Market Models of Security Investments with Shared Spectrum

Zongyun Xie and Randall A. Berry
Northwestern University
e-mails: zongyun.xie@northwestern.edu, rberry@northwestern.edu

***Abstract*—Security is a critical concern in shared spectrum environments, where attacks can degrade service and influence market interactions between competing service providers (SPs). This paper examines market models in shared spectrum defense, focusing on the strategic interplay between SPs and attackers within licensed shared bands. We develop models to study SPs' investments in security against revenue-minimizing attackers, i.e., attackers that account for the underlying competition between SPs and seek to minimize the revenue they obtain in this market. We further consider both competitive and collaborative settings. In the competitive setting, we characterize equilibrium investment outcomes, while in the collaborative case, we consider the investments made by a central planner. Our numerical results show that at times the competitive setting can lead to over-investment.**

I. Introduction

Spectrum sharing is a promising approach for enabling new spectrum uses while retaining incumbent users. Notable implementations include the Citizens Broadband Radio Service (CBRS) in the U.S. 3.5 GHz band [1] and the Automated Frequency Coordination (AFC) in the 6 GHz band [2]. However, as noted in [3], [4] and [5], shared spectrum environments are potentially more susceptible to security attacks compared to traditional exclusively licensed spectrum. Attacks in these environments can affect service availability and the competitive behavior of service providers (SPs) in the market. This paper explores these issues by studying market models for shared spectrum defense, focusing on strategic defense investments by SPs against such attacks.

Our approach is based in part on [6], which models the competition between wireless SPs with shared spectrum using a framework of Cournot competition with congestible and intermittent spectrum resources. In this approach, SPs compete by determining the number of customers they can serve on their spectrum. These quantities, in turn, determine a market clearing price for their services and a latency cost that their customers experience (modeling the congestible nature of the spectrum). Here, the intermittent nature of the resources is modeling a band of spectrum that is temporally shared with an incumbent, as in the CBRS system, so it may not always be available to use by an SP. Building on this framework in [7], we considered a model with a single attacker that seeks to disrupt the spectrum by making it less available. This can model different types of denial-of-service (DoS) attacks, such as primary emulation attacks [8] and jamming attacks [9]. Here, we again consider such an attacker but also consider the possibility that SPs can invest to improve the defense of their networks.

We consider a scenario where there are two competing SPs, each serving customers using a given band of *licensed shared spectrum*, meaning that each SP has exclusive access to their band of spectrum when it is not being used by an incumbent (similar to PAL spectrum in the CBRS system). Compared to [6] and [7], we assume that this is the only spectrum band available to each SP so that they can not offload traffic into other bands. As in [7], we consider an attacker that seeks to disrupt the market by minimizing the total revenue obtained by the two SPs. However, our approach could be adapted to other objectives.

We adopt a three-stage game model. In the first stage, SPs simultaneously decide their investment levels aiming to minimize their loss due to an attack. In the second stage, the attacker adjusts its tactics based on these investments. In the third stage, SPs decide on the quantity of consumers to serve. We characterize the sub-game perfect Nash equilibrium.

Our analysis shows that SP investments have two effects: they can reduce the impact of an attack on their spectrum and can redirect the attacker to the other SP, creating a complicated strategic interaction. We also compare the equilibrium outcome with that obtained by a planner who jointly decides on investment levels and seeks to minimize the revenue loss due to attacks and the investment cost. We find that in some instances, the competitive outcome leads to over-investment compared to the planner, suggesting that SPs may be incentivized to cooperate on security investments.

In terms of related work, we add to the existing literature that explores shared spectrum from a market perspective, including [10], [11], [12], [13], and [14]. However, these studies didn't address security issues. Additionally, there is a significant body of work applying game-theoretic approaches to model attacks and defenses, as seen in [15], [16], [17], [18] [19], and [20]. Yet, these studies often do not consider the broader market implications of such cybersecurity challenges. Instead of looking into specific attack methods, our work abstracts them to a broader market perspective, offering insights for SPs and social planners.

