EVOLUTIONARY GAMES

APPLICATIONS TO SECURITY AND RESOURCE ALLOCATION IN NETWORKS

By

AHMED A. ALABDEL ABASS

A dissertation submitted to the

School of Graduate Studies

Rutgers, The State University of New Jersey

In partial fulfillment of the requirements

For the degree of

Doctor of Philosophy

Graduate Program in Electrical and Computer Engineering

Written under the direction of

Narayan B. Mandayam and Zoran Gajic

And approved by

_____

_____

_____

_____

New Brunswick, New Jersey

October, 2018

ABSTRACT OF THE DISSERTATION

Evolutionary Games

Applications to Security and Resource Allocation in Networks

By AHMED A. ALABDEL ABASS

Dissertation Director:

Narayan B. Mandayam and Zoran Gajic

Modern life is getting more complicated and people rely more on the intelligence embedded in their electronic gadgets. It is expected these gadgets will take larger roles in making, at least some simple, decisions instead of us. It is not difficult to see how many gadgets will be needed in an Internet of Things environment, or smart home settings, or any sort of connected devices. Interaction among these devices can be addressed using game theoretical models. However for a large number of devices interacting/playing with each other, the classical game models can be complicated. One way to approach this problem is by using evolutionary game theory (EGT). Evolutionary games deal with large number of players by making assumptions such as some common similarities in the players' interests, payoffs, and bounded rationality. Both of these assumptions seem to fit in modeling the large number of players'/devices' interaction. On the other hand, evolutionary games can model the user behavior in taking decisions when repeatedly played. Meaning that, each time a player does a move, the player observes the payoff and can compare it with the average payoff, and in the next play the player can choose a different move if it gives higher payoff and so on so forth. By using the concept of replicator dynamics, evolutionary games make it possible to observe how the choice dynamics is made. It can be looked at as learning until reaching to a very stable choice which is an evolutionary stable choice.

This thesis first presents the problem of communications under a denial of service attack through a jamming threat. We consider the problem where the players try to communicate with a base station under the threat of jammers who, possible cooperatively, try to block their communications. The users have the option to work cooperatively too. The second problem this thesis deals with a generalized network model known as ephemeral network under the threat of a malicious attack with the absence of any central authority. The only control to the network is a set of rules which are agreed upon before setting a connection. Thirdly, we study the problem of advanced persistent threats (APTs), which is the problem of a powerful and stealthy attacker who wants to infiltrate the system. Evolutionary game theory is used by giving the players, the APT attacker and the system defender, the opportunity to adapt their decisions according to the replicator dynamics to reach to the robust decision,i.e, to choose the defend/attack strategy.

The final part of this work uses evolutionary game theory to model the coexistence between WiFi and LTE-U technologies. We consider a scenario where there are two heterogeneous populations, one population represents the set of LET-U APs and the other one represents the set of WiFi AP. Furthermore, we assume that AP's belong to the same population do not interfere with each other. We study, under a given set of transmission strategies, the stability of the strategies that can appear in such a conflict. We specify the conditions under which, a coexistence with minimal interference can be established.

Acknowledgements

I would like to thank my advisers Prof. Narayan B. Mandayam and Prof. Zoran Gajic for their guidance and support throughout my graduate study and research at WINLAB, Rutgers University. Their encouragement during different stages of my Ph.D. gave me the opportunity to explore and learn valuable aspects of applying evolutionary game theory to solve problems related to wireless communications.

I am thankful to my WINLAB labmates and my friends for supporting me during this journey.

I thank Prof. Wade Trappe and Prof. Melike Baykal-Gürsoy for being on my dissertation defense committee and for their suggestions and comments on earlier draft of this dissertation. I would like also to thank Prof. William Sandholm from University of Wisconsin-Madison for detailed discussions on evolutionary game theory.

I deeply thank my first teachers, my parents Abdelhadi Fadhil and Nadwah Abdulhasan, the people who taught me to unconditionally love and help others, your prayers were with me all the time. Thank you to my brothers Osama and Mustafa, and my sister Safa for all the love and support during the toughest of times.

Lastly, thank you so much to my kids Fadhl, Yusur, and baby Dur. Nothing could have been done or enjoyed without their presence in my life. Their unconditional love and unlimited beautiful smiles and fight made me feel so strong and so blessed. To my wife Zainab, no words are enough to acknowledge the value of her support to me. Thank you so much.

My graduate work is supported by the Higher Committee for Education Development in Iraq (HCEDIraq), the Iraqi Ministry of Higher Education and Scientific Research represented by University of Thiqar, and the Electrical Engineering Dept. at Rutgers. I am very thankful for their funding.

Dedication

To my parents, my wife, and my kids.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Security of wireless networks, data centers, or any other cyber physical system is a necessity that is not new or temporary. It has been an attractive area of research for many researchers around the globe. Incidents of attacks against different systems are too many to count. Starting from eavesdropping wireless communication systems, creating denial of service attacks, intruding networks to gain access to sensitive information, attacking data centers, attacking industrial systems, and even manipulating the governmental election systems. The attackers can range from students who want to get fame, as with the case of Rutgers DDoA which lasted from Fall, 2014 to Fall 2016 [4], to army special units which use jammers to disarm explosives [5].

Furthermore, current evidences show attacks which are organized by countries against others. For example, Gueye has mentioned in [6], based on a Symantec white paper, that a virus called Stuxnet was targeting industrial control systems possibly in Iran. However, some security specialists suspected that Stuxnet was designed in Israel to sabotage the Iranian nuclear power plants. On the other hand, Iran launched its attack which is known by Thamar reservoir [7] in which, and according to Clearsky in Israel, several different attacks aiming for taking over the victim's email account and computer. Another attack example is reported by Kaspersky Labs in [8], the Dark Hotel, where the attackers get control over some hotels' networks, then they used these infected networks to get access to the hotels' guests computers. According to Kaspersky Labs, this attack was there since 2007 and is still active now. The last attack was not to sabotage the system or to jam the signal. Instead, it was to get information from the victims and to stay in their systems.

The last two attacks bring more sophistication to the network/system defender,

and this is the reason for calling them Advanced Persistent Threats (APTs). An APTs attack is a well funded, powerful and long term attack. Some strategies for 22 APTs attack campaigns are given in [9]. APTs attacks are now under the investigation of many researchers and security labs, because of their huge damages.

Aside from jamming a wireless network or performing a stealthy APTs attack, other types of attacks emerged as the world is getting more connected. Smart cities, smart grids, smart homes, Internet of Things (IoT), machine to machine communications,and so on are terms that we hear each day. All these connections need to be secured. How can we build a central authority (CA) system to ensure the security of these connections? Can these smart devices agree on protocols to defend themselves? Why will these devices cooperate? If these devices are smart, then how will they respond to a smart attacker(s)? Is it possible for an attacker to gain access through the cloud to the victims heart pump or Insulin pump? These are new challenges which were not on the surface 10 years ago.

Fortunately, there are always new models and approaches to deal with security problems. New approaches come from the hardware capabilities, understanding new mathematical models, and software advancements. Game theory represents a natural candidate to solve problems of conflict. It captures the behavior of the competitors to reach a feasible solution. In wireless networks, the players, people or devices, compete to gain the network resources. It is difficult to build a controller that can manage all the interaction scenarios. Game theory enables the players to reach to a solution called Nash Equilibrium, in a decentralized way since it can be considered as a distributed optimization tool. However, networks have many players that makes the extension of two-player game model challenging.

On the other hand, if the game is played over some time interval, the players may change their behavior and, subsequently, their actions. As a result, there is some dynamic behavior that needs to be addressed.

One solution is to use Evolutionary Game Theory (EGT) to model these problems. Nash mentioned EGT [10] in his dissertation and called it the mass-action. In page 21

of his dissertation, Nash made three assumptions about the players, and later he considered them as populations. Specifically, he assumed it is unnecessary for the players to have the ability of any complex thinking, and the players are supposed to accumulate empirical knowledge on the advantages of their pure strategies. The absence of complex thinking enables judging the behavior of many players in the population by analyzing the behavior of two players. In addition, the accumulated empirical knowledge can be interpreted as the use of the of some dynamics, later will be known as replicator dynamics, to reach to the best strategy.

Specifically, evolutionary games can capture the action of many players over a period of time that gives the players the chance to observe their behavior and adjust it. The dynamic part of the game can be looked at as a learning tool that is being used by the players to refine their decisions. At the same time, evolutionary games can be used between two players where each player can adjust her decision according to their past cumulative experience to reach to a robust decision.

In the first part of this thesis, we study the problem of cooperative users who want to communicate with a base station in the presence of cooperative jammers. Then we address the security problem of short life networks called ephemeral networks. These networks consist of nodes connected in a decentralized way, and the nodes have to defend themselves against intruder(s). Finally, we address the APTs attack problems on data center(s). The second part of the dissertation studies the coexistence interaction between a WiFi access point and LTE-U node. The WiFi AP controls its downlink power level, while the LTE-U AP controls its duty cycle and downlink power. We model this interaction as a noncooperative evolutionary game.

1.1 Distributed Denial of Service Attacks in a Wireless Network Evolutionary Game [1]

We consider a wireless network of M users connected to an access point in the presence of N jammers whose purpose is to deny or degrade the performance of the users by injecting interference. Using the achieved signal to inference plus noise ratio (SINR) as

the performance metric, we study the dynamics of such a distributed denial of service attack (DDoA) by using Evolutionary Game Theory (EGT). Specifically, we consider a cooperative network model, where the M users (and N jammers) can collectively enhance their achieved SINR (degrade the user SINR). We model the strategic transmission decisions of the users (and the jammers) using simple random access techniques where the users (and jammers) decide to transmit or not with a transmission probability, taking into account their energy costs. Using the replicator dynamics (RD), we characterize the evolutionary stable strategies (ESS's) of the game and observe that the resulting transmission probabilities turn out to be either 0 or 1. Further, given a network (channel) setting, we show using a phase portrait of the replicator dynamics how the ESS strategies evolve for different cooperation levels of the users and jammers populations. We also provide insights into resulting ESS strategies as a function of the number of users and jammers, and their channel qualities. The results are presented in Chapter 3.

1.2 Threat Revocation in Ephemeral Networks [2]

We consider a wireless network of M nodes connected together in a decentralized way (for example as an ad hoc network), and according to pre-specified rules. There are other malicious node(s) which can be either inserted or infected which are trying to disturb the operation of the network. The nodes are cooperating to defend the network (and eventually themselves) by isolating the misbehaved node(s). We approach this problem using Evolutionary Game Theory (EGT), and characterize the robust equilibrium point(s) for this game. The game is formulated such that all the nodes take part in the decision process to avoid problems caused by unsuccessful revocation or over reacted revocation decisions. Each node in the network (interchangeably called benign node to distinguish it from the malicious node or the intruder) has three decisions to make: (a) abstain or do nothing; (b) self-sacrifice by disconnecting the intruder and itself; and (c) voting to isolate the intruding node. Each decision has its advantages and disadvantages and the Replicator Dynamics (RD) is used to show the dynamics of the nodes' decisions. By simulating the RD equation, two different cases emerge as

Evolutionary Stable Strategies (ESS) where one of them is the desired ESS, and the other is not. Phase portrait diagrams are used to characterize the fraction of the M nodes needed to choose each one of these ESS's, the rate of convergence, and the effect of increasing the cooperation rewards. The results obtained are presented in Chapter 4.

1.3 Advanced Persistent Threats [3]

Advanced Persistent Threats (APTs) represent stealthy, powerful, long term, and well funded attacks against cyber systems, such as data centers and cloud storage. Evolutionary game theory is used to capture the long term continuous behavior of APTs on cloud storage devices. Two APT defense games with discrete strategies are formulated, in which both an APT attacker and a defender compete to control one or multiple storage devices regarding their attack or defense intervals. The dynamical stability of each defense and attack strategy pair is studied according to the replicator dynamics criteria to characterize the locally asymptotically stable equilibrium strategies. The Evolutionary stable strategy is discussed in each game, which is a subset of the asymptotically stable Nash Equilibrium (NE). The phase portraits provide the locally asymptotically stable points of the APT defense game, which represent the NE showing the relationship between the asymptotic stability and evolutionary stability. The analysis and experimental results are presented in Chapter 5.

1.4 Coexistence between LTE- and WiFi

Coexistence between different wireless communication technologies is a necessity which stems from the need for dynamic spectrum sharing between users. We study the spectrum coexistence problem between the LTE-U and the WiFi technologies using using evolutionary game theory (EGT). Specifically, we study the effect of the transmission cost on each LTE AP (eNodeB) and WiFi AP and find the conditions under which long term coexistence can be established. We model this long term coexistence by finding the evolutionary stable strategies (ESSs) of the evolutionary game. We analyze the cost

functions for the LTE-U and the WiFi APs, and show that the LTE-U AP behavior is more sensitive to the cost than to the number of users, while WiFi is more sensitive to the number of users than to the transmission power cost. We also consider the case where the WiFi AP removes users that can not establish the minimum SINR required in order to reduce the interference to the LTE-U AP users. Interestingly this creates more interference due to the aggressive/selfish behavior of the WiFi APs. We solve this problem by introducing a modified cost function. Finally, we formulate a classical game theoretic model for the coexistence problem, find its Nash equilibrium (NE), and study its stability under the Replicator Dynamics (RD) of the evolutionary game. The results obtained are presented in Chapter 6.

Chapter 2

Introduction to Evolutionary Game Theory

Evolutionary games are used to model the behavior of large number of players under certain assumptions. If all the players have the same interests, and suffer the same loses then they can be grouped in one population. Examples of this case can be users who try to associate themselves with base stations that give them better quality of service. This type of games is called symmetric games. In symmetric games, if the players get the same payoff regardless of their role in the game, then the game is called doubly symmetric game. The payoff matrix is symmetric in the case of doubly symmetric games [11]. The other class of evolutionary games is asymmetric games where players have different payoffs according to their role in the game. Examples of this is the case of the game between users and jammers. For two roles, we have a bimatrix game which also can be used to represent a game between two populations with excluding the intra-specific interaction, i.e, users compete with jammers in that game and there is no user-user competition [12].

It is well known that each mixed-strategy game has an NE [13],i.e, the players choose their strategies with a probability $\mathbf{p}$. The probability vector $\mathbf{p}$ has the usual probability properties, i.e, $p_i \geq 0$ and $\sum_{i=1}^{n} p_i = 1$. As a result, a strategy corresponds to a point $\mathbf{p}$ in $\mathbb{S}^n$. Assume that the players in the population were playing one of two pure strategies, E_1 and E_2, according to probability vectors $\mathbf{p}$ and $\mathbf{q}$. A population that uses the strategy E_1 is said to be evolutionary stable, if when a small part (ϵ) of it switches to the strategy E_2, the strategy E_1 keeps giving its players higher payoff. In equations, let the payoff function for each player be denoted as $u(E_1, E_1)$, then the strategy E_1 is an evolutionary/evolutionarily stable strategy (ESS) (will resist the

mutant or invading strategy E_2) if

$$u(E_1, \epsilon E_1 + (1-\epsilon)E_2) > u(E_2, \epsilon E_1 + (1-\epsilon)E_2) \tag{2.1}$$

for all sufficiently small ϵ. The conditions under which the ESS exists are given by the following:

Theorem 1 [14]: *For a population* Γ*, where each player has a set of* n *pure strategies* $E_i,\ 1 \leq i \leq n$*, the mixed strategies* $\mathbf{p}$ *and* $\mathbf{q}$ *in the game with an associated payoff matrix* A*. The strategy* $\mathbf{p} \in \mathbb{S}^n$ *is an ESS if and only if:*

$$\mathbf{p}^T A\mathbf{q} > \mathbf{q}^T A\mathbf{q} \tag{2.2}$$

for all $\mathbf{p} \neq \mathbf{q} \in \mathbb{S}^n$.A population Γ contains the players of the same interests, and apply the same strategies. Each player has a set of pure strategies $E_i,\ i = 1, .., n$. Each player chooses each of the n strategies with a probability p_i. Sometimes we use the alternative equivalent ESS conditions from [15] to simplify the calculations. If we define $A = Q$ to be the payoff matrix, then the above conditions can be rewritten as:

(1) Equilibrium condition: $\mathbf{f}_\sigma = \sigma^{\star T} Q \sigma^{\star T} - \sigma^{\star T} Q \sigma > 0$

(2) Stability condition: if $\mathbf{f}_\sigma = 0$, then $\mathbf{g}_\sigma = \sigma^{\star T} Q \sigma - \sigma^T Q \sigma > 0$ over all mixed strategies vectors σ in the neighbor of the ESS strategies $\sigma^\star$. The first condition is the definition of NE that the strategy $\sigma^\star$ is the best reply to itself. However, this condition by itself does not guarantee the ESS, because it allows another alternatives best response if $\mathbf{f}_\sigma = 0$ [16]. The stability condition assures that the incumbent strategy, $\sigma^\star$, do better than the mutant strategy,σ, against itself.

For two populations, we have asymmetric (bimatrix) game, and Theorem 2 below provides the ESS existence conditions.

Theorem 2 [14]: *The ESS for two populations* Γ *and* Θ *with pure strategies* $E_i,\ i = 1, .., n$*, and* $F_j,\ j = 1, .., m$*, with payoff matrices* A *and* B *respectively, is the strategy* $(\mathbf{p}^*, \mathbf{q}^*)$ *where* $\mathbf{p}^* \in \mathbb{S}^n$ *and* $\mathbf{q}^* \in \mathbb{S}^m$ *that satisfies:* ${\mathbf{p}^*}^T A\mathbf{q}^* > \mathbf{p}^T A\mathbf{q}^*$*, for all* $\mathbf{p} \in \mathbb{S}^n$ *and* $\mathbf{p} \neq \mathbf{p}^*$*, and,* ${\mathbf{q}^*}^T B\mathbf{p}^* > \mathbf{q}^T B\mathbf{p}^*$*, for all* $\mathbf{q} \in \mathbb{S}^m$ *and* $\mathbf{q} \neq \mathbf{q}^*$*, where* $\mathbf{p}$ *and* $\mathbf{q}$ *are the probability vectors over the pure strategies of the two populations* Γ *and* Θ*, respectively.*

Evolutionary games can be dynamically characterized using the replicator dynamics (RD) which are a set of nonlinear differential equations that capture the evolution of the strategies in the population. RD can be thought of a set of learning rules used by the players to shape their strategy choices. At each time, a player compares her payoff with the average payoff in the population and change her strategy each time. The RD has a wide range of applications because of its simplicity and practicality. The RD for one population evolutionary game is given as:

$$\dot{p_i} = p_i[u(p_i, \mathbf{p}) - \overline{u}] \tag{2.3}$$

$$\overline{u} = \sum_{i=1}^{n} p_i u(p_i, \mathbf{p}), \tag{2.4}$$

where the initial conditions are $p_i(0) = p_{i,0}$ over all possible strategies. The differential equation (2.3) says that at any time, the number of users (the user strategy preference) who are using strategy p_i can increase or decrease by comparing the payoff to the average payoff given in formula (2.4). For the case of more than one population, the RD systems of equations will be expanded to take in consideration the probabilities of choosing the other strategies in the other populations.

2.1 Relation between Asymptotic Stability and Evolutionary Stability

Any asymptotically stable[1] strategy (point) is a NE, but the reverse does not hold in general. Any ESS is a NE, and the reverse does not hold in general. Any strict NE is an ESS and vice versa, see for example [11, 16]. Specifically, for a one population game with more than two strategies, asymptotic stability does not guarantee evolutionary stability (see for example the game proposed by Zeeman [15], and mentioned in [17]). If we have one population with each player has a symmetric payoff function and the payoff matrix is symmetric, the asymptotic stability implies evolutionary stability [17].

[1]Asymptotic stability means any solution that starts near the equilibrium point converges to that equilibrium point. Here we refer to local asymptotic stability. Local stability in this work is used, because there are multiple equilibrium points, where each equilibrium point has a specific region where all solutions inside that region convergence to it. Formally, this region is called the region of attraction (RoA).

The ESS is more stable than the local asymptotic stability, and thus a Zeeman's game shows that the region of attraction of the ESS is larger than that of the regular attractor (asymptotically stable point) [15]. Furthermore, symmetric games can admit a mixed strategy as an ESS, but it has to be unique.

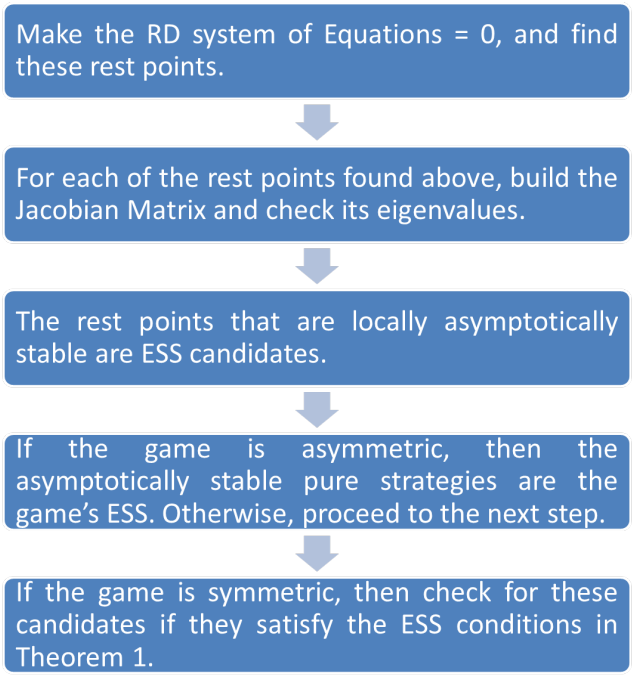


Figure 2.1: Flowchart to find the ESS in the evolutionary game with multiple strategies.

On the other hand, in asymmetric/two population games the asymptotic stability also implies evolutionary stability [12]. Finally, mixed strategies are always unstable in asymmetric games [16].

A general procedure for finding the ESS of any evolutionary game with more than two strategies is shown in Fig.2.1.

Chapter 3

Distributed Denial of Service Attacks in a Wireless Network Evolutionary Game

3.1 Introduction

Wireless networks are prone to many attacks because of the inherent openness of the transmission medium. One of these attacks is the distributed denial of service attack (DDoA). A malicious node (device, or user) can perform DDoA by jamming another node's (user or device) transmission by degrading its signal quality and denying correct reception at the intended receiver. This problem can be formulated as a game between the user(s) and the jammer(s), and it has been studied extensively in the literature. The more general scope of this problem is within the physical layer security framework where signal processing approaches, and error correcting codes are used to solve this problem, see for example [18], and the references therein. Statistical signal processing techniques that take advantage of the radio channel properties are shown to mitigate attacks against wireless networks in [19, 20]. However, these methods often use centralized approaches that optimize various transmission parameters and receiver techniques [21]. On the other hand, game theory (both cooperative and noncooperative) provides a distributed optimization solution to the above problem [22]. Static game theoretic approaches typically characterize the stable operating points (equlibria) as well as the strategies chosen by the users and jammers to achieve these. In this chapter, we are interested in studying the dynamics of such DDoA in a network (population) consisting of a collection of users and jammers when each of the populations are allowed to cooperatively transmit (and jam). Specifcally, we will use Evolutionary game Theory (EGT) [23] to study the dynamics of DDoA in a wireless network with M users connecting to an access point in the presence of N jammers whose goal is

disrupt the user transmissions. The chapter is organized as follows. A brief review of related work is provided in Section 6.2. Section 4.3 gives the details of the problem formulation and the parameter derivations. Simulation results are given in Section **??**, and we conclude in Section 6.6.

3.2 Related work

Evolutionary Game Theory has been used to study the dynamics of wireless networks in many competing situations [24–30]. These situations range from radio resource management among competing users for rate adaptation, base station assignment and spectrum sharing, to routing in mobile networks as well pricing of wireless resources. In almost all of the above cases, the models result in symmetric games where all users optimize the same utility function, typically get identical rewards and face similar costs. In this chapter, we consider a setting where the underlying model involving users and jammers inherently results in an asymmetric situation regarding the rewards and costs. Earlier work in [31] has considered secrecy rate adaptation using a EGT formulation but the model considered there is quite different from the one under consideration here. Specifically, in this work, we formulate a doubly asymmetric evolutionary game between two populations (users and jammers) and implicitly solve the evolutionary stable strategies for the game using a potential function formulation. Besides EGT formulations, there have been many efforts that consider static formulations of user and jammer interactions (see e.g. [32–38]).

3.3 Problem Formulation

We consider a single-cell system with M users connected to a base stations (BS) in the presence of N jammers. The jammers launch an attack by transmitting signals (with some probability) that interfere with the users' transmissions, there by reducing their $SINR$ while incurring a transmission cost. The users on the other hand decide (with some probability) either to transmit or not. Further, we consider a cooperative network model where the M users (and N jammers) can collectively enhance their

achieved $SINR$ (degrade the user $SINR$). The M-users and the N-jammers form two different populations with conflicting goals. The users are trying to enhance their $SINR$ at the BS, while the jammers are launching their attack to lower the users' $SINR$. This conflict is modeled using Evolutionary Game Theory (EGT), where the sets of player of strategies are to transmit or to not, and the sets of payoffs consist of the rewards that are represented by the difference between the achieved $SINR$ and the transmission cost. At any time instant, some players (users or jammers) are transmitting, while the others are not. After several interactions, the initial transmitting portion of the players will change and settle at a stable point. This point is a potential evolutionary stable strategy (ESS) for the game. This evolution from the initial population to the stable population is captured by the concept of Replicator Dynamics (RD) [11, 17, 23]. At this stability point, no one can do better by deviating from this equilibrium point. This equilibrium point is known as Nash Equilibrium (NE), but with the addition of the condition of being stable against small population deviations from this NE, it will evolve to an ESS.

3.3.1 Cooperative Users vs. Cooperative Jammers

Cooperation among players means that all the players in a certain population have an objective function that they are trying to maximize. In the context of the communication model, it implicitly implies that all users are delivering joint messages for each other. If the users' population succeeds in forcing the jammers' to stop jamming (by making the jamming cost higher than its reward), then all users benefit from this, and the same motivation holds for the jammers' population. Assume that players (users and jammers) in each population are cooperating to transmit their signal. As the number of the participating players in transmissions increases, the $SINR$ for each player will increase, but at the price of additional transmission cost. The channel coefficients play an important role to enhance the $SINR$ and add uncertainty to the players' payoffs. Thus players learn from their past moves through the RD learning process.

Users' utility function formulation

Let the utility of user i when the user chooses to transmit be:

$$U_{Tx_i|T} = \frac{h_i P_i + \rho \sum_{k=1,k\neq i}^{M} h_k P_k}{\sigma^2 + \delta \sum_{j=1,}^{N} h'_j P'_j} - C_u(P_i + \rho \sum_{k=1,k\neq i}^{M} P_k) \tag{3.1}$$

h_i's and h'_j's are the channel coefficients between the users and the base station, and between the jammers and the base station, respectively. ρ and δ are the probabilities (portions of community) that the users and the jammers are transmitting, respectively. This is the same as saying that when user-i starts transmitting, there is a portion ρ of other users who are transmitting and helping her to increase her SINR (the same holds for the jammers). C_u is the cost that users pay for transmitting. σ^2 is the noise power. Because of the users' cooperation (the same argument holds for the jammers, as will be shown later) the utility function for each user in equation (5.4)can be written as the average utility: $U_{Tx|T} = \frac{1}{M} \sum_{i=1}^{M} U_{Tx_i|T}$. After some manipulations, we get the following expression:

$$U_{Tx|T} = \frac{\frac{(\rho(M-1)+1)}{M} \sum_{k=1}^{M} h_k P_k}{\sigma^2 + \delta \sum_{j=1,}^{N} h'_j P'_j} - C_u(\frac{(\rho(M-1)+1)}{M} \sum_{k=1}^{M} P_k) \tag{3.2}$$

Let the utility of the user i and the average utility of the population in the not-transmit case be:

$$U_{Tx_i|NT} = \frac{\rho \sum_{k=1,k\neq i}^{M} h_k P_k}{\sigma^2 + \delta \sum_{j=1,}^{N} h'_j P'_j} - C_u(\rho \sum_{k=1,k\neq i}^{M} P_k) \tag{3.3}$$

$$U_{Tx|NT} = \frac{\frac{(\rho(M-1))}{M} \sum_{k=1}^{M} h_k P_k}{\sigma^2 + \delta \sum_{j=1,}^{N} h'_j P'_j} - C_u(\frac{(\rho(M-1))}{M} \sum_{k=1}^{M} P_k) \tag{3.4}$$

There are two reasons for writing the utility as shown in equations (**??** and **??**). The first is to convert the game from doubly asymmetric to asymmetric. In other words, to unify the users' goal, because they share the same motivation and also because the presence of different channel coefficients is an undesired technicality. The latter is undesirable since it destroys the intuition behind constituting the users' population which should contain the players with the same interest. The second reason is mathematically justifiable, that is, the average utility function for all the players constitutes a potential function as will be shown in Claim 3.1.

