can take to reach the equilibrium of coexistence. To avoid confusion, we denote $p^*(t)$ and $q^*(t)$ as the probability node i plays *Attack* and node j plays *Monitor* respectively with time. It is noted that these probabilities are different from the ones we obtained in Chapter 5.1.3. Also, since this game is no longer Bayesian, we are more interested in obtaining a subgame perfect Nash Equilibrium.

We first derive the Nash Equilibrium using indifference conditions. Suppose the post-detection game is played at t^{th} repetition, i.e., subgame t. The expected payoff for player j

playing *Monitor* is

$$
u_j^{(k)}(Monitor) = \{p^*(k)[(1 - p_e)\gamma(g_A - c_M) + (1 - p_e)(1 - \gamma)(g_A - c_M) - p_e(1 - \gamma)c_M
$$

$$
- \quad p_e\gamma(g_A + c_M)]\} \Pr(\mathcal{C}_i \geq \tau) + (1 - p_e)p^*(k)(g_A - c_M) \Pr(\mathcal{C}_i < \tau) - (1 - p^*(k))c_M
$$

$$
= \quad [(1 - p_e + \gamma p_e)g_A - c_M]p^*(k) \Pr(\mathcal{C}_i \geq \tau) + (1 - p_e)p^*(k)(g_A - c_M) \Pr(\mathcal{E}_i < \tau)
$$

$$
- \quad (1 - p^*(k))c_M.
$$

$$
(5.21)
$$

If node j plays *Idle*, the expected payoff is always

$$
u_j^{(k)}(Idle) = -\gamma p^*(k)g_A. \tag{5.22}
$$

Thus, the indifference condition require $u_j^{(k)}(Monitor) = u_j^{(k)}(Idle)$, and hence p^* is

obtained as:

$$
p^*(k) \frac{c_M}{[(1 - p_e + \gamma p_e)g_A - c_M] \Pr(\mathcal{C}_i \geq \tau) + (1 - p_e)(g_A - c_M) \Pr(\mathcal{C}_i < \tau) + c_M + \gamma g_A}.
$$

$$
(5.23)
$$

Similarly, we can apply the indifference condition to node i as:

$$
u_i^{(k)}(Attack) = q^*(k)\{-(1 - p_e)(g_A + c_A) \Pr(\mathcal{C}_i < \tau)
$$

$$
+ \quad (1 - p_e)[\gamma(g_A - c_A) - (1 - \gamma)c_A] \Pr(\mathcal{C}_i \geq \tau) + p_e\gamma(g_A - c_A) - p_e(1 - \gamma)c_A\}
$$

$$
- \quad (1 - q^*(k))[(1 - \gamma)c_A - \gamma(g_A - c_A)]
$$

$$
= \quad q^*(k)\{-(1 - p_e)(g_A + c_A) \Pr(\mathcal{C}_i < \tau) + (\gamma g_A - c_A)[(1 - p_e) \Pr(\mathcal{C}_i \geq \tau) + p_e]\}
$$

$$
+ \quad (1 - q^*(k))(\gamma g_A - c_A). \tag{5.24}
$$

$$
u_i^{(k)}(Forward) = -c_F. \tag{5.25}
$$

Therefore, q^* can be expressed as:

$$q^*(k) = \frac{c_A - \gamma g_A - c_F}{-(1 - p_e)(g_A + c_A)\Pr(\mathcal{C}_i < \tau) + (1 - p_e)(\gamma g_A - c_A)(\Pr(\mathcal{C}_i \geq \tau) - 1)} \quad (5.26)$$

The problem is then reduced to obtaining the probability distribution of $\mathcal{C}_i$. Let us assume at the beginning of the post-detection game $\mathcal{C}_i = c_0 \geq \tau$. For the sake of discussion, we also assume that node j is constantly monitoring. Hence, if we consider l subgames, in each of the subgame, $\mathcal{C}_i$ is updated.

We denote a random variable $y = \mathcal{C}_i = c_0 + \hat{n}_F c_F - \hat{n}_A g_A$. Since the mixed strategy profile requires node i to choose *Attack* with probability $p*$, $\hat{n}_F$ and $\hat{n}_A$ are binomially distributed as:

$$\Pr(\hat{n}_F = \hat{N}_F) = C_l^{\hat{N}_F}[(1 - p^*(t))(1 - p_e)]^{\hat{N}_F}[1 - (1 - p^*(t))(1 - p_e)]^{l - \hat{N}_F} \quad (5.27)$$

$$\Pr(\hat{n}_A = \hat{N}_A) = C_l^{\hat{N}_A}[p^*(t)(1 - p_e)]^{\hat{N}_F}[1 - p^*(t)(1 - p_e)]^{l - \hat{N}_F} \quad (5.28)$$

Since $y = c_0 + \hat{n}_F c_F - \hat{n}_A g_A = c_0 + \hat{n}_F c_F - (l - \hat{n}_F)g_A = (c_F + g_A)\hat{n}_F - l g_A + c_0$ and l, c_F, g_A, c_0 are constants, to get the distribution of y, we first get the distribution of $w = y + l g_A - c_0$.

We use the probability generation function (pgf). For discrete random variable x, its pgf is defined as

$$G_X(z) = E[z^X] = \sum_{x=0}^{\infty} z^x \Pr(X = x) \quad (5.29)$$

The pgf for w is

$$
\begin{aligned}
G_W(z) &= E[z^W] = E[z^{\hat{N}_F(c_F+g_A)}] \\
&= \{\sum_{\hat{n}_f=0}^{l} z^n C_l^{\hat{n}_f}[(1-p^*(t))(1-p_e)]^{\hat{n}_f}[1-(1-p^*)(1-p_e)]^{l-\hat{n}_f}\}^{(c_F+g_A)} \\
&= \{(1-p^*(t))(1-p_e)+[1-(1-p^*(t))(1-p_e)]z\}^{(c_F+g_A)l}
\end{aligned}
$$

(5.30)

Let $f^{(n)}(x) = \frac{\partial^n f(x)}{\partial x^n}$,

$$
\mathbf{P}(w=\omega) = \frac{G_W^{(\omega)}(0)}{\omega!}
$$

(5.31)

The probability terms in (5.23) and (5.26) are given by,

$$
\Pr(\mathcal{C}_i \geq \tau) = \Pr(w \geq lg_A + \tau - c_0) = \sum_{n \geq lg_A + \tau} \frac{G_W^{(n)}(0)}{n!}
$$

(5.32)

$$
\Pr(\mathcal{C}_i < \tau) = 1 - \sum_{n \geq lg_A + \tau - c_0} \frac{G_W^{(n)}(0)}{n!}
$$

(5.33)

To relax the assumption of node j's constant monitoring, the current stage t for the analysis is $\lceil t = l/q^*(t) \rceil$. Therefore, we have obtained the equilibrium strategy parameter $p^*(t)$ and $q^*(t)$ for every subgame.

So far, we have shown that for the mixed strategy profile, attaining a Nash Equilibrium is feasible. As a matter of fact, every game has a mixed strategy Nash Equilibrium. To further refine the equilibrium, we apply the One-Shot Deviation Property to derive the condition for subgame perfect Nash Equilibrium.

We take node j as an example and assume the repeated game has no discount. In our previous equilibrium analysis using the indifference condition, we have proved that deviation

from $p^*(t)$ or $q^*(t)$ will not increase the payoffs. Hence, in the following derivation, we show the deviation strategy is related to $\mathcal{C}_i$.

From (5.21) and (5.22), we can express the expected payoff for node j as:

$$
\begin{aligned}
U_j &= \sum_{t=0}^{T} q^*(t)\{[g_A(1 - p_e + \gamma p_e) - c_M]p^*(t)\Pr(\mathcal{C}_i \geq \tau) \\
&+ (g_A - c_M)p^*(t)(1 - p_e)\Pr(\mathcal{C}_i < \tau) - (1 - p^*(t))c_M\} - (1 - q^*(t))p^*(t)\gamma g_A (5.34)
\end{aligned}
$$

Suppose node j deviates at rth stage and $r \leq T$. The deviation can be either of the following two cases.

Case 1: Isolate node i while $\mathcal{C}_i \geq \tau$. In this case, if node j attacks and is successfully observed, it will be isolated. The expected payoff at this stage for node j is

$$
\begin{aligned}
U_{j,dev,1}^{(r)} &= \{q^*(t)\{p^*(t)(1 - p_e)(g_A - c_M) - p^*(t)\gamma p_e(g_A + c_M) \\
&- [p^*(t)(1 - \gamma)p_e + (1 - p^*(t))]c_M\} - (1 - q^*(t))p^*(t)\gamma g_A\}\Pr(\mathcal{C}_i \geq \tau) \ (5.35)
\end{aligned}
$$

Case 2: Keep node i while $\mathcal{C}_i < \tau$. Since node j only deviates one stage, node i will be isolated in the next stage. The expected payoff for node j at this stage is the same as above expect for the last probability term.

$$
\begin{aligned}
U_{j,dev,2}^{(r)} &= \{q^*(t)\{p^*(t)(1 - p_e)(g_A - c_M) - p^*(t)\gamma p_e(g_A + c_M) \\
&- [p^*(t)(1 - \gamma)p_e + (1 - p^*(t))]c_M\} - (1 - q^*(t))p^*(t)\gamma g_A\}\Pr(\mathcal{C}_i < \tau) \ (5.36)
\end{aligned}
$$

In this way, the total expected payoff for node j under deviation is

$$
U_{j,dev} = \sum_{t=0}^{r-1} U_j^{(t)} + U_{j,dev,1}^{(r)} + U_{j,dev,2}^{(r)} + \sum_{t=r+1}^{T} U_j^{(t)} \tag{5.37}
$$

87

OSDP require $U_{j,dev} \leq U_j$. After algebraic manipulation, we have

$$g_A\gamma(q^*(t)p_e + 1) + q^*(t)p_e(\gamma c_M + 1 - \gamma)$$

$$\geq (1 - q^*(t))\gamma g_A + q^*(t)[\gamma g_A \Pr(\mathcal{C}_i < \tau) + p_e c_M \Pr(\mathcal{C}_i \geq \tau)] \tag{5.38}$$

or

$$g_A\gamma[p_e + 1 - \Pr(\mathcal{C}_i < \tau)] \geq p_e[c_M \Pr(\mathcal{C}_i \geq \tau) + \gamma - 1 - \gamma c_M]. \tag{5.39}$$

To sum up, for the equilibrium on the post-detection game, we state the following theorem.

Theorem 5.2. *The post-detection game has a mixed strategy Nash Equilibrium when node i attacks with $p^*(t)$ and node j monitors with $q^*(t)$. This strategy is also subgame perfect if $g_A\gamma[p_e + 1 - \Pr(\mathcal{C}_i < \tau)] \geq p_e[c_M \Pr(\mathcal{C}_i \geq \tau) + \gamma - 1 - \gamma c_M].*

5.2.3   Convergence of the Coexistence Equilibrium

The post-detection game described above ends when $\mathcal{C}_i < \tau$. Since $\Pr(\mathcal{C}_i < \tau) > 0$, the game is of finite stages. In this subsection, we try to derive the expected length (number of stages) of the game.

We focus on the random variable $\mathcal{C}_i$. As we mentioned earlier, $C_i = c_0 + \hat{n}_F c_F - \hat{n}_A g_A$. Again, we assume node j is constantly monitoring. After one stage game, the probability of $\hat{n}_F = \hat{n}_F + 1$ is $(1 - p^*(t))(1 - p_e)$, and the probability of $\hat{n}_A = \hat{n}_A + 1$ is $p^*(t)(1 - p_e)$. Thus, we model the evolution of $\mathcal{C}_i$ as a random process similar to a 1-dimensional random walk, where the value of $\mathcal{C}_i$ increases by c_F with probability $(1 - p^*(t))(1 - p_e)$, and decreases by g_A with probability $p^*(t)(1 - p_e)$. The $1 - p_e$ term comes from the unreliability of the channel.

To obtain the expected length of the post-detection game, it is equivalent to calculating the expected first hitting time of the random process with the absorbing boundary $\mathcal{C}_i = \tau$.

Theorem 5.3. *The expect length of the post-detection game is*

$$
\sum_{\eta > 0} \eta \frac{\binom{\eta}{\hat{n}_F} - \sum_{d}^{\hat{n}_F - 1} \binom{\frac{(c_0 - \tau)/c_F + d}{g_A/c_F} + d}{d} \binom{\eta - \frac{(c_0 - \tau)/c_F + d}{g_A/c_F} - d}{\hat{n}_F - d}}{2^\eta}
$$

.

Proof. Let η be a random variable representing the first hitting time. We assume that time is divided into slots and each slot represent a stage game. It is easy to see that $\eta = \hat{n}_F + \hat{n}_A$. At every slot, the random process has 2 possible evolution directions, i.e., $\hat{n}_F + 1$ or $\hat{n}_A + 1$. Therefore, for η slots, there are 2^η possible realizations.

We try to calculate how many paths hit the boundary exactly on the ηth slot. The following notations are made. Let $m = \frac{g_A}{c_F}$, $s = (c_0 - \tau)/c_F$ and m, s are integers. In Figure 5.2, we interpret how to move on a grid according to a random process. Consider a random walk from the left bottom point. If $\hat{n}_F$ increases, move one block right. If $\hat{n}_A$ increases, move m blocks up. While each block is a squarelet with the length c_F, the width of the grid is $\hat{n}_F c_F$, the height is $g_A \hat{n}_A$, and diagonal line represents $\mathcal{C}_i = \tau$. Each walk consists of η moves and must end on or beyond the upper rightmost corner. What we are interested in is the number of monotonic paths that wholly falls under the diagonal line, because each of those paths is a realization of the random process which hits the boundary for the first time at the ηth slot.