Claim 3.1. *The average utility function (in equations (3.2) and (3.4)) of all players form a potential function for the population.*

Proof.

$$U_{Tx_i|T} - U_{Tx_i|NT} = \frac{h_i P_i}{\sigma^2 + \delta \sum_{j=1,}^{N} h'_j P'_j} - C_u P_i \tag{3.5}$$

$$\begin{aligned} U_{Tx|T} - U_{Tx|NT} &= \frac{\sum_{i=1}^{M} h_i P_i}{M(\sigma^2 + \delta \sum_{j=1}^{N} h'_j P'_j)} - \frac{\sum_{i=1}^{M} C_u P_i}{M} \\ &= \frac{1}{M} \sum_{i=1}^{M} (U_{Tx_i|T} - U_{Tx_i|NT}) \end{aligned} \tag{3.6}$$

According to the definition of potential games in [39], the average function is an ordinal potential function since

$$U_{Tx_i|T} - U_{Tx_i|NT} > 0 \Longleftrightarrow U_{Tx|T} - U_{Tx|NT} > 0. \tag{3.7}$$

Furthermore, it has been shown in [39] that the sum function is an exact potential function. The average is just a scaled version of the sum. As a result it is an ordinal potential function. We can use the fact the NE is invariant under scaling and shifting to prove that the sum and the average function have the same NE. The meaning of Eq.s (3.6) and (3.5) is when all players use the transmit strategy, they get higher payoff. This is established by either optimizing their individual utility functions or by the potential function and this completes the proof. □

Jammers' utility function formulation

The utility function of the jammer is assumed to be the reciprocal of the user's utility. This formulation is different from the formulation that is usually used in the literature (for example in [32]). The formulation we use lends itself to mathematical manipulation. For jammer j, the utility that she will get in the transmission case is:

$$U_{Jx_j|T} = \frac{\sigma^2 + h'_j P'_j + \delta \sum_{l=1, l\neq j}^{N} h'_l P'_l}{\epsilon + \rho \sum_{i=1,}^{M} h_i P_i} - C_J(P'_j + \delta \sum_{l=1, l\neq j}^{N} P'_j) \tag{3.8}$$

where ϵ is a very small positive number added to keep the jammers' equations mathematically tractable (to be shown later) . As a result, the average utility for the jammers'

community can be written as: $U_{Jx|T} = \frac{1}{N}\sum_{j=1}^{N} U_{Jx_j|T}$. After manipulations, we get the following equation:

$$U_{Jx|T} = \frac{\sigma^2 + \frac{(\delta(N-1)+1)}{N}\sum_{j=1}^{N} h'_j P'_j}{\epsilon + \rho\sum_{i=1,}^{M} h_i P_i} - C_J(\frac{(\delta(N-1)+1)}{N}\sum_{j=1}^{N} P'_j) \tag{3.9}$$

The utility function and the average utility function for the jammer in the not-transmitting case are given in equations (3.10) and (3.11), respectively:

$$U_{Jx_j|NT} = \frac{\sigma^2 + \delta\sum_{l=1,l\neq j}^{N} h'_l P'_l}{\epsilon + \rho\sum_{i=1,}^{M} h_i P_i} - C_J(\delta \sum_{l=1,l\neq j}^{N} P'_j) \tag{3.10}$$

$$U_{Jx|NT} = \frac{\sigma^2 + \frac{(\delta(N-1))}{N}\sum_{j=1}^{N} h'_j P'_j}{\epsilon + \rho\sum_{i=1,}^{M} h_i P_i}$$

$$-C_J(\frac{(\delta(N-1))}{N}\sum_{j=1}^{N} P'_j) \tag{3.11}$$

Justifying the jammers' average utility in (3.9) and (3.11) and proving that they constitute a potential function follows the same reasoning and approach used for the users' utility function and Claim 3.1.

Stability Analysis

The game is an asymmetric game, and according to [11, 17, 23], there is no mixed ESS under the RD. The RD equation in its general form is given in (2.3). Substituting the utility functions in (3.2) and (3.4), on one hand, and (3.9) and (3.11), on the other hand, in (2.3) and (2.4), we get differential equations for the user and the jammer transmission probabilities, respectively. Denote the user and jammer transmission probabilities by ρ and δ, respectively. Let $\frac{d\rho}{dt} = \dot{\rho}$ and $\frac{d\delta}{dt} = \dot{\delta}$, then:

$$\dot{\rho} = \rho(1-\rho)(\frac{\frac{1}{M}\sum_{k=1}^{M} h_k P_k}{\sigma^2 + \delta\sum_{j=1,}^{N} h'_j P'_j} - \frac{C_u}{M}\sum_{k=1}^{M} P_k) \tag{3.12}$$

for $\rho(0) = \rho_0$ and $0 \leq \rho_0 \leq 1$. Similarly, for the jammer, it will be:

$$\dot{\delta} = \delta(1-\delta)(\frac{\frac{1}{N}\sum_{j=1}^{N} h'_j P'_j}{\epsilon + \rho\sum_{k=1}^{M} h_k P_k} - \frac{C_J}{N}\sum_{j=1}^{N} P'_j) \tag{3.13}$$

for $\delta(0) = \delta_0$ and $0 \leq \delta_0 \leq 1$. To simplify the notation, we introduce the following variables:

$$x_1 = \frac{1}{M}\sum_{k=1}^{M} h_k P_k \ \ , x_2 = \sum_{j=1}^{N} h'_j P'_j \ \ , x_3 = \frac{C_u}{M}\sum_{k=1}^{M} P_k. \tag{3.14}$$

$$y_1 = \frac{1}{N}\sum_{j=1}^{N} h'_j P'_j \ \ , y_2 = \sum_{k=1}^{M} h_k P_k \ \ , y_3 = \frac{C_J}{N}\sum_{j=1}^{N} P'_j. \tag{3.15}$$

Rewriting (3.12) and (3.13) in terms of (3.14) and (3.15), we get:

$$\dot{\rho} = \rho(1-\rho)(\frac{x_1}{\sigma^2 + \delta x_2} - x_3), \ \ \rho(0) = \rho_0 \tag{3.16}$$

$$\dot{\delta} = \delta(1-\delta)(\frac{y_1}{\epsilon + \rho y_2} - y_3), \ \ \delta(0) = \delta_0 \tag{3.17}$$

Equations (3.12) and (3.13) are nonlinear ordinary differential equations. The equilibrium points of these equations can serve as potential ESS's. The asymptotic stability will be checked to see the long run behavior of the system. We form the *Jacobian* matrix whose elements are $\frac{\partial\dot{\rho}}{\partial\rho}, \frac{\partial\dot{\rho}}{\partial\delta}, \frac{\partial\dot{\delta}}{\partial\rho}$, and $\frac{\partial\dot{\delta}}{\partial\delta}$. For an equilibrium point to be asymptotically stable, the eigenvalues of the *Jacobian* matrix should have negative real parts. This is equivalent to i) the determinant of the *Jacobian* > 0, and ii) the trace of the *Jacobian* < 0. The system of differential equations given in (3.16) and (3.17) has 9 equilibrium points (4 of them correspond to pure strategies, while the others are mixed strategies). The phase portraits for these nonlinear second order differential equations are shown for different cases in the figures in Sec. 4.4. These phase portraits indicate that the only motion starting in the square $(0,1),(1,0),(0,0)$, and $(1,1)$ will tend to two stable points (in this special case it will go to $(0,1),(1,0)$), and this rules out any mixed strategy. In what follows, the *Jacobian* for the pure strategies will be built and analyzed. It can be shown that $(0,0)$ and $(1,1)$ are not asymptotically stable points. Similarly, we can prove the other cases.

Building the Jacobian for (0,1) strategy: This means that the user will choose the not-transmit strategy and the jammer will choose the transmit strategy, i.e., $\rho = 0$ and $\delta = 1$. This strategy will sometimes be referred to as the jammers' desired strategy.

$$\mathsf{J}_{(0,1)} = \begin{pmatrix} \frac{x_1}{x_2+\sigma^2} - x_3 & 0 \\ 0 & -\frac{y_1}{\epsilon} + y_3 \end{pmatrix} \tag{3.18}$$

Building the Jacobian for (1,0) strategy: This means that the user will choose the transmit strategy and the jammer will choose the not-transmit strategy, i.e., $\rho = 1$ and $\delta = 0$. This strategy will sometimes be referred to as the users' desired strategy.

$$\mathsf{J}_{(1,0)} = \begin{pmatrix} -\frac{x_1}{\sigma^2} + x_3 & 0 \\ 0 & \frac{y_1}{y_2+\epsilon} - y_3 \end{pmatrix} \tag{3.19}$$

Conditions to get asymptotic stability for the cooperative users, and cooperative Jammers

By applying the determinant rule and the rank rule to each of the Jacobian matrices in (3.18) and (3.19), we get the following conditions.

Testing the (0,1) as a potential ESS: $\det(J_{(0,1)}) = (\frac{x_1}{x_2+\sigma^2} - x_3)(-\frac{y_1}{\epsilon} + y_3) > 0$, which leads to the requirement that both terms should be < 0 (because $-\frac{y_1}{\epsilon} < 0$). $Trace(J_{(0,1)}) = (\frac{x_1}{x_2+\sigma^2} - x_3) + (-\frac{y_1}{\epsilon} + y_3) < 0$, which is guaranteed because of the second term. As a result, a sufficient and necessary condition for $(0, 1)$ to be an ESS is $(\frac{x_1}{x_2+\sigma^2} - x_3) < 0$. This can be written as:

$$\frac{\frac{1}{M}\sum_{k=1}^{M} h_k P_k}{\sigma^2 + \sum_{j=1,}^{N} h'_j P'_j} < \frac{C_u}{M} \sum_{k=1}^{M} P_k \tag{3.20}$$

Testing the (1,0) as a potential ESS: $\det(J_{(1,0)}) = (-\frac{x_1}{\sigma^2} + x_3)(\frac{y_1}{y_2+\epsilon} - y_3) \approx (-\frac{x_1}{\sigma^2} + x_3)(\frac{y_1}{y_2} - y_3) > 0$, and $Trace(J_{(1,0)}) = (-\frac{x_1}{\sigma^2} + x_3)(\frac{y_1}{y_2+\epsilon} - y_3) \approx (-\frac{x_1}{\sigma^2} + x_3) + (\frac{y_1}{y_2} - y_3) < 0$. This leads to the requirement that both terms in both equations should be less than zero, i.e., $(\frac{x_1}{\sigma^2} > x_3)$ and $\frac{y_1}{y_2} < y_3$, or:

$$\frac{\frac{1}{M}\sum_{k=1}^{M} h_k P_k}{\sigma^2} > \frac{C_u}{M} \sum_{k=1}^{M} P_k \tag{3.21}$$

$$\frac{\frac{1}{N}\sum_{j=1}^{N} h'_j P'_j}{\sum_{k=1}^{M} h_k P_k} < \frac{C_J}{N} \sum_{j=1}^{N} P'_j \tag{3.22}$$

3.3.2 Relation between asymptotic stability and ESS in the cooperative users and cooperative jammers game:

In general, each ESS is not asymptotically stable point (see for example [23]). However, according to [12] in asymmetric games with two strategies, asymptotically stability is equivalent to being an ESS.

3.3.3 Convergence to Asymptotically Stable Points

Convergence to asymptotically stable points will be verified by simulations in the later sections in addition to the analytical verification in this section. The approach used here closely follows what is done in [31].

Claim 3.2. *: The Cooperative users and Cooperative Jammers game converges to the one of ESSs:* $(0,1)$ *or* $(1,0)$ *according to the conditions in equations (3.20) or (3.21) and (3.22) being true.*

Proof. By Claim J1, we have a game with two potential functions for two populations. Each player in each population will work towards maximizing her population potential function. According to [39], the solution for the above game is unique, and this proves the convergence part of the claim. For the second part, if equation (3.20) is true, then $(0,1)$ is an asymptotically stable point. Similarly if equations (3.21) and (3.22) are true, then $(1,0)$ is an asymptotically stable point. Furthermore, from the discussion of the relation between the asymptotic stability, and evolutionary stability in 3.3.2, we know that these points are corresponding to the ESS points of the game. As a result, the game will converge to one of them (either $(0,1)$ or $(1,0)$). □

Under some special conditions, one can show that the game will settle at a specific ESS. Each ESS depends on the channel coefficients, the initial probabilities, and the number of users and jammers who are active (transmitting). However if one of the population players have better channels, and larger numbers, then a specific ESS can be predicted. These conditions are stated and proved in Claim 3 below.

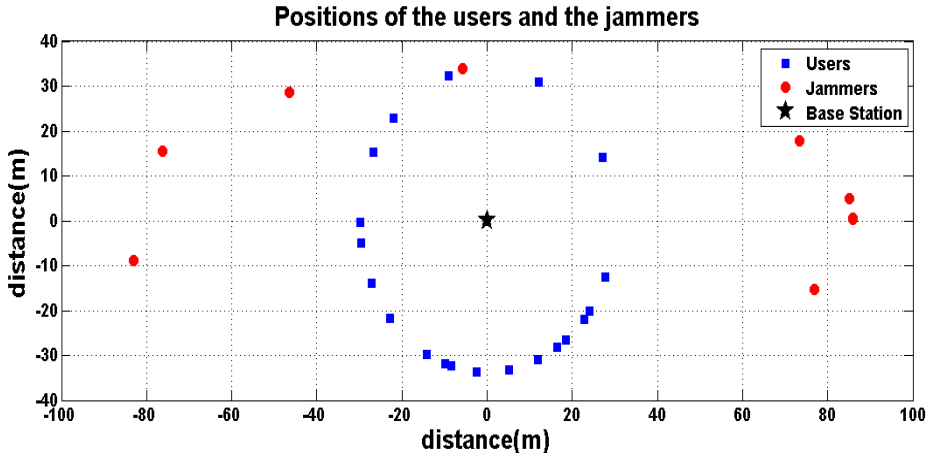
Claim 3.3. *: For equal transmission powers, then regardless of the initial population points, we have:*
(1) If the number of users is greater than the number of jammers, then $(1,0)$ *is the ESS, if the ratio of the average of the users channel gains to the sum of the jammers channel gains is greater than the users transmission cost.*
(2) If the number of jammers is greater than the number of users, then $(0,1)$ *is the ESS, if the ratio of the average of the jammers channel gains to the sum of the users channel gains is greater than the jamming cost.*

Proof. To eliminate $(0,1)$ from being an ESS, it is enough to show that it is not asymptotically stable. By Claim 3.2 the game converges to an ESS, then we are left with $(1,0)$ which is our desired ESS. From the stability analysis in 3.3.1, $(0,1)$ can be a saddle point (and hence not asymptotically stable) if (3.20) is not satisfied. Assuming the noise is very small with respect to the jammers' interference power will simplify the calculations as follows: we need $(\frac{x_1}{\sigma^2+x_2} - x_3 > 0)|_{\sigma^2<<x_2} \Rightarrow \frac{\frac{1}{M}\sum_{k=1}^{M} h_k P_k}{\sum_{j=1}^{N} h'_j P'_j} > \frac{C_u}{M}\sum_{k=1}^{M} P_k \Rightarrow \frac{\frac{1}{M}\sum_{k=1}^{M} h_k}{\sum_{j=1}^{N} h'_j} > C_u P_k$which is true,and hence $(0,1)$ will be a saddle point. The second part of the claim can be proved similarly by excluding $(1,0)$ from being asymptotically stable. □

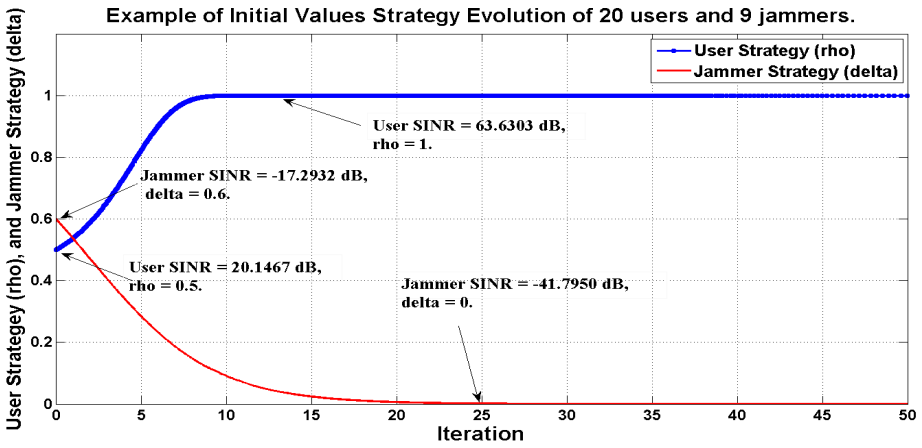
What the above claim reveals is that if users are greater in number and have significantly better channels than the jammers, the ESS results in victory for the user population, and vice-versa.

3.4 Conclusions

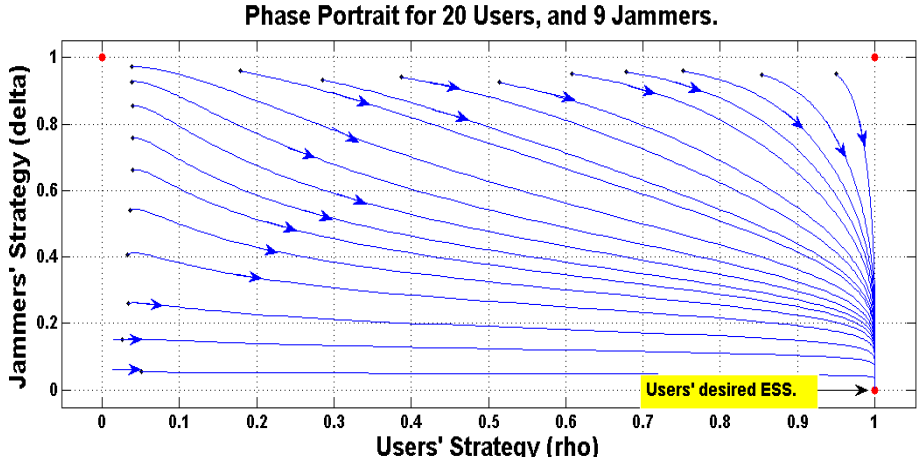
We considered a wireless network of M users connected to an access point in the presence of N jammers whose purpose is to deny or degrade the performance of the users by injecting interference. Using the achieved signal to inference plus noise ratio ($SINR$) as the performance metric, we studied the dynamics of such a distributed denial of service attack (DDoA) by using Evolutionary Game Theory (EGT). Specifically, we considered a cooperative network model, where the M users (and N jammers) can collectively enhance their achieved $SINR$ (degrade the user $SINR$). We modeled the



(a) Positions of the 20 users and 9 jammers.



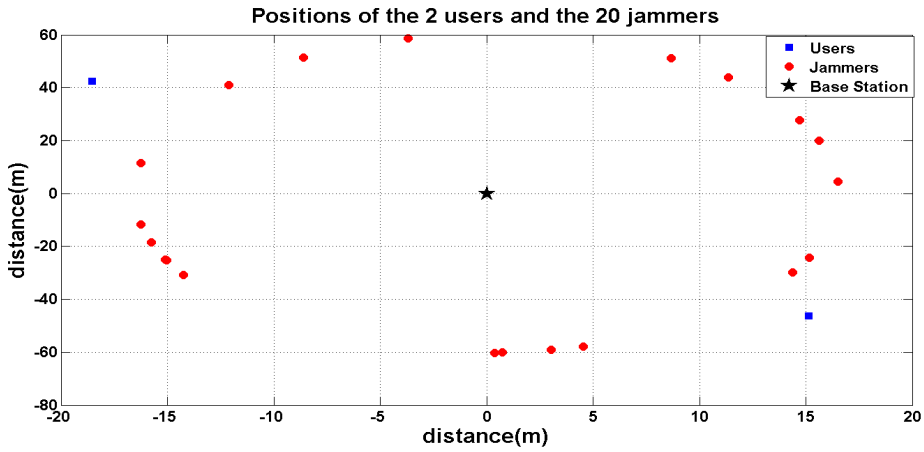
(b) Example of strategies evolution for 20 users, 9 jammers, $\rho = 0.5$, and $\delta = 0.6$.



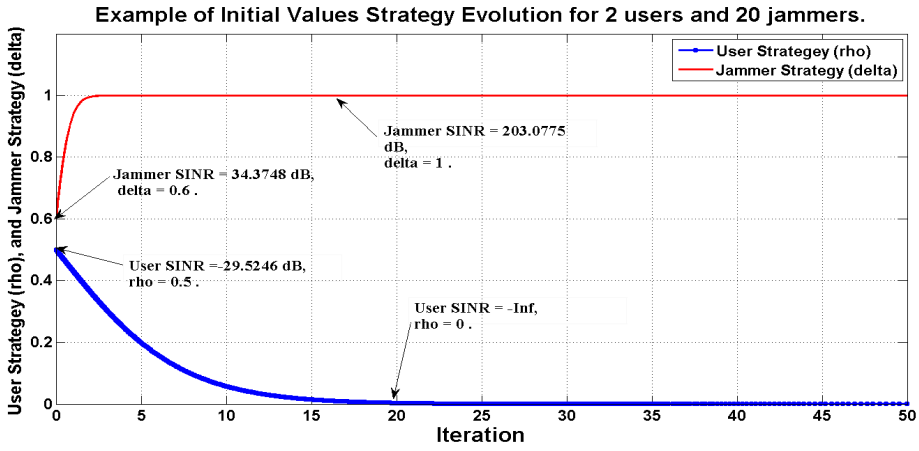
(c) Phase Portrait for 20 Users and 9 Jammers.

Figure 3.1: 20 users and 9 jammers.

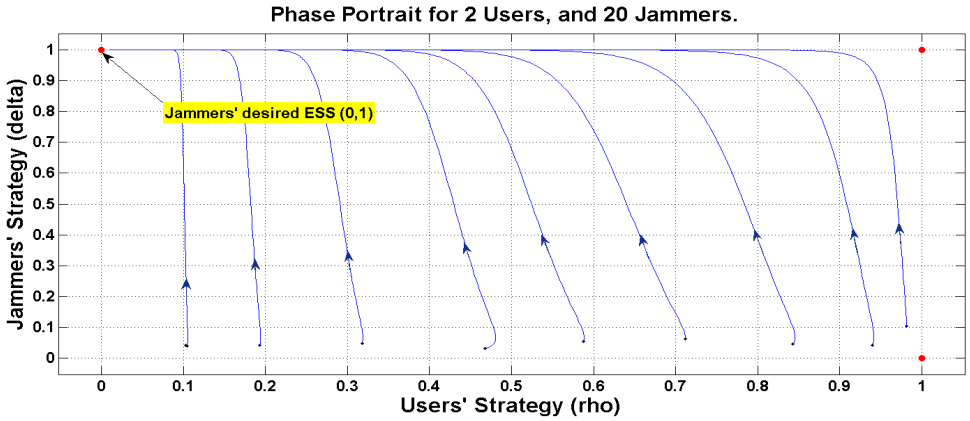
strategic transmission decisions of the users (and the jammers) using simple random access techniques where the users (and jammers) decide to transmit or not with a transmission probability taking into account their energy costs. Using the replicator dynamics (RD) we characterized the evolutionary stable strategies (ESS's) of the game and observed that the resulting transmission probabilities turn out to be either 0 or 1. Further, given a network (channel) setting, we showed using a phase portrait of the replicator dynamics how the ESS strategies evolve for different cooperation levels of the users and jammers populations. We also provided insights into resulting ESS strategies as a function of the number of users and jammers, and their signal strengths (locations). Typically, if users are greater in number and have significantly better channels than the jammers, the ESS results in victory for the user population, and vice-versa.



(a) Positions of the 2 users and 20 jammers.

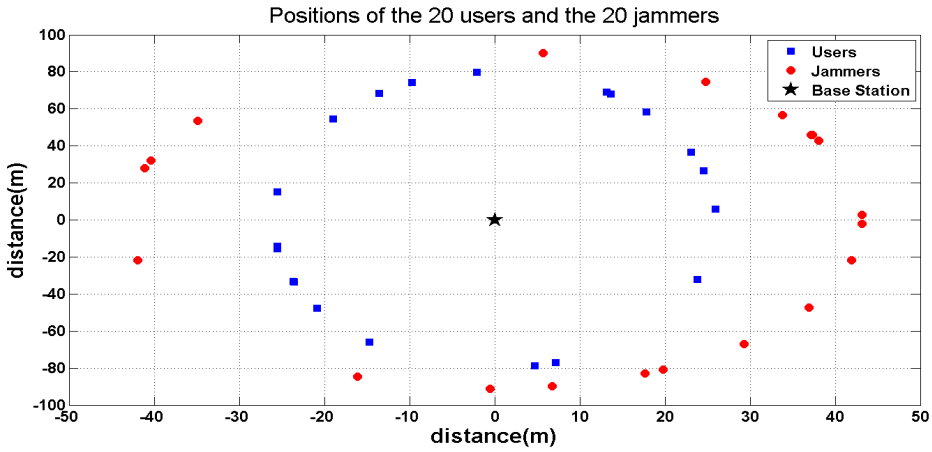


(b) Example of strategies evolution for 2 users, 20 jammers, $\rho = 0.5$, and $\delta = 0.6$.

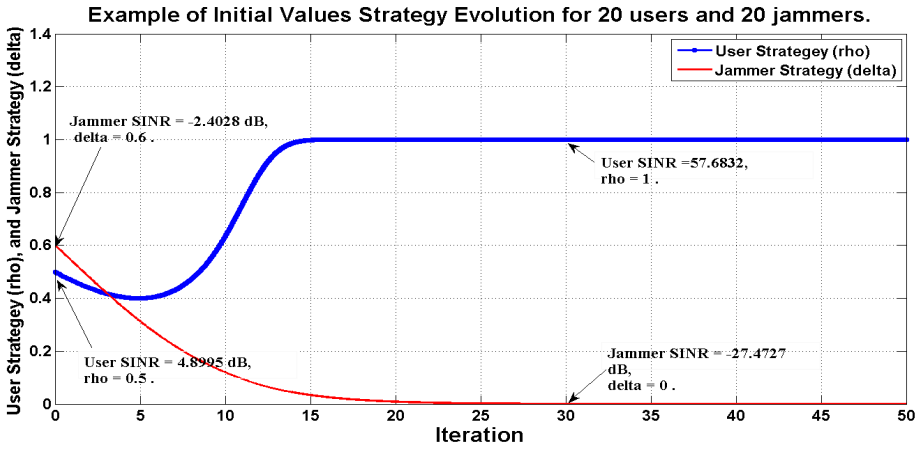


(c) Phase Portrait for 2 Users and 20 Jammers.

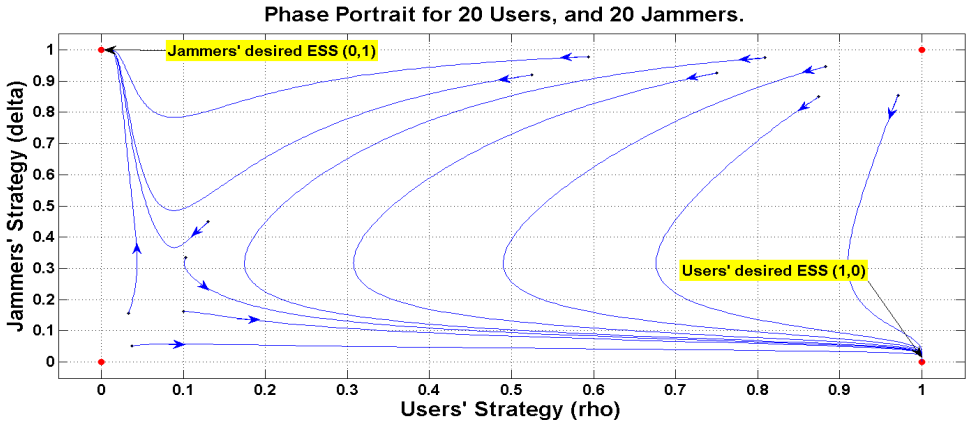
Figure 3.2: 2 users and 20 jammers.



(a) Positions of the 20 users and 20 jammers.



(b) Example of strategies evolution for 20 users, 20 jammers, $\rho = 0.5$, and $\delta = 0.6$.



(c) Phase Portrait for 20 Users and 20 Jammers.

Figure 3.3: 20 users and 20 jammers.

Chapter 4

Threat Revocation in Ephemeral Networkst

4.1 Introduction

Ephemeral networks are those in which the nodes of the network are connected in a decentralized way where the life time of the network could be short. Examples of these networks can be ad hoc networks, vehicular networks, and delay tolerant networks [22, 40]. Revocation games can be used to model security threats for Internet of Things (IoT) where each device can be considered as a benign node with an intruder who tries to launch an attack to disturb the network. The model considered here is suitable to describe any network structure where there is no Centralized Authority (CA), to constantly monitor the network [40].

In this chapter, we are interested in studying the dynamics of the misbehavior introduced by an intruder(s) in an ephemeral network (population) consisting of a collection of benign nodes and malicious ones when the population of the benign node is allowed to cooperatively take a decision on how to deal with such threat optimally. Specifically, we will use Evolutionary Game Theory (EGT) [23] to study the dynamics of such attack in a wireless network with M users connected in an ad hoc manner in the presence of intruders whose goal are to disrupt the users' communications.

The chapter is organized as follows. A brief review of related work is provided in Section 4.2. Section 4.3 gives the details of the problem formulation and the parameter derivations. Simulation results are given in Section 4.4, and we conclude in Section 4.5.

4.2 Related work

Applying game theory to address the security of vehicular networks can be found in [41] and the references therein, where various game models such as zero sum game models, fuzzy games, and fictitious play have been applied. For ephemeral networks, the work in [40] uses a dynamic (sequential) game to collect certain number of votes to declare node revocation. In [42], the authors use a static game to find the optimal revocation procedure. In this chapter, we propose an evolutionary game model to the problem, where the benign nodes are assumed to form a homogeneous population of players.

Evolutionary Game Theory has been used to study the dynamics of wireless networks in many competing situations [24–30]. These situations range from radio resource management among competing users for rate adaptation, base station assignment, and spectrum sharing, to routing in mobile networks, as well pricing of wireless resources. In almost all of the above cases, the models result in symmetric games where all users optimize the same utility function, typically get identical rewards and face similar costs. Earlier work in [1, 31, 43] used EGT for wireless network security where the objective function was either the secrecy rate as in [31], signal to noise ratio in [1], or in terms of building a reputation system to monitor the misbehavior in the network by the CA as in [43].

4.3 Problem Formulation

We assume a decentralized short range network consisting of a population of M benign nodes threatened by intruder(s). Each node has equal opportunity to be able to face that intruder to make a decision. The set of available strategies for each node to choose from is $\{A, S, V\}$ [40], and [42]. A stands for abstain or do nothing (the free rider problem). S stands for self-sacrifice, where the node takes the ultimate decision by disconnecting the intruder and itself from the network to protect the whole population (however, for the network connectivity, it is not desired that large number of nodes to use this strategy). V is for voting to isolate the suspected node or not. Each decision has its benefits and consequences which are represented as rewards and costs. As a

Table 4.1: Players' Payoffs

	A	S	V
A	$(-c, -c)$	$(\beta, B - c_s)$	$(-c, -(c + v))$
S	$(B - c_s, \beta)$	$((B - c_s)/2, (B - c_s)/2)$	$(B - c_s, b - v)$
V	$(-(c + v), -c)$	$(b - v, B - c_s)$	$(b - v, b - v)$

result the node cost function (that has to be minimized) is given as [22],

$$J_i(A_i, k) = \begin{cases} (1-k)c & \text{if} \quad A_i = A \\ v + (1-k)c - kb & \text{if} \quad A_i = V \\ c_s - B & \text{if} \quad A_i = S \end{cases} \tag{4.1}$$

where all the variables are non-negative. $k = 1$ if the revocation is successful and equals zero if not. v is the cost of voting, b is the benefit of voting (if revocation was not successful, then the voting node(s) can suffer or being attacked by the intruder(s)), c_s is the cost of self-sacrifice, B is the benefit of self-sacrifice, and c is the attack cost (damage to the network).

According to the game formulation as either static or dynamic, different decision rules are derived in [40] and [42]. However, formulating the problem as an evolutionary game, gives an intuitive way to think about the problem. If node-1 decides to use a strategy A, then why should node-2 commit strategy S or V? By setting some pre-specified rules, one can control how the decision could be made. This is captured by the cost terms associated with each decision. We assume that all the nodes are identical in their interests, payoffs, and decision costs. Furthermore, these nodes are threatened by the same intruder. By formulating an appropriate payoff function, this game is a typical symmetric evolutionary game. The payoff matrix is defined under the following constraints: $\beta > b - v > B - c_s$. All the variables are non negative real numbers. The variables c, c_s, b, v, B are defined as in (4.1), and β is the benefit from not using strategy S when not needed. For any ordered pair (x, y) in the payoff table above, Table 4.1, the first entry represents the payoff to the row player and the second entry represents the benefits for the column player. As it can be seen, the game encourages removing the attacker quickly by the constraint above. Also, the game is discouraging the strategy

A when there is a threat, and promoting using strategy S. However, excessive use of strategy S could lead to the network be disconnected, and this is undesired solution. As a result, the costs for both players playing S is high, since one of them is needed to play it to isolate the intruder. The pair $\{V, A\}$ has the worst cost, because it will not lead to a successful revocation, and as a result the attacker might take revenge from the node which voted for revocation, or might change its position to avoid that node and start a new attack that could be tolerated by the presence of more nodes that play the strategy A. Let each node chooses the strategies $\{A, S, V\}$ with probabilities given by the probability vector $\rho = [\rho_1, \rho_2, \rho_3]^T$, and the payoff matrix (for the row player which is the same for all players in the game) can be written as,

$$Q = \begin{bmatrix} -c & \beta & -c \\ B - c_s & (B - c_s)/2 & B - c_s \\ -(c + v) & b - v & b - v \end{bmatrix} \tag{4.2}$$

then each node will solve the following optimization problem,

$$\begin{aligned} \max_{\rho} \quad & \rho^T Q \rho \\ \text{subject to} \quad & \sum_{i=1}^{3} \rho_i = 1, \\ & 0 \leq \rho_i \leq 1, \;\; i = 1, 2, 3. \end{aligned} \tag{4.3}$$

The problem above is not convex, because the matrix Q is neither positive definite, nor semi definite. Also, although we assumed that the game is symmetric on its players' interests, the payoff matrix is not symmetric (see (4.2)). If it was symmetric, then we would have a doubly symmetric evolutionary game [11]. In doubly symmetric evolutionary games, (4.3) can be solved as a quadratic convex program. However, by using the RD concept, we can find the locally asymptotically stable strategies, and then test them for being ESS using the f_σ and g_σ conditions. Finally, it is assumed (as in [22]) that there is a detection mechanism that is responsible for identifying and declaring the intruder(s), so that the other nodes can make their decisions upon that. We will follow the procedure given in Fig.2.1.

4.3.1 The Game Dynamics

The dynamic stability of the game is studied in the scope of RD, where each player compares her payoff with the average payoff and updates her strategy according to this. For this game, the ESS can be in the mixed strategies or in the pure ones. In all cases, the eigenvalues of the Jacobian of the RD at the equilibrium should have negative real parts. In some cases it is easier to look at the Jacobian, but not always. For this game, the RD is represented by the following system of nonlinear ordinary differential equation,

$$\dot{\rho_i} = \rho_i(u(\rho_i, \rho) - \overline{u}),\ i = 1, 2, 3. \tag{4.4}$$

Furthermore, there are two independent equations in the system (4.4), since $\dot{\rho_3} = -(\dot{\rho_1} + \dot{\rho_2})$. To find the ESS potential points, we need to solve the above system of nonlinear equations (4.4) to find all the rest points, then finding the eigenvalues correspond to each rest point. If the eigenvalues have negative real parts, then we have asymptotic stability which has to be further investigated for being ESS by applying them to f_σ and g_σ. The Jacobian matrix is given as,

$$J = \begin{bmatrix} \frac{\partial \dot{\rho_1}}{\partial \rho_1} & \frac{\partial \dot{\rho_1}}{\partial \rho_2} \\ \frac{\partial \dot{\rho_1}}{\partial \rho_2} & \frac{\partial \dot{\rho_2}}{\partial \rho_2} \end{bmatrix} \tag{4.5}$$

Unfortunately, finding the rest points for the system of equations (4.4) in a general form is difficult to express analytically. However, finding it for the pure strategies is relatively an easier task.

In this game, and for the sake of simplicity, we use the RD (4.4) to visualize the evolution of the probabilities ($\{\rho_1, \rho_2, \rho_3\}$), while we use the conditions (f_σ and g_σ) to check the strategy for being an ESS. However, for a strategy to not being asymptotically stable, means it is not an ESS.

Claim 4.1. *Among all the available pure strategies $\{A, S, V\}$, the strategy V (which corresponds to $(\rho_1 = 0, \rho_2 = 0, \rho_3 = 1)$) is an ESS in its neighborhood.*

Proof. We can check the asymptotic stability (through computing the eigenvalues) of the Jacobian matrix which corresponds to each of the given strategies. If the strategy

is not asymptotically stable, then it is not an ESS. If it is asymptotically stable, then we check if it satisfies f_σ (and g_σ if $f_\sigma = 0$) condition. To prove that V (which corresponds to $(\rho_1 = 0, \rho_2 = 0, \rho_3 = 1)$ is an ESS in its neighborhood, we substitute it in the condition f_σ, to get $[0\ 0\ 1]Q[0\ 0\ 1]^T - [\rho_1\ \rho_2\ \rho_3]Q[0\ 0\ 1]^T = ((b-v)+c)\rho_1 + ((b-v)-(B-c_s))\rho_2 \rightarrow f_\sigma > 0$ which proves V as an ESS. For the strategy A ($\{\rho_1 = 1, \rho_2 = 0, \rho_3 = 0\}$), the corresponding Jacobian is

$$J_{(1,0)} = \begin{bmatrix} -v & c_s - c - v - B \\ 0 & B - c_s + c \end{bmatrix} \tag{4.6}$$

with eigenvalues $-v < 0$ and $B - c_s + c > 0$, this strategy is not asymptotically stable, and as a result it is not an ESS. Similarly, for the strategy S ($\{\rho_1 = 0, \rho_2 = 1, \rho_3 = 0\}$), the corresponding Jacobian is

$$J_{(0,1)} = \begin{bmatrix} \beta - 0.5(B - c_s) & 0 \\ (b-v) - \beta & (b-v) - 0.5(B - c_s) \end{bmatrix} \tag{4.7}$$

with eigenvalues $\beta - 0.5(B - c_s) > 0$ and $(b-v) - 0.5(B - c_s) > 0$, this strategy is not asymptotically stable, and as a result it is not an ESS too. □

Claim 1 shows two things: (1) It is possible to get each node involved in the decision making process to avoid the free rider problem (where nodes just use the A strategy), given that there are enough nodes that are using the V strategy. (2) although the other strategies (A and S) cannot dominate the population by themselves (which is good), there still the possibility that an undesired mixed strategy (which is given by $\{A, S, 0\}$), where strategy V will not used, be an ESS. Characterizing the conditions under which such an ESS emerges can be done by finding the asymptotically stable points of (4.4), while the required potion of population (initial conditions and the region of attraction) that is required to converge to such an ESS is shown by the phase portrait diagrams.

4.4 Simulation Results

In this section, two cases correspond to two different values for the payoff matrix Q will be analyzed to find the ESS and simulated using the package in [44] to show the convergence rates of different strategies to the asymptotically stable points.

Table 4.2: Example 1 Strategies and their Eigenvalues

Strategy (ρ_1, ρ_2, ρ_3)	Eigenvalues
$(0, 0, 1)$	$(-2, -0.5)$
$(0.54, 0.46, 0)$	$(-0.8, -0.7)$
$(0, 1, 0)$	$(1.75, 0.75)$
$(0.25, 0.46, 0.29)$	$(-0.64, 0.42)$
$(0.8, 0, 0.2)$	$(1.5, 0.4)$
$(1, 0, 0)$	$(1.5, -0.5)$

4.4.1 Case 1

In this case, we take the following values for the game parameters, $\beta = 2; b = 1.5; v = 0.5; B = 1.5; c_s = c = 1$. The payoff matrix is

$$Q = \begin{bmatrix} -1 & 2 & -1 \\ 0.5 & 0.25 & 0.5 \\ -1.5 & 1 & 1 \end{bmatrix} \tag{4.8}$$

We search for the rest points of the RD (4.4) using [44] to get the asymptotically stable points. Table 4.2 shows these strategies with their eigenvalues. The phase portrait is shown in Figure 4.1. The solid dots are the asymptotically stable points, while the empty dots are not asymptotically stable. The speed of convergence is captured by the color, the darker the color, the higher the speed of convergence. The first asymptotically stable strategy V, $(\rho_1 = 0, \rho_2 = 0, \rho_3 = 1)$, has been proven as an ESS in Claim 1. Similarly, we prove that the second asymptotically stable point $(0.54, 0.46, 0)$ to be an ESS as follows, $[0.54\ 0.46\ 0]Q[0.54\ 0.46\ 0]^T - [\rho_1\ \rho_2\ \rho_3]Q[0.54\ 0.46\ 0]^T = 0.73\rho_3 > 0 \rightarrow f_\sigma > 0$. The phase portrait in Figure 5.2 shows that the region of attraction of strategy V is larger than that of the other ESS. This highlights that nodes can tune their decisions by assigning in advance proper parameters to induce cooperation and eliminate the free rider problem as well as to avoid the network self destruction where strategy S could be seen as the only strategy used to eliminate the intruder. Figures 4.2 and 4.3 show the probability evolution for some specific initial conditions (portion of populations use each strategy).

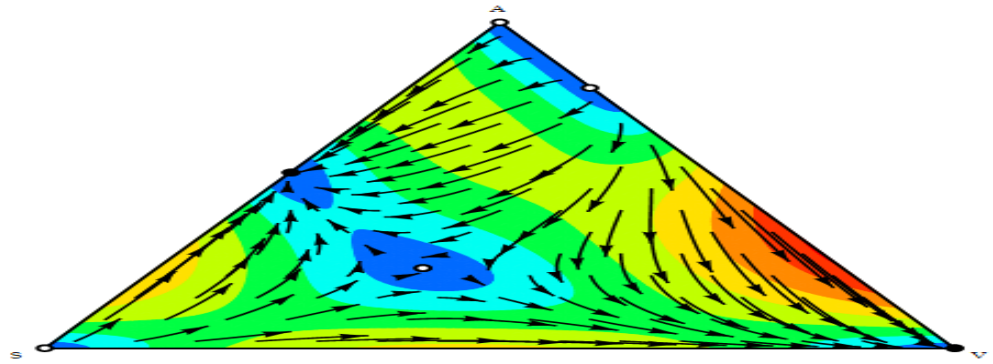


Figure 4.1: Phase Portrait for $\beta = 2; b = 1.5; v = 0.5; B = 1.5; c_s = c = 1$. Solid dots are the asymptotically stable points.

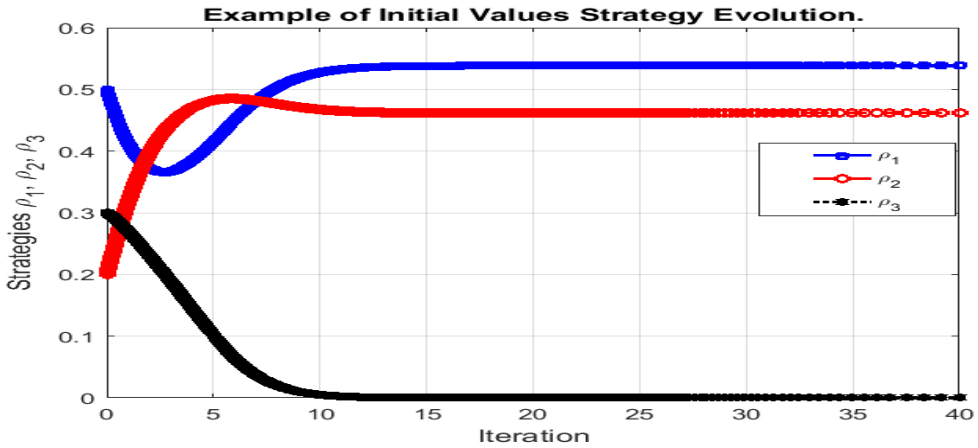


Figure 4.2: Convergence to the ESS $(0.54, 0.46, 0)$ given that $\beta = 2; b = 1.5; v = 0.5; B = 1.5; c_s = c = 1$, and with initial points $\rho_1 = 0.5, \rho_2 = 0.2, \rho_3 = 0.3$.

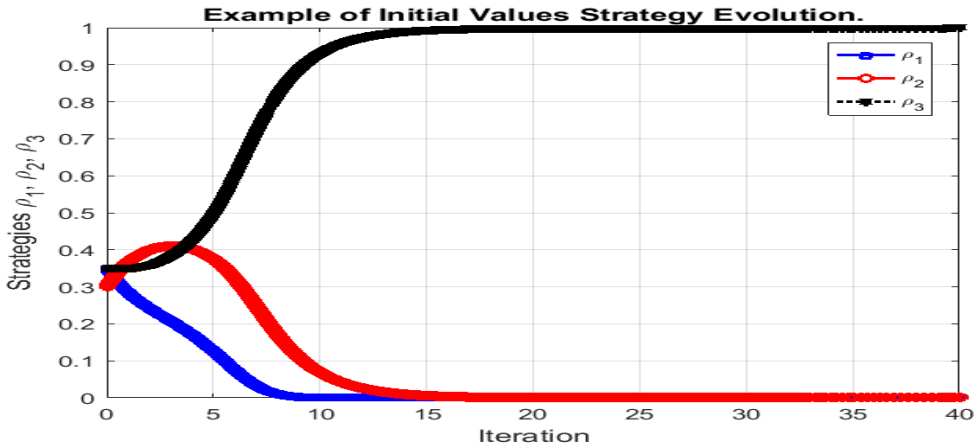


Figure 4.3: Convergence to the ESS $(0, 0, 1)$ given that $\beta = 2; b = 1.5; v = 0.5; B = 1.5; c_s = c = 1$, and with initial points $\rho_1 = 0.35, \rho_2 = 0.3, \rho_3 = 0.35$.

4.4.2 Case 2

In this case, we take the following values for the game parameters, $\beta = 2; b = 2; v = 0.5; B = 1.5; c_s = c = 1$. For this case, the game has the same asymptotically stable points and the ESS's as found in Section 4.4.1. However, the difference is that the region of attraction for the desired ESS V $(0, 0, 1)$ is larger than that of the other ESS (where no player plays V) as can be seen from Figure 4.4 (the calculations details are omitted because the space limitation). This change has been made by increasing the value of b from 1.5 to 2, which means more payoff for cooperation (or voting). Figures 4.5 and 4.6 show the convergence to the mixed and pure strategies. Comparing them with Figures 4.2 and 4.3, it can be seen that much less portion of the population (benign nodes) needs to use the V strategy to motivate the other nodes to use it.

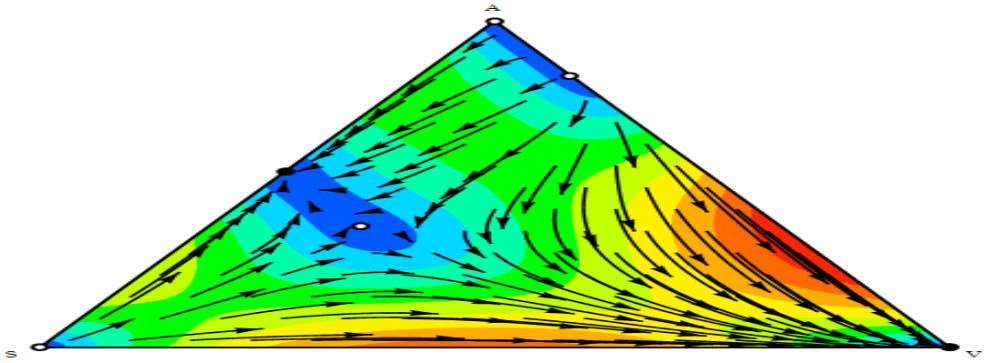


Figure 4.4: Phase Portrait for $\beta = 2; b = 2; v = 0.5; B = 1.5; c_s = c = 1$, and with initial points $\rho_1 = 0.35, \rho_2 = 0.3, \rho_3 = 0.35$.

4.5 conclusions

We considered a wireless network of M nodes connected together in a decentralized way, and according to pre-specified rules. We assumed that there are other malicious node(s) which could be either inserted or infected which are trying to disturb the operation of the network. We assumed the nodes to be cooperating to defend the network (and eventually themselves) by isolating the misbehaved node(s). We approached this

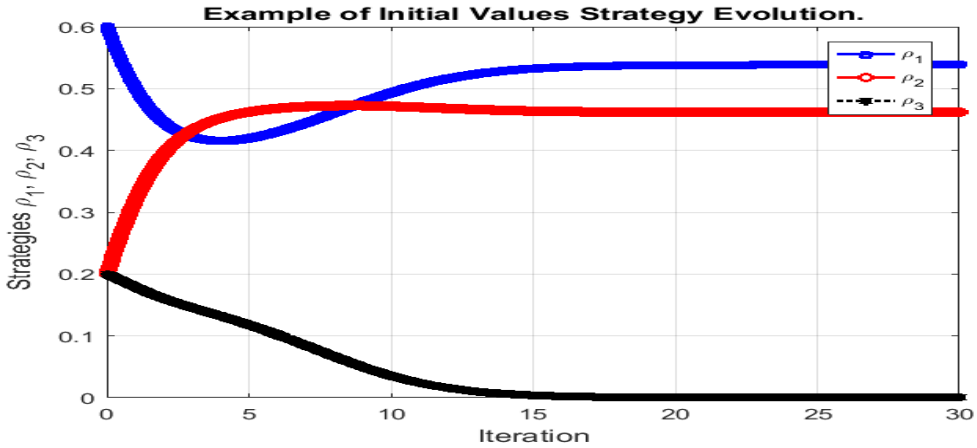


Figure 4.5: Convergence to the ESS $(0.54, 0.46, 0)$ given that $\beta = 2; b = 2; v = 0.5; B = 1.5; c_s = c = 1$, and with initial points $\rho_1 = 0.6, \rho_2 = 0.2, \rho_3 = 0.2$.

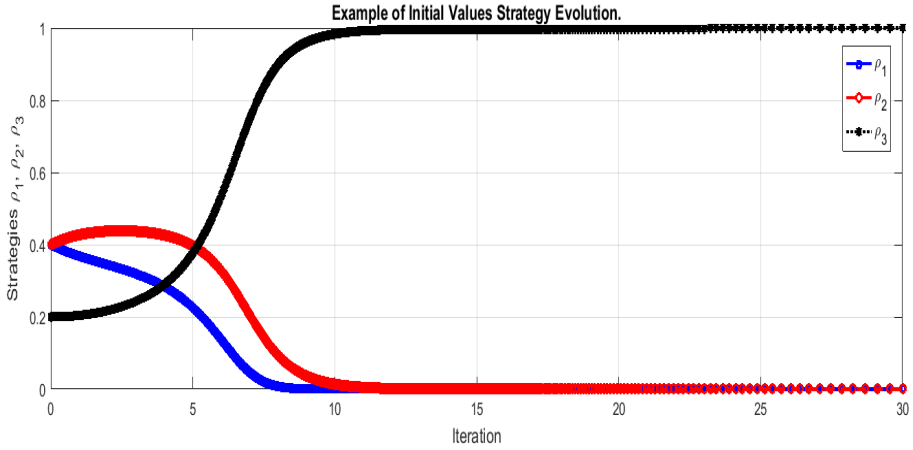


Figure 4.6: Convergence to the ESS $(0, 0, 1)$ given that $\beta = 2; b = 2; v = 0.5; B = 1.5; c_s = c = 1$, and with initial points $\rho_1 = 0.4, \rho_2 = 0.4, \rho_3 = 0.2$.

problem using Evolutionary Game Theory (EGT), and characterized the robust equilibrium point(s) for this game. We formulated a game such that all the nodes take part in the decision process to avoid problems caused by unsuccessful revocation or over reacted revocation decisions. Each node in the network (interchangeably called benign node to distinguish it from the malicious node or the intruder) is assumed to have three decisions to make: (a) abstain or do nothing; (b) self-sacrifice by disconnecting the intruder and itself; and (c) voting to isolate the intruding node. Each decision has its advantages and disadvantages and the Replicator Dynamics (RD) is used to show the dynamics of the nodes' decisions. By simulating the RD equation, two different cases emerged as Evolutionary Stable Strategies (ESS) where one of them is the desired ESS, and the other is not. We showed using phase portrait diagrams the fraction of the M nodes needed to choose each one of these ESS's, the rate of convergence, and the effect of increasing the cooperation rewards.

Chapter 5

Advanced Persistent Threats

5.1 Introduction

Continuous targeting of storage devices by a well funded, powerful attacker are called Advanced Persistent Threats (APTs) [45]. A study of APT in [9] shows that an attacker can apply advanced attack techniques such as spear phishing and watering-hole-attacks against cyber systems such as cloud storage and servers. The nature of these attacks reflects deep conflicts among many factors such as the attacker's desire to control the system versus the attacking cost. Attackers can also use social engineering to pretend to be trustworthy. As a result, game theory has been used in [46] to model the conflict between an APT attacker and the defender.

In this chapter, we study the dynamics of the APT defense of cloud storage regarding the APT attack and scan intervals, according to the replicator dynamics (RD). Evolutionary game theory [12, 14, 17, 23] and the replicator dynamics, together, provide a dynamic picture of the APT defense over a finite set of time intervals. This study can help understand the APT attacks against smart facilities such as in a smart city, medical devices, and Internet of Things. Specifically, we consider two asymmetric evolutionary games, in which the APT attacker and the defender can learn the optimal strategy by using the RD criteria. Under RD, players compare their payoffs using a certain strategy with the average payoff gained in their population, and choose the strategy which gives them the higher than average payoff.

In the APT defense game one or multiple storage devices or data centers are threatened by an APT attacker who can choose the attack intervals, i.e., the time periods before launching APT, while the defender chooses the waiting periods before scanning the devices. The importance of each storage device to the attacker and the defender,

such as the size of the stored data and their priority is described by the attack cost and the defense gain. In addition, by further testing the locally asymptotically stable points of the RD, which are the stable Nash equilibrium (NE) solutions for the APT defense game, we study the evolutionary stable strategy (ESS) of the APT defense game. The phase portrait is presented to show dynamic games, and help one to understand the conditions under which a specific strategy will be played and if that strategy is going to withstand some small perturbations in the players' attitudes to replace it. The best defense strategy against APT is analyzed under various APT attack and defend models, such as the intervals required to successfully launch attacks against a given storage device. A systematic RD-based procedure is derived to solve the evolutionary game of APT defense.

Most existing game theoretic studies on APT such as [46–48] focus on modeling the attack behavior and assume that both the attacker and the defender reach a solution to their conflict through the Nash equilibrium, which represents the stable state of the system. However, the NE in an evolutionary game is not always the ultimate solution or even asymptotically stable. Therefore, we apply ESS to investigate whether the NE of the proposed APT defense game is resilient to small perturbations. The main contribution of this work is characterized by the following:

(1) We formulate an APT defense game using evolutionary game theory to study the dynamic behavior of the APT attacker and defender with replicator dynamics.

(2) The stability and the robust solutions of the APT defense game are studied according to the ESS criteria.

(3) We indicate the conditions under which the APT defense game has the ESS for given initial conditions, and depict them pictorially.

The chapter is organized as follows: related work is reviewed in Section 6.2. Section 5.3 provides the evolutionary game model. Section 5.4 presents the ESS of the dynamic APT defense game. Finally, conclusions are drawn in Section 6.6.

5.2 Related work

Evolutionary game theory has been used to study the dynamics of many competing scenarios. For example, in wireless networks, users compete for network resources [24–29]. In [24], two evolutionary games used to model multiple access control in a slotted Aloha wireless network and power control for a wide band CDMA system are presented. The evolutionary stable strategies (ESS's) for the games are studied under different wireless channels and pricing schemes. A user-base station association study using evolutionary games is presented in [25]. In [26], evolutionary games are used to study distributed resource allocation in small cells. Potential games and evolutionary dynamics are used to address the noncooperative routing problem in [27]. Coexistence in cognitive radio where the available channels have different qualities and the associated user behavior in channel selection is modeled as an evolutionary game in [28], and the ESS for the corresponding symmetric game is derived. A pricing evolutionary game between users and video streaming service providers is studied in [29].

Evolutionary games have been used in modeling security conflicts as in [31], [43], and [1]. The work in [31] addresses the secrecy rate adaptation between a sensor node and its responsible cluster head as an evolutionary game to solve the conflict between increasing the secrecy rate, and minimizing the cost for data transmission in a wireless sensor network. In [43], an indirect reciprocity-based security system for large-scale wireless networks is presented where malicious users are punished by building a reputation system. The jamming evolutionary game as presented in [1], uses cooperation between users to defend against cooperative jammers, and finds the ESS under different channels and power cost conditions. A recent survey on evolutionary game applications is presented in [49], where the authors considered specific engineering applications based on evolutionary games, such as building dynamic dispatch algorithms in smart grids.