While counting the number of realizations under the diagonal line might be difficult, we calculate the realizations that do cross the line. Let the number of realizations crossing the line be M, the number of realizations under the line is then $C_n^{\hat{n}_F} - M$, where $C_n^{\hat{n}_F}$ is the total number of possible realizations on the grid. Consider a sample realization crossing the line as shown in Figure 5.2. Let d be the number of horizontal steps taken in the path before hitting the diagonal line. To hit the line, at least $\frac{s+d}{m}$ vertical steps should be taken, covering a total height of $(d + s)c_F$. The total number of such paths is $\sum_d C_{\frac{s+d}{m} + d}^d$. After hitting the line, the rest of the path should consist of $\hat{n}_F - d$ vertical steps and the total number of moves left is $\eta - \frac{s+d}{m} - d$. So, the total number of paths that cross the diagonal line is $M = \sum_d^{\hat{n}_F - 1} C_{\frac{s+d}{m} + d}^d C_{\eta - \frac{s+d}{m} - d}^{\hat{n}_F - d}$.

To sum up, out of 2^η realizations, $C_n^{\hat{n}_F} - \sum_d^{\hat{n}_F - 1} C_{\frac{s+d}{m} + d}^d C_{\eta - \frac{s+d}{m} - d}^{\hat{n}_F - d}$ realizations hit the diagonal line for the first time at the ηth move. The probability of game length being η is then $\frac{C_\eta^{\hat{n}_F} - \sum_d^{\hat{n}_F - 1} C_{\frac{s+d}{m} + d}^d C_{\eta - \frac{s+d}{m} - d}^{\hat{n}_F - d}}{2^\eta}$. Finally, we can express the expected length of the post detection game as

89
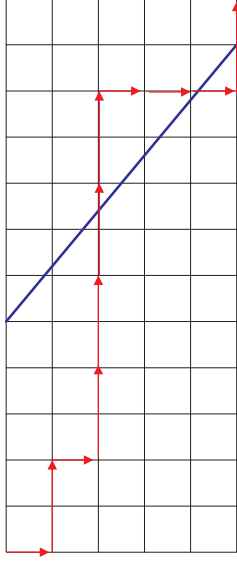
Figure 5.2: Realizations of the random walk.

$$E[length] = \sum_{\eta > 0} \eta \frac{C_\eta^{\hat{n}_F} - \sum_d^{\hat{n}_F - 1} \binom{\frac{s+d}{m}+d}{d}\binom{\eta - \frac{s+d}{m} - d}{\hat{n}_F - d}}{2^\eta}. \tag{5.40}$$

$\square$

5.3   Countermeasures for the Malicious Node

In our discussions so far, we haven shown that it is feasible to design strategies in order to achieve the proposed PBE in the malicious node detection game. However, there are still some issues that must be resolved before the equilibrium strategies can be applied and followed by practitioners. These issues can be categorized into two aspects. First, the PBE requires the malicious node perfectly know the belief held by the regular node. However, in practice, the belief information is never shared. Second, the malicious node may not remain

passive in the detection game; instead, it can also form its belief about the current status in the game and adjust its strategy accordingly.

It is natural that not only the regular node but also the malicious node (node i) study the game through observation. In particular, node i understands that although the unreliable channel makes the observations inaccurate, the more often it attacks, the quicker node j can form a correct belief about its malicious type. Thus, node j should take different strategies when different beliefs are held by node j. These strategies (e.g., the PBE strategy in equation (5.17)) are Markovian when we view the beliefs as a set of states. The Markovian strategies adopted by node i is only determined by the current state of the belief, i.e., when the belief update process takes place. However, the belief held by node j is its private information, and by no means can node i access this information. Therefore, it is essential for node i to construct its own belief system, which is the belief on the belief node j holds towards node i and we call this belief developed by node i *nested belief*.

We denote $\mu_i(\mu_j(\theta_i))$ as the belief node i holds about node j's belief about node i, i.e., $\mu_i(\mu_j(\theta_i))$ is the nested belief about $\mu_j(\theta_i)$. For the game we presented in Table 5.2(a), depending on the actions nodes i and j take, the payoff of node i, u_i, can be one of the three different values: $-g_A - c_A$, $g_A - c_A$ or $-c_F$. While the observations of the payoffs are node i's private information, given a specific observation o_i, node i can predict the actions taken by node j, despite the prediction may be inaccurate. For example, when $o_i = -g_A - c_A$, node i knows for sure $a_j = Monitor$. However, when $o_i = -c_F$, node i cannot tell what node i has done. Further, based on the prediction of the actions node j takes, node i can update

91

its belief $\mu_i(\mu_j(\theta_i))$ on how node j's belief $\mu_j(\theta_i)$ has changed due to a_j. Continuing with the same examples, when $o_i = -g_A - c_A$, $a_j = Monitor$, so node j observes the *Attack* launched by node i and it will update $\mu_j(\theta_i)$ according to equation 5.7. Similarly, when $o_i = g_A - c_A$, node i knows that node j is idle and $\mu_j(\theta_i)$ will not change. However, the uncertainty comes when $o_i = -c_F$, where node i cannot accurately update its belief about $\mu_j(\theta_i)$.

To construct the belief update system for node i, we employ the Bayes' Theorem. At stage t of the game, based on the observation $o_i^{(t)}$, node i's belief $\mu_i(\theta_i)$ is updated as:

$$\mu_i^{(t+1)}(\mu_j(\theta_i)) = \frac{\mu_i^{(t)}(\mu_j(\theta_i))P(o_i^{(t)}|\theta_i)}{\sum_{\tilde{\theta}_i \in \Theta} \mu_i^{(t)}(\mu_j(\tilde{\theta}_i))P(o_i^{(t)}|\tilde{\theta}_i)}, \tag{5.41}$$

where $\Theta=\{0,1\}$.

The conditional probabilities of observing o_i given its type θ_i can be calculated as follows. To distinguish from the strategy profiles we used previously, we denote $\tilde{p}$ as the probability node i launches attacks, and $\tilde{q}$ as the probability node j monitors. Therefore, the probabilities that arise due to the different observations and node i's type are:

$$P(o_i^{(t)} = -g_A - c_A|\theta_i = 1) = (1 - p_e)\tilde{p}\tilde{q} + \alpha(1 - \tilde{p})\tilde{q} \tag{5.42}$$

$$P(o_i^{(t)} = -g_A - c_A|\theta_i = 0) = \alpha\tilde{q} \tag{5.43}$$

$$P(o_i^{(t)} = g_A - c_A|\theta_i = 1) = \tilde{p}[p_e\tilde{q} + (1 - \tilde{q})] \tag{5.44}$$

$$P(o_i^{(t)} = g_A - c_A|\theta_i = 0) = 0 \tag{5.45}$$

$$P(o_i^{(t)} = -c_F|\theta_i = 1) = (1 - \tilde{p})[(1 - \alpha)\tilde{q} + (1 - \tilde{q})] \tag{5.46}$$

$$P(o_i^{(t)} = -c_F|\theta_i = 0) = (1 - \alpha)\tilde{q}. \tag{5.47}$$

With the above equations, for each of the observations $o_i \in \mathbf{O}$, where $\mathbf{O} = \{-g_A - c_A, \ g_A - c_A, \ -c_F\}$, $\mu_i^{(t+1)}(\theta_i)$ is updated independently. Since for the malicious node i, its type $\theta_i = 1$ is known to itself, the overall belief is hence updated considering each of the possible observations.

$$\mu_i^{(t+1)}(\mu_j(\theta_i)) = \sum_{o_i \in \mathbf{O}} P(o_i^{(t)}|1) \frac{\mu_i^{(t)}(\mu_j(\theta_i))P(o_i^{(t)}|\theta_i)}{\sum_{\tilde{\theta}_i \in \Theta} \mu_i^{(t)}(\mu_j(\tilde{\theta}_i))P(o_i^{(t)}|\tilde{\theta}_i)}. \tag{5.48}$$

Further, with the belief system of node i, the malicious node detection game can be solved again to obtain the sequential rationality. The derivation process is similar to what we have presented in equations (5.13) to (5.16), with the exception that $\mu_i^{(k)}(\mu_j(\theta_i))$ will be considered. The equilibrium strategy profiles that reaches sequential rationality are,

$$\tilde{p}^{(t)} = \frac{c_M}{\mu_i^{(t)}(\mu_j(\theta_i = 1))(1 - p_e)(1 + \gamma)g_A} \tag{5.49}$$

$$\tilde{q}^{(t)} = \frac{g_A\gamma - c_A + c_F}{(1 - p_e)(1 + \gamma)g_A}. \tag{5.50}$$

Moreover, it is easy to justify that the belief update process for node i also satisfies the Bayesian condition in Definition 5.1. In addition, equation (5.49) suggests that node i's strategy is purely dependent on the current belief it holds. Thus, we can further refine the PBE in malicious detection game.

Theorem 5.4. *With the nested belief system for node i, the dynamic malicious node detection game has a Markov Perfect Bayes-Nash Equilibrium (MPBNE) when the strategy profiles are $(\sigma_i^{(t)}, \ \sigma_j^{(t)}) = (\tilde{p}^{(t)}, \ \tilde{q}^{(t)})$.*

The equilibrium is called Markov because the strategies associated are Markovian based on the beliefs. It is noted that the PBE obtained in Theorem 5.1 is also a MPBNE, however,

the strategy profile has limited applicability because the equilibrium profile for node i requires the knowledge of node j's state (belief). On the contrary, the profiles in Theorem 5.4 only rely on the private information available to the nodes themselves.

A special case for the strategy profile σ_i is "Always attack when $\mu_i^{(k)}(\mu_j(\theta_i = 1)) < \bar{\mu}$ and forward otherwise, for a predefined threshold $\bar{\mu} \in (0, 1)$". In this strategy, when $\mu_i^{(k)}(\mu_j(\theta_i = 1)) < \bar{\mu}$, $\tilde{p} = 1$ and node j will progressively update its belief when it monitors because node i is always behaving maliciously. However, when the belief threshold is reached, node i will refrain from launching attacks, and hence its payoff will decrease. It is clear that the strategy deviates from the MPBNE because $\tilde{p}$ does not adhere to the equilibrium. As a result, node i will be identified quickly and it will be dormant for the rest of the time. While this strategy is favorable to node j and the network, from node i's perspective, this strategy will limit its attacks and hence it is not desirable.

5.4   Summary

In this chapter, we apply game theory to study the coexistence of malicious and regular nodes. We formulate a malicious node detection game and a post-detection game played by the regular and malicious nodes. While both games are of imperfect information type, we show that the former game has a mixed strategy perfect Bayesian Nash equilibrium and provide a solution to achieve that equilibrium. For the latter game, a coexistence index is proposed. We also prove that keeping the coexistence index above a threshold, the

post-detection game has a subgame perfect Nash Equilibrium which is also the coexistence equilibrium for malicious and regular nodes. We also propose a nested belief system that can be used by the malicious node to predict if it has been detected. We also prove the existence of a Markov Perfect Bayes-Nash Equilibrium when both nodes constantly update their beliefs.

CHAPTER 6
EXPERIMENTAL STUDY

In this chapter, we discuss the experimental studies that we conduct to validate the theoretic models we developed in Chapters 3, 4 and 5. Our experimental findings are presented in the same order as the analysis, i.e., cooperation in the homogeneous channel, cooperation in the heterogeneous channel, and coexistence with malicious attackers. In particular, Section 6.1 shows the games played by a cooperation enforcement strategy and a collusion strategy with homogeneous noise. In Section 6.2, we setup a multi-hop wireless network scenario with heterogeneous channel conditions and study the performance of our proposed state machine based cooperation enforcement schemes. Finally, in Section 6.3, we illustrate attacker detection process and show the network properties when the equilibria are reached.

6.1 Anti-collusion Game

To illustrate how the dynamics of the population evolves and how collusion can be resisted in the packet forwarding, we represent our findings through simulation which is based on the framework proposed in [35]. In the simulation, a total number of 100 nodes adopting two different strategies are considered. Homogeneous noise is added to simulate the channel unreliability. We take the average population share over five simulation runs and plot how

the population evolves as the games are played. The strategies adopted by the nodes are

CORE and a naive collusion strategy (CS) defined as follows:

Definition 6.1. *Naive Collusion Strategy (CS): Forward all packets from the colluding group, discard all packets from outside of the group. i.e.,*

$$p_i = \begin{cases} 1 & \text{if node } -i \text{ is also a colluding node.} \\ 0 & \text{otherwise} \end{cases}$$
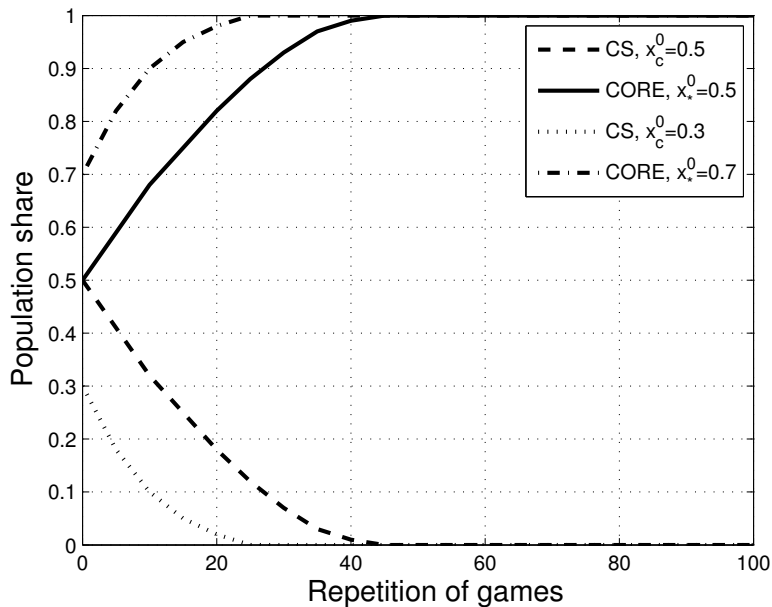
Figure 6.1: The effect of initial population share.

In Figure 6.1, we show how the population evolves with different initial population share. The plots are obtained with $p_e = 0.2$, $\alpha = 1.1$. For CORE, we consider a history of last 10 steps ($b = 10$). With the parameter settings, Theorem 3.1 infers that CORE is SPNE. It is very clear from the plots that the population adopting CORE overtakes that adopting CS and the games eventually converge to a point where all the population adheres to CORE, i.e.,

97

all the nodes are cooperative. It is also suggested that a larger initial cooperative population

($x_*^0 = 0.7$) leads to a faster convergence of the population evolution.
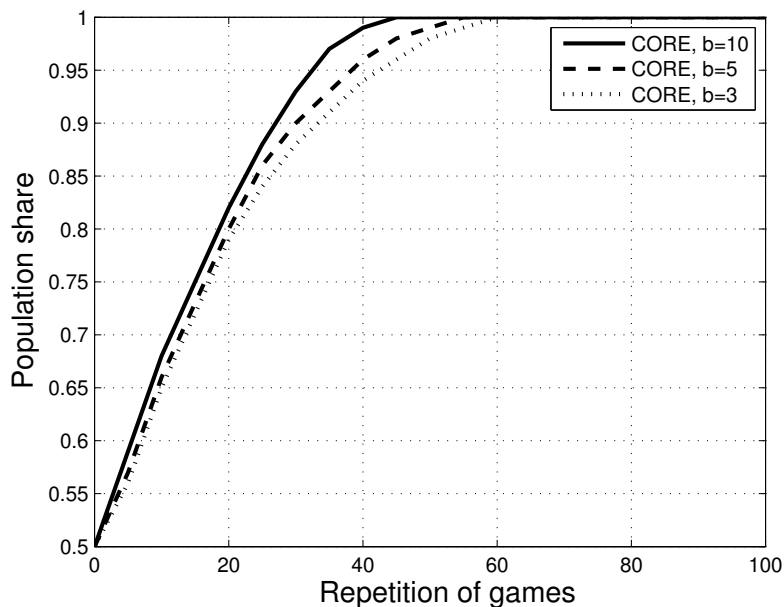
Figure 6.2: The effect of history length of CORE.

We further study how the reputation history length b affects the performance of CORE. In Figure 6.2, we compare the population evolution of three different values of b. While the rest of the parameter settings remain the same, we only focus on the population dynamics of CORE. Although the results show that cooperation can be enforced with CORE, the convergence rates are different. The comparison states that large values of b help fast convergence. This is due to the longer history it takes into account, the less observation error it is likely to make.
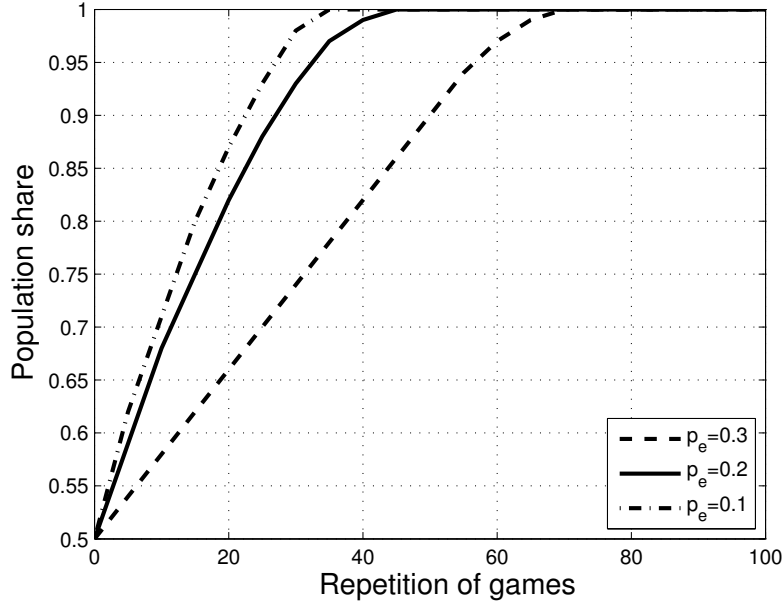
Figure 6.3: The effect of channel unreliability.

Figure 6.3 presents the effect of the channel unreliability on the population dynamics. The plots clearly imply that the more reliable the channel is, the faster cooperation can be enforced.

Figure 6.4 shows the combined effect of incentive value α and the initial population share. The first observation is that with a small α, the population converges faster than that of a larger α. This is because when α is large, the more benefit colluding can get and hence the evolution takes a longer time. Another interesting observation is that with the same α value, very small initial population share $(x_*^0 = 0.2)$ fails to reach the $+1$ population state (i.e., cooperation). The reason behind is the effect of SPNE. In Theorem 3.2, we have shown that cooperation can only be obtained if the cooperative strategy is ESS or the initial

population reaches a threshold. In case of Figure 6.4, the SPNE condition of CORE requires $\alpha < \frac{1}{1-p_e} = 1.25$, so when $\alpha = 2$, CORE is no longer an ESS. Thus, a small initial population share will not be able to lead the entire population to cooperation.
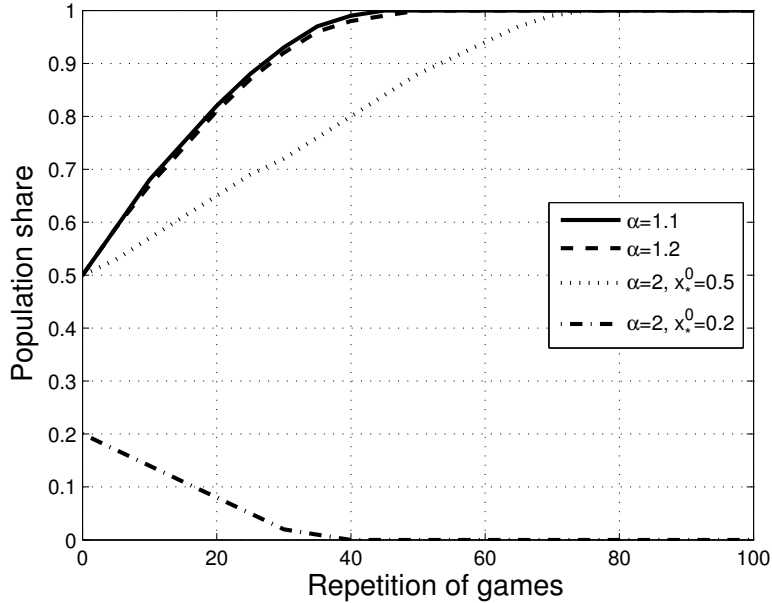
Figure 6.4: SPNE and the population dynamics.

6.2 Multihop Cooperation Enforcement

In this section, we evaluate our state machine based cooperation enforcement packet forwarding strategies by simulation. We also show the network performance under the proposed strategies.

We consider 50 nodes that are randomly scattered in an area of $1000m \times 1000m$. The physical communication range is set to be $250m$. During the simulation, log-distance path

loss with exponent of 3 is adopted as the propagation model, and IEEE 802.11 is the under-lying MAC protocol with a bandwidth of 2 Mbps. The data packet size is 64 bytes carried by Constant Bit Rate (CBR) type of traffic with 2 packet per second, unless specially mentioned. We allow only one data session at a time. The data sessions originate and terminate at randomly selected source and destination nodes. For the routing based packet forwarding strategy, a DSR like routing agent is in place to handle the route discovery and maintenance. For the hop-by-hop forwarding, GPSR like forwarding is employed and it finds the reachable node with minimum distance to the destination as the next hop. The source nodes have equal probability in selecting the forwarding type.

To simulate the repeated nature of the packet forwarding games, any node pair engaged in packet forwarding, play a number of games with respect to the discount factor δ defined as a system parameter. For a given δ, the average number of subgames is $1/(1-\delta)$. Therefore, in our simulation, a data session has at least $1/(1-\delta)$ packets with one packet forwarding as a game.

The simulation runs for 1000 seconds with different channel loss probabilities. p_e is set to a random number in [0.01, 0.2] as the default value.

Our investigation starts with the one hop packet forwarding (i.e., two-player packet forwarding game). We set the game payoff matrix as $T = 0.8$, $R = 0.7$, $P = 0.1$ and $\delta = 0.99$. Figure 6.5 shows the average payoff for each of the nodes using our state machine based forwarding strategy. For comparison, we plot the payoff for "Full Cooperation" strategy as well. Full cooperation implies node will always forward others packet unconditionally. The

theoretical boundaries for our proposed strategy are also presented. The plot shows that the payoffs of the proposed strategy are within the theoretical limits developed in Corollary 4.2. Also, it is observed that the payoffs are very close to the unconditional "Full Cooperation" strategy. The average payoffs are much closer to the upper bound than the lower bound because when the games reach sequential equilibria, mutual cooperation is enforced.
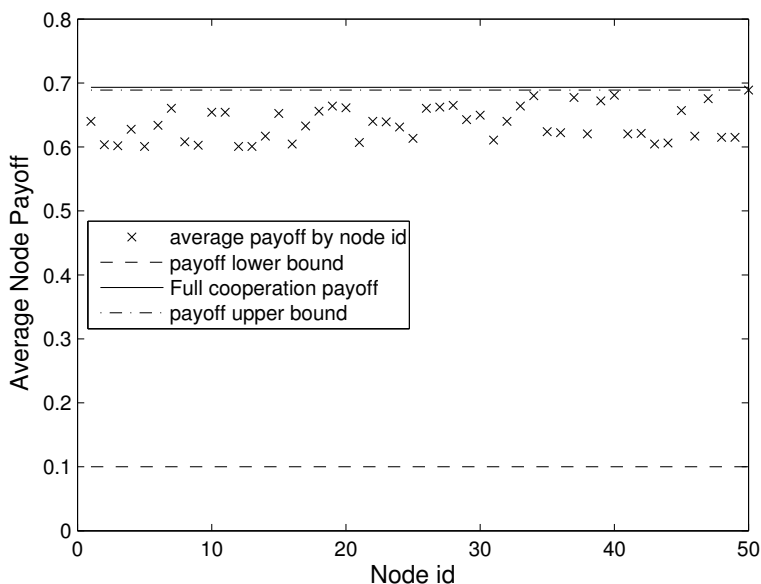
Figure 6.5: Average node payoff for state machine based forwarding strategy.

Figure 6.6 presents the average node payoffs with different channel loss probabilities p_e and discount factor δ. Note that $\delta = 0.999$ implies 1000 subgames played while $\delta = 0.99$ implies 100 subgames. The plots provide two insights. (1) As the channel becomes more unreliable, the average payoff drops. (2) The more games played, the more average payoff is generated. These observations also suggest that it is more desirable to have more packets in one continuous data session before switching for another relaying nodes.
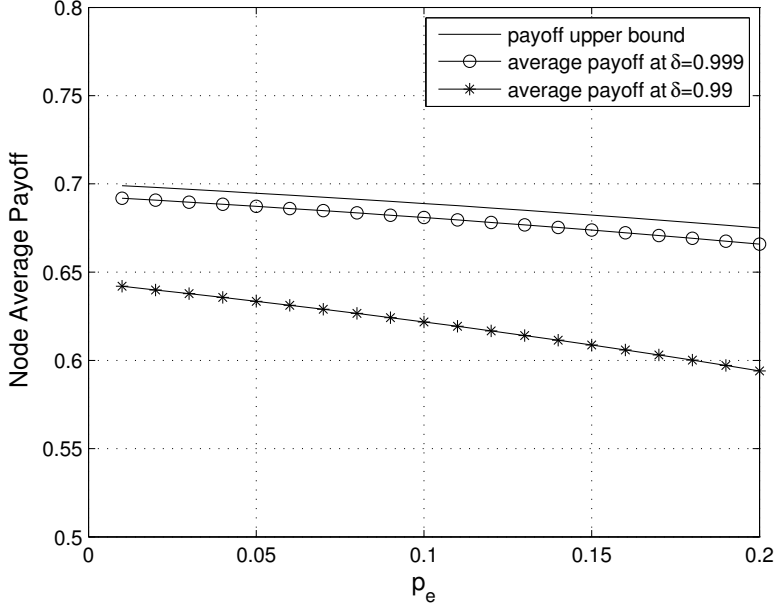
Figure 6.6: Average node payoff with different channel loss probability and discount factor.

We show the equilibrium nature of the proposed state machine based forwarding strategy in Figure 6.7. The payoffs of deviation strategies are plotted. In the deviation strategies, when the node in state C, it always plays $Discard$ with probability $q_C = 0.1$ or $q_C = 0.15$ (Recall that in our equilibrium strategy, q_C is a very small value.). In this setting, $\delta = 0.999$ and $p_e = 0.01$. Figure 6.7 clearly shows that the payoffs with our proposed strategy are strictly greater that the deviation strategies.

To further evaluate our proposed strategies, we consider the network performance. In Figure 6.8, we present the normalized network throughput at $\delta = 0.99$. We denote 1 as the state that all the generated packets are successfully delivered from source to destination. It is shown that with a small channel loss probability ($p_e = 0.01$), our proposed Multi-hop Packet

Forwarding Strategy (MHPFS) reaches almost the same throughput as the fully cooperative strategy. With a larger p_e, the throughput difference between MHPFS and the unconditional cooperation case is larger.
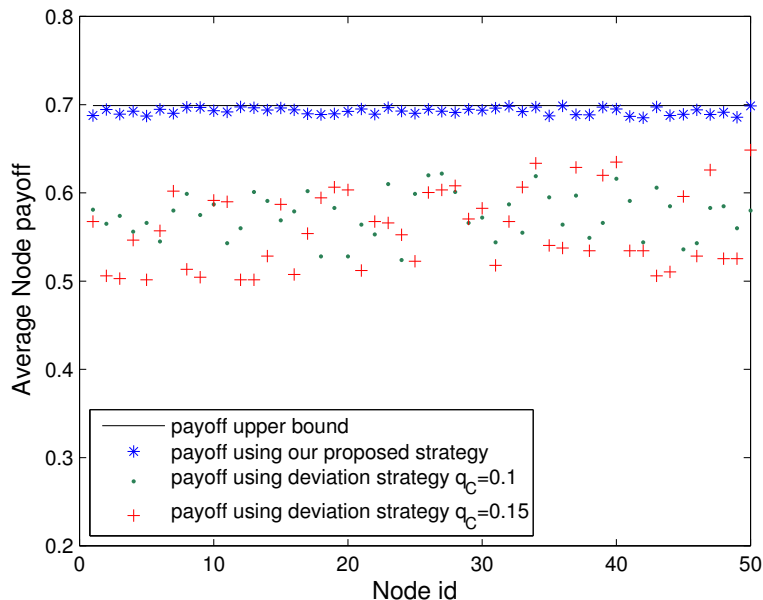
Figure 6.7: Average node payoff comparison with deviation strategies.