Since the seminal work in [46] proposed the game theoretic formulation of the APT problem, other studies have followed. For example, the APT defense game with a resource constraint environment as presented in [47] analyzes two games. A dynamic

Table 5.1: Summary of Symbols

S	Number of storage devices
x_i^k/y_i^k	Defense/attack interval at time k against device i
z_i^k	Duration to complete the k-th attack against device i
G_i	Defense gain of device i
C_i	Attack cost against device i
L	Number of non-zero attack duration levels
$\mathbf{x}/\mathbf{y}$	Defender/Attacker pure strategies
ρ/δ	Defender/Attacker mixed strategies
J	Jacobian matrix
D/A	Defender/Attacker payoff matrices

game proposed in [50] studies the interactions between the defender and the attacker, while the insiders were competing among themselves to sell the information to the attacker at the risk of being caught by the defender. A three-player game model as presented in [48], investigates the interactions among an APT attacker, a cyber system defender, and insiders. The prospect theoretic study on APT defense in [51] discloses the impact of the subjective view of an APT attacker on the data safety levels of a cloud storage. In this chapter, we formulate an asymmetric evolutionary game between the APT attacker and the cloud storage defender to find the evolutionary stable strategies in the APT defense games.

5.3 Evolutionary Game of APT Defense Game

Evolutionary APT games are dynamic games in which the attacker and the defender apply learning rules in multiple (attack and defense) time-intervals. According to the theory presented in Ch.2, the ESS of the game is expected, if it exists, to be over the pure strategies.

We consider S storage devices threatened by an APT attacker (A) and defended by a cloud storage defender (D). The attacker (or defender) wishes to take control of the storage devices by launching attacks (or performs scan) during specific time intervals. However, the time period to finish an attack is not known in advance to any of the players. During the k^{th} interactions between the attacker and the defender, we use y_i^k,

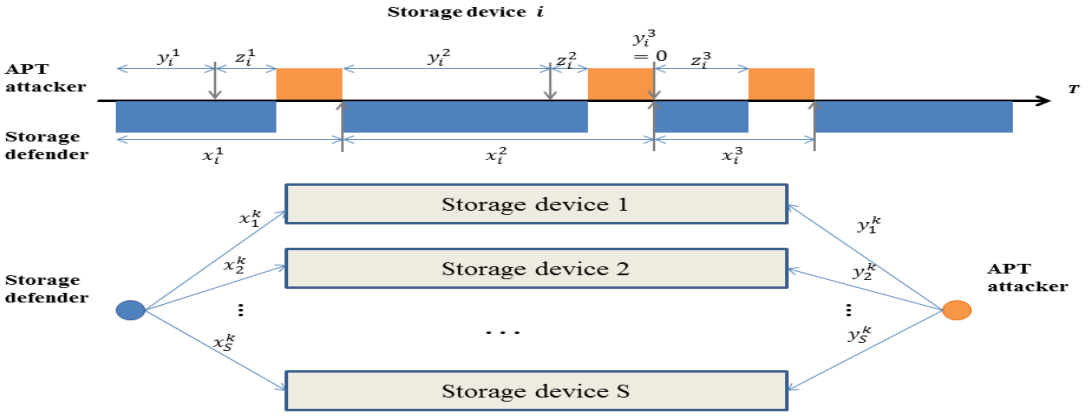


Figure 5.1: Illustration of the APT defense game.

x_i^k, and z_i^k as the time periods between two attacks, two scans, and the time to finish an attack on the i^{th} storage device, respectively. It is clear that $x_i^k > 0$ because the defender needs time to scan the storage device for any possible APT attacks.

Let y_i^k and x_i^k be the strategy for the attacker and defender to maximize their payoff. However, the evolutionary stable strategy is stronger and more stable than NE, since it is stable against small deviations from the ESS. In this game, each player will resist the small perturbations, and stick to the same strategy. The payoff of the defender depends on the gain to a defender to scan the i^{th} storage device denoted by G_i. The cost for the attacker to launch APT on the i^{th} storage device is denoted by C_i. As shown in Figure 5.1, the data stored on the i^{th} storage device is safe with a probability $\min((y_i+z_i)/x_i, 1)$, where the random variable z_i is the time required to finish the APT attack on the i^{th} device, which is usually not known in advance.

Similar to the assumption in [51], z is quantized into L non zero levels with the distribution $[P_l^i]_{0\le l\le L}$, where $P_l^i = Pr(z_i = l/L)$, with $0 \le l \le L$ and $0 \le i \le S$. The utility of the attacker denoted by $u_A(\mathbf{x}, \mathbf{y})$ and the utility of the defender $u_D(\mathbf{x}, \mathbf{y})$, are given by [51] as:

$$u_D(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{S} \sum_{l=0}^{L} P_l^i \min(\frac{Ly_i + l}{Lx_i}, 1) + x_i G_i \tag{5.1}$$

$$u_A(\mathbf{x}, \mathbf{y}) = -\sum_{i=1}^{S} \sum_{l=0}^{L} \left(P_l^i \min(\frac{Ly_i + l}{Lx_i}, 1) + I(y_i < x_i) C_i \right). \tag{5.2}$$

For the readers' convenience, we summarize our commonly used notations in Table 5.1.

5.4 ESS of the Dynamic APT Game

Each player aims to maximize his or her own utility optimization problem as follows:

$$\begin{aligned} \max_{\mathbf{x}} \quad & u_D(\mathbf{x}, \mathbf{y}) \\ \max_{\mathbf{y}} \quad & u_A(\mathbf{x}, \mathbf{y}) \\ \text{subject to} \quad & 0 < \sum_{i=1}^{S} x_i \leq 1, \\ & 0 \leq \sum_{i=1}^{S} y_i \leq 1, \\ & 0 < x_i \leq 1, \;\; 0 \leq y_i \leq 1, \forall 1 \leq i \leq S. \end{aligned} \tag{5.3}$$

The feasible action sets of the players in this game are predefined and known by both players. According to [51], potential NEs of the APT defense game with one storage device are $(0.5, 0)$, $(1, 0)$, and $(1, 1)$, which are the candidates of ESS.

We fist consider the ESS of the APT detection game with one storage device. In this case, Eqs.(5.1) and (5.2)can be simplified into:

$$u_D(x, y) = \sum_{l=0}^{2} P_l \min(\frac{2y + l}{2x}, 1) + xG \tag{5.4}$$

$$u_A(x, y) = -(\sum_{l=0}^{2} P_l \min(\frac{2y + l}{2x}, 1) + I(y < x)C), \tag{5.5}$$

where the strategies $(\mathbf{x}, \mathbf{y})$ are given by $\mathbf{x} = [x_1 \; x_2]^T = [0.5 \; 1]^T$, $\mathbf{y} = [y_1 \; y_2 \; y_3]^T = [0 \; 0.5 \; 1]^T$, and T denotes the transpose operation. In the mixed-strategy game, the attacker randomly chooses the strategy y with probability vector $[\delta_i]_{1 \leq i \leq 3}$, and the defender selects a strategy from x with probability vector $[\rho_i]_{1 \leq i \leq 2}$.The payoff table for this game is given in Table 5.2, where $a(i, j)$ means the payoff of an attacker plays strategy y_j against a defender plays strategy x_i. Similarly, $d(i, j)$ means the payoff of a defender plays strategy x_i against an attacker plays strategy y_j. According to [14], there is no mixed ESS under the RD. The RD equation in its general form is given in (2.3). Let $d\rho_i/dt = \dot{\rho}_i$ and $d\delta_j/dt = \dot{\delta}_j$, and define the following dummy variables: $\alpha_1(\rho_1, \rho_2) = a_{11}\rho_1 + a_{21}\rho_2$ and $\alpha_2(\rho_1, \rho_2) = a_{12}\rho_1 + a_{22}\rho_2$. Then the RD equations are

Table 5.2: Payoffs in an APT defense game with one device.

	$y_1 = 0$	$y_2 = 0.5$	$y_3 = 1$
$x_1 = 0.5$	(d_{11}, a_{11})	(d_{12}, a_{12})	(d_{13}, a_{13})
$x_2 = 1$	(d_{21}, a_{21})	(d_{22}, a_{22})	(d_{23}, a_{23})

given by the following system of nonlinear differential equations:

$$\dot{\rho_i} = \rho_i(1-\rho_i)(u_D(x_i, \mathbf{y}) - u_D(x_j, \mathbf{y})),\ if\ i \neq j \tag{5.6}$$

$$\dot{\delta_j} = \delta_j(u_A(\mathbf{x}, y_j) - \overline{u}_A(\mathbf{x}, \mathbf{y})) \tag{5.7}$$

$$\overline{u}_A(x, y) = (\alpha_1(\rho_1, \rho_2) + 1)\delta_1 + (\alpha_2(\rho_1, \rho_2) + 1)\delta_2 - 1, \tag{5.8}$$

where $\dot{\rho_i}$ represents the evolution of the defender choice towards using the strategy x_i, and $\dot{\delta_j}$ is the evolution of the APT-attacker choice towards using the strategy δ_j.

The ESS condition for the asymmetric game is given by Theorem 2 [14]. Note that we used 3 variables out of 5 variables, i.e, we used ρ_1, δ_1, and δ_2, and removed ρ_2 and δ_3. The reason is that they are dependent variables, so their time derivatives can be expressed in terms of the other variables as: $\rho_2 = 1 - \rho_1 \Rightarrow \dot{\rho_2} = -\dot{\rho_1}$, and $\delta_3 = 1 - \delta_1 - \delta_2 \Rightarrow \dot{\delta_3} = -\dot{\delta_1} - \dot{\delta_2}$. For an equilibrium point to be asymptotically stable [52], the eigenvalues of the Jacobian matrix should have negative real parts. Any point which is asymptotically stable will be an ESS candidate. As a result, the Jacobian matrix that is represented by (5.9) will be checked for the above pure strategies.

$$J = \begin{bmatrix} \frac{\partial \dot{\rho_1}}{\partial \rho_1} & \frac{\partial \dot{\rho_1}}{\partial \delta_1} & \frac{\partial \dot{\rho_1}}{\partial \delta 2} \\ \frac{\partial \dot{\delta_1}}{\partial \rho_1} & \frac{\partial \dot{\delta_1}}{\partial \delta_1} & \frac{\partial \dot{\delta_1}}{\partial \delta_2} \\ \frac{\partial \dot{\delta_2}}{\partial \rho_1} & \frac{\partial \dot{\delta_2}}{\partial \delta_1} & \frac{\partial \dot{\delta_2}}{\partial \delta_2} \end{bmatrix} \tag{5.9}$$

Claim 5.1. *Among all the game pure strategies, the following strategies are the only ESS candidates:*

(a) $(0,0,0)$ *or* $(\rho_2 = 1,$ *and* $\delta_3 = 1)$ *if* $0.5P_1 + P_0 < C$ *and* $0.5P_0 < C$.

(b) $(0,1,0)$ *or* $(\rho_2 = 1,$ *and* $\delta_1 = 1)$ *if* $G > P_1$, $C < 0.5P_1 + P_0$, *and* $P_1 + P_0 > 0$.

(c) $(1,1,0)$ *or* $(\rho_1 = 1,$ *and* $\delta_1 = 1)$ *if* $P_0 > C$ *and* $P_1 > G$.

Proof. The proof is divided into two parts, where in the first part we have to prove that the strategies mentioned in the claim above are asymptotically stable under some conditions. In the second part, we have to prove that the other strategies are not ESS candidates by proving them to be not asymptotically stable under any conditions. Testing for asymptotic stability is done by checking the negativity of eigenvalues of the Jacobian matrix that corresponds to each one of these strategies. Some of the eigenvalues of the Jacobian of these strategies will always have positive real part, which will exclude them from being asymptotically stable. Re-write equations (5.6) and (5.7) yielding,

$$\dot{\rho_1} = \rho_1(1-\rho_1)(D_1\delta_1 + D_2\delta_2 + D_3) \tag{5.10}$$

where,

$$D_1 = d_{11} + d_{23} - d_{21} - d_{13} \tag{5.11a}$$

$$D_2 = d_{12} + d_{23} - d_{22} - d_{13} \tag{5.11b}$$

$$D_3 = d_{13} - d_{23} \tag{5.11c}$$

$$\dot{\delta_1} = \delta_1((1+\alpha_1(\rho_1,\rho_2))(1-\delta_1) - (1+\alpha_2(\rho_1,\rho_2))\delta_2) \tag{5.12}$$

$$\dot{\delta_2} = \delta_2((1+\alpha_2(\rho_1,\rho_2))(1-\delta_2) - (1+\alpha_1(\rho_1,\rho_2))\delta_1) \tag{5.13}$$

The Jacobian matrix for the last RD system is given by (5.14),

$$J = \begin{bmatrix} T_3(1-2\rho_1) & D_1\rho_1(1-\rho_1) & D_2\rho_1(1-\rho_1) \\ \delta_1(T_5(1-\delta_1) - T_4\delta_2) & T_2(1-2\delta_1) - T_1\delta_2 & T_1\delta_1 \\ \delta_2(T_4(1-\delta_2) - T_5\delta_1) & -T_2\delta_2 & -(T_2\delta_1 + T_1(1+2\delta_2)) \end{bmatrix} \tag{5.14}$$

$T_1 = a_{12}\rho_1 + a_{22}(1-\rho_1) + 1$, $T_2 = a_{11}\rho_1 + a_{21}(1-\rho_1) + 1$, $T_3 = D_3 + D_1\delta_1 + D_2\delta_2$, $T_4 = a_{12} - a_{22}$, and $T_5 = a_{11} - a_{21}$. For the sake of simplicity, we represent the pure strategies in terms of the mixed strategies as follows: $(\rho_1,\ \rho_2,\ \delta_1,\ \delta_2,\ \delta_3)$, where $\rho_i's$ are the defender probabilities of choosing pure strategies and $\delta_j's$ are the attacker probabilities of choosing pure strategies, is written as $(\rho_1, \delta_1, \delta_2)$.

We first check the asymptotic stability of (0,0,0), which corresponds to the pure strategy that the defender will choose to wait longer before scanning the device, and the attacker will do the same, i.e, choosing x_1 $w.p$ $\rho_1 = 0,$ x_2 $w.p$ $\rho_2 = 1,$ y_1 $w.p$ $\delta_1 = 0,$ y_2 $w.p$ $\delta_2 = 0,$ y_3 $w.p$ $\delta_3 = 1.$

$$J_{(0,0,0)} = \begin{bmatrix} D_3 & 0 & 0 \\ 0 & a_{21}+1 & 0 \\ 0 & 0 & a_{22}+1 \end{bmatrix} \tag{5.15}$$

The strategy is asymptotically stable if $0.5P_1+P_0 < C$ and $0.5P_0 < C$. For the defender $D_3 < 0$ as given by (5.11a), if the attacker is using the strategy y_3, then the defender can gain more by using the strategy x_2 rather than the strategy x_1. On the other hand, the attacker needs to have $a_{21} < -1$ and $a_{22} < -1$, meaning that choosing the shorter waiting times $y_1 = 0$ and $y_2 = 0.5$ against a defender uses her longer waiting time strategy, x_2, will give the attacker lower rewards than when using her longest waiting time strategy y_3. In terms of the the payoffs, a_{21} and a_{22} are giving less than a_{23}.

Similarly, we can prove the asymptotic stability of (0,1,0) and (1,1,0), which is equivalent to check stability of the scenario in which the defender chooses the longest waiting period before scanning a device, and the attacker starts attacking without waiting, and the scenario in which the defender chooses the shorter waiting period to scan the device and an attacker continuously keeps attacking.

Checking (0,0,1) for Asymptotic Stability

This is equivalent to check the pure strategy where the defender chooses the longer waiting period, $x_2 = 1$, and the attacker uses the shorter waiting period, $y_2 = 0.5$, i.e, choosing x_2 $w.p$ 1, and y_2 $w.p$ 1. The eigenvalues are $D_2+D_3,$ $a_{21}-a_{22}$, and $-(a_{22}+1)$. However, to make the condition $a_{21} - a_{22} < 0$ means we need $P_1 + P_0 < 0$, which does not hold. As a result this strategy is not asymptotically stable. Similarly, we can prove that (1,0,0) and (1,0,1) are not asymptotically stable. □

Based on Claim 5.1, we can see that we are left with $(0, 0, 0)$, $(0, 1, 0)$, and $(1, 1, 0)$ as potential ESS strategies. Next, the ESS test given in Theorem 2 will be applied to

Table 5.3: Eigenvalues for pure strategies in Example 1

Point	Eigenvalues	Equivalent Strategy
$(0,0,0)$	$-0.45, -0.4, -0.05$	$(0,1,0,0,1)$
$(0,0,1)$	$-0.35, 0.4, 0.35$	$(0,1,0,1,0)$
$(0,1,0)$	$-0.2, 0.05, -0.35$	$(0,1,1,0,0)$
$(1,0,0)$	$-0.3, 0, 0.45$	$(1,0,0,0,1)$
$(1,1,0)$	$0.2, 0.3, 0.3$	$(1,0,1,0,0)$
$(1,0,1)$	$0.35, 0, -0.3$	$(1,0,0,1,0)$

each asymptotically stable point. In the next section, we will take a numerical example and show how the simulation results agree with the derivations shown above.

Numerical Example 1

In this example, an attacker and a defender compete to take control over a cloud storage device. The game is given by (5.3). For $G = 0.9, C = 0.5, P_0 = 0.2$, and $P_1 = 0.5$, the payoff matrices, and the replicator dynamics equations are given by:

$$D = \begin{bmatrix} d_{11} & d_{12} & d_{13} \\ d_{21} & d_{22} & d_{23} \end{bmatrix} = \begin{bmatrix} 1.25 & 1.45 & 1.45 \\ 1.45 & 1.8 & 1.9 \end{bmatrix} \tag{5.16}$$

$$A = \begin{bmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \\ a_{13} & a_{23} \end{bmatrix} = \begin{bmatrix} -1.3 & -1.05 \\ -1 & -1.4 \\ -1 & -1 \end{bmatrix} \tag{5.17}$$

$$\dot{\rho_1} = \rho_1(1-\rho_1)[0.25\delta_1 + 0.1\delta_2 - 0.45] \tag{5.18}$$

$$\dot{\delta_1} = -\delta_1[(0.05 - 0.25\rho_1)(1-\delta_1) + (-0.4 + 0.4\rho_1)\delta_2] \tag{5.19}$$

$$\dot{\delta_2} = \delta_2[(-0.4 - 0.4\rho_1)(1-\delta_2) + (0.05 + 0.25\rho_1)\delta_1] \tag{5.20}$$

The eigenvalues for each pure strategy were found, using the procedure in Figure 2.1, in order to validate our theoretical analysis. The Jacobian will be with respect to ρ_1, δ_1, and δ_2. The eigenvalues are given in Table 5.3.

One can see that $(0,0,1)$, $(1,0,0)$, and $(1,0,1)$ have positive eigenvalues as predicted by Claim 1. Next, the $(0,1,0)$ and $(1,1,0)$ strategies are eliminated too, because the asymptotic stability conditions for them do not hold, i.e, there are some eigenvalues that have nonnegative real parts. Finally, we are left with $(0,0,0)$ (which is $(0,1)$ for the defender and $(0,0,1)$ for the attacker) strategy as an asymptotically stable point, and hence a NE. According to [12], this asymptotically stable strategy is an ESS. However we find the same result by applying Theorem 2 to it as follows:
$(0,0,0) \Rightarrow \rho_1 = 0, \rho_2 = 1, \delta_1 = 0, \delta_2 = 0, \delta_3 = 1$. For the defender, $[0\ 1]D\mathbf{y}^T > \mathbf{x}D\mathbf{y}^T$. Where $\mathbf{y} = [y_1\ y_2\ y_3]$, $\mathbf{x} = [x_1\ x_2]$, and D is given by (5.16). After algebraic simplifications, we get $(0.2y_1 + 0.35y_2 + 0.45y_3)x_1 > 0$ for nonzero $y_j s,\ j = 1,2,3$ and x_1. At the same time, the attacker must have $[0\ 0\ 1]A\mathbf{x}^T > \mathbf{y}A\mathbf{x}^T$, and A is given by (5.17). After simplifications, we get $0.3x_1y_1 + (0.05y_3 + 0.4y_2)x_2 > 0$ for any nonzero $y_j's,\ j = 1,2,3$ and $x_i,\ i = 1,2$. Finding the regions where these inequalities hold is a problem that is known in nonlinear control literature [52] as the problem of finding the region of attraction. However, we will not discuss it here and will use the phase portrait to get a pictorial representation of these regions. The simulation results are shown in Figure 5.2, which shows clearly the concept of regions of attraction. Note that we used the pure strategies instead of the mixed strategies, which are used in Theorem 2. Figure 6.3 shows the strategies evolution from some initial conditions and the payoff associated with each strategy. Clearly, the payoff associated with the ESS strategy, which is in this case the defender chooses the shorter waiting period, $x_2 = 0.5$, $w.p\ 1$, and the attacker chooses the longest waiting period, $y_3 = 1$, $w.p\ 1$, is the highest payoff among all the other strategies for both players. The following claims provide more insight depending on the values of the defending gain and the attacking cost.

Claim 5.2. *If $C > 0.5P_1 + P_0$ and $G < P_1$, the APT defense game has one ESS candidate, which is the strategy* $(0,1,0,0,1)$.

Proof. : If $C > 0.5P_1 + P_0$, the conditions for asymptotic stability of $(0,1,1,0,0)$ and $(1,0,1,0,0)$ will not hold. In other words, the Jacobian matrix of these strategies will have eigenvalues with positive real parts, which means that they are not asymptotically

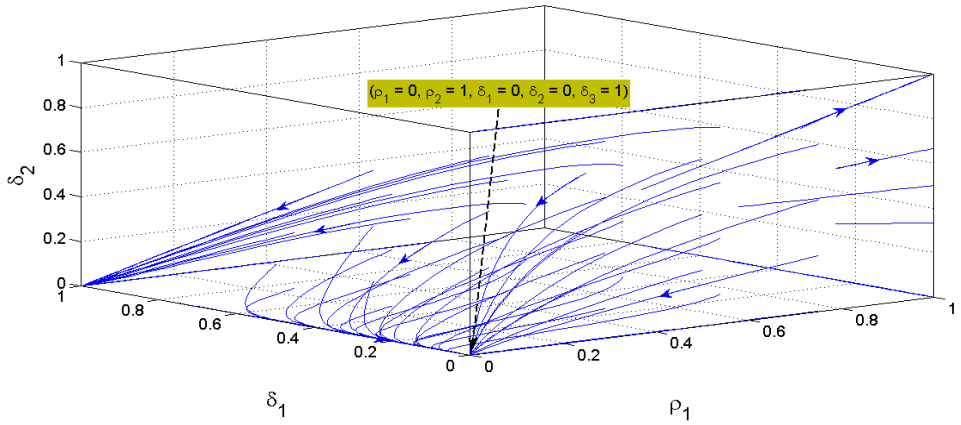


Figure 5.2: Phase portrait of of the dynamic game with $G = 0.9$, $C = 0.5$, $P_0 = 0.2$, and $P_1 = 0.5$.

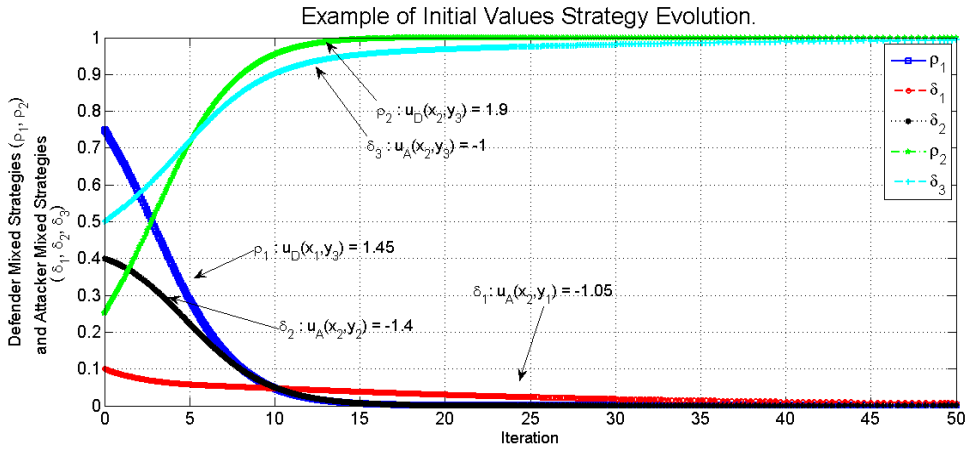


Figure 5.3: Strategies probability evolution of the APT defense game with $G = 0.9$, $C = 0.5$, $P_0 = 0.2$, and $P_1 = 0.5$. Initial values are: $\rho_1(0) = 0.75$, $\rho_1(0) = 0.25$, $\delta_1(0) = 0.1$, $\delta_2(0) = 0.4$, and $\delta_3(0) = 0.5$.

Table 5.4: Eigenvalues for pure strategies in Example 2

Point	Eigenvalues	Equivalent strategy
$(0,0,0)$	$-1.4, -1.05, -0.05$	$(0,1,0,0,1)$
$(0,1,0)$	$2, 1.05, -0.35$	$(0,1,1,0,0)$
$(1,1,0)$	$-0.2, 1.3, 1.3$	$(1,0,1,0,0)$

stable. As a result, the only asymptotically stable strategy will be $(0,1,0,0,1)$. The last strategy will be the only ESS candidate for the game. □

Numerical Example 2

The following example is to validate Claim 5.2. We assume the following parameters: $G = 0.1$, $C = 1.5$, $P_0 = 0.2$, and $P_1 = 0.5$. The cost of launching the attack is much higher than the defense gain. Initial values that represent the players' initial mixed strategies or weighted decisions of how to choose their pure strategies are: $\rho_1(0) = 0.75$, $\rho_1(0) = 0.25$, $\delta_1(0) = 0.1$, $\delta_2(0) = 0.4$, and $\delta_3(0) = 0.5$. From the stability analysis, we get the following eigenvalues, where the rest of the strategies are eliminated based on Claim 5.1. Figure 5.4 illustrates the probability evolution for selecting the pure strategies and the payoff for each strategy. It can be seen that the asymptotically stable strategies have the highest payoffs for both players. The phase portrait for this example is given by Figure 5.5.

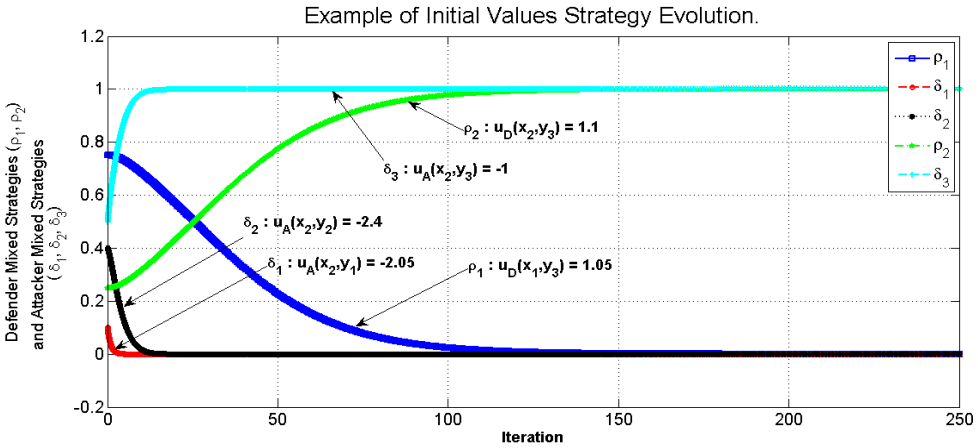


Figure 5.4: Strategies probability evolution of the APT defense game with $G = 0.1$, $C = 1.5$, $P_0 = 0.2$, and $P_1 = 0.5$. Initial values are: $\rho_1(0) = 0.75$, $\rho_1(0) = 0.25$, $\delta_1(0) = 0.1$, $\delta_2(0) = 0.4$, and $\delta_3(0) = 0.5$.