In addition, we analyze the effects of hop count and channel unreliability on the throughput. The results are shown in Figure 6.9 with $\delta = 0.999$. It can be noted that throughput drops when channel becomes more unreliable or hop count increases. Also, our proposed MHPFS yields throughput performance very close to the situation where all the nodes are unconditionally cooperative.
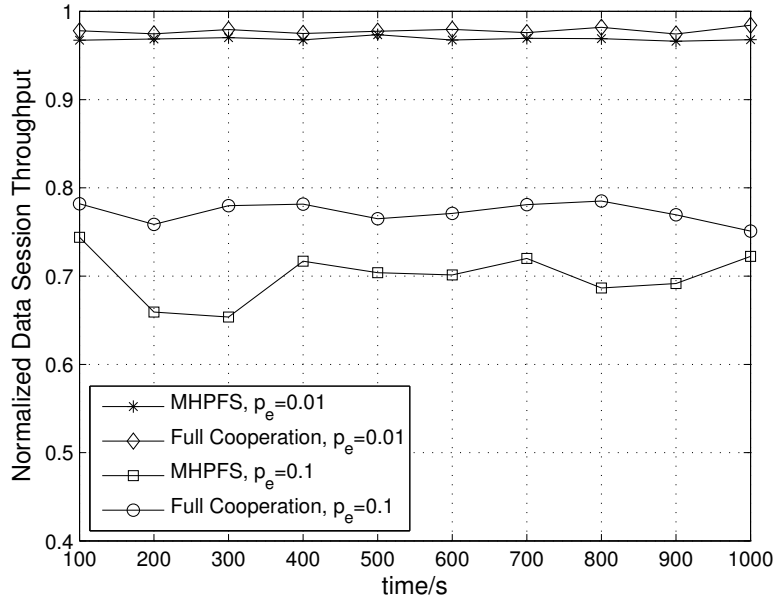
Figure 6.8: Normalized data session throughput for different channel loss probability and strategies.

The relationship of packet generation rate and throughput is presented in Figure 6.10. δ is set to 0.99. The plots do not show much difference for different packet rates and the throughput remains almost constant.

Last but not least, we study the effect of mobility. In this setting, $p_e = 0.01$, $\delta = 0.999$. The mobility profile we use is Random WayPoint (RWP) with 5 seconds of pause in between two consecutive moves. Figure 6.11 plots the throughput performance for two different speeds. The results suggest that mobility introduces link break probability and decreases the throughput for our proposed forwarding strategy.
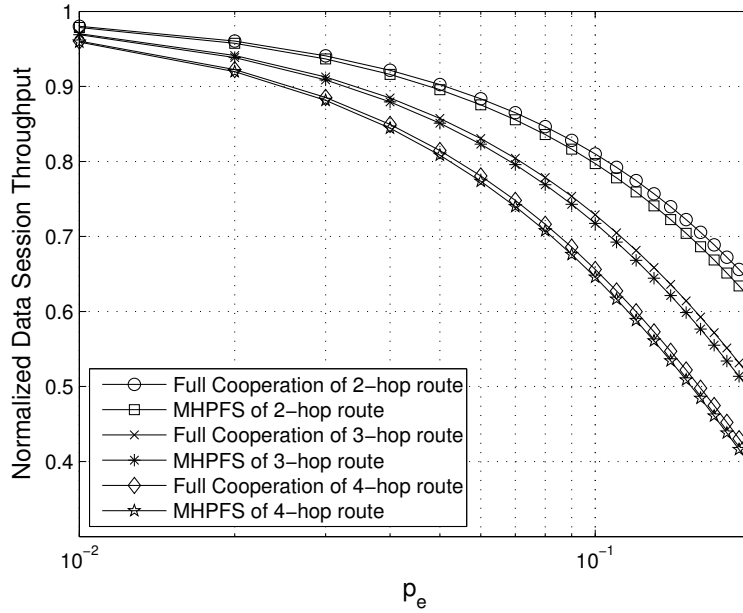
Figure 6.9: Normalized data session throughput vs. hop count and channel loss probability.

6.3   Attacker Detection and Coexistence

In this section, we study the properties of the perfect Bayesian Nash equilibrium in the malicious node detection game and the post-detection subgame perfect Nash equilibrium derived in Chapter 5 through simulations. In our simulator, two players play the games repeatedly; the payoffs and strategy profiles for each of the subgames are recorded to analyze the properties of the equilibria.
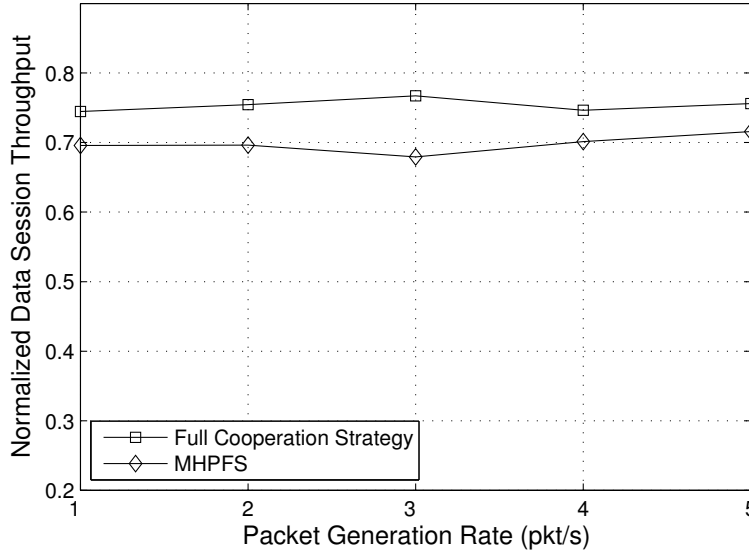
Figure 6.10: Normalized data session throughput for different packet generation rates.

6.3.1 Malicious Node Detection Game

We first present the simulation results on the malicious node detection game. In Figure 6.12, we show how the monitoring probability in PBE strategy increases with the malicious node attack success rate. The plots infer that the equilibrium require node j to increase its monitoring frequency as the attack success rate increases. Also, as the channel becomes more unreliable, node j must play *Monitor* more frequently.

Figure 6.13 compares the convergence of node j's belief system when different attack gains are presented. The plots are shown with $p_e = 0.01$, $\gamma = 0.95$ and $\alpha = 0.01$. In Figure 6.13(a), we show how the belief system forms a correct belief on the type of node i when only *Attack* is observed. The convergence of the belief system under PBE is illustrated

107
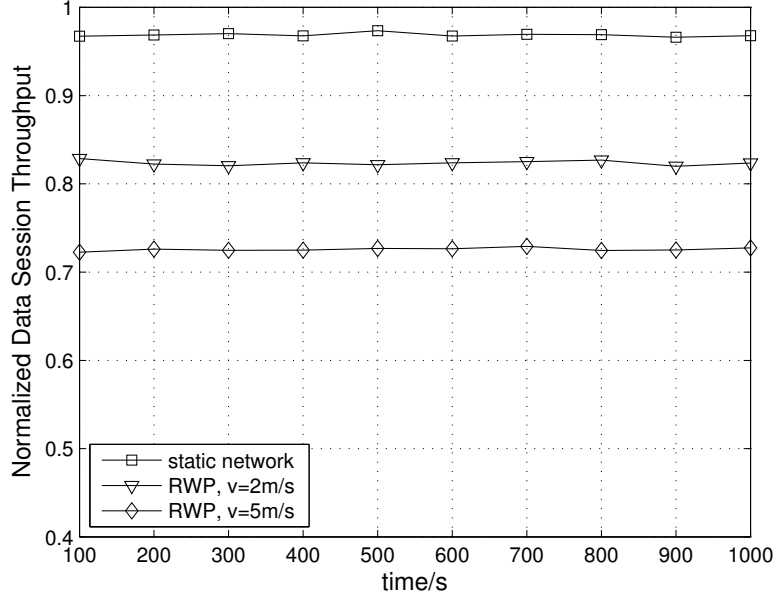
Figure 6.11: Normalized data session throughput for mobile nodes.

in Figure 6.13(b). The plots suggest that the lower the attack gain is, the quicker the belief system converges. This property can be explained as follows. A smaller attack gain requires node i to attack more often in order to get more payoff, and increasing the attack frequency also increases the risk of being successfully observed. With more observations, the belief is updated more frequently and accurately. Belief system converges slower in Figure 6.13(b) than in Figure 6.13(a) because in the PBE, instead of constantly monitoring, node j only monitors with probability q.

A more complete study on the convergence of the belief system is shown in Figure 6.14. Plots in Figure 6.14(a) indicate the larger the disguise cost c_F/c_A is, the less time it takes to converge. This is because, with a larger disguise cost, it is unprofitable for node i to disguise
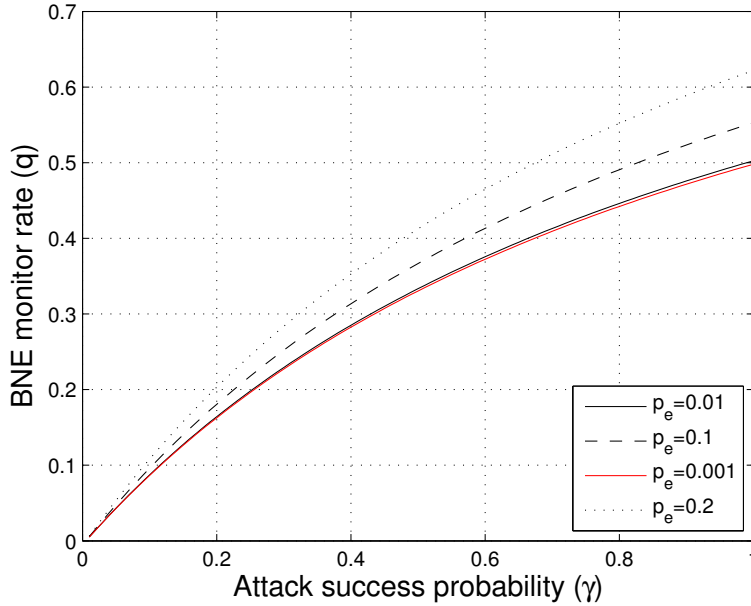
Figure 6.12: Equilibrium strategy q vs. the attack success rate in malicious node detection game.

by forwarding packets. Instead, it will launch more attacks, thus increasing the chances to be identified. Figure 6.14(b) shows a quicker converged belief system for a smaller detection gain because node j needs to monitor more often to be profitable. Figures 6.14(c) and 6.14(d) relate the convergence with less errors and uncertainties in the system. As expected, with errors and uncertainties (i.e., low channel loss, high attack success rate and low false alarm rate), the belief system converges quickly.

Finally, the parameters affecting the PBE attack probability p are investigated in Figure 6.15. The attack gain is a very important factor in determining the value of p as shown in Figure 6.15(a). A large attack gain means more payoff gained from an attack, which implies less number of attacks are needed. Hence p should be smaller. Figures 6.15(b) and 6.15(c)
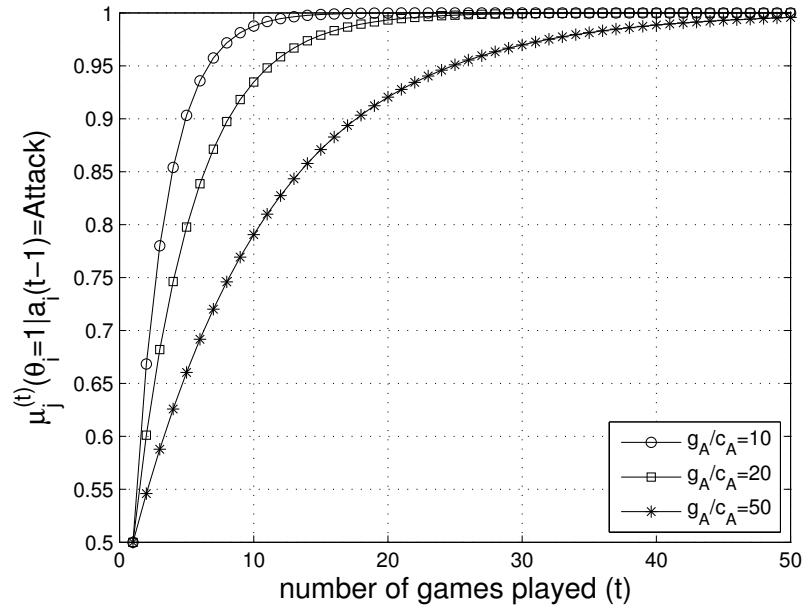
(a) constant monitoring
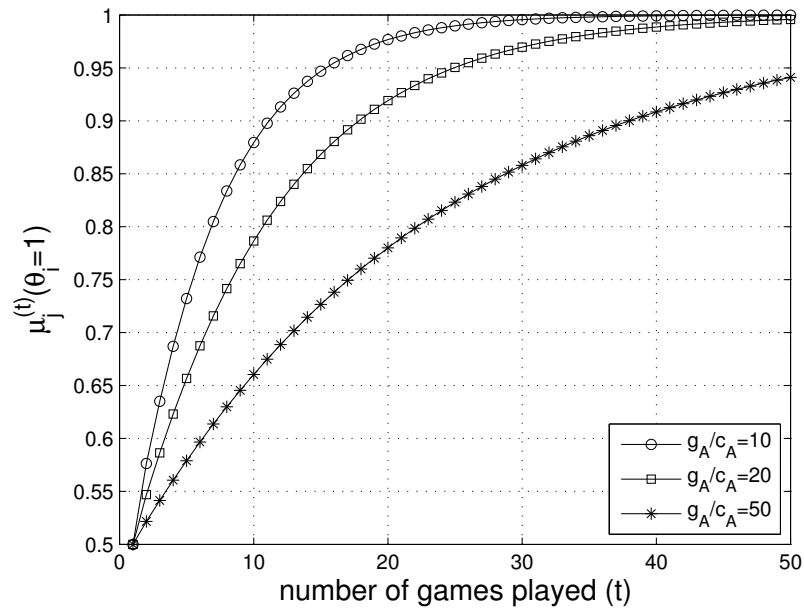
(b) PBE

Figure 6.13: Belief system update with different attack gains.
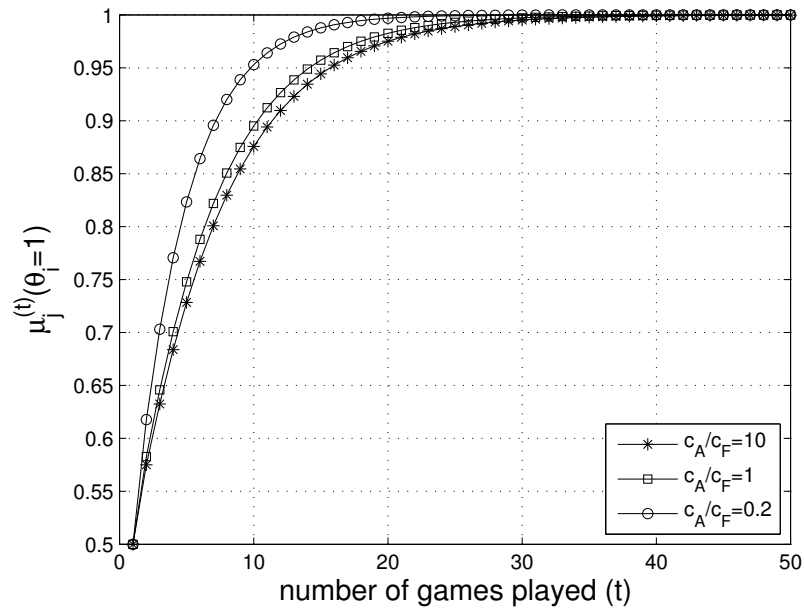
(a) disguise cost c_F/c_A
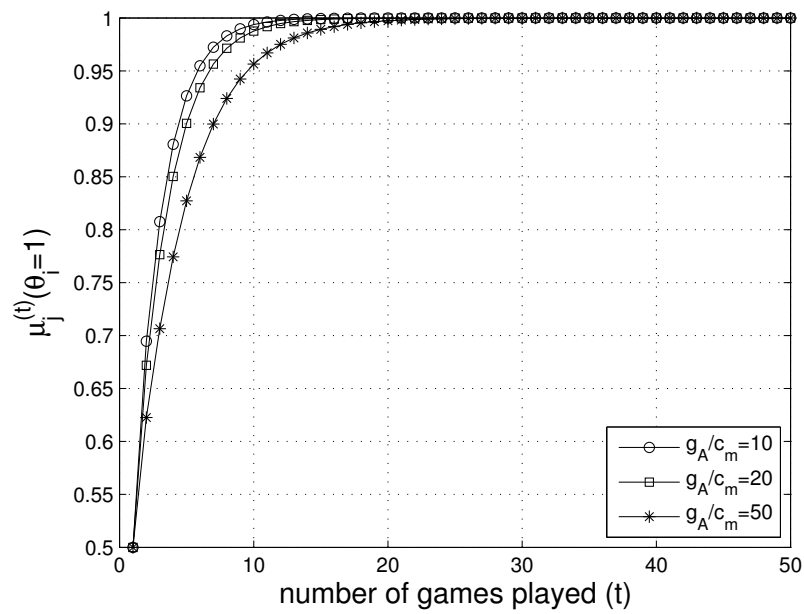
(b) detection gain g_A/c_M

Figure 6.14: Effects of parameters on belief system update.
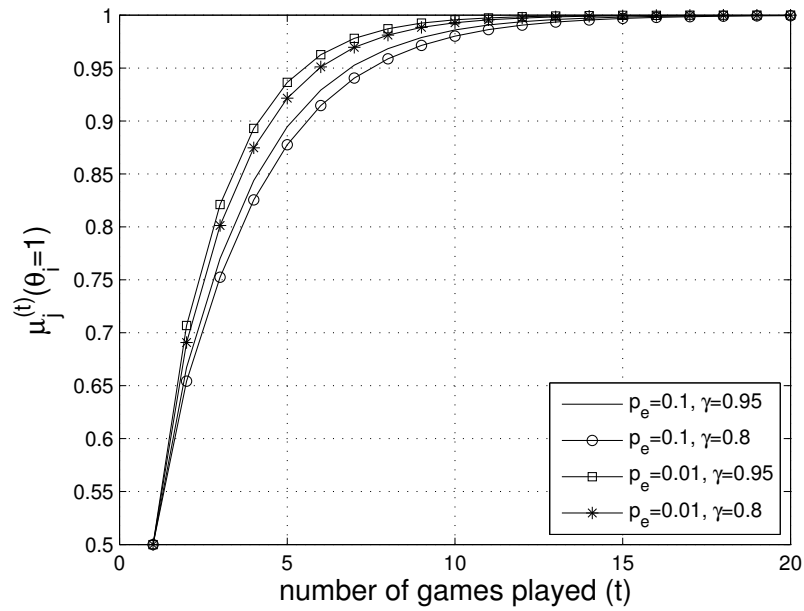
(c) channel unreliability and attack success rate
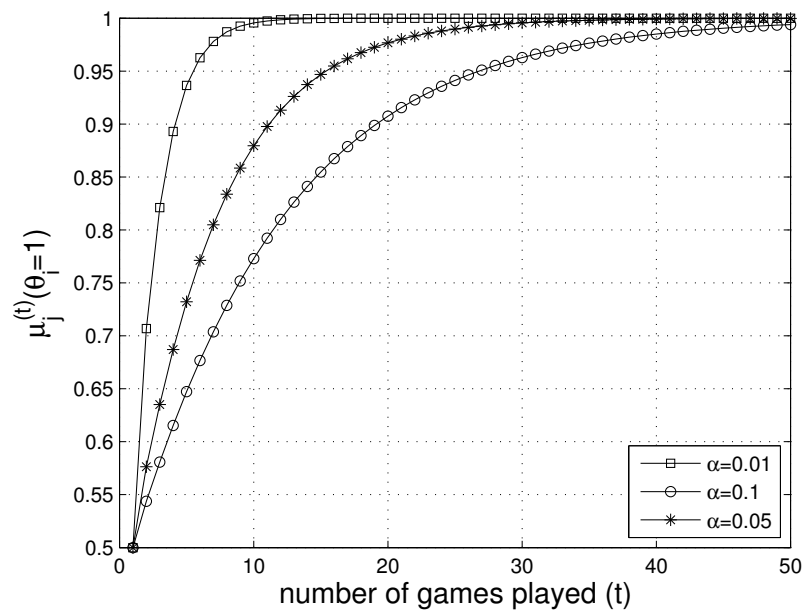
(d) false alarm rate

Figure 6.14: Effects of parameters on belief system update (cont.).

indicate that node i should attack less frequently under a reliable channel as every attack is more likely to be successful. However, as suggested in Figure 6.14(d), if the false alarm rate is high for the regular node, the malicious node can take advantage of it and attack more often.

6.3.2   Post-detection Game

After the belief system of node j converges ($\theta_i \geq 0.99$), we can safely conclude that node j has detected the malicious node. Therefore, the post-detection game starts. To show the continuity, at the beginning of the post detection game, node i sticks to its PBE strategy.

Figure 6.16 presents how the attack probability $p^*(t)$ evolves to the SPNE strategy from the PBE. It is clear in the plots that in the SPNE, node i should decrease its attack probability to avoid isolation. Figure 6.16(a) shows a larger detection gain that corresponds to a smaller attack rate; thus in the equilibrium, the payoffs for node j will not increase due to the large detection gain. Figure 6.16(b) states that if the channel is lossy, node i should attack more often. The reason behind this claim is that the more unreliable the channel is, the less probable node j can accurately observe an attack. Plots in Figure 6.16(c) are obtained from detection gain equals to 5. This figure shows that the equilibrium is not sensitive to the initial value and threshold of the coexistence index $\mathcal{C}_i$.

The expected length of the post-detection game is shown in Figure 6.17. First, the figure states that the less errors (i.e., less channel loss and more successful attack) in the system,
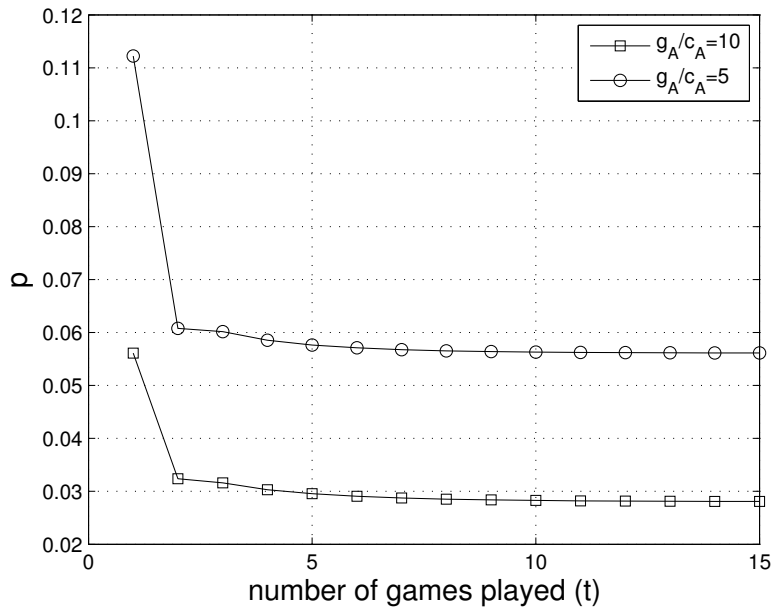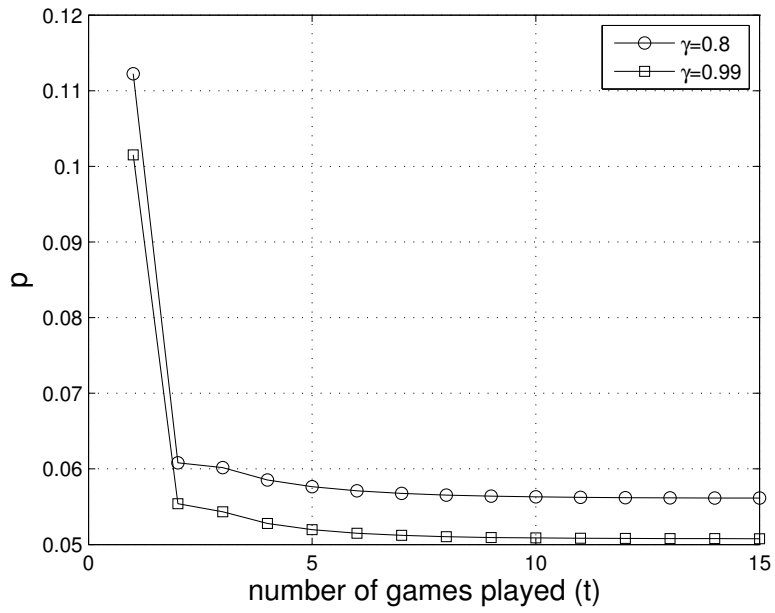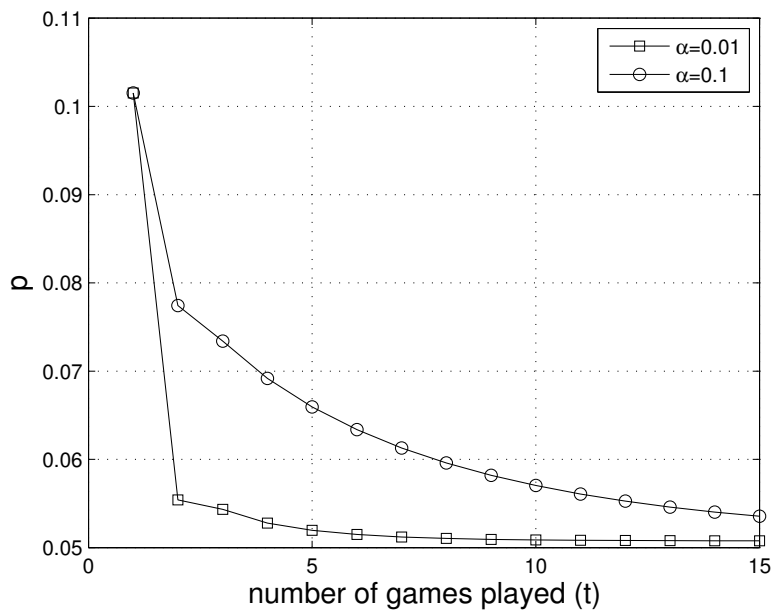
(a) attack gain g_A/c_A
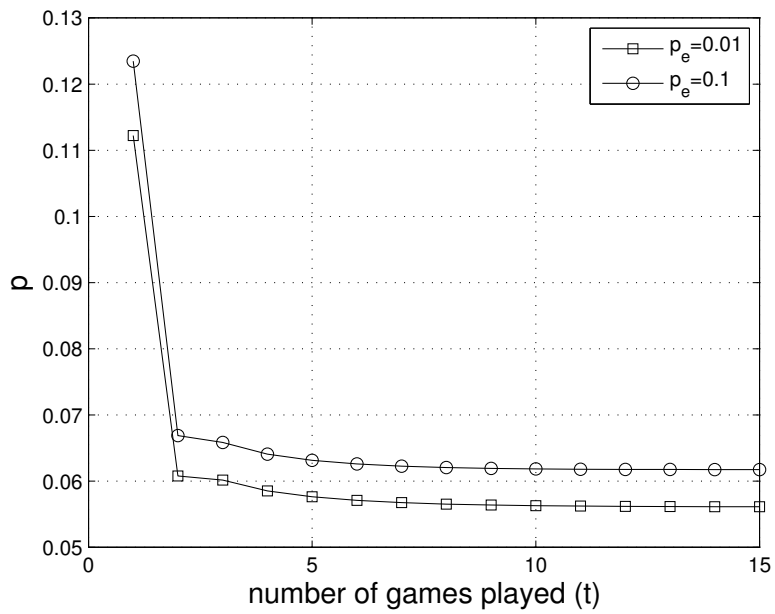
(b) channel unreliability