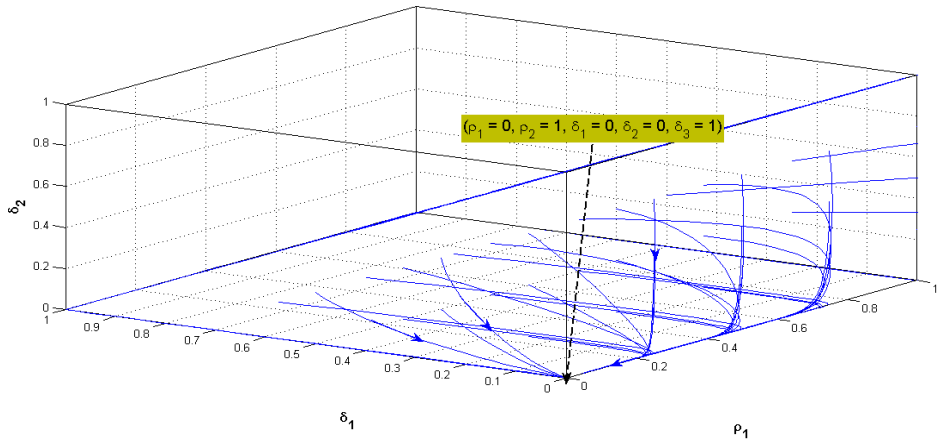


Figure 5.5: Phase portrait of the dynamic game with $G = 0.1$, $C = 1.5$, $P_0 = 0.2$, and $P_1 = 0.5$.

Table 5.5: Eigenvalues for pure strategies in Example 3

Point	Eigenvalues	Equivalent strategy
$(0, 0, 0)$	$-10.75, 0, 0.35$	$(0, 1, 0, 0, 1)$
$(0, 1, 0)$	$-0.5, -0.35, -0.35$	$(0, 1, 1, 0, 0)$
$(1, 1, 0)$	$-0.1, -0.1, 0.5$	$(1, 0, 1, 0, 0)$

Claim 5.3. *If the defending gain is $G > P_1$ and the attacking cost is $C < 0.5P_0$, then the game has one ESS candidate. The attacker will continuously keep attacking the device and the defender will choose the longest waiting period to scan the device, i.e,* $(0, 1, 1, 0, 0)$.

Proof. The proof follows from Claim 1, where we have three possible asymptotically stable points. If $G > P_1$ and $C < 0.5P_0$, the conditions for asymptotic stability for $(1, 0, 1, 0, 0)$ and $(0, 1, 0, 0, 1)$ do not hold, because the Jacobian matrix for these strategies will have eigenvalues with positive real part which makes them unstable. On the other hand, the only asymptotically stable point is $(0, 1, 1, 0, 0)$. □

Numerical Example 3

The following example is to validate Claim 5.3. We take the following parameters: $G = 1.5$, $C = 0.1$, $P_0 = 0.2$, $P_1 = 0.5$, $\boldsymbol{\rho}(\mathbf{0}) = [0.75, 0.25]$, and $\boldsymbol{\delta}(\mathbf{0}) = [0.1, 0.4, 0.5]$. The probability evolutions of the game show that the asymptotically stable strategies have the highest payoffs for both players (see Figure 5.6). The phase portrait as shown

in Figure 5.7 indicates that the $(0, 1, 0)$ is the only asymptotically stable strategy.

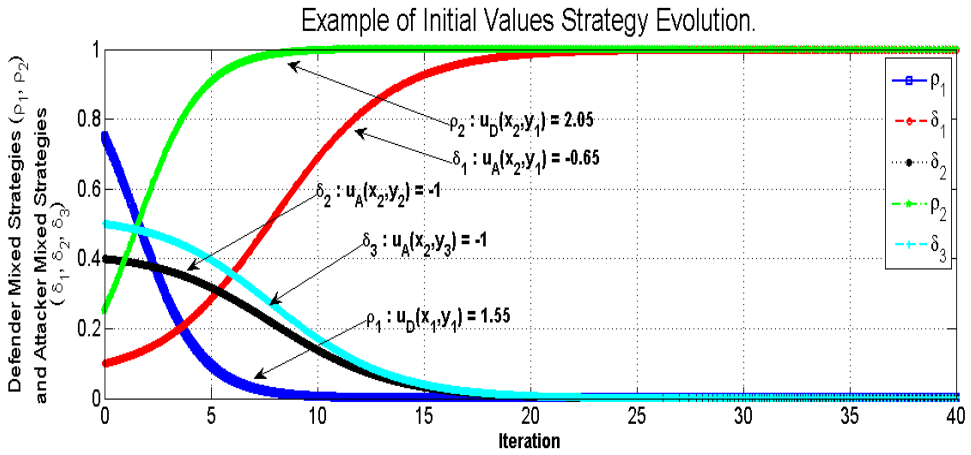


Figure 5.6: Strategy evolution of the APT defense game with $G = 1.5$, $C = 0.1$, $P_0 = 0.2$, and $P_1 = 0.5$. Initial values are: $\rho_1(0) = 0.75$, $\delta_1(0) = 0.1$, and $\delta_2(0) = 0.4$.

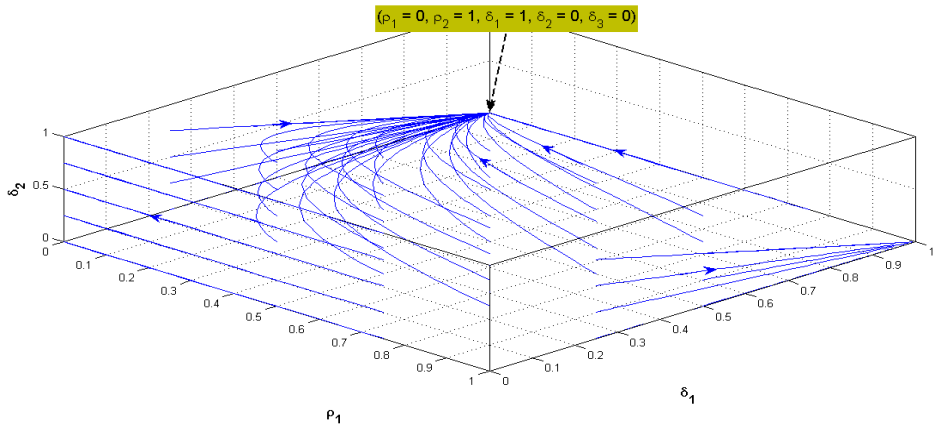


Figure 5.7: Phase portrait of the dynamic game with $G = 1.5$, $C = 0.1$, $P_0 = 0.2$, and $P_1 = 0.5$.

Now we consider the ESS of the APT defense game with multiple storage devices, which are S storage devices or data centers that are threatened by an APT attacker, whose strategies are $[y_{i,j}]_{1\leq j\leq S},\ i = 1, 2$. The defense strategies are $[x_{i,j}]_{1\leq j\leq S},\ i = 1, 2$, meaning that the attacker waits y_s time units before attacking the s^{th} device and the defender waits x_s time units before scanning the s^{th} device. The strategies in the mixed-strategy APT defense game are given by $\delta = [\delta_i]_{1\leq i\leq 2}$ and $\rho = [\rho_i]_{1\leq i\leq 2}$, where δ_i is the probability for the attacker to choose $\mathbf{y}_i$, and ρ_i is the probability for the defender to choose $\mathbf{x}_i$. The cost vector for attacks denoted by $\mathbf{C}$ is given by $[C_i]_{1\leq i\leq S}$, and the defense vector gain $\mathbf{G}$ is given by $[G_i]_{1\leq i\leq S}$. The utilities for the strategies are given in

Table 5.6: Payoffs in the storage game

	$\mathbf{y_1}$	$\mathbf{y_2}$
$\mathbf{x_1}$	$u_D(\mathbf{x_1}, \mathbf{y_1}), u_A(\mathbf{x_1}, \mathbf{y_1})$	$u_D(\mathbf{x_1}, \mathbf{y_2}), u_A(\mathbf{x_1}, \mathbf{y_2})$
$\mathbf{x_2}$	$u_D(\mathbf{x_2}, \mathbf{y_1}), u_A(\mathbf{x_2}, \mathbf{y_1})$	$u_D(\mathbf{x_2}, \mathbf{y_2}), u_A(\mathbf{x_2}, \mathbf{y_2})$

Table 5.6 according to $u_H(\mathbf{x_i}, \mathbf{y_j}) = \sum_{s=1}^{S} u_H^s(\mathbf{x_i}, \mathbf{y_j})$, where $H = \{D, A\}$ and $u_H^s(\mathbf{x_i}, \mathbf{y_j})$ is the utility function of player H for defending (attacking) the s^{th} storage device.

Replicator Dynamics

The ESS of the asymmetric APT defense game with two strategies can be derived via the procedure as shown in Figure 2.1. According to Theorem 9.8 in [23], any asymptotically stable strategy is equivalent to an ESS. Let $\rho_1 = \rho$, $\rho_2 = 1 - \rho$, $\delta_1 = \delta$, and $\delta_2 = 1 - \delta$, we get the following system of nonlinear differential equations,

$$\dot{\rho} = \rho(1 - \rho)(u_D(\mathbf{x_1}, \mathbf{y}) - u_D(\mathbf{x_2}, \mathbf{y})) \tag{5.21}$$

$$\dot{\delta} = \delta(1 - \delta)(u_A(\mathbf{x}, \mathbf{y_1}) - u_A(\mathbf{x}, \mathbf{y_2})). \tag{5.22}$$

Notice that $\dot{\rho}_2 = -\dot{\rho}$ or $\dot{\delta}_2 = -\dot{\delta}$. Let $\hat{d}_{ij} = u_D(\mathbf{x_i}, \mathbf{y_j})$, and $\hat{a}_{ij} = u_A(\mathbf{x_i}, \mathbf{y_j})$.
After simplification, we have

$$\dot{\rho} = \rho(1 - \rho)(\hat{D}_1\delta + \hat{D}_2) \tag{5.23}$$

and

$$\dot{\delta} = \delta(1 - \delta)(\hat{D}_3\rho + \hat{D}_4), \tag{5.24}$$

where

$$\hat{D}_1 = \hat{d}_{11} + \hat{d}_{22} - \hat{d}_{12} - \hat{d}_{21} \tag{5.25a}$$

$$\hat{D}_2 = \hat{d}_{12} - \hat{d}_{22} \tag{5.25b}$$

$$\hat{D}_3 = \hat{a}_{11} + \hat{a}_{22} - \hat{a}_{12} - \hat{a}_{21} \tag{5.25c}$$

$$\hat{D}_4 = \hat{a}_{21} - \hat{a}_{22}. \tag{5.25d}$$

The Jacobian matrix of the dynamic game is given by

$$J_{(\rho,\delta)} = \begin{bmatrix} (1-2\rho)(\hat{D}_1\delta + \hat{D}_2) & \hat{D}_1(1-\rho)\rho \\ \hat{D}_3(1-\delta)\delta & (1-2\delta)(\hat{D}_3\rho + \hat{D}_4) \end{bmatrix}. \tag{5.26}$$

The ESS(s), if any, are the pure strategies that are asymptotically stable. Asymptotic stability of the pure strategies corresponds to the strategies which give stable eigenvalues to the Jacobian matrix given in (5.26).

Without loss of generality, we now focus on the case of two storage devices (S=2) and discuss the specifics of the ESS and asymptotically stable NE obtained for this case. Each player has two strategies to choose from, i.e, each player divides the waiting time to scan (attack) between the two devices. The available strategies for the players are: $\mathbf{x_1} = (0.75, 0.25)$, meaning that the defender will wait 0.75 time units before scanning the first device and 0.25 time units before scanning the second device, and $\mathbf{x_2} = (0.5, 0.5)$ for the defender. Similarly, the attacker strategies are $\mathbf{y_1} = (1, 0)$ and $\mathbf{y_2} = (0.5, 0.5)$. The strategies are chosen as, $\mathbf{y_1}$ w.p δ_1, $\mathbf{y_2}$ w.p δ_2, $\mathbf{x_1}$ w.p ρ_1, and $\mathbf{x_2}$ w.p ρ_2. $u_H(\mathbf{x} = \mathbf{x_i}, \mathbf{y} = \mathbf{y_j}) = u_H^1(\mathbf{x} = \mathbf{x_i}, \mathbf{y} = \mathbf{y_j}) + u_H^2(\mathbf{x} = \mathbf{x_i}, \mathbf{y} = \mathbf{y_j})$, where $H = \{D, A\}$, and $u_H^1(\mathbf{x} = \mathbf{x_i}, \mathbf{y} = \mathbf{y_j})$ is the utility function for defending (attacking) the first storage device. Similarly, $u_H^2(\mathbf{x} = \mathbf{x_i}, \mathbf{y} = \mathbf{y_j})$ is the utility function for defending (attacking) the second storage device.

Based on the stability of the rest points of the RD system in (5.21) and (5.22), we get the following claim:

Claim 5.4. *In the APT defense game with two devices, the mixed strategy* $(\rho, \delta) = ([0, 1], [1, 0])$ *is not an ESS.*

Proof. This claim has two parts. First, we prove that the other game pure strategies can be asymptotically stable under some conditions. This will be shown through asymptotic stability. Second, we prove that this strategy is not asymptotically stable. We start by proving that there are ESS candidates under some conditions.

Checking (0,0) for Asymptotic Stability

This is equivalent to checking the pure strategy $(\mathbf{x_2}, \mathbf{y_2})$ for being asymptotically stable.

$$J_{(0,0)} = \begin{bmatrix} \hat{D}_2 & 0 \\ 0 & \hat{D}_4 \end{bmatrix}. \tag{5.27}$$

The eigenvalues of the Jacobian matrix in (5.27) are $\hat{D}_2$ and $\hat{D}_4$. By Eq.s (5.25b and 5.25d), this strategy is locally asymptotically stable if $G_1 + G_2 > 2.68P_0$ and $P_0 < C_2$. Furthermore, the eigenvalue $\hat{D}_2$ which is given by (5.25b) has to be negative, indicating that $\hat{d}_{22} > \hat{d}_{12}$ which holds as long as $0.25G_1 + 0.5G_2 < P_0$ holds. For the attacker, the eigenvalue $\hat{D}_4$, where $\hat{D}_4$ is given by (5.25d), has to be negative. This means that $\hat{a}_{21} < \hat{a}_{22}$ or the payoff for the attacker uses the strategy $\mathbf{y_2}$, is higher than using the strategy $\mathbf{y_1}$ against a defender using the strategy $\mathbf{x_2}$. This holds by setting $P_0 < C_2$, which is the second condition. Similarly, we can prove that $(1, 0)$, $(1, 1)$, and $(0, 1)$ are not asymptotically stable as well. As a result, this strategy cannot be locally asymptotically stable. □

Let $P_0 = 0.4,\ G_1 = 0.4,\ G_2 = 0.4,\ C_1 = 0.3$, and $C_2 = 0.5$. It is clear that the conditions to get negative eigenvalues of the Jacobian matrix in (5.27) hold and thus the strategy $(0, 0)$ (i.e., $\rho_1 = 0,\ \rho_2 = 1,\ \delta_1 = 0$, and $\delta_2 = 1$) is locally asymptotically stable in the game with two storage devices. Figure 5.8 presents the evolution of the probabilities for selecting the pure strategies for a specific set of initial conditions accompanied with the utility of each player at each of these strategies, showing that the ESS strategy gives both player the highest payoff. Figure 5.9 shows that for all the initial conditions, the game will evolve to $(0, 0)$.

5.5 Conclusions

In this chapter, we analyzed the APT attack/defense strategies for cloud storage using evolutionary game theory, and we formulated two APT games with discrete strategies. The first game corresponds to the APT defense of a single one storage device regarding the attack and defense time periods. The second game extends the discussion to

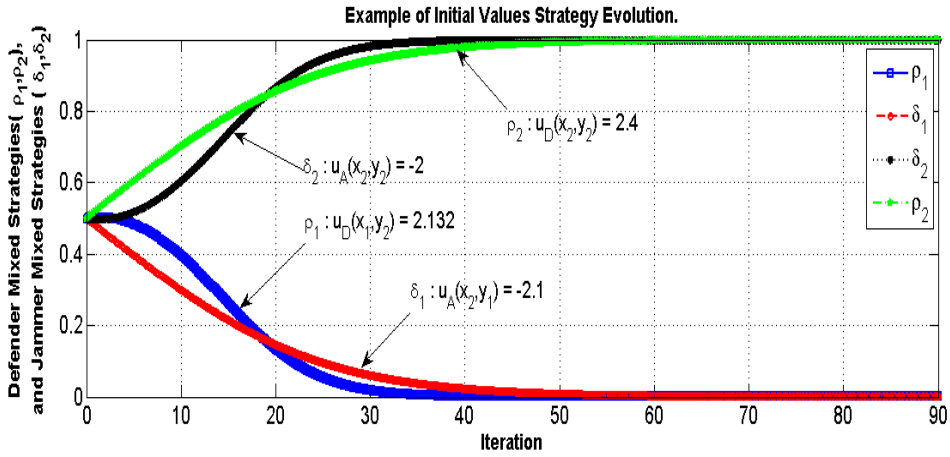


Figure 5.8: Strategies probability evolution of the APT defense game with $P_0 = 0.4$, $G_1 = 0.4$, $G_2 = 0.4$, $C_1 = 0.3$, $C_2 = 0.5$, and $\rho_1(0) = \rho_2(0) = \delta_1(0) = \delta_2(0) = 0.5$.

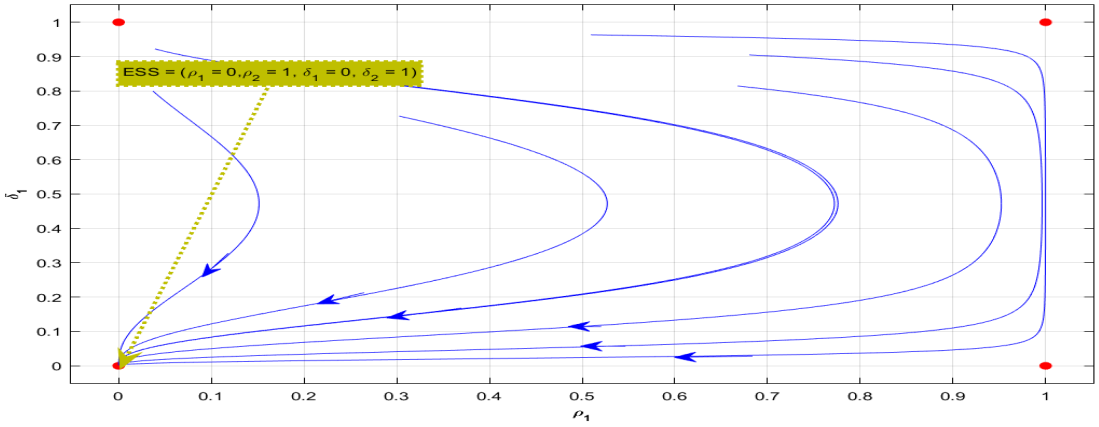


Figure 5.9: Phase portrait of the dynamic game with two storage devices with $P_0 = 0.4$, $G_1 = 0.4$, $G_2 = 0.4$, $C_1 = 0.3$, and $C_2 = 0.5$.

multiple storage devices. The dynamical stability of the cloud storage systems were investigated using the replicator dynamics criteria to characterize the locally asymptotically stable equilibrium strategies. The ESS of the APT defense game is derived and the conditions under which each ESS exists are provided to show how the initial scan and attack intervals, the APT attack duration and cost, and the defense cost change the APT defense performance. We have provided the phase portraits to show the locally asymptotically stable points of each game, which represent the NE of the game, and show the relation between the asymptotic stability and evolutionary stability.

Chapter 6

LTE-U WiFi Coexistence

6.1 Introduction

The number of wireless devices has been increasing over the last decade and it has been estimated that the data traffic requirement is going to rise as well. According to the study by Cisco, the traffic carried over mobile wireless networks will observe a 7x growth by 2021 [53]. These high demands have motivated opening of newer wireless spectrum bands and prompted the research community to look for innovative techniques to increase the spectrum usage efficiency. Providing high throughput while maintaining the quality-of-service (QoS) in wireless networks is a primary goal for service providers. Towards this goal, several revisions have been proposed in Long Term Evolution (LTE), which is currently the most popular standard for mobile wireless communication with capabilities such as carrier aggregation (CA), use of higher order multiple-input multiple-output (MIMO) techniques, and small cell deployment with enhanced intercell interference coordination (eICIC) to support Heterogeneous Networks (HetNets). However, all these improvements are still restricted by the limited bandwidth of licensed spectrum. Therefore the service providers are looking towards readily available unlicensed spectrum for further improvement in the throughput. LTE-unlicensed (LTE-U) has been proposed in LTE release 13 as a technique for accessing the unlicensed spectrum in conjunction with the licensed spectrum. One of the major challenges for LTE-U is the presence WiFi devices in the unlicensed spectrum. WiFi is a widely popular and ubiquitous technology for enabling wireless broadband access, and therefore it is very important for any new entrant such as LTE-U to coexist amicably with WiFi in the unlicensed bands. The main challenge of such coexistence is the difference in medium access techniques of these two technologies. WiFi uses carrier-sense

multiple access with collision avoidance (CSMA/CA) which supports exponential back-off to coexist with other unlicensed devices. LTE-U accesses the channel in a periodic manner such that it transmits the signal only in a fractional duration of this period. The ON duration of this transmission is determined by the duty cycle which is one of the most important parameters for LTE-U. In an uncoordinated environment, the WiFi can attempt to transmit only during the OFF duration of LTE-U. The duty cycle of the transmission is a configurable parameter, thus making the LTE-U transmission more adaptable to any changes in the environment.

The main contributions of this work are as follows: (1) We formulate a coexistence game using the evolutionary game theory to study the dynamic behavior of the LTE-U and WiFi APs serving multiple users in the same area with replicator dynamics. (2) The stability and the robust solutions of the coexistence game are investigated according to the ESS criteria. (3) We indicate the conditions under which the coexistence game has the ESS for any given initial conditions, and depict some of them pictorially. (4) We formulate an optimization problem where the WiFi AP can exclude some of its users based on a given minimum SINR and derive the corresponding stable strategies and their stability conditions. (5) We formulate a classical game theoretical model that assumes continuum of strategies and study the stability of the derived Nash Equilibrium (NE) under the Replicator Dynamics (RD).

6.2 Related work

The coexistence between LTE and WiFi has been addressed from different perspectives in the literature. However, the following papers, which are by no means intended to be a comprehensive list, are of particular interest to our work. The authors in [54] addressed the coexistence problem by controlling both the duty cycle and the power level of LTE-U AP using a multi-armed bandit algorithm. The authors found that the LTE-U AP has incentives to reduce its transmission power/duty cycle because the interference to other LTE-U APs and WiFi APs would make them use higher power levels and this will create more interference in the network. A joint uplink-downlink LTE-U/WiFi coexistence problem is addressed in [55], where the LTE-U APs

optimize the aggregate data rate on both the licensed and the unlicensed bands by optimizing user and spectrum association parameters. These parameters are chosen according to a learning algorithm called Echo State Networks. A multi-game framework is proposed in [56], where the WiFi users are considered as leaders, while the LTE-U APs are the followers. Another game theoretic formulation to this problem is given in [57], where the authors considered the coexistence as a power control game. The last two papers share with this work, independently, the ability of the WiFi AP to be an active player in the game. However, in this work, the strategies to be controlled by the LTE-U and WiFi APs are different from the previous efforts. In addition to the usage of different game parameters, we use evolutionary game theory to address this problem where the game dynamics are captured by the use of replicator dynamics. Replicator dynamics is considered here as a learning tool to reach to a more robust equilibrium strategy. Evolutionary game theory has been used to study the dynamics of many competing scenarios. In [24], two evolutionary games to model multiple access control in a slotted Aloha wireless network and power control for a wideband CDMA system are presented. In [26], evolutionary games are used for small cells distributed resource allocation, where it is used for subcarrier and power allocation for the small cell base stations. Potential games and evolutionary dynamics are used to address the noncooperative routing problem in [27]. A pricing evolutionary game between users and video streaming service providers is presented in [29]. A recent survey on evolutionary game applications is presented in [49], where the authors considered specific engineering applications based on evolutionary games, such as building dynamic dispatch algorithms in smart grids. In this chapter, we formulate an asymmetric evolutionary game between two populations (the WiFi APs and the LTE-U APs) and explicitly find the evolutionary stable strategies for the proposed games using the evolutionary game theories. For the reader's convenience, we summarize our commonly used symbols in Table 6.1.

6.3 Evolutionary Game of LTE-U and WiFi Coexistence

In this chapter, we consider wireless users with capabilities of opportunistically utilizing any of the multiple available wireless technologies. Fig. 6.1 presents once such case for

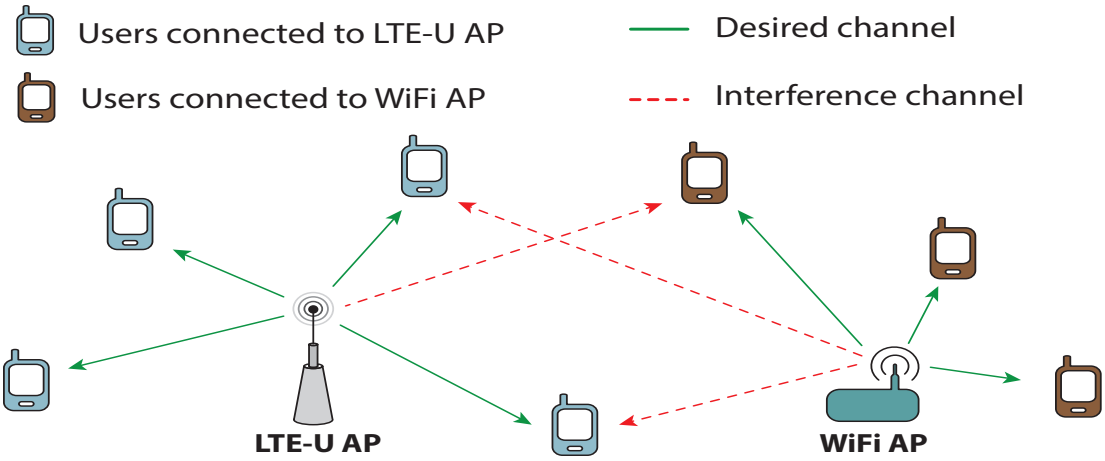


Figure 6.1: Illustration of The WiFi/LTE-U Coexistence Game.

Table 6.1: Summary of Symbols

Symbol	Description
N_L/N_W	Number of users connected to the LTE-U AP/WiFi AP
$P^L_{(.)}/P^W_{(.)}$	Power level used by the LTE-U AP/WiFi AP
h^L_i/h^W_i	Channel coefficient between the i^{th} user and LTE-U AP/WiFi AP
T_o	ON duration in a duty cycle for LTE-U AP transmission
α	A non negative number that reflects the benefit from increasing the duty cycle measured in per time unit.
γ	A non negative number that reflects the cost of increasing the duty cycle measured in power per time unit.
C_L/C_W	The transmission cost for the LTE-U AP/ WiFi AP

a scenario with two wireless technologies namely WiFi and LTE-U. In our analysis, we assume that devices utilizing the same technologies do not interfere with each other. This is a valid assumption since the WiFi interference is taken care by CSMA/CA, and LTE-U interference is handled by proper scheduling of resources. We formulate a game between the two populations using these two different technologies, where each population has different interests and strategies. We assume that each WiFi AP has discrete transmission powers to choose from, while the LTE-U AP can not only select discrete power levels but also the duty cycle. We also assume, as in [58], that each AP utility is a function of its users' utility functions. Because the interaction is continuous, the game can be viewed as a dynamic game. The ESS in such a case is a pure strategy that is asymptotically stable under the RD.

- The utility function for the i^{th} user of LTE-U AP is

$$u_i^L(P_k^L, T_o, P_j^W) = \frac{1}{N_L}\left(\frac{h_i^L P_k^L}{\sigma^2 + h_i^W P_j^W} + \alpha T_o\right) - (P_k^L + \gamma T_o)C_L,\ i = 1, ..., N_L. \tag{6.1}$$

- The utility function for the m^{th} user of WiFi AP is

$$u_m^W(P_k^L, T_o, P_j^W) = \frac{1}{f(N_W)}\left(\frac{h_m^W P_j^W}{\sigma^2 + h_m^L P_k^L} - \alpha T_o\right) - P_j^W C_W,\ m = 1, ..., N_W. \tag{6.2}$$

where $f(N_W)$ is an increasing function that indicates that the WiFi AP utility is affected by increasing the number of users more than the LTE-U. It is assumed here, for simplicity, as $f(N_W) = \beta N_W,\ \beta \geq 1$. Without loss of generality and for the sake of mathematical simplifications, we assume that each WiFi AP can choose from two power levels, i.e, $P_{(.)}^W \in \mathbb{P} = \{P_1, P_2\}$, and the LTE-U APs can choose from two transmission power levels $P_{(.)}^L \in \mathbb{P}$ and two transmit durations, i.e, $T_o \in \mathbb{T} = \{T_1, T_2\}$. The WiFi and LTE-U AP's utilities are increasing functions of their users' utilities. These utilities are defined below.