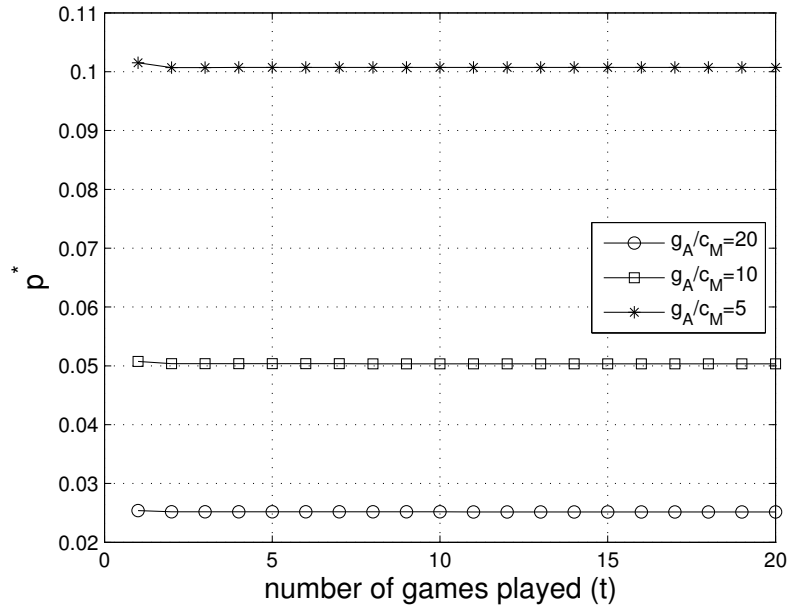Figure 6.15: Effects of parameters on the PBE strategy.
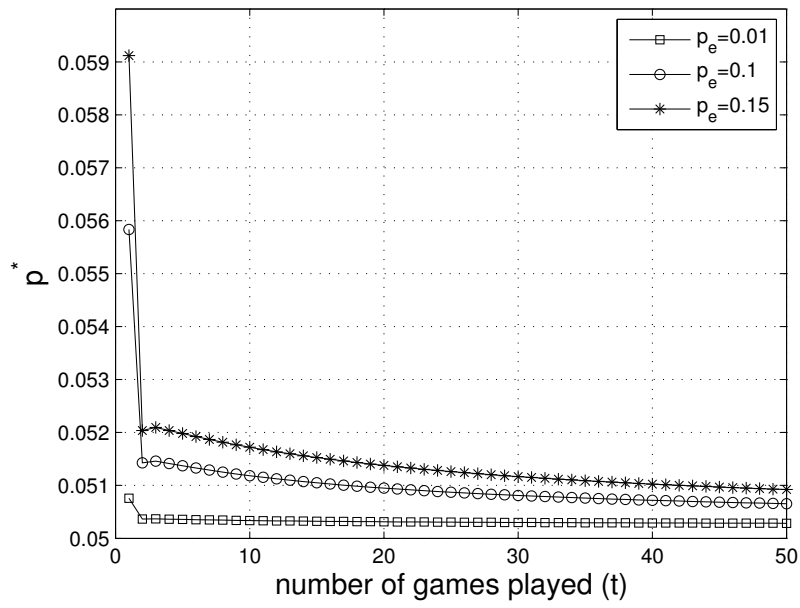
(c) attack success rate

(d) false alarm rate

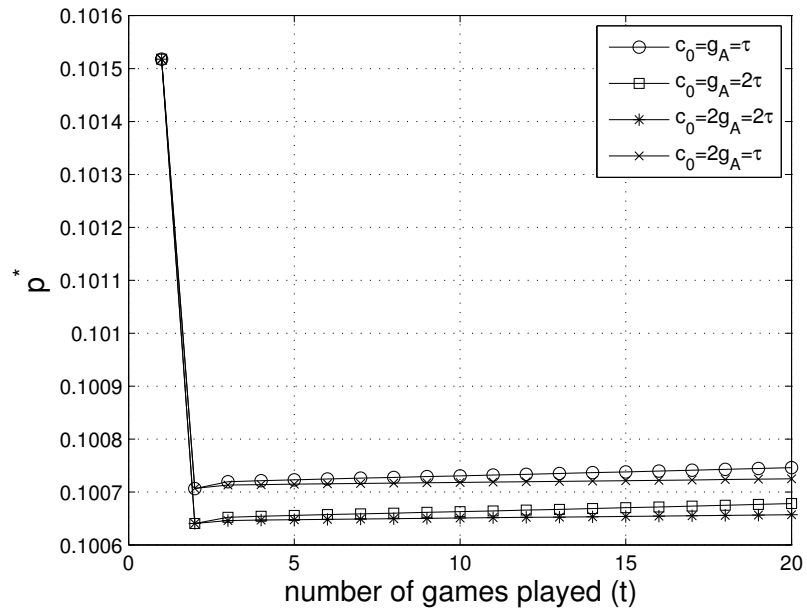Figure 6.15: Effects of parameters on the PBE strategy (cont.).

(a) detection gain g_A/c_M

(b) channel unreliability

Figure 6.16: Effects of parameters on the SPNE strategy.

(c) coexistence index

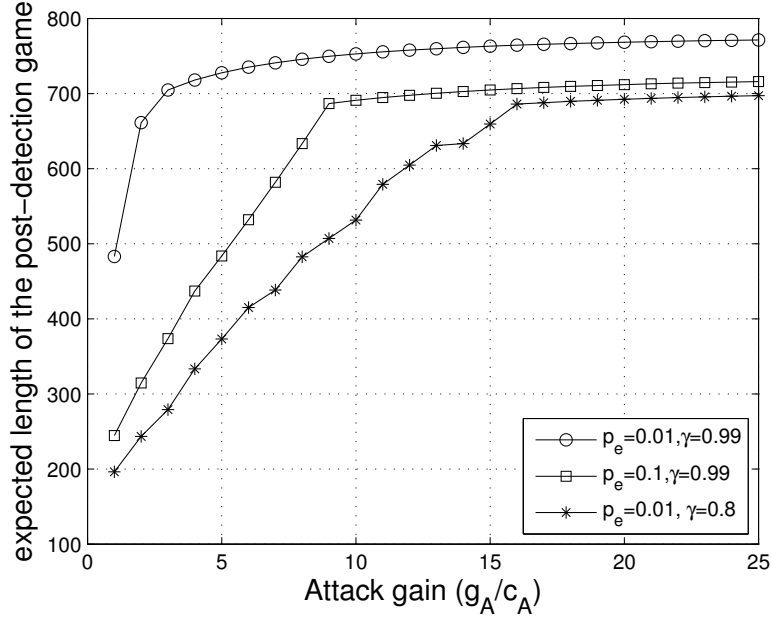Figure 6.16: Effects of parameters on the SPNE strategy (cont.).

Figure 6.17: Expected length of the post-detection game.

the longer the post-detection games can be played. Second, the length of the game grows with the attack gain. This interesting phenomena can be explained in the following way. The larger attack gain enables the malicious node to attack less while keeping its payoff high. Thus, more often, the malicious node will play as a regular node to avoid isolation. This will increase the time for the regular and malicious nodes to coexist. This property can be used to extend the lifetime of the network.

Last but not least, we show how the network throughput can benefit from coexistence in Figure 6.9. Similar observations can be made as the game length property. With a larger attack gain, the malicious node decreases its attack rate and does more packet forwarding as a regular node. Therefore, the malicious nodes can be utilized to increase the through-put more often as the attack gain grows. The throughput gain property illustrates clearly
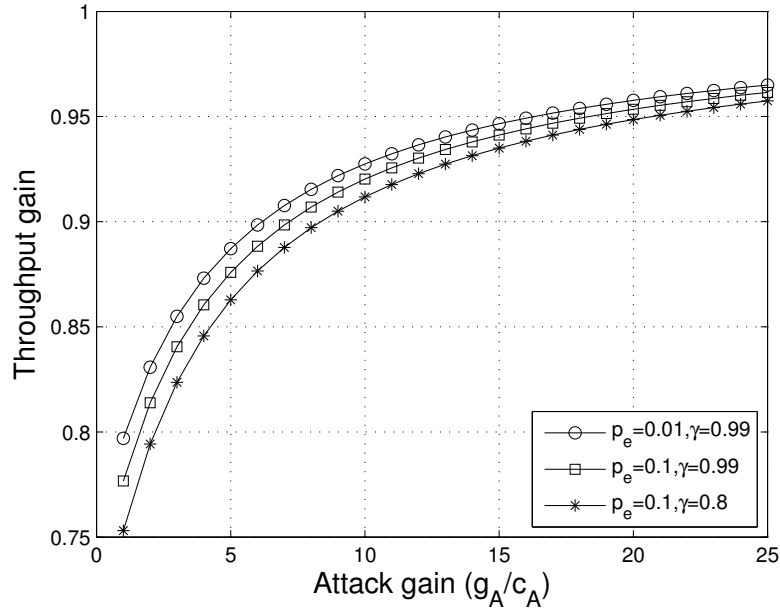
118

Figure 6.18: Throughput gain.

that malicious and regular nodes can coexist, and the coexistence equilibria improve the throughput of the network.

6.3.3 Characteristics of MPBNE

We study the characteristics of the Markov Perfect Bayes-Nash Equilibrium. In particular, we are interested in the properties of node i's belief update system (i.e., belief about belief) and how the introduction of node i's belief would affect the results we obtained in Section 6.3.1.

In Figure 6.19, we study node i's belief system in the MPBNE. The plots are obtained with $p_e = 0.01$, $\gamma = 0.95$ and $\alpha = 0.05$. To better show the properties of node i's belief

system in the MPBNE, we also present node j's belief system. In particular, we plot μ_i as node i's belief system in MPBNE according to equation (5.48), μ_j as node j's belief system in PBE as stated in equation (5.12) and μ_j^* as node j's belief system update in the MPBNE as a result of node i's actions in the belief about belief model. A common observation is that node i's belief μ_i converges much faster than the belief μ_j in PBE, which means that node i holds a false belief that node j can identify its malice quicker than node j actually could. As a result of the inaccuracy in node i's belief, it takes longer time for node j to form a belief on node i. This is evident from the plots that show μ_j^* converges much slowly than it does in PBE, when node i does not employ any belief system.

In addition, Figure 6.19 shows some similar properties of node i's belief system to what we have observed in Figure 6.14. For example, Figure 6.19(b) indicates a larger detection gain will force node i's belief system converge quicker. Figures 6.19(c) and 6.19(d) infer that reliable channel, high attack success rate and accurate detection (low false alarm rate) will also induce a fast convergence of μ_i. However, the only discrepancy is with the disguise cost; for node i, a high disguise cost makes update of μ_i slow, while for node j, a high disguise cost helps μ_i converge faster. The reason lies in the inaccuracy of node i's belief system. From our previous discussion, it is stated that when the observed payoff is $-c_F$, node i cannot predict what node j's action is. Thus, an internal error resides in node i's belief system, and this error is amplified when c_F is large (i.e., c_F, takes a high weight in the payoff), which corresponds to a large disguise cost.

The properties of the MPBNE strategy are further investigated in Figure 6.20. Once again, similarity is found between Figures 6.20(a) and 6.15(a), as well as Figure 6.20(b) and Figures 6.15(b), 6.15(c), 6.15(d). Both the MPBNE strategy attack probability, denoted as p_M and the PBE strategy attack probability in Figure 6.15 will increase with smaller attack gain and attack success rate, as well as larger channel error rate and false alarm rate. Moreover, it is noted that p_M is smaller than what node j believes it would be (denoted as p_{j*i} in the Figures 6.20(b)). In addition, p_M is larger than the PBE strategy attack probability p_PBE in the first several stage games, however, as the games repeat, p_M drops below p_PBE. This interesting observation implies that when node i implements the belief system, it attacks more aggressively (than without the belief about belief model, i.e., in PBE) in the first several games, because it believes node j is far from reaching a successful detection. As the game unfolds, node i adjusts its attack rate to prevent from detection. The difference between p_M and p_PBE also explains why node j's belief system alters in the MPBNE as shown in Figure 6.19.