- The LTE-U AP Utility Function

$$U_L(P_k^L, T_o, P_j^W) = \frac{1}{N_L}\left(\frac{\sum_{i=1}^{N_L} h_i^L P_k^L}{I_W(P_j^W)} + N_L \alpha T_o\right) - N_L(P_k^L + \gamma T_o)C_L, \tag{6.3}$$

where $I_W(P_j^W) = \sum_{i=1}^{N_L}(\sigma^2 + h_i^W P_j^W)$ is the interference from the WiFi AP that uses power transmission level j, $T_o \in \mathbb{T}$, and $\{P_k^L, P_j^W\} \in \mathbb{P}$.

- The WiFi AP Utility Function

$$U_W(P_k^L, T_o, P_j^W) = \frac{\sum_{m=1}^{N_W} h_m^W P_j^W}{\beta N_W I_L(P_k^L)} - \frac{\alpha T_o}{\beta} - N_W P_j^W C_W \tag{6.4}$$

where $I_L(P_k^L) = \sum_{m=1}^{N_W}(\sigma^2 + h_m^L P_k^L)$ is the interference from the WiFi AP that uses power transmission level k, $T_o \in \mathbb{T}$, and $\{P_k^L, P_j^W\} \in \mathbb{P}$. There are intuitive reasons for adding the cost terms in (6.1) and (6.2). In [57], the authors justified it as the

transmit power cost of the APs. In [58], the authors justified it as the interference cost to the other APs. In this chapter, we consider it as a combination of costs which result from power consumption and interference. The next claim uses the concept of potential functions to prove that maximizing the AP's utilities in (6.3) and (6.4) is the same as maximizing each AP user's utility, as expressed in (6.1) and (6.2), respectively. Potential functions are very useful, because they allow studying the NE of a single function that does not depend on a particular player [39]. More explicitly, the NE of the individual players and the NE that results from the potential function are the same. In this chapter, this equivalence in the NE means that when each AP optimizes its potential function, it optimizes the utility functions of the users connected to it.

Claim 6.1. ***(a)*** *(6.3) is a potential function for the LTE-U users whose individual utility function is given by (6.1).* ***(b)*** *(6.4) is a potential function for the WiFi users whose individual utility function is given by (6.2).*

Proof. **(a)** According to [39], for $U_L(P_k^L, T_o, P_j^W)$ to be a potential function, it must satisfy the conditions that if

$$u_i^L(P_2^L, T_o, P_j^W) - u_i^L(P_1^L, T_o, P_j^W) \geq 0,$$

then

$$U_L(P_2^L, T_o, P_j^W) - U_L(P_1^L, T_o, P_j^W) \geq 0,$$

and vice versa. By using Eqs. (6.1) and (6.3), we get:

$$\frac{h_i^L(P_2 - P_1)}{N_L I_W(P_j^W)} - (P_2 - P_1)C_L \geq 0,$$
$$\frac{\sum_{i=1}^{N_L} h_i^L(P_2 - P_1)}{N_L I_W(P_j^W)} - N_L(P_2 - P_1)C_L \geq 0.$$

As a result Eqs. (6.3) and (6.4) are potential functions. Proving part **(b)** results from redoing the previous calculations to Eqs. (6.2) and (6.4). □

6.4 ESS of the Dynamic Coexistence Game

The game in its normal form is shown in Table 6.2, where the WiFi AP is represented by the column player and the LTE-U AP is the row player. The WiFi AP chooses

Table 6.2: Normal Form Coexistence Game

		WiFi AP	
		P_1 w.p. δ_1	P_2 w.p. δ_2
LTE-U AP	$x_1 = (P_1, T_1)$ w.p. ρ_1	(a_{11}, b_{11})	(a_{12}, b_{12})
	$x_2 = (P_1, T_2)$ w.p. ρ_2	(a_{21}, b_{21})	(a_{22}, b_{22})
	$x_3 = (P_2, T_1)$ w.p. ρ_3	(a_{31}, b_{31})	(a_{32}, b_{32})
	$x_4 = (P_2, T_2)$ w.p. ρ_4	(a_{41}, b_{41})	(a_{42}, b_{42})

it strategies $\mathbf{P} = \{P_i\}_{i=1,2}$ with probabilities $\boldsymbol{\delta} = \{\delta_i\}_{i=1,2}$. Similarly, the LTE-U AP chooses its strategies $\mathbf{x} = \{x_j\}_{j=1,2,3,4}$ with probabilities $\boldsymbol{\rho} = \{\rho_j\}_{j=1,2,3,4}$. It can be noted that a_{ji} is the payoff of the LTE-U AP when it uses the strategy x_j against a WiFi AP using the strategy P_i , and similarly, b_{ji} is the payoff of the WiFi AP using the strategy P_i against an LTE-U AP using the strategy x_j. Each player (AP) aims to maximize its own utility by solving the following optimization problems:

$$\begin{aligned}
&\underset{\boldsymbol{\rho}}{\text{maximize}} \;\; U_L(P_k^L, T_o, P_j^W) \\
&\underset{\boldsymbol{\delta}}{\text{maximize}} \;\; U_W(P_k^L, T_o, P_j^W) \\
&\text{subject to:} \quad 0 \leq \sum_{i=1}^{4} \rho_i \leq 1, \quad 0 \leq \sum_{i=1}^{2} \delta_i \leq 1, \\
&\qquad\qquad 0 \leq \{\rho_i\}_{i=1,2,3,4} \leq 1, \; 0 \leq \{\delta_i\}_{i=1,2} \leq 1.
\end{aligned} \tag{6.5}$$

The feasible action sets of the players in this game are predefined and known by both players. According to [14], there is no mixed ESS under the RD. The RD equation in its general form is given in (2.3). Let $\frac{d\rho_i}{dt} = \dot{\rho}_i$ and $\frac{d\delta_j}{dt} = \dot{\delta}_j$, then the RD equations are given by the following system of nonlinear differential equations:

$$\dot{\delta}_i = \delta_i(1 - \delta_i)(U_W(\mathbf{x}, P_1^W) - U_W(\mathbf{x}, P_2^W)), \tag{6.6}$$

$$\dot{\rho_j} = \rho_j(U^L(x_j, \mathbf{P}) - \overline{U}^L(\mathbf{x}, \boldsymbol{\delta})), \tag{6.7}$$

$$\overline{U}^L(\mathbf{x}, \boldsymbol{\delta}) = \sum_{j=1,2,3,4} \rho_j U^L(x_j, \mathbf{P}) \tag{6.8}$$

$$U^L(x_j, \mathbf{P}) = \sum_{i=1,2} \delta_i a_{ji}, \; j = 1, 2, 3, 4, \tag{6.9}$$

$$U_W(\mathbf{x}, P_i^W) = \sum_{j=1,2,3,4} \rho_j b_{ji}, \; i = 1, 2, \tag{6.10}$$

where $\dot{\delta}_i$ represents the evolution of the WiFi AP choice towards using the strategy P_i, and $\dot{\rho}_j$ is the evolution of the LTE-U AP choice towards using the strategy x_j.

For an equilibrium point to be asymptotically stable [52], the eigenvalues of the Jacobian matrix should have negative real parts. Generally speaking, any point which is asymptotically stable will be an ESS candidate. As a result, the following Jacobian matrix will be checked for the above pure strategies.

$$J = \begin{bmatrix} \frac{\partial \dot{\delta_1}}{\partial \delta_1} & [\frac{\partial \dot{\delta_1}}{\partial \rho_{j=1,2,3}}] \\ [\frac{\partial \dot{\rho}_{j=1,2,3}}{\partial \delta_1}] & [\frac{\partial \dot{\rho}_{j=1,2,3}}{\partial \rho_{j=1,2,3}}] \end{bmatrix}_{4\times 4} \tag{6.11}$$

Claim 6.2. *All the pure game strategies can be locally asymptotically stable given that their trajectories start sufficiently close in their neighborhood and the convergence conditions given in Table 6.3 hold.*

Proof. We provide a detailed proof only for Case 1 since the other cases follow a similar pattern. Pure strategies for Case 1 are: the WiFi AP chooses to use the higher transmission power level, P_2, with probability one, i.e. $\delta_2 = 1$, while the LTE-U AP chooses the first strategy $x_1 = (P_1, T_1)$ with probability one, i.e $\rho_1 = 1$. This strategy shows that the WiFi AP is getting aggressive, uses P_2, against a friendly LTE-U AP. The Jacobian matrix of the RD for Case 1 is

$$J_{(0,1,0,0)} = \begin{bmatrix} b_{11} - b_{12} & 0 & 0 & 0 \\ 0 & a_{42} - a_{12} & a_{42} - a_{22} & a_{42} - a_{32} \\ 0 & 0 & a_{22} - a_{12} & 0 \\ 0 & 0 & 0 & a_{32} - a_{12} \end{bmatrix}.$$

The eigenvlaue $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ of $J_{(0,1,0,0)}$ are the diagonal elements of this matrix.

$$\lambda_1 = a_{22} - a_{12}, \quad \lambda_2 = a_{32} - a_{12}$$
$$\lambda_3 = a_{42} - a_{12}, \quad \lambda_4 = b_{11} - b_{12}$$

By using Eqs. (6.3) and (6.4) and collecting terms, we get:

$$\lambda_1 < 0, \text{ if } \frac{\alpha}{\gamma} < N_L C_L$$
$$\lambda_2 < 0, \text{ if } \frac{h^L}{N_L I_w(P_2)} < N_L C_L$$
$$\lambda_3 < 0, \text{ if } \frac{1}{\Delta P + \gamma \Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P_2)} + \alpha \Delta T\right) < N_L C_L$$

$$\lambda_4 < 0, \text{ if } N_W C_W < \frac{h^W}{\beta N_W I_L(P_1)}$$

which implies that for the LTE-U AP, represented by λ_1, λ_2, and λ_3, the collective power transmission cost, $N_L C_L$, is higher than the payoffs from increasing the transmission power level or the transmission time period when the WiFi AP is aggressive, i.e, uses P_2. Also, when a WiFi AP uses this strategy it means that transmit power cost is low, and as a result, it increases its transmission power level regardless of any costs to increase its rewards. This is manifested by $\lambda_4 < 0$, and it is a typical selfish behavior in noncoopeartive games. As a result, this strategy is asymptotically stable if the conditions specified for Case 1 in Table 6.3 are satisfied. Overall, the entries of Table 6.3 show the conditions under which the eigenvalues of the Jacobian matrix have negative real parts for given suitable initial conditions for different cases. They also present the comparison between the benefits from two considered technologies in terms of the SINR and the cumulative costs. Transmission is said to be more expensive when the cumulative cost is higher than the transmission benefits. □

Observations Based on Claim 6.2

(a) The worst equilibrium strategy from the perspective of a WiFi AP is given by Case 8, because it creates the most interference to the WiFi users. Breaking any of the above-mentioned conditions will guarantee that the game will not converge to it.

(b) The best equilibrium strategy is given by Case 5. Therefore, by ensuring that the above-mentioned conditions are satisfied and the initial portion of the two populations are within a close neighborhood of this equilibrium point, it guarantees that the game will converge to it.

(c) A sufficient condition to force the LTE-U AP to be friendly, i.e., preventing it from playing the aggressive strategies x_2, x_3, and x_4 which create more interference to the WiFi AP, is by ensuring that the value of $N_L C_L$ exceeds the following

$$\max\left\{\frac{\alpha}{\gamma}, \frac{h^L}{N_L I_w(P)}, \frac{1}{\Delta P + \gamma \Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P)} + \alpha \Delta T\right)\right\}.$$

(d) The worst equilibrium strategy from the coexistence perspective is given by Case

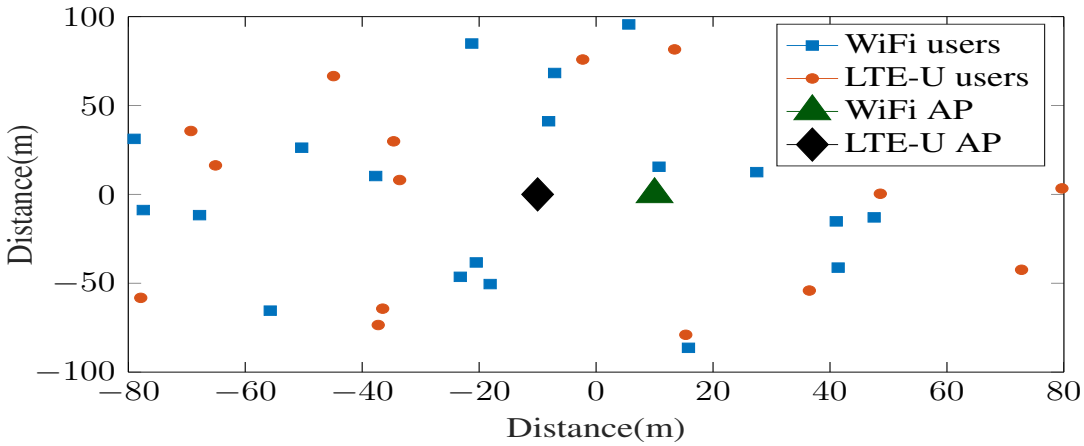


Figure 6.2: Users Locations for Example 1.

4, since it creates the most interference to all users in the network. Breaking any of the conditions will guarantee that the game will not converge to it.

6.4.1 Choosing β in $f(N_W)$

Current WiFi technology is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. In this protocol, the WiFi user equipment senses the channel for any possible ongoing transmission and if there is none, the user starts its own transmission. However, if the channel is occupied, the WiFi device defers the transmission for some period of time and then repeats the sensing activity and so on. Based on the analysis presented in [59] and [60], the WiFi throughput depends on multiple factors such as the channel, the probability of successful transmission (P_s), the number of idle slot times, the average time the channel is captured with a successful transmission, and the average time the channel is captured with a collision. In this work, we take the probability of successful transmission, P_s, as the criteria to find the value of β in $f(N_W)$ in Eq. (6.2). Based on [59] and [60],

$$P_s = \frac{\tau(1-\tau)^{N_W-1}N_W}{1-(1-\tau)^{N_W}} \in [0,1] \tag{6.12}$$

where $\tau \in [0,1]$ is the user's transmission probability. As N_W gets large, $1-(1-\tau)^{N_W} \simeq 1$ and $\tau(1-\tau)^{N_W-1} \simeq \epsilon$, where $\epsilon > 0$ is a very small number. In case of the WiFi, it shows that increasing the number of users decreases the probability of successful transmission and as a result reduces the throughput. In this paper, we assume that

$\beta = \frac{1}{P_s} \geq 1$, which is a rough, but a valid approximation. On the other hand, the LTE technology uses OFDMA for multiple access, which allows multiple users to share the time and frequency resources, and as a result, it is not severely affected by increasing the number of users as the case with the WiFi.

6.4.2 Numerical Examples

We consider two examples to show the effect of increasing the WiFi AP transmission cost, C_W. If the WiFi AP can handle the cost, as in Example 1, then it will be aggressive regardless of the LTE-U AP behavior. In Example 2, we show that we can achieve the best coexistence situation, Case 5 in Table 6.3, by increasing C_W. In both examples, we show the convergence to the ESS through mathematical analysis and simulation. Each figure, Figs. 6.3 and 6.8, shows the evolution of the probabilities of choosing the pure strategies for each player. Additionally, we provide the net payoff for each AP alongside with each strategy to show that the ESS strategies have the highest payoffs. To clarify, in Example 1, Fig. 6.3 shows that the WiFi AP chooses the strategy P_2 with probability one, $\delta_2 = 1$, against an LTE-AP playing strategy x_1, and this strategy gives the WiFi AP a higher payoff, $b_{12} = 0.22081$. b_{12} is larger than the payoff that the WiFi AP gets when playing P_1 strategy against the same LTE-U AP which is $b_{11} = 0.010405$. In a similar way, we can interpret the other curves in Figs. 6.3 and 6.8. Furthermore, show the dynamics of Eqs. (6.3) and (6.4) as the players' decisions evolve. These payoffs are shown in Figs. 6.4-6.7 and Figs. 6.9-6.12. The game utilities are proportional to the signal to interference plus noise ratio (SINR) metric which reflects the users' throughput. The higher the utility, the higher SINR. However, the utilities values do not reflect the exact SINR values that players get through out the game. We assumed also that the AP's keep transmitting regardless of the SINR achieved at the users' end.

Example 1

In this example, the WiFi AP plays the coexistence aggressive strategy, P_2, while the LTE-U plays the coexistence friendly strategy, $x_1 = (P_1, T_1)$. We assume that the users are uniformly distributed in the area shown in Fig. 6.2. For $N_W = 20,\ N_L = 15,\ \mathbb{P} =$

$\{0.1, 0.2\}$, $\mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 5C_W = 0.5$, the payoff matrices are given by:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \\ a_{41} & a_{42} \end{bmatrix} = \begin{bmatrix} -2.1976 & -2.2772 \\ -4.1476 & -4.2272 \\ -2.4451 & -2.6044 \\ -4.3951 & -4.5544 \end{bmatrix} \tag{6.13}$$

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \\ b_{41} & b_{42} \end{bmatrix}^T = \begin{bmatrix} 0.0104 & 0.2208 \\ -0.1896 & 0.0208 \\ -0.0816 & 0.0368 \\ -0.2816 & -0.1632 \end{bmatrix}^T \tag{6.14}$$

where A and B are the payoff matrices for the LTE-U AP and the WiFi AP receptively. The RD equations can be written as:

$$\dot{\rho_k} = \rho_k \left(\sum_{j=1}^{2} \delta_j a_{kj} - \sum_{i=1}^{4} \sum_{j=1}^{2} a_{ij} \delta_j \rho_i \right), \ k = 1, 2, 3. \tag{6.15}$$

$$\dot{\delta_1} = \delta_1 (1 - \delta_1) \sum_{i=1}^{4} (b_{i1} - b_{i2}) \rho_i. \tag{6.16}$$

The eigenvalues for this strategy are $\lambda_{\text{case1}} = [-1.95, -0.3272, -2.2772, -0.2104]$. According to [12], this strategy should be an ESS. However, it is instructive to prove this by the definition given by Theorem 2. The $(0, 1, 0, 0)$ strategy means that the LTE-U AP will use $(\rho_1 = 1, \rho_2 = 0, \rho_3 = 0, \rho_4 = 0)$ and the WiFi AP will use $(\delta_1 = 0, \delta_2 = 1)$. By substituting for the values of the payoff matrices from (6.13) and (6.14). For the LTE-U AP, we get:

$$\begin{aligned} &\begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} A \begin{bmatrix} \delta_1 & \delta_2 \end{bmatrix}^T - \begin{bmatrix} \rho_1 & \rho_2 & \rho_3 & \rho_4 \end{bmatrix} A \begin{bmatrix} \delta_1 & \delta_2 \end{bmatrix}^T > 0 \\ &\Rightarrow (1.95\rho_2 + 0.2475\rho_3 + 2.1975\rho_4)\delta_1 \\ &\qquad + (1.95\rho_2 + 0.3272\rho_3 + 2.2772\rho_4)\delta_2 > 0 \end{aligned} \tag{6.17}$$

which satisfies the ESS condition given in Theorem 2. Similarly, for the WiFi AP,

$$\begin{bmatrix} 0 & 1 \end{bmatrix} B \begin{bmatrix} \rho_1 & \rho_2 & \rho_3 & \rho_4 \end{bmatrix}^T - \begin{bmatrix} \delta_1 & \delta_2 \end{bmatrix} B \begin{bmatrix} \rho_1 & \rho_2 & \rho_3 & \rho_4 \end{bmatrix}^T > 0$$

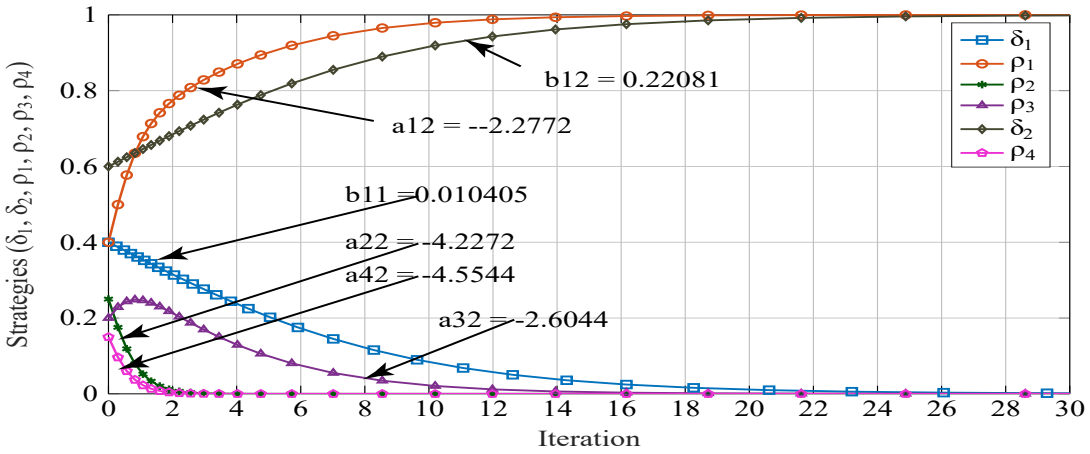


Figure 6.3: Example 1 Strategies Evolution. $N_W = 20$, $N_L = 15$, $\mathbb{P} = \{0.1, 0.2\}$, $\mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 5C_W = 0.5$. It shows the LTE-U AP chooses the strategy $x_1 = (P_1, T_1)$ w.p $\rho_1 = 1$ and the WiFi AP chooses the strategy P_2 w.p $\delta_2 = 1$.

$$\Rightarrow 1 + 0.092(\rho_1 + \rho_2) > 0 \tag{6.18}$$

This satisfies the ESS condition in Theorem 2 which agrees with the simulation results shown in Fig. 6.3. Figs. 6.4 and 6.6 show the evolution of the average payoffs that are calculated from Eqs. (6.3) and (6.4) for the LTE-U AP and the WiFi AP, respectively. It cab be seen that on average the ESS strategies of this scenario are having the higher payoffs. On the other hand, Figs. 6.5 and 6.7 show the payoffs at the ESS of the game which are the final payoffs that players get. It is also noticed that the LTE-U payoff is lower than the WiFi AP payoff. The reason is the values of the cost parameters that are chosen in this example.

Example 2

The following example is to show the effect of increasing the WiFi transmission cost from $C_W = 0.1$ to $C_W = 0.3$. This will converge to the most desirable case, Case 5, which we call it the friendly coexistence because both APs create the lowest interference level to each others' users. This strategy is an ESS too. Asymptotic stability can be shown by checking the eigenvalues and then according to [12], the ESS is established. Alternatively, it can be proved from Theorem 2 as we did in Example 1 above. All other parameters are kept the same as in Example 1. The probability evolution is shown in Fig. 6.8. Similar to Example 1 above, Figs. 6.9 and 6.11 show the average payoff for the

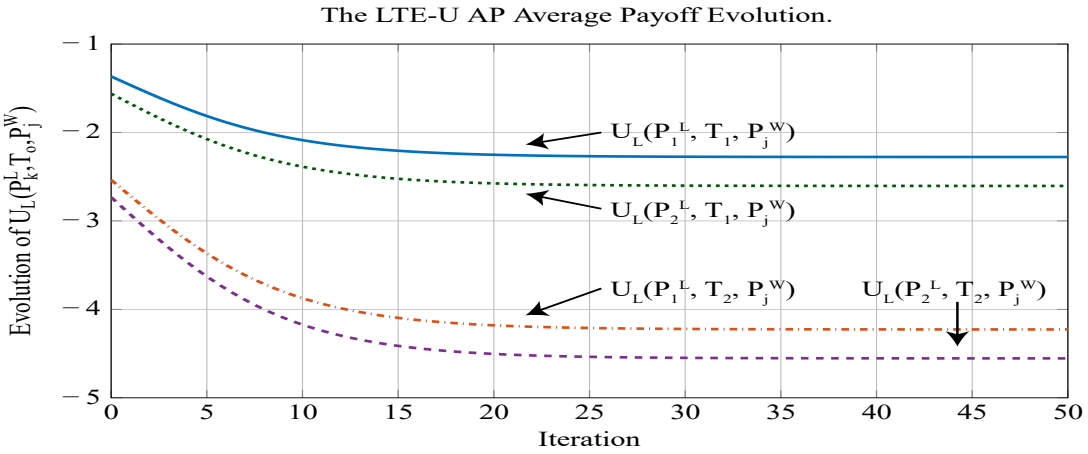


Figure 6.4: Example 1 LTE-U Average Utility Function Evolution. $N_W = 20,\ N_L = 15,\ \mathbb{P} = \{0.1, 0.2\},\ \mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1,\ \beta = 1.5$, and $C_L = 5C_W = 0.5$. It shows the LTE-U AP gets a higher average payoff when it chooses strategy $x_1 = (P_1, T_1)$ w.p $\rho_1 = 1$ against a WiFi AP regardless of its used strategy.

LTE-U AP and the WiFi AP calculated from 6.3 and (6.4), respectively. The payoffs evolution at the ESS are show in Figs. 6.10 and 6.12. Here we notice that increasing the WiFi users transmission cost leads the WiFi AP to adapt a friendlier behavior by choosing the lower transmission power level, P_1, or equivalently to make $\delta_1 = 1$.