6.3.4   Transition from Detection Game to Post-detection Games

Our discussions above are focused on how the involvement of node i's belief system would make the MPBNE different from the PBE. However, since the detection of the malicious node is not the only aim of this research, we are also motivated to find the link between the MPBNE and/or PBE in the detection game and the SPNE in the post detection game.
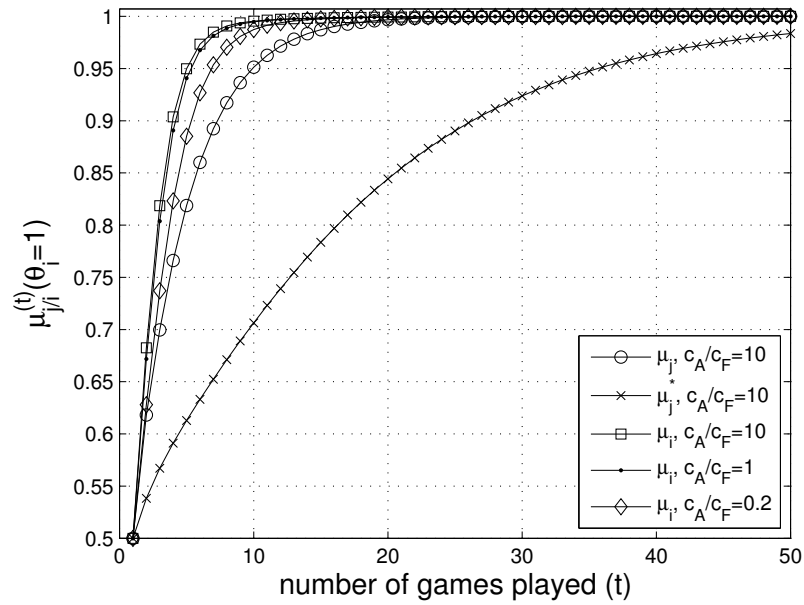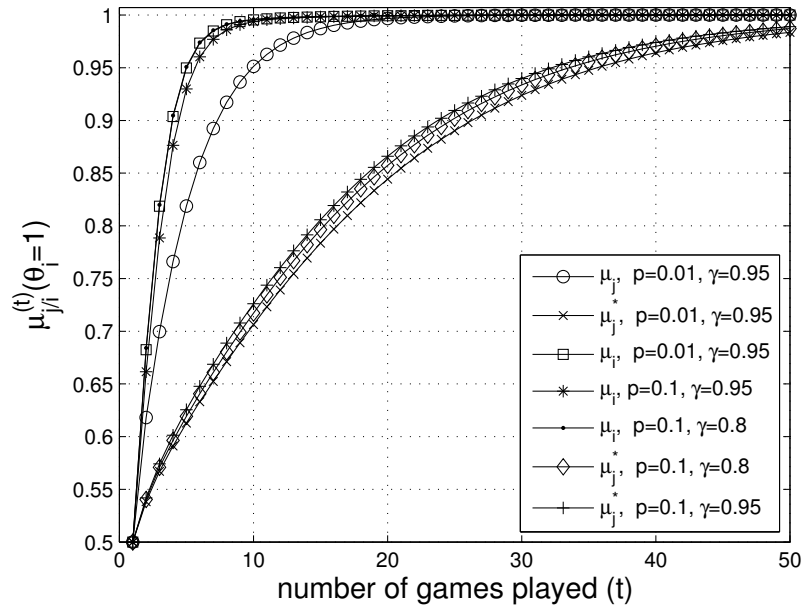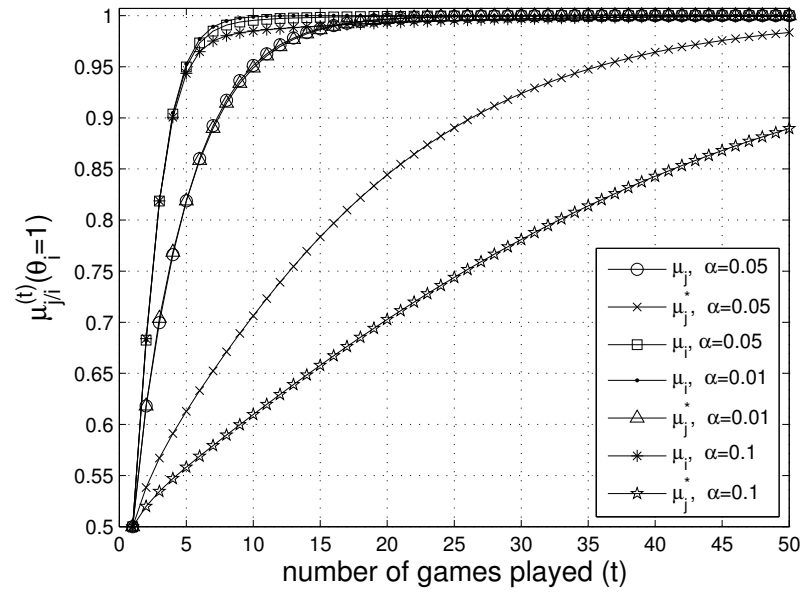
(a) disguise cost c_F/c_A
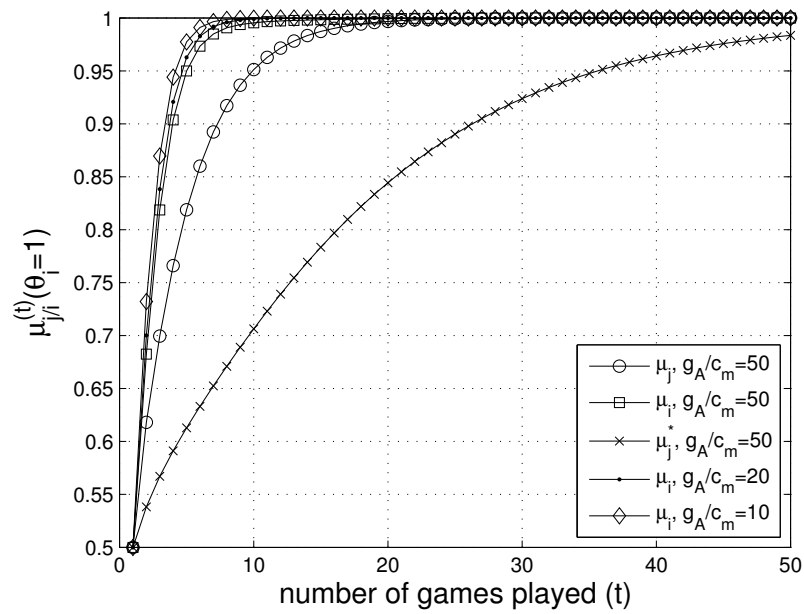
(b) detection gain g_A/c_M

Figure 6.19: Node i's belief system update in the Markov Perfect Bayes-Nash Equilibrium.
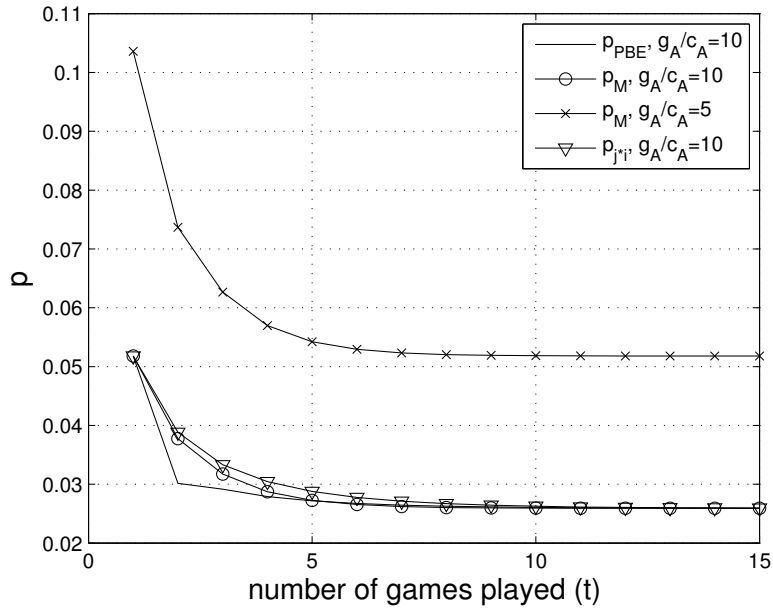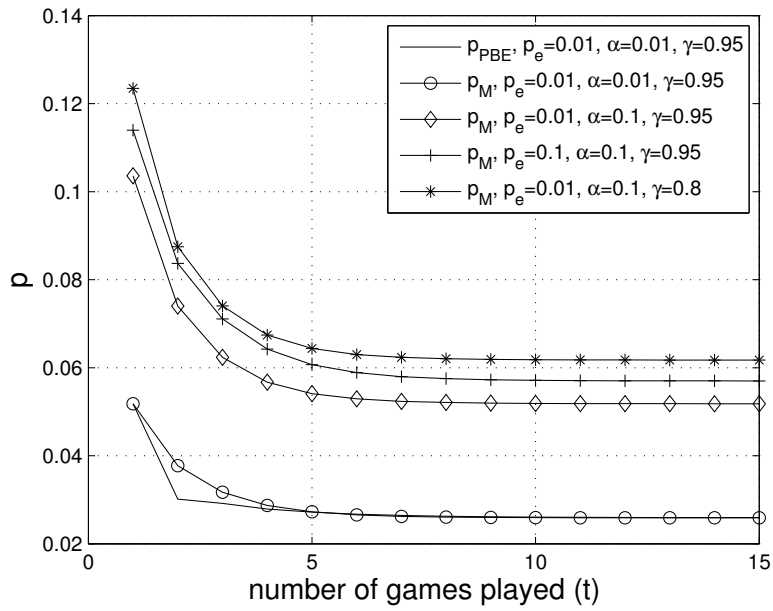
(c) channel unreliability and attack success rate

(d) false alarm rate

Figure 6.19: Node i's belief system update in the Markov Perfect Bayes-Nash Equilibrium (cont.).

(a) attack gain g_A/c_A

(b) channel unreliability, attack success rate and false alarm rate

Figure 6.20: Effect of parameters on the Markov Perfect Bayes-Nash Equilibrium strategy.

Figure 6.21 shows the equilibrium strategy profiles in terms of attack probability. It is clearly evident from the plot that although in MPBNE, node i attacks less often in PBE, in order to reach SPNE, node i still needs to further lower its attack probability. As a matter of fact, the post-detection game is initialized by node j when its belief about node i's malice reaches a threshold value ($\mu_j(\theta_i) > 0.99$ in our setting). However, this information is never revealed to node i, so that node i has no idea if the post-detection game has started or not. When node i is also equipped with the belief system, it can make a prediction on when the post-detection game starts based on its belief about node j's belief. For example, if node i's belief $\mu_i(\mu_j(\theta_i)) > 0.99$, node i might assume that the post-detection game has begun and adjust its strategy profile accordingly.

Figure 6.22 examines the transition process through simulation. In our simulation, once $\mu_i(\mu_j(\theta_i))$ reaches 0.99, node i's attack probability is set to be the same as the probability in SPNE (denoted as p_{SPNE}). Despite the change, node j still sticks to its criteria and does not start the post-detection game until its belief crosses the threshold. In other words, in this setting, node i deviates from the MPBNE and plays the SPNE strategy even when node j still plays the detection game. Figure 6.22(a) shows although node i deviates from MPBNE, the attack probability node j believes node i takes (p_{i*j}) and p_{PBE} are very close. Furthermore, Figure 6.22(b) indicates that when node i adheres to p_{SPNE}, node j's belief updates are slightly slower than that in the PBE. The simulation results suggest that with node i's belief system, malicious node detection game and the post-detection game can be integrated with an effective transition process.
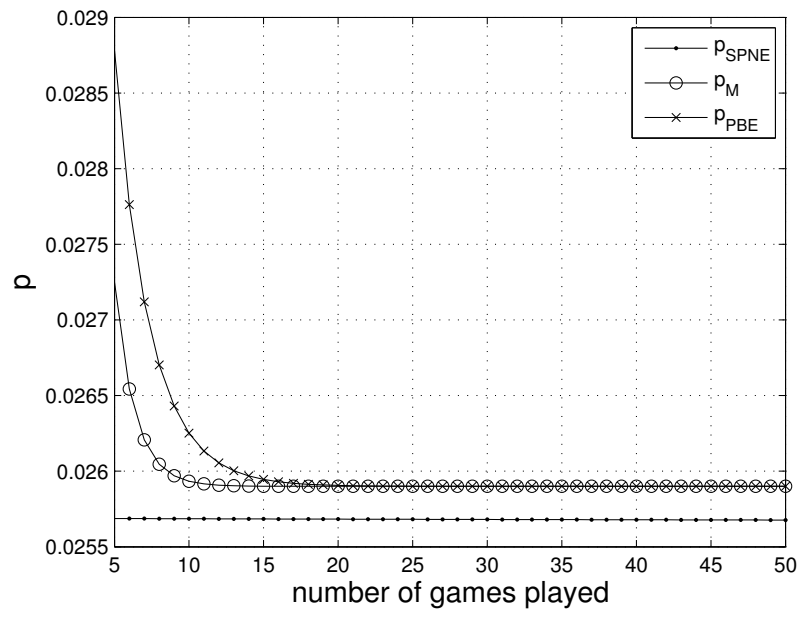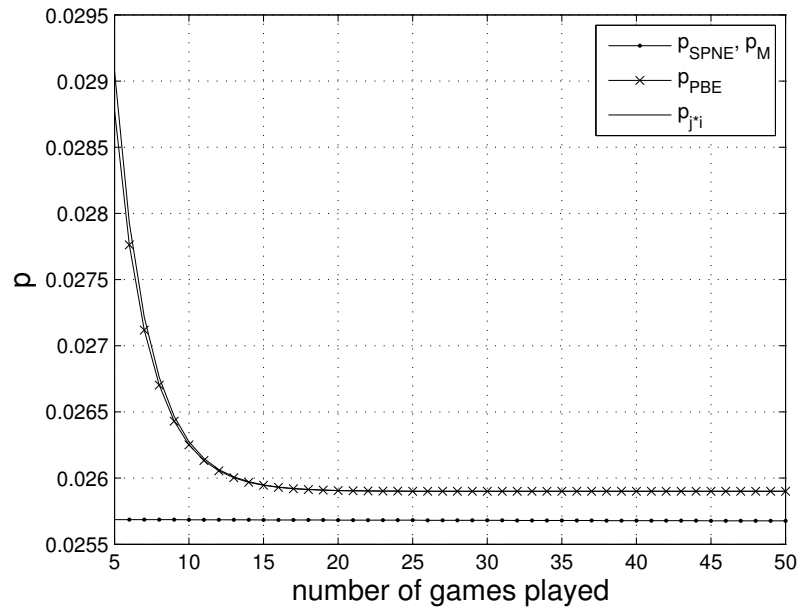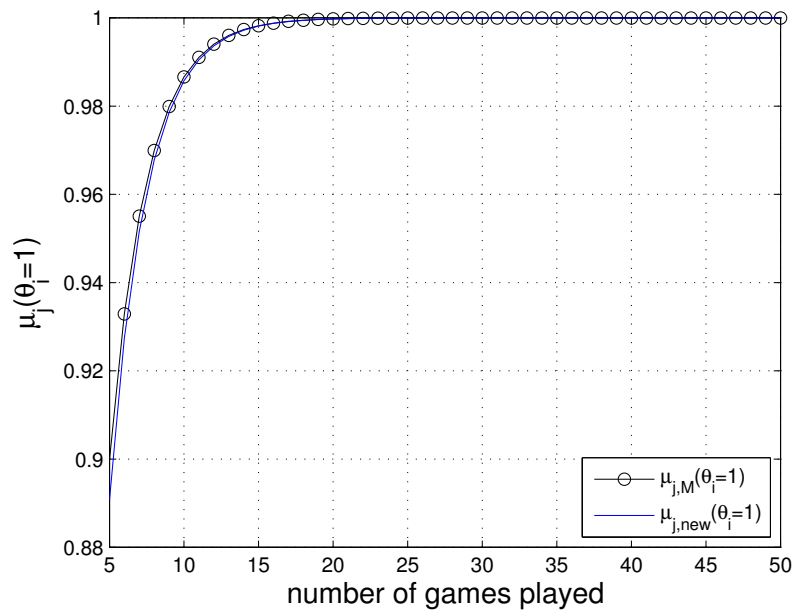
Figure 6.21: Comparison of node i's strategy profiles.

(a) Node i's strategy profiles.

(b) Node j's belief update.

Figure 6.22: Effects of the integration of the detection and post-detection games.

CHAPTER 7
CONCLUSIONS AND FUTURE DIRECTIONS

Misbehavior of nodes is a big threat to the wireless network security and quality of service provisioning. To ensure communication security, data integrity, and information fidelity, advanced cryptographic techniques can be employed at lower layers in the network stack. However, from a distributed system perspective, it is quite desirable that every node in the network can participate in the process of identification and mitigation of the misbehavior.

The body of work presented in this dissertation addresses mitigating the misbehavior in wireless networks from a game theoretic perspective. In particular, we take the packet forwarding process as an example and discuss in detail how to stimulate and enforce every node in the network to be cooperative. Due to the unreliable nature of the wireless channel, the cooperation enforcement design covers both homogeneous and heterogeneous channel conditions. In the former scenario, we derive the necessary and sufficient conditions to achieve cooperation with various strategies. We also examine the cooperation enforcement process with evolutionary game theory by proposing an anti-collusion game. Our analysis shows that any strategy that resists collusion will lead to full cooperation in the network. In the latter scenario, we model the effect of heterogeneous unreliable channel as imperfect private monitoring in the game. We propose a state machine based strategy that ensures

the cooperative actions are the sequential equilibrium. In addition, extensions are made to the strategy profile so that it can also enforce cooperation in a multi-hop wireless network.

Our discussion on mitigating the misbehavior continues with the presence of malicious attacks in the network. Since the malicious nodes bear the goal to cause harm to the network, it does not fall into the scope of cooperation enforcement schemes. Because the malicious node can camouflage as regular nodes when it is not attacking, we devise a Bayesian detection game to model the malice detection process. As the detection process goes, the regular node that monitors updates its belief on the identity of the malicious node. This problem gets complicated when we consider the channel unreliability that affects the observation accuracy. We further study the even more complicated problem when the countermeasures are available to the malicious node, i.e., the malicious node can also study the games and form beliefs about whether its identity has been revealed. Equilibrium solutions are obtained to show the properties of the detection process. Unlike other methods that isolate the malicious nodes upon detection, we argue that it is beneficial to keep them in the network as long as they can be taken advantage of. Hence, we formulate a post-detection game and derive the equilibrium that enables regular and malicious nodes to coexist. Moreover, we also obtain the expected time when the malicious node should not be kept any longer.

Our analysis is backed by extensive simulations. The experimental study not only validates our design notion, but also shows the properties of our solutions. In the anti-collusion game with homogeneous unreliable channel, we illustrate the effects of initial population share, channel unreliability, and payoff matrix on the convergence of cooperation evolution.

129

Under heterogeneous lossy channel scenarios, the simulation results illustrate the efficiency of the proposed state machine based forwarding strategies. In addition, network throughput performance is measured with respect to parameters like channel loss probability, route hop count and mobility. Results suggest that the performance due to our proposed strategy is in close agreement with that of unconditionally cooperative nodes. In the study of coexistence, through simulation, we show that the coexistence equilibrium helps to extend the length of the games and improves the throughput of the network. Experimental results also indicate that with the help of the proposed nested belief system, the malicious node is able to adjust its strategy in the game and finally the detection game and post-detection game are integrated with effective transition.

The research presented in this dissertation also serves as a starting point for future research in the subject of misbehavior identification and mitigation. For example, our research on malicious node detection game only considers single user detection, therefore, the channel condition is invariant. In follow-up work, networked detection scheme can be designed such that every regular node in the network can participate in the detection process and share their observations. In a networked scenario, the channel conditions are heterogeneous and cooperation among all regular nodes are desirable. From this perspective, the findings in Chapter 4 might be applicable. Nonetheless, many issues remain open, e.g., the channel unreliability effects on the information exchange among regular nodes, the topology dynamics when the nodes are mobile, and unbalanced data flows. Furthermore, the solutions proposed in the research and their properties can provide insights to other similar security methods,

because in our approach, we focus on the perspective of individual nodes and the solutions obtained herein reach the equilibrium in the network.

LIST OF REFERENCES

[1] D. Abreu, D. Pearce and E. Stacchetti, "Towards a theory of discounted repeated games with imperfect monitoring", *Econometrica*, 58, pp. 1041-1064, 1990.

[2] A. Agah, S. K. Das, K. Basu and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach", Proceedings of *IEEE NCA 2004*, pp. 343-346.

[3] L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents", Proceedings of *ACM Mobicom 2003*, pp. 245-259.

[4] E. Altman, V. S. Borkar, A. Kherani, P. Michiardi and R. Molva, "Some Game-Theoretic Problems in Wireless Ad-Hoc Networks", Proceedings of *EuroNGI Workshop 2004*, pp. 82-104.

[5] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks", *Tech. Report*, Standford University, 2003.

[6] D. Bertsekas, "Dynamic Programming and Optimal Control", *Athena Scientific*, Belmont, MA, 2001.

[7] V. Bhaskar and I. Obara, "Belief-based equilibria in repeated prisoners' dilemma with private monitoring", *Journal of Economic Theory* 102, pp. 40-69, 2002.

[8] L. Blazevic, L. Buttyán, S. Capkun, S. Giordiano, J.P. Hubaux, and J.Y. Le Boudec, "Self-organization in mobile ad-hoc networks: the approach of terminodes", *IEEE Communications Magazine*, 39(6), pp. 166-174.

[9] S. Buchegger and J. L. Boudec, "Performance analysis of the confidant protocol: Cooperation of nodes- fairness in dynamic ad-hoc networks", Proceedings of *ACM MobiHoc 2002*, pp. 226-236.

[10] L. Buttyán and J. P. Hubaux, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks", *Tech. Report EPFL*, 2001.

[11] L. Buttyán and J. P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs", Proceedings of *ACM Mobihoc 2000*, pp. 87-96.

[12] L. Buttyán and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad-hoc networks", *ACM/Kluwer Mobile Networks and Applications*, 8(5), pp. 579-592.

132

[13] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modeling incentives for collaboration in mobile ad hoc networks", *Performance Evaluation*, 57(4), pp. 427-439.

[14] M. Felegyhazi, J.-P. Hubaux and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks", *IEEE Trans. on Mobile Computing*, 5(5), pp. 463-476.

[15] M. Feldman, J. Chuang, I. Stoica and S. Shenker, "Hidden-action in multi-hop routing", Proceedings of *ACM E-Commerce 2005*, pp. 117-126.

[16] D. Fudenberg and J. Tirole, *Game Theory*, MIT press, Cambridge, MA, 1991.

[17] J. J. Jaramillo and R. Srikant, "DARWIN: distributed and adaptive reputation mechanism for wireless ad-hoc networks", Proceedings of *ACM MobiCom 2007*, pp. 87-97.

[18] Z. Ji, W. Yu and K. J. R. Liu, "Cooperation enforcement in autonomous MANETs under noise and imperfect observation", Proceedings of *IEEE SECON 2006*, pp. 460-468.

[19] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", *Mobile Computing*, pp. 153-181, *Kluwer Academic Publishers*, 1996.

[20] M. Kandori, "Introduction to repeated games with private monitoring", *Journal of Economic Theory* 102, pp. 1-15, 2002.

[21] M. Kandori and I. Obara, "Efficiency in repeated games revisited: the role of private strategies", *Econometrica* 74(2), pp. 499-519, 2006.

[22] B. Karp and H. T. Kung, "Greedy Perimeter Stateless Routing for Wireless Networks", Proceedings of *ACM/IEEE Mobicom 2000*, pp. 243-254.

[23] M. Kodlialam and T. V. Lakshman, "Detecting network intrusion via sampling: a game theoretic approach", Proceedings of *IEEE Infocom 2003*, pp. 1880-1889.

[24] D. M. Kreps and R. Wilson, "Sequential Equilibria", *Econometrica* 50(4), pp.863-894, 1982.

[25] F. Li and J. Wu, "Hit and Run: A Bayesian Game Between Malicious and Regular Nodes in MANETs", Proceedings of *IEEE SECON 2008*, pp. 432-440.

[26] X. -Y. Li, Y. Wu, P. Xu, G. Chen and M. Li, "Hidden Information and Actions in Multi-Hop Wireless Ad Hoc Networks", Proceedings of *ACM Mobihoc 2008*, pp. 283-292.

[27] H. Lin, M. Chatterjee, S. K. Das and K. Basu, "ARC: An Integrated Admission and Rate Control Framework for Competitive Wireless CDMA Data Networks Using Non-cooperative Games", *IEEE Trans. on Mobile Computing*, 4(3), pp. 243-258, 2005.

[28] P. Liu, W. Zhang and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives, and strategies", *ACM Trans. on Information and System Security*, 56(3), pp. 78-118, 2005.

[29] Y. Liu, C. Comaniciu and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks", Proceedings of *ACM GameNets 2006.*

[30] A. B. Mackenzie and S. B. Wicker, "Game theory and the design of self-configuring, adaptive wireless networks", *IEEE Communication Magazine*, Nov. 2001, pp. 126-131.

[31] A. B. Mackenzie and L. A. DaSilva, *Game Theory for Wireless Engineers*, San Rafael, California: Morgan & Claypool Publishers, 2006.

[32] R. Mahajan, M. Rodrig, D. Wetherall and J. Zahorjan, "Sustaining cooperation in multi-hop wireless networks", Proceedings of *NSDI 2005*, pp. 231-244.

[33] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", Proceedings of *ACM Mobicom 2000*, pp. 255-265.

[34] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", Proceedings of *Communication and Multimedia Security Conference 2002*, pp. 107-121.

[35] P. Michiardi and R. Molva, "Analysis of coalition formation and cooperation strategies in mobile ad hoc networks", *Ad Hoc Networks*, 3(2005), pp. 193-219.

[36] P. Michiardi and R. Molva, "A game theoretical approach to evaluate cooperation enforcement mechanisms in mobile ad hoc networks", Proceedings of *WiOpt* 2003.

[37] F. Milan, J. J. Jaramillo and R. Srikant, "Achieving cooperation in multihop wireless networks of selfish nodes", Proceedings of *ACM GameNets 2006.*

[38] M. J. Osborne, "An introduction to Game Theory", *Oxford University Press*, New York, NY, 2004.

[39] M. T. Refaei, V. Srivastava, L. DaSilva and M. Eltoweissy, "A reputation-based mechanism for isolating selfish nodes in ad hoc networks, Proceedings of *Mobiquitous 2005*, pp. 3-11.

[40] E. M. Royer and C. E. Perkins. "An Implementation Study of the AODV Routing Protocol", *IEEE WCNC 2000*, pp. 1003-1008.

[41] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks", Proceedings of *IEEE Infocom 2003*, pp. 807-817.

[42] G. Theodorakopoulos and J. S. Baras, "Malicious Users in Unstructured Networks", Proceedings of *IEEE Infocom 2007*, pp. 884-891.

[43] J. Ratliff, http://www.virtualperfection.com/gametheory.

[44] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, NJ, 1944.

[45] W. Wang, S. Eidenbez, Y. Wang and X.-Y. Li, "OURS: Optimal unicast routing system in non-cooperative wireless networks", Proceedings of *ACM Mobicom 2006*, pp. 402-413.

[46] W. Wang, X.-Y. Li and Y. Wang, "Truthful multicast routing in selfish wireless networks", Proceedings of *ACM Mobicom 2004*, pp. 245-259.

[47] W. Wang, M. Chatterjee and K. Kwiat, "Cooperation enforcement in ad hoc networks under unreliable channel", Proceedings of *IEEE MASS 2008*, pp. 456-462.

[48] J. W. Weibull, "Evolutionary Game Theory", *MIT Press*, Cambridge, MA, 1995.

[49] W. Yu and J. K. R. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks", *IEEE Trans. on Mobile Computing* 6(5), pp. 507-521, 2007.

[50] J. Zhang and Q. Zhang, "Stackelberg Game for Utility-Based Cooperative Cognitive Radio Networks", Proceedings of *ACM Mobihoc 2009*, pp. 23-32.

[51] S. Zhong, J. Chen and Y. Yang, "Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks", Proceedings of *IEEE Infocom 2003*, pp. 1987-1997.

[52] S. Zhong, L. Li, Y. Liu and Y. Yang, "On Designing Incentive-Compatible Routing and Forwarding Protocols in Wireless Ad-Hoc Networks—An Integrated Approach Using Game Theoretical and Cryptographic Techniques", Proceedings of *ACM Mobicom 2005*, pp. 117-131.

[53] S. Zhong and F. Wu, "On designing collusion-resistant routing schemes for non-cooperative wireless ad hoc networks", Proceedings of *ACM MobiCom 2007*, pp. 278-289.

[54] Q. Zhu, C. Fung, R. Boutaba and T. Başar, "A Game-Theoretical Approach to Incentive Design in Collaborative Intrusion Detection Networks", Proceedings of *GameNets 2009*, pp. 384-392.