6.4.3 The Effect of The Transmission Cost and The Number of Users on The Players' Utilities

In this section, we study the effect of the cost and the number of users on the players' utility functions. To simplify the analysis we assume equal channel coefficients for both APs users. We fix the transmission power level, so that the power levels are P^L and P^W for the LTE-U AP and the WiFi AP in (6.3) and (6.4), respectively, P^L and $P^W \in \mathbb{P}$. We also assume that $(1-\tau)^{N_W-1} \approx (1-\tau)^{N_W} \approx 0$ for large number of WiFi AP users. The utilities under the previous assumptions are given as:

$$U_L(P^L, T_o, P^W) = \frac{h_i^L P^L}{(\sigma^2 + h_i^W P^W) N_L} + \alpha T_o - (P^L + \gamma T_o) N_L C_L, \tag{6.19}$$

$$U_W(P^L, T_o, P^W) = \frac{h_m^W P^W}{(\sigma^2 + h_m^L P^L)\beta N_W} - \alpha\beta^{-1} T_o - N_W P^W C_W. \tag{6.20}$$

By taking the partial derivatives of Eqs. (6.19) and (6.20), we get:

$$\frac{\partial U_L}{\partial C_L} = -(P^L + \gamma T_o) N_L \tag{6.21}$$

$$\frac{\partial U_L}{\partial N_L} = \frac{-h_i^L P^L}{(\sigma^2 + h_i^W P^W) N_L^2} - (P^L + \gamma T_o) C_L \tag{6.22}$$

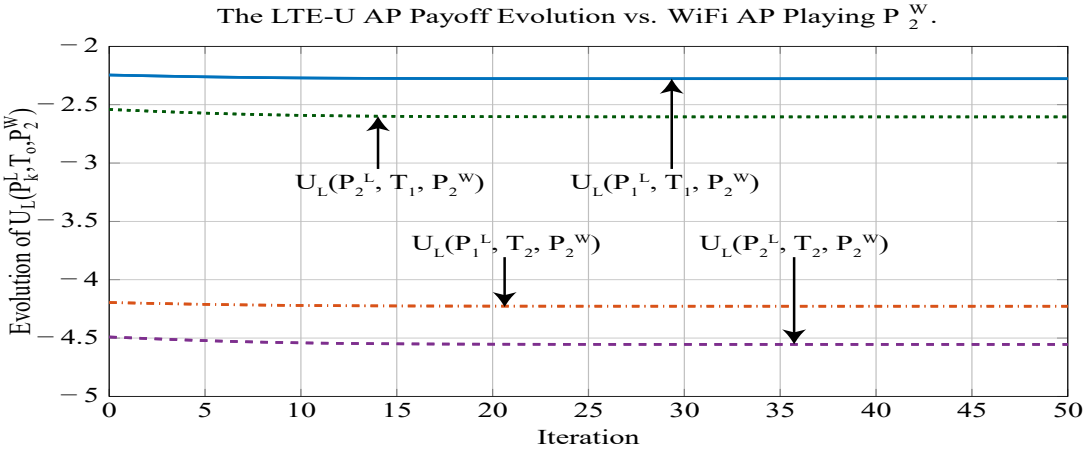


Figure 6.5: Example 1 LTE-U Utility Function Evolution vs. a WiFi AP uses P_2^W . $N_W = 20$, $N_L = 15$, $\mathbb{P} = \{0.1, 0.2\}$, $\mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 5C_W = 0.5$. It shows the LTE-U AP gets a higher payoff when chooses strategy $x_1 = (P_1, T_1)$ against a WiFi AP playing the strategy P_2.

$$\frac{\partial U_W}{\partial C_W} = -P^W N_W \tag{6.23}$$

$$\frac{\partial U_W}{\partial N_W} \approx -C_W P^W, \; N_W \; is \; large, \tag{6.24}$$

$$\frac{\partial U_W}{\partial \tau} \approx -(\frac{h_m^W P^W}{\sigma^2 + h_m^L P^L} - \alpha T_o N_W)(N_w \tau - 1)(1-\tau)^{N_W - 2} \tag{6.25}$$

From (6.21), it is clear that increasing the LTE-U AP cost, C_L, and comparing it to the corresponding term in the WiFi AP utility in Eq. (6.23), will hurt the LTE-U AP more than the WiFi AP. The reason for this is that the LTE-U AP is charged for increasing the transmission period and the power level. Also, it shows that the WiFi AP is less sensitive to increasing the transmission power cost. Furthermore, the WiFi AP may keep creating interference to the LTE-U AP users without really serving its users, i.e. some WiFi users may get very low SINR that is not enough to establish a link between to the AP. The second observation stems from (6.21) and (6.22), shows that the dominant cost term is the transmission cost and it is almost a linear decreasing term in both equations. For the WiFi AP, the payoff seems to decrease linearly with the cost given large number of users. However, since the WiFi uses CSMA/CA, increasing the number of users will bring the probability of successful transmission, (6.12), to zero. To capture the effect of the users' transmission on the WiFi AP payoff we use (6.25), that is under the assumption that $(1-\tau)^{N_W - 2} \neq 0$, the users' optimal transmission probability, τ^*, can be derived from (6.25) as

$$(i) \; \tau^* > \frac{1}{N_W}, \; if \; \frac{h_m^W P^W}{(\sigma^2 + h_m^L P^L)} < \alpha T_o N_W \tag{6.26}$$

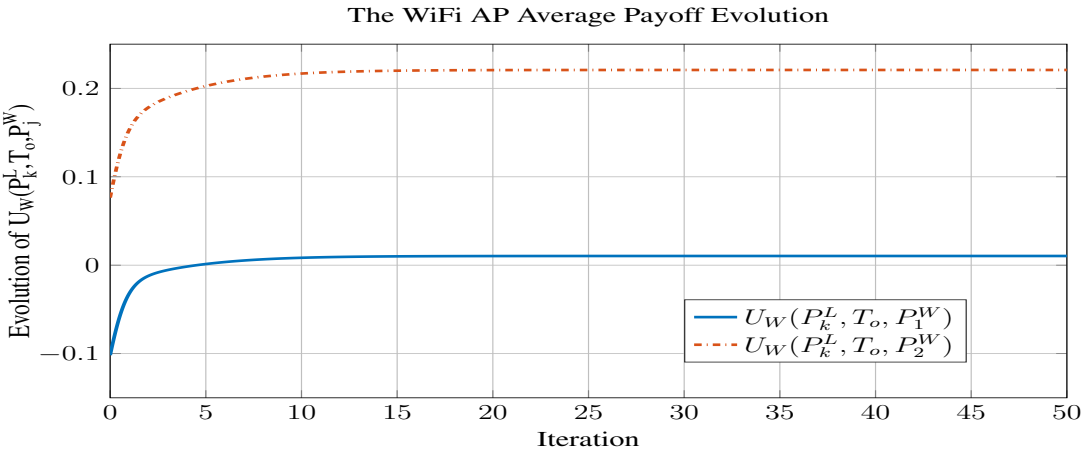


Figure 6.6: Example 1 WiFi Average Utility Function Evolution. $N_W = 20$, $N_L = 15$, $\mathbb{P} = \{0.1, 0.2\}$, $\mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 5C_W = 0.5$. It shows the WiFi AP gets a higher payoff when it chooses strategy P_2 (the dotted line) w.p $\rho_1 = 1$ against a LTE-U AP regardless of its used strategy.

$$(ii)\ \tau^* < \frac{1}{N_W},\ if\ \frac{h_m^W P^W}{(\sigma^2 + h_m^L P^L)} > \alpha T_o N_W \tag{6.27}$$

Fig. 6.13 helps to explain these equations, where it can be seen that the WiFi AP utility function approaches a constant value, $-N_W P^W C_W$, regardless of the transmission probabilities. Increasing the transmission probabilities does not affect as it can be seen from (6.25) and Fig. 6.13.[1]

6.4.4 The WiFi AP Serves a Subgroup of Its Users

In this section, we assume the WiFi AP, depending on the information it has about each user SINR, transmits only to a subgroup of users who satisfy a minimum SINR requirement, i.e. $\text{SINR} \geq \text{SINR}^{Threshold}$. Mathematically, the WiFi AP optimization

[1] In this figure we assumed that all channel coefficients sum to one which means all the WiFi AP users are equidistant from the LTE-U AP and the WiFi AP.

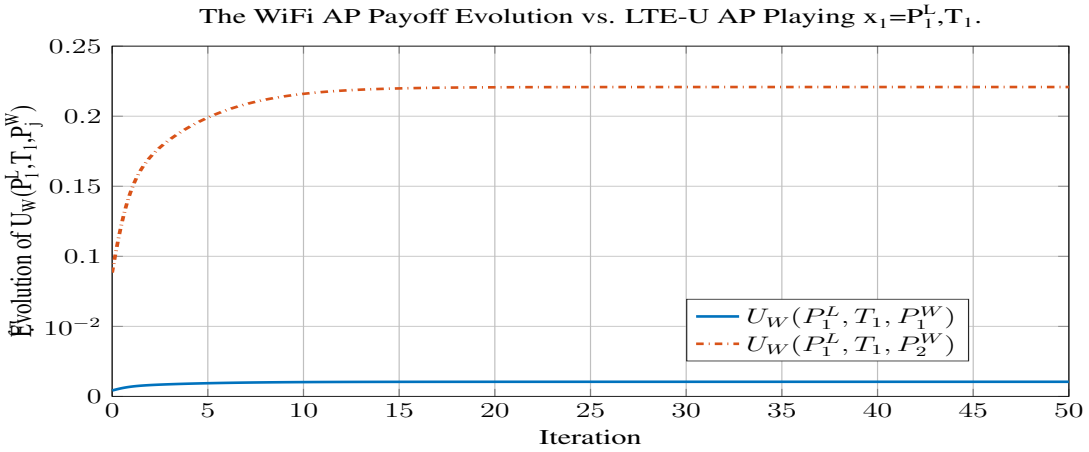


Figure 6.7: Example 1 WiFi Utility Function Evolution vs. a LTE-U AP uses $x_1 = (P_1, T_1)$. $N_W = 20$, $N_L = 15$, $\mathbb{P} = \{0.1, 0.2\}$, $\mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 5C_W = 0.5$. It shows the WiFi AP gets a higher payoff when it chooses strategy P_2 (the dotted line) against a WiFi AP playing the strategy x_1.

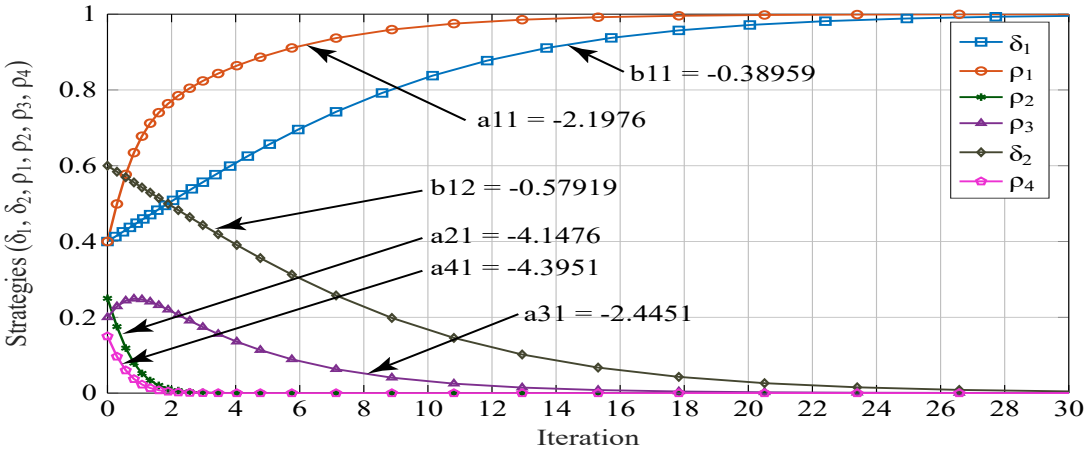


Figure 6.8: Strategies Evolution for Example 2. $N_W = 20$, $N_L = 15$, $\mathbb{P} = \{0.1, 0.2\}$, $\mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 0.5$, $C_W = 0.3$. It shows the LTE-U AP chooses the strategy $x_1 = (P_1, T_1)$ w.p $\rho_1 = 1$ and the WiFi AP chooses the strategy P_1 w.p $\delta_1 = 1$.

problem becomes:

$$
\begin{aligned}
\max_{\{\delta_i\}_{i=1,2}} \quad & U_W(P_k^L, Tr, P_j^W) \\
\text{subject to} \quad & \text{SINR}^{Threshold} \leq \text{SINR}_j^W(P_k^L, P_j^W) \\
& \text{SINR}_m^W(P_k^L, P_j^W) = \frac{h_m^W P_j^W}{\sigma^2 + h_m^L P_k^L}, \ m = 1, ..., N_W, \\
& \{P_j^W, P_k^L\} \in \boldsymbol{P} \\
& 0 \leq \sum_{i=1}^{4} \rho_i \leq 1, \\
& 0 \leq \sum_{i=1}^{2} \delta_i \leq 1, \\
& 0 \leq \{\rho_i\}_{i=1,2,3,4} \leq 1, \ \ 0 \leq \{\delta_i\}_{i=1,2} \leq 1.
\end{aligned}
\tag{6.28}
$$

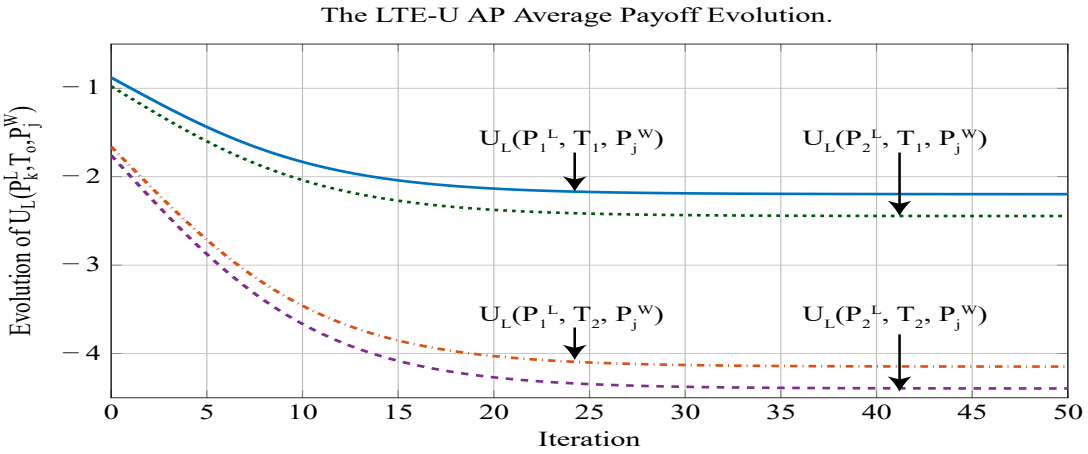


Figure 6.9: Example 2 LTE-U Average Utility Function Evolution. $N_W = 20$, $N_L = 15$, $\mathbb{P} = \{0.1, 0.2\}$, $\mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 0.5$, $C_W = 0.3$. It shows the LTE-U AP gets a higher average payoff when it chooses the strategy $x_1 = (P_1, T_1)$ w.p $\rho_1 = 1$ against the WiFi AP regardless of its used strategy.

The dynamic nature of the problem, captured by $\text{SINR}_j^W(P_k^L, P_j^W)$, requires the WiFi to find the correct $\text{SINR}_j^W(P_k^L, P_j^W)$ to make the decision of transmitting or dropping the m^{th} user. For the specific case of $\mathbf{P} = \{P_1, P_2\}$, there are four possible outcomes. As a result, we propose that the WiFi AP drops the m^{th} user that can not satisfy the threshold under the best received SINR, i.e. under $\text{SINR}_m^W(P_1^L, P_2^W) = \frac{h_m^W P_2^W}{\sigma^2 + h_m^L P_1^L}$. The reasoning behind this, is that if the WiFi AP is transmitting at its highest power level, P_2, while the LTE-U AP creates the lowest interference, P_1, and the user still not able to establish a link, then there is no point from keep transmitting to that user, since this will lead to more power transmission cost and more interference to the LTE-U AP users. The rationale behind this is to lower the interference on both LTE-U and WiFi APs, which will motivate the friendly coexistence. However, this suggests that the WiFi AP will use the lower power level P_1, but our theory and results suggest the opposite as shown in Fig. 6.14, where it shows that the WiFi AP will keep playing the aggressive strategy, P_2, regardless of the LTE-U AP used strategy, which happens to be the friendliest strategy $x_1 = P_1, T_1$. The parameters used to produce this figure are the same ones used in Example 2.

The observations in Section 6.4.3 suggest that the WiFi AP will not decrease its transmission power level even if the LTE-U works in the friendly mode. This seems counter-intuitive, but as shown in Fig. 6.14 it is an expected behavior for the WiFi AP.

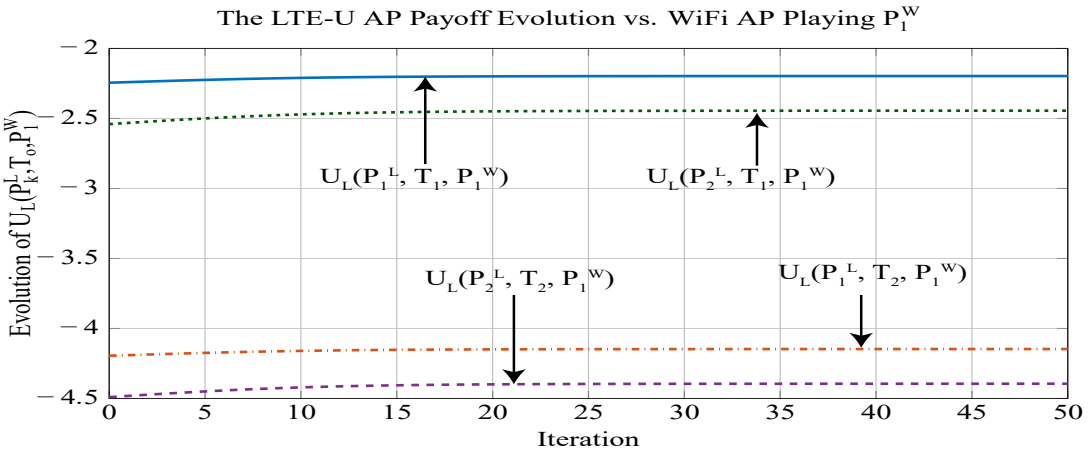


Figure 6.10: Example 2 LTE-U Utility Function Evolution vs. a WiFi AP uses P_1^W . $N_W = 20$, $N_L = 15$, $\mathbb{P} = \{0.1, 0.2\}$, $\mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 0.5$, $C_W = 0.3$. It shows the LTE-U AP gets a higher payoff when it chooses the strategy $x_1 = (P_1, T_1)$ against a WiFi AP playing the strategy P_1.

The reason behind this behavior is the mechanism of the RD. Each time, the WiFi AP will weight its strategies. If the LTE-U AP is in the friendly mode, then the WiFi AP will gain more payoffs from using the higher transmission power level than the lower transmission power level although the latter power level guarantees the required SINR. Also, it is because, WiFi AP is less sensitive to the transmission power cost because of the formulation of the utility function (see (6.3) and (6.4)). Fig. 6.14 shows the stable strategies for the both APs. Finally, the number of the WiFi AP users who satisfy a minimum SINR = 15 dB is 3 out of 20 users and the WiFi uses the higher power level, P_2. In this example, we used the parameters from Example 2, where increasing the cost for the WiFi should lead to the friendly ESS. However, in this case, even by increasing the WiFi AP transmission cost to 0.9, the WiFi keeps using the higher power level which is P_2. In the next section, we modify the WiFi utility function to limit such aggressive behavior.

Finally, Table 6.4 shows the different parameters that were changed to manipulate the WiFi AP to return to its friendly behavior. The table shows that although the WiFi AP cost of transmission has been increased 9 times of the cost given in Example 1 (see Fig. 6.3), the WiFi AP keeps using the higher power level due to higher rewards. Table 6.4 also shows that the initial probabilities for using the transmission power level did not affect the WiFi AP decision. In the next section, we introduce a power dependent

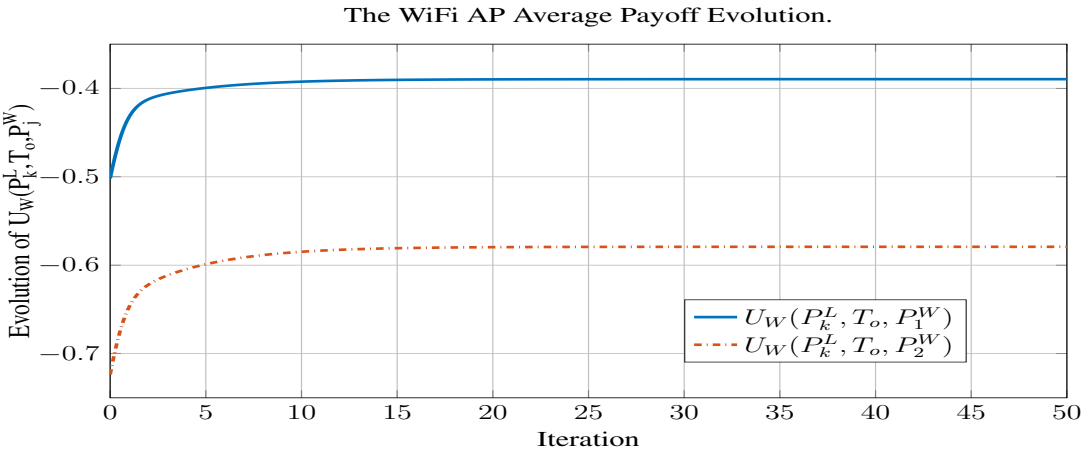


Figure 6.11: Example 2 WiFi Average Utility Function Evolution. $N_W = 20,\ N_L = 15,\ \mathbb{P} = \{0.1, 0.2\},\ \mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1,\ \beta = 1.5$, and $C_L = 0.5,\ C_W = 0.3$. It shows the WiFi AP gets a higher average payoff when it chooses the strategy P_1 (the solid line) w.p $\delta_1 = 1$ against a LTE-U AP regardless of its used strategy.

cost to the WiFi AP service to users who satisfy the proposed SINR criteria.

The WiFi AP Serves a Subgroup of Its Users Based on a Power Dependent Cost Approach

In this part, we introduce a cost function for the WiFi AP which depends on the transmission power level. We derive the conditions under which the resulted strategy is asymptotically stable. The model is given in (6.29). Assume that $C_{W_j},\ j = 1, 2, ...,$ is the cost of using the j^{th} power level. For two power levels, P_1, P_2, we have

$$C_{W_2} = f(C_{W_1}) = gC_{W_1},\ g \geq 1, \tag{6.29}$$

where the function $f(C_{W_1})$ can be chosen to be any monotonically increasing function. The conditions under which the ESS of the new modified game established are given in Claim 6.3.

Claim 6.3. *All the modified WiFi AP power pricing game pure strategies can be locally asymptotically stable given that their trajectories start sufficiently close in their neighborhood and the convergence conditions given below hold. Furthermore, the stability conditions for the LTE-U AP are the same as in Claim 6.2 and are given in the first part of each case of Claim 6.2. The second part of each case, which captures the WiFi*

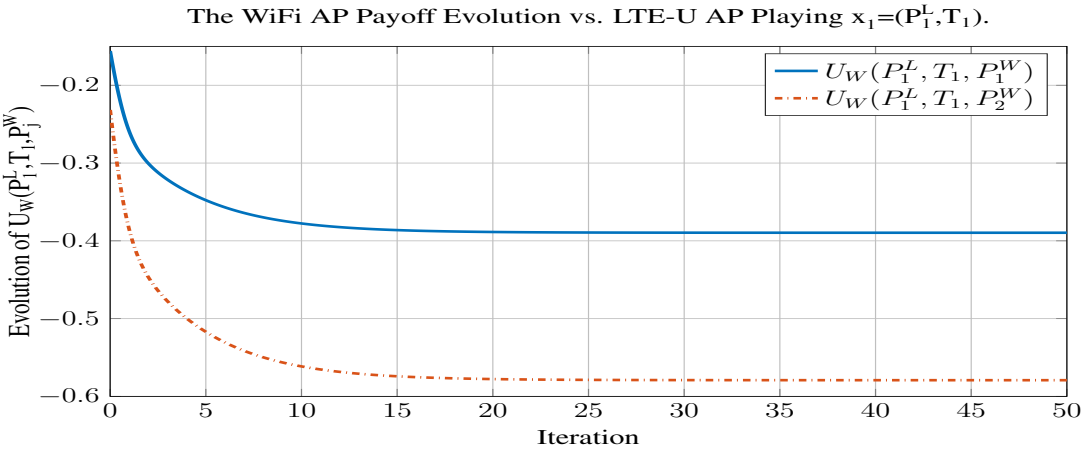


Figure 6.12: Example 1 WiFi Utility Function Evolution vs. a LTE-U AP uses $x_1 = (P_1, T_1)$. $N_W = 20,\ N_L = 15,\ \mathbb{P} = \{0.1, 0.2\},\ \mathbb{T} = \{0.3, 0.6\}, \gamma = \alpha = 1,\ \beta = 1.5$, and $C_L = 0.5,\ C_W = 0.3$. It the WiFi AP gets a higher payoff when it chooses the strategy P_1 against a LTE-U AP playing the strategy x_1.

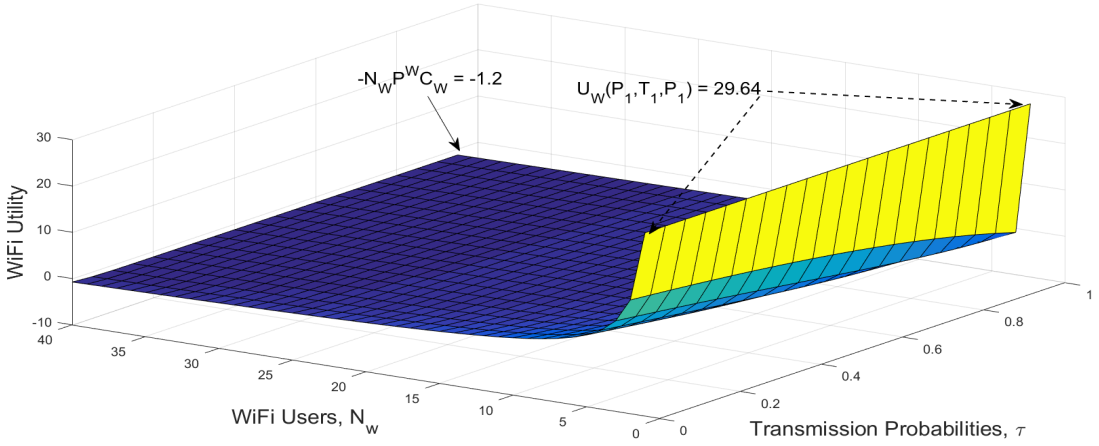


Figure 6.13: Example 2 WiFi Utility Function with a LTE-U AP uses $x_1 = (P_1, T_1)$. $P_1 = 0.1,\ T_1 = 0.3, \gamma = \alpha = 1,\ \beta = 1.5$, and $C_L = 0.5,\ C_W = 0.3$.

AP, is changed as given below:

Case 1: $(0, 1, 0, 0)$ *or* $(\delta_2 = 1,$ *and* $\rho_1 = 1)$ *if*

(1) LTE-U AP conditions as in Claim 6.2, and

(2) $N_W \Delta C_W(P^W) < \frac{h^W}{\beta N_W I_L(P_1)}$.

Case 2: $(0, 0, 1, 0)$ *or* $(\delta_2 = 1,$ *and* $\rho_2 = 1)$ *if*

(1) LTE-U AP conditions as in Claim 6.2, and

(2) $N_W \Delta C_W(P^W) < \frac{h^W}{\beta N_W I_L(P_1)}$.

Case 3: $(0, 0, 0, 1)$ *or* $(\delta_2 = 1,$ *and* $\rho_3 = 1)$ *if*

(1) LTE-U AP conditions as in Claim 6.2, and

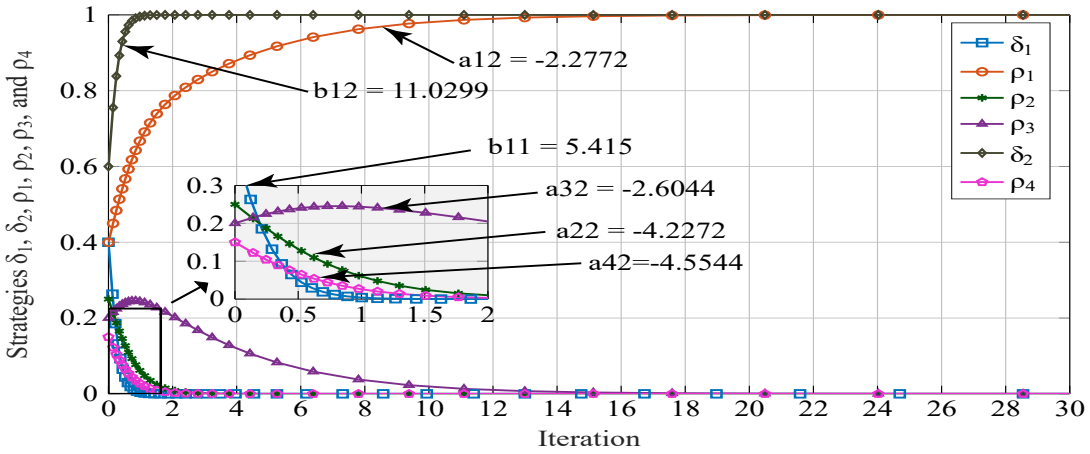


Figure 6.14: Strategies Evolution for the Optimization Problem in Eq. (6.28). $N_W = 20$, $N_L = 15$, $P_1 = 0.1$, $P_2 = 2P_1$, $T_1 = 0.3$, $T_2 = 2T_1, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 0.5$, $C_W = 0.3$. The final results are the same even with $C_W = 0.9$.

(2) $N_W \Delta C_W(P^W) < \frac{h^W}{\beta N_W I_L(P_2)}$.

Case 4: $(0,0,0,0)$ *or* $(\delta_2 = 1,$ *and* $\rho_2 = 1)$ *if*

(1) LTE-U AP conditions as in Claim 6.2, and

(2) $N_W \Delta C_W(P^W) < \frac{h^W}{\beta N_W I_L(P_2)}$.

Case 5: $(1,1,0,0)$ *or* $(\delta_1 = 1,$ *and* $\rho_1 = 1)$ *if*

(1) LTE-U AP conditions as in Claim 6.2, and

(2) $N_W \Delta C_W(P^W) > \frac{h^W}{\beta N_W I_L(P_1)}$.

Case 6: $(1,0,1,0)$ *or* $(\delta_1 = 1,$ *and* $\rho_2 = 1)$ *if*

(1) LTE-U AP conditions as in Claim 6.2, and

(2) $N_W \Delta C_W(P^W) > \frac{h^W}{\beta N_W I_L(P_1)}$.

Case 7: $(1,0,0,1)$ *or* $(\delta_1 = 1,$ *and* $\rho_3 = 1)$ *if*

(1) LTE-U AP conditions as in Claim 6.2, and

(2) $N_W \Delta C_W(P^W) > \frac{h^W}{\beta N_W I_L(P_2)}$.

Case 8: $(1,0,0,0)$ *or* $(\delta_1 = 1,$ *and* $\rho_4 = 1)$ *if*

(1) LTE-U AP conditions as in Claim 6.2, and

(2) $N_W \Delta C_W(P^W) > \frac{h^W}{\beta N_W I_L(P_2)}$, *where* $\Delta C_W(P^W) = C_{W_2} P_2 - C_{W_1} P_1$.

Proof. Similar to Claim 6.2, we have to check the new asymptotic stability conditions for the WiFi AP. We take the first case, which is $(0,1,0,0)$ or $(\delta_2 = 1,$ and $\rho_1 = 1)$.

The difference is in calculating the condition under which the eigenvalue related to the WiFi AP is asymptotically stable. This eigenvalue is given by $\lambda_4 = b_{11} - b_{12}$. This strategy is asymptotically stable if $\lambda_4 < 0$.

By substituting in Eqs. (6.3) and (6.4), using (6.29) for the cost, and collecting terms, we get: $N_W \Delta C_W(P^W) < \frac{h^W}{\beta N_W I_L(P_2)}$. In a similar way we can prove the other conditions. By using the conditions given in Claim 6.3, one can derive the threshold cost at which the WiFi AP can be forced to play a certain strategy. As an example, the cost at which the WiFi AP in Case 1 of Claim 6.3 will not play P_2 is found to be: $C_{W_2} > \frac{1}{P_2}\left(\frac{h^W}{\beta N_W I_L(P_1)} + C_{W_1} P_1\right)$. □

Fig. 6.15 shows the simulation results that validate Claim 6.3. It can be seen that with setting a higher cost for P_2, the WiFi AP returns to the friendly behavior. In this example, g in (6.29) is set to 49. The other parameters are set as in Example 2 for consistency, and the users' and the APs' locations are as shown in Fig. 6.2.

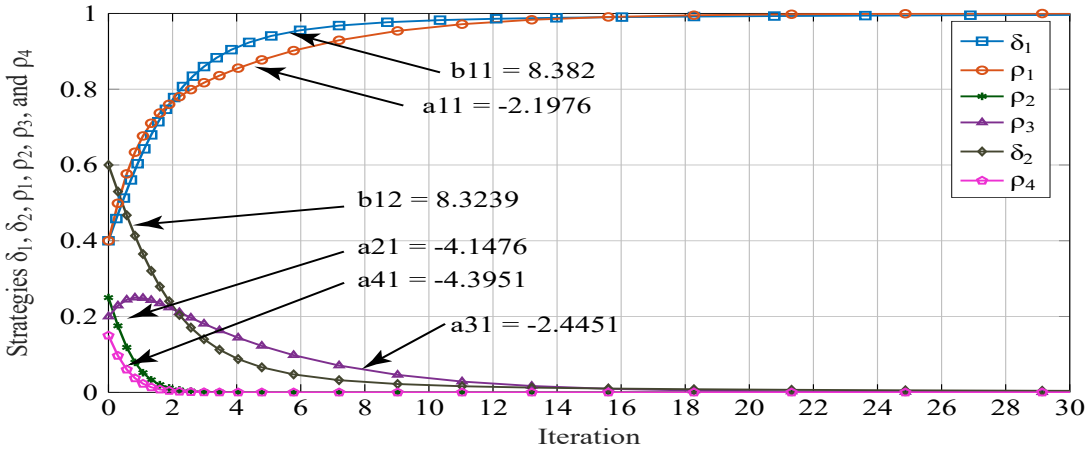


Figure 6.15: Strategies Evolution after Adapting the Cost Function in Eq. (6.29) in the Optimization Problem in Eq. (6.28) . $N_W = 20$, $N_L = 15$, $P_1 = 0.1$, $P_2 = 2P_1$, $T_1 = 0.3$, $T_2 = 2T_1, \gamma = \alpha = 1$, $\beta = 1.5$, and $C_L = 0.5$, $C_{W_1} = 0.3$, and $C_{W_2} = 49C_{W_1}$.

6.4.5 The Effect of the Distance between the LTE-U AP and WiFi AP

We did simulations were the distance between the APs change. We do not show the results here, since we did not get a difference. This can be easily proved. However, we present a sketch of the proof. Changing the distance between as AP, let's say the WiFi

AP, and its users affects the channel parameters, in this case h_m^L and h_m^W. As a result, regardless of the position of the APs, our model in (6.1) and (6.2) has these channel parameters effect, so the stability conditions will stay the same.

6.5 General Game Theoretic Formulation

In this section, we formulate and solve the coexistence game using classical game theory. In other words, we assume that the game is played once. We assume that $P^L \in [0, P_{max}^L]$, $T_o \in [T_o^{min}, T_o^{max}]$, and $P^W \in [0, P_{max}^W]$. The players' optimization problems are given below,

$$\begin{aligned} &\underset{P^L, T_o}{\text{maximize}} \;\; U_L(P^L, T_o, P^W) \\ &\underset{P^W}{\text{maximize}} \;\; U_W(P^L, T_o, P^W) \\ &\text{subject to:} \quad P^L \in [0, P_{max}^L], \quad T_o \in [T_o^{min}, T_o^{max}], \\ &\qquad\qquad\quad P^W \in [0, P_{max}^W], \end{aligned} \tag{6.30}$$

where $U_L(.)$ and $U_W(.)$ are just the continuous version of (6.3) and (6.4). In fact, they are the potential functions for the LTE-U AP and the WiFi AP respectively given under the continuum version of strategies given in (6.30). Under this limited power and duty cycle settings with (6.3) and (6.4), the NE of the game is defined as $P^{L*},\ T_o^*,\ , P^{W*}$ and found by solving (6.30). Furthermore, by setting the partial derivatives of (6.3) and (6.4) with respect to the variables $\{P^L, T_o\}$ for the LTE-U utility function and P^W for the WiFi utility function, we get the game NE strategies as,

$$P^{L*} = \begin{cases} \frac{1}{\sum_{m=1}^{N_W} h_m^L} \left(\frac{\sum_{m=1}^{N_W} h_m^W}{\beta N_W^2 C_W} - N_W \sigma^2 \right), & \frac{\sum_{m=1}^{N_W} h_m^W}{\beta N_W^2 C_W} > N_W \sigma^2 \\ 0, & otherwise \end{cases} \tag{6.31}$$

$$T_o^* = \begin{cases} T_o^{max}, & \alpha > \gamma C_L N_L \\ T_o^{min}, & otherwise \end{cases}$$

$$P^{W*} = \begin{cases} \frac{1}{\sum_{i=1}^{N_L} h_i^W} \left(\frac{\sum_{i=1}^{N_L} h_i^L}{N_L^2 C_L} - N_L \sigma^2 \right), & \frac{\sum_{i=1}^{N_L} h_i^L}{N_L^2 C_L} > N_L \sigma^2 \\ 0, & otherwise. \end{cases} \tag{6.32}$$

T_o is a linear independent variable in the LTE-U utility. As a result, it takes the maximum value when the condition in (6.31) holds, $\alpha > \gamma C_L N_L$, and the minimum

value if it does not hold. (6.31) and (6.32) represent the classical NE of the game. They do not give information about the game dynamics. However, they are the optimal strategies for both players at a certain point of time. The robustness of these NE strategies against all other available strategies can be formulated as an asymmetric evolutionary game and tested for asymptotic stability under the replicator dynamics. In this game, the players represented by the LTE-U AP and the WiFi AP choose the NE strategies in (6.31) and (6.32) with probability ρ_1 and δ_1, respectively. Also the players, the LTE-U AP and the WiFi AP, choose any other alternative strategy from the continuum of the rest of strategies with probabilities ρ_2 and δ_2, respectively. Define $x_1 = (P^{L*}, T_o^*)$, $x_2 = (P^L \neq P^{L*}, T_o \neq T_o^*)$, $y_1 = P^{W*}$, and $y_2 = P^W \neq P^{W*}$, then x_1 is chosen with probability ρ_1 and y_1 is chosen with probability δ_1. The replicator dynamics equations from (2.3) and (2.4) are used to study the stability of the NE as follows,

$$\dot{\rho_1} = \rho_1(1-\rho_1)(k_1^L\delta_1 - k_2^L), \tag{6.33}$$

$$k_1^L = U_L(x_1, y_1) - U_L(x_2, y_1) - U_L(x_1, y_2) + U_L(x_2, y_2),$$

$$k_2^L = U_L(x_2, y_2) - U_L(x_1, y_2),$$

$$\dot{\delta_1} = \delta_1(1-\delta_1)(k_1^W\rho_1 - k_2^W), \tag{6.34}$$

$$k_1^W = U_W(x_1, y_1) - U_W(x_2, y_1) - U_W(x_1, y_2) + U_W(x_2, y_2),$$

$$k_2^W = U_W(x_2, y_2) - U_W(x_2, y_1),$$

The utilities of both players at any strategy other than the NE, (x_1, y_1), are the expected values over all the range of P^L, T_o, and P^W. It can be seen that this stability rule can find if the NE is an asymptotically stable strategy or not without being able to study the stability of all the possible strategies. For example in the WiFi case, there is an infinite number of possible values in the interval $P^W \in [0, P_{max}^W]$. A similar argument holds for the LTE-U AP set of strategies.

Claim 6.4. *The NE P^{L*}, T_o^*, P^{W*} is an asymptotically stable NE under the replicator dynamics given in (6.33) and (6.34) if the following conditions hold,* (1) *For the LTE-U AP the NE strategy, $x_1 = (P^{L*}, T_o^*)$, is a strict NE. This condition is captured by the*

inequality:
$\big(\frac{\sum_{i=1}^{N_L} h_i^L}{I_W(P^{W*})} - N_L^2 C_L\big)\frac{(P^{L*}-P^L)}{N_L} > (N_L C_L \gamma - \alpha)(T_o^* - T_o),\ P^L \neq P^{L*} \in [0, P_{max}^L],\ T_o \neq T_o^* \in [T_o^{min}, T_0^{max}]$,

(2) *For the WiFi AP the NE strategy,* $y_1 = P^{W*}$*, is a strict NE and this condition holds if either:*
(2-i) $\frac{\sum_{m=1}^{N_W} h_m^W}{\beta N_W I_L(P^{L*})} < N_W C_W$ *and* $P^{W*} < P^W$*, or*
(2-ii) $\frac{\sum_{m=1}^{N_W} h_m^W}{\beta N_W I_L(P^{L*})} > N_W C_W$ *and* $P^{W*} > P^W$ *and* $P^W \neq P^{W*} \in [0, P_{max}^W]$.

Proof. In this proof, we derive the conditions under which the NE strategy, $x_1 = (P^{L*}, T_o^*)$ and $y_1 = P^{W*}$, is asymptotically stable. This corresponds to linearizing the RD system of equations in (6.33) and (6.34) near $\rho_1 = 1$ and $\delta_1 = 1$. The Jacobian matrix is,

$$J_{(1,1)} = \begin{bmatrix} \frac{\partial \dot{\rho_1}}{\partial \rho_1} & \frac{\partial \dot{\rho_1}}{\partial \delta_1} \\ \frac{\partial \dot{\delta_1}}{\partial \rho_1} & \frac{\partial \dot{\delta_1}}{\partial \delta_1} \end{bmatrix} = \begin{bmatrix} -(k_1^L - k_2^L) & 0 \\ 0 & -(k_1^W - k_2^W) \end{bmatrix}. \tag{6.35}$$

For asymptotic stability, the eigenvalues of (6.35) has to have negative real parts [52]. Substituting for k_1^L, k_2^L, k_1^W, and k_2^W from (6.33) and (6.34) in (6.35) and simplifying, we get the conditions in Claim 6.4. □

6.6 Conclusions

In this chapter, we studied the coexistence problem between different technologies to achieve dynamic spectrum sharing among users using evolutionary game theory. Specifically, we studied the coexistence problem between LTE-U and WiFi APs, where we assumed APs which belong to different technologies are located in the same area where they can create interference to each others' users on the downlink. Additionally, we investigated the effect of the transmission cost on each AP and specified the conditions under which long-term coexistence can be achieved. The long-term coexistence is modeled by finding the evolutionary stable strategies of the evolutionary game. We analyzed the cost functions for the LTE-U and the WiFi APs, and showed that the LTE-U AP behavior is more sensitive to the cost than to the number of users. For the WiFi, we found its behavior is more sensitive to the number of users than to the transmission

power cost. On the other hand, we studied the case where the WiFi AP removes users that could not establish the minimum SINR required to establish a communication link to reduce the interference to the LTE-U AP users. We found that this will create more interference in the network. We solved this problem by introducing a modified cost function for the WiFi AP to reduce the interference to the LTE-U technology users by penalizing the WiFi AP when it shows unnecessary aggressive/selfish behavior. Finally, we presented a classical game-theoretic formulation to the coexistence problem and found the corresponding NE strategies. Furthermore, we analyzed the stability of these strategies under the RD and presented the asymptotic stability conditions for the NE.

There are several possible extensions of this work such as considering the case where the LTE-U APs create interference to each other. We excluded this scenario by assuming that LTE-U APs belong to the same operator. It is expected that this will produce a different set of stable strategies, if any. Proposing new/modified utility functions, that are not a scaled or shifted versions from the ones presented here in (6.1) and (6.2), may result in a different NEs and ESSs (if any). The stability of the players' strategies in both games presented here was studied under the RD. However, there are other dynamics that can be considered, see for example [17].

Table 6.3: Convergence Conditions for Claim 6.2

#	Strategies (δ_1, ρ_1, ρ_2, ρ_3)	Conditions
Case 1	$(0,1,0,0)$ or $(\delta_2=1,\ \rho_1=1)$	$N_L C_L > \max\left\{\frac{\alpha}{\gamma}, \frac{h^L}{N_L I_w(P_2)}, \frac{1}{\Delta P+\gamma\Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P_2)}+\alpha\Delta T\right)\right\}$, $N_W C_W < \frac{h^W}{\beta N_W I_L(P_1)}$
Case 2	$(0,0,1,0)$ or $(\delta_2=1,\ \rho_2=1)$	$\frac{\alpha}{\gamma} > N_L C_L > \max\left\{\frac{h^L}{N_L I_w(P_2)}, \frac{1}{\Delta P-\gamma\Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P_2)}-\alpha\Delta T\right)\right\}$, $N_W C_W < \frac{h^W}{\beta N_W I_L(P_1)}$
Case 3	$(0,0,0,1)$ or $(\delta_2=1,\ \rho_3=1)$	$\min\left\{\frac{h^L}{N_L I_w(P_2)}, \frac{1}{\Delta P-\gamma\Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P_2)}-\alpha\Delta T\right)\right\} > N_L C_L > \frac{\alpha}{\gamma}$, $N_W C_W < \frac{h^W}{\beta N_W I_L(P_2)}$
Case 4	$(0,0,0,0)$ or $(\delta_2=1,\ \rho_2=1)$	$N_L C_L < \min\left\{\frac{\alpha}{\gamma}, \frac{h^L}{N_L I_w(P_2)}, \frac{1}{\Delta P+\gamma\Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P_2)}+\alpha\Delta T\right)\right\}$, $N_W C_W < \frac{h^W}{\beta N_W I_L(P_2)}$
Case 5	$(1,1,0,0)$ or $(\delta_1=1,\ \rho_1=1)$	$N_L C_L > \max\left\{\frac{\alpha}{\gamma}, \frac{h^L}{N_L I_w(P_1)}, \frac{1}{\Delta P+\gamma\Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P_1)}+\alpha\Delta T\right)\right\}$, $N_W C_W > \frac{h^W}{\beta N_W I_L(P_1)}$
Case 6	$(1,0,1,0)$ or $(\delta_1=1,\ \rho_2=1)$	$\frac{\alpha}{\gamma} > N_L C_L > \max\left\{\frac{h^L}{N_L I_w(P_1)}, \frac{1}{\Delta P-\gamma\Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P_1)}-\alpha\Delta T\right)\right\}$, $N_W C_W > \frac{h^W}{\beta N_W I_L(P_1)}$
Case 7	$(1,0,0,1)$ or $(\delta_1=1,\ \rho_3=1)$	$\min\left\{\frac{h^L}{N_L I_w(P_1)}, \frac{1}{\Delta P-\gamma\Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P_1)}-\alpha\Delta T\right)\right\} > N_L C_L > \frac{\alpha}{\gamma}$, $N_W C_W > \frac{h^W}{\beta N_W I_L(P_2)}$
Case 8	$(1,0,0,0)$ or $(\delta_1=1,\ \rho_4=1)$	$N_L C_L < \min\left\{\frac{\alpha}{\gamma}, \frac{h^L}{N_L I_w(P_1)}, \frac{1}{\Delta P+\gamma\Delta T}\left(\frac{h^L \Delta P}{N_L I_w(P_1)}+\alpha\Delta T\right)\right\}$, $N_W C_W > \frac{h^W}{\beta N_W I_L(P_2)}$

Table 6.4: Changing the Transmission Cost for the WiFi AP.

C_W	P_1 w.p δ_1	P_2 w.p δ_2	Stable Strategy
$0.3-0.9$	0.4	0.6	P_2
$0.5-0.9$	0.6	0.4	P_2
$0.5-0.9$	0.8	0.2	P_2

Chapter 7

Conclusions and Future Work

7.1 Summary of Research

The work presented here can be broadly divided into two main categories. First, the use of evolutionary game theory to address different security problems in wireless networks and data storage. The second part is applying evolutionary games to solve the coexistence problem among different technologies, in general, and between LTE-U and WiFi in particular.

7.1.1 Evolutionary Games to Address Wireless and Storage Security Problems

We formulated a denial of service attack through jamming evolutionary game. We used potential functions to formulate the utilities of two asymmetric populations and studied their asymptotically stable and hence evolutionary stable strategies. We showed that such attack can be mitigated given a high enough number of cooperative users.

We addressed another security problem called threat revocation in ephemeral networks. Such networks are expected to be widely adopted although under different names such as Internet of Things, or vehicular networks, and so on. We broadly proposed an evolutionary game that captures how nodes in such networks can, independently, thwart the threat by taking into account the connectivity cost. Evolutionary stable strategies were used to show the conditions under which the network can be kept safe.

Our final contribution in this category was using evolutionary games to model an attacker and defender competing to get control over storage device(s) by continuous attacking and defending over specified periods of time. Evolutionary stable strategies

are derived and the conditions that make them hold are specified explicitly. The ESS's show, under given cost(gain), the more robust attack (defense) strategies.

7.1.2 Evolutionary Games to Address Coexistence among Different Technologies

In this part, we proposed using evolutionary game theory as a mechanism for coexistence between WiFi technology and LTE-U one. We formulated the utility functions for each AP such that it is the potential function of its own users. We considered two different cases where the WiFi users who could not establish a link and where they could establish it. We found that for the case where the WiFi AP can drop out some of its users who can not maintain a threshold SINR, the power cost function for the WiFi AP needs to increased significantly to prevent it from raising its downlink transmission power. Such kind of behavior benefits the WiFi AP users, because it increases their SINR, but at the same it creates unnecessary interference to the LTE-U AP users.

7.2 Future Work

Using Evolutionary games on graphs to model the problems addressed in this dissertation is a natural extension to our work. Graph theory allows for specific formulation of the utility function for each player based on its neighbors. For example, in a game where players can choose to cooperate of defect as strategies, a player who is surrounded by defectors does not care about cooperators who are not interacting with her, and vise versa.

The coexistence problem addressed in Chapter 6 can be extended to deal with many technologies. In this work, we analyzed the game under the replicator dynamics. The others possible scenarios can be interference reduction by means of cooperation between the technologies. Another scenario can use a different learning rule rather than the replicator dynamics, see for example [17]. Coexistence under a hostile environment is another interesting extension.

References

[1] A. A. Alabdel Abass, M. Hajimirsadeghi, N. B. Mandayam, and Z. Gajic, "Evolutionary game theoretic analysis of distributed denial of service attacks in a wireless network," in *Proc. Annual Conference on Information Science and Systems (CISS)*, 2016, pp. 36–41.

[2] A. A. A. Abass, N. B. Mandayam, and Z. Gajic, "An evolutionary game model for threat revocation in ephemeral networks," in *2017 51st Annual Conference on Information Sciences and Systems (CISS)*, March 2017, pp. 1–5.

[3] A. A. A. Abass, L. Xiao, N. B. Mandayam, and Z. Gajic, "Evolutionary game theoretic analysis of advanced persistent threats against cloud storage," *IEEE Access*, vol. 5, 2017.

[4] The Daily Targum, Cybersecurity Expert Identifies Rutgers Student as DDoS Perpetrator. [Online]. Available: http://www.dailytargum.com/article/2017/01/cybersecurity-expert-identifies-rutgers-student-as-ddos-perpetrator

[5] J. A. Dayton, "Risk of using past to predict future a case study of jamming rcieds," Master's thesis, Operations Research Department, Naval Postgraduate School, June 2009. [Online]. Available: http://calhoun.nps.edu/handle/10945/4762

[6] A. Gueye, "A game theoretical approach to communication security," Ph.D. dissertation, EECS Department, University of California, Berkeley, Mar 2011. [Online]. Available: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2011/EECS-2011-19.html

[7] Clearsky. Thamar Reservoir – An Iranian Cyber-attack Campaign. [Online]. Available: http://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf

[8] Kaspersky Labs, Global Research and Analysis Team: The Darkhotel APT-A Story of Unusual Hospitality. [Online]. Available: https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf

[9] M. Ussath, D. Jaeger, F. Cheng, and C. Meinel, "Advanced persistent threats: Behind the scenes," in *Proc. Annual Conference on Information Science and Systems (CISS)*, 2016, pp. 181–186.

[10] J. F. Nash, "Non-cooperative games," Ph.D. dissertation, Princeton University, May 1950. [Online]. Available: https://rbsc.princeton.edu/sites/default/files/Non-Cooperative_Games_Nash.pdf

[11] J. W. Weibull, *Evolutionary Game Theory*. MIT press, 1997.

[12] K. Sigmund *et al.*, *Evolutionary Game Dynamics: American Mathematical Society Short Course.* American Mathematical Society, 2011, vol. 69.

[13] T. Basar and G. J. Olsder, *Dynamic Noncooperative Game Theory.* SIAM, 1995, vol. 200.

[14] J. Hofbauer and K. Sigmund, *The Theory of Evolution and Dynamical Systems: Mathematical Aspects of Selection.* Cambridge University Press, 1988.

[15] E. C. Zeeman, "Population dynamics from game theory," in *Global Theory of Dynamical Systems.* Springer, 1980, pp. 471–497.

[16] J. Hofbauer and K. Sigmund, *Evolutionary Games and Population Dynamics.* Cambridge University Press, 1998.

[17] W. H. Sandholm, *Population Games and Evolutionary Dynamics.* MIT Press, 2010.

[18] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, 2013.

[19] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, 2008.

[20] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 63–70, 2010.

[21] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems.* Springer Science & Business Media, 2013.

[22] T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach.* Cambridge University Press, 2010.

[23] J. N. Webb, *Game Theory: Decisions, Interaction and Evolution.* Springer Science & Business Media, 2007.

[24] H. Tembine, E. Altman, R. El-Azouzi, and Y. Hayel, "Evolutionary games in wireless networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 40, no. 3, pp. 634–646, 2010.

[25] S. Moon, Y. Yi, and H. Kim, "Energy-efficient user association in cellular networks: A population game approach," in *Proc. 11th International Symposium and Workshops on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, 2013, pp. 388–395.

[26] P. Semasinghe, K. Zhu, and E. Hossain, "Distributed resource allocation for self-organizing small cell networks: An evolutionary game approach," in *Proc. IEEE Globecom Workshop on Heterogeneous and Small Cell Networks*, 2013, pp. 702–707.

[27] E. Altman, Y. Hayel, and H. Kameda, "Evolutionary dynamics and potential games in non-cooperative routing," in *Proc. 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks and Workshops*, 2007, pp. 1–5.

[28] M. F. Amjad, M. Chatterjee, O. Nakhila, and C. C. Zou, "An evolutionary game theoretic framework for coexistence in cognitive radio networks," in *Proc. IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2014, pp. 278–282.

[29] W. Sabrina and K. J. R. Liu, "Pricing game and evolution dynamics for mobile video streaming," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2011.

[30] C. Jiang, Y. Chen, and K. J. R. Liu, "On the equivalence of evolutionary stable strategies," *IEEE Communications Letters*, vol. 18, no. 6, pp. 995–998, 2014.

[31] G. Jiang, S. Shen, K. Hu, L. Huang, H. Li, and R. Han, "Evolutionary game-based secrecy rate adaptation in wireless sensor networks," *Int. J. Distrib. Sen. Netw.*, vol. 2015, pp. 25:25–25:25, Jan. 2015.

[32] Y. E. Sagduyu, R. Berry, and A. Ephremides, "Mac games for distributed wireless network security with incomplete information of selfish and malicious user types," in *Proc. International Conference on Game Theory for Networks*, 2009, pp. 130–139.

[33] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Başar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in *Proc. Military Communications Conference(MILCOM)*, 2011, pp. 119–124.

[34] A. Garnaev and W. Trappe, "The eavesdropping and jamming dilemma in multi-channel communications," in *Proc. IEEE International Conference on Communications (ICC)*, 2013, pp. 2160–2164.

[35] D. Yang, J. Zhang, X. Fang, A. Richa, and G. Xue, "Optimal transmission power control in the presence of a smart jammer," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 5506–5511.

[36] L. Xiao, J. Liu, Y. Li, N. B. Mandayam, and H. V. Poor, "Prospect theoretic analysis of anti-jamming communications in cognitive radio networks," in *Proc. IEEE Global Communications Conference*, 2014, pp. 746–751.

[37] A. Garnaev, Y. Hayel, and E. Altman, "A bayesian jamming game in an ofdm wireless network," in *Proc. 10th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, 2012, pp. 41–48.

[38] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "Incorporating attack-type uncertainty into network protection," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1278–1287, 2014.

[39] G. Scutari, S. Barbarossa, and D. P. Palomar, "Potential games: A framework for vector power control problems with coupled constraints," in *Proc. IEEE International Conference on Acoustics Speech and Signal Processing Proceedings*, vol. 4, 2006, pp. IV–IV.

[40] M. Raya, M. H. Manshaei, M. Félegyházi, and J.-P. Hubaux, "Revocation games in ephemeral networks," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 199–210.

[41] T. Alpcan and S. Buchegger, "Security games for vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 280–290, 2011.

[42] I. Bilogrevic, M. H. Manshaei, M. Raya, and J. P. Hubaux, "Optimal revocations in ephemeral networks: A game-theoretic framework," in *Proc. 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, 2010, pp. 21–30.

[43] L. Xiao, Y. Chen, W. S. Lin, and K. J. R. Liu, "Indirect reciprocity security game for large-scale wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1368–1380, 2012.

[44] E. D. W. H. Sandholm and F. Franchetti. (2012) Dynamo: Diagrams for evolutionary game dynamics. Accessed Feb. 19, 2018. [Online]. Available: http://www.ssc.wisc.edu/~whs/dynamo.

[45] E. Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Newnes, 2012.

[46] M. Van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "Flipit: The game of "stealthy takeover"," *Journal of Cryptology*, vol. 26, no. 4, pp. 655–713, 2013.

[47] M. Zhang, Z. Zheng, and N. B. Shroff, "A game theoretic model for defending against stealthy attacks with limited resources," in *Proc. Springer International Conference on Decision and Game Theory for Security*, 2015, pp. 93–112.

[48] X. Feng, Z. Zheng, P. Hu, D. Cansever, and P. Mohapatra, "Stealthy attacks meets insider threats: A three-player game model," in *Proc. IEEE Military Communications Conference (MILCOM)*, 2015, pp. 25–30.

[49] N. Quijano, C. Ocampo-Martinez, J. Barreiro-Gomez, G. Obando, A. Pantoja, and E. Mojica-Nava, "The role of population games and evolutionary dynamics in distributed control systems: The advantages of evolutionary game theory," *IEEE Control Systems*, vol. 37, no. 1, pp. 70–97, 2017.

[50] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders," in *Proc. IEEE Conference on Computer Communications (INFOCOM)*, 2015, pp. 747–755.

[51] L. Xiao, D. Xu, C. Xie, N. B. Mandayam, and H. V. Poor, "Cloud storage defense against advanced persistent threats: A prospect theoretic studey," *IEEE Journal on Selected Areas in Communications*, 2017.

[52] H. K. Khalil, *Nonlinear Systems*. Prentice Hall New Jersey, 1996, vol. 2.

[53] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021," Cisco, White paper, March 2017.

[54] M. G. S. Sriyananda, I. Parvez, I. Güvene, M. Bennis, and A. I. Sarwat, "Multi-armed bandit for lte-u and wifi coexistence in unlicensed bands," in *2016 IEEE Wireless Communications and Networking Conference*, April 2016, pp. 1–6.

[55] M. Chen, W. Saad, and C. Yin, "Optimized uplink-downlink decoupling in lte-u networks: An echo state approach," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.

[56] K. Hamidouche, W. Saad, and M. Debbah, *Multi-Games for LTE and WiFi Co-existence over Unlicensed Channels*. Springer International Publishing, 2017.

[57] H. Zhang, X. Chen, and Z. Han, "A zero-determinant approach for power control of multiple wireless operators in lte unlicensed," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[58] E. J. Hong, S. Y. Yun, and D. H. Cho, "Decentralized power control scheme in femtocell networks: A game theoretic approach," in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, Sept 2009, pp. 415–419.

[59] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535–547, March 2000.

[60] E. Ziouva and T. Antonakopoulos, "Csma/ca performance under high traffic conditions: Throughput and delay analysis," *Comput. Commun.*, vol. 25, no. 3, Feb. 2002.