This work was supported in part by the National Science Foundation (NSF) SII-Center: SpectrumX—An NSF Spectrum Innovation Center Grant (Federal Grant Number 2132700) and by NSF grants CNS-1908807 and CNS-2148183.

II. Market Model with Security Investment

In this section, we introduce the market model we use to study the SPs' security investments. In Section III, we will subsequently specialize this to the case of licensed shared spectrum.

We consider a scenario in which two SPs compete for a common pool of customers. Additionally, there is an attacker whose objective is to minimize the overall SP revenue, similar to [7]. This can be motivated by a setting in which an attacker seeks to extract the maximum payment that it can collect from the SPs for not attacking. Meanwhile, SPs can make defensive investments to shield themselves from potential attacks, albeit at a cost.

We model this as a game with the following stages:

1) The SPs decide the investment levels.
2) The attacker decides how to attack.
3) The SPs decide on the quantity of consumers to serve.

The SPs seek to maximize their profit given by:

$$R_i = x_i p_i - C_i(I_i), \tag{1}$$

where x_i, p_i, I_i, and $C_i(I_i)$ denote the consumer quantity, the service price, the investment level, and the investment cost of SP i at I_i, respectively. In stage 3, given their investment levels and the attacker's choice, the SPs compete via Cournot competition to determine the quantity of users served and the service price. The details of this competition will be discussed in the following section.

We consider an attacker with a total attack power Q, which models their ability to attack the SPs' spectrum. Let q_i denote the portion of this power used to attacked SP i's spectrum, where

$$\sum_i q_i \leq Q. \tag{2}$$

We assume that the SPs are using intermittently available spectrum that is available with probability α in the absence of an attack. This models a temporal spectrum sharing scheme as in CBRS, where the intermittency is due to the activity of an incumbent user. The impact of an attack (and of the SP's security investment) is to change this availability to $tilde\alpha_i$ given by:

$$\tilde{\alpha}_i = \alpha_i - G(\mathbf{I})q_i. \tag{3}$$

Here, $G(\mathbf{I})$ models the *investment effectiveness* as a function of the vector of investment levels of each SP i, $\mathbf{I}$, where, in general, larger levels of investment will lead to lower values of $G(\mathbf{I})$ and thus make attacks less effective. We will consider the more specific form of this in the following sections. As discussed in the following section, the SPs' revenue in stage 3 will, in turn, be impacted by this availability. Hence, given the SP's investment levels in stage 1, the attacker will distribute its attack power to minimize the sum of revenue.

To optimize revenue, an SP in stage 1 seeks to decide their investments to minimize the sum of revenue loss and investment cost:

$$\min_{I_i} R_{i,loss}(I_i, q_i) := \Delta R_i + C_i(I_i), \tag{4}$$

where $\Delta R_i = R_i(\alpha_i) - R_i(\tilde{\alpha}_i)$ depicts the revenue loss caused by the resulting attack. Notice that this change can be negative if the revenue gets boosted. Also note that we are modeling this as a full information game so that in stage 1, the SPs are investing by anticipating the resulting attack in stage 2, i.e., it is a setting where the attacker's motives are known.

III. Licensed Shared Bandwidth Defense

Next, we consider a market where each SP i has its own band of licensed shared spectrum with bandwidth w_i, meaning that only the SP i can use the band when it is available. With some abuse of notation, we assume the investment effectiveness is given by

$$G(I_i) = 1 - I_i, \tag{5}$$

and the cost of investment, $C(I_i) = c_i I_i^2$, where $I_i \in [0, 1]$ represents the investment by service provider i and $c_i > 0$ is a constant. This assumption models a case where each SP's investment only impacts its own band of spectrum.

A. Competition model

With licensed shared spectrum, in stage 3, the SPs compete via Cournot competition, in which they announce quantities of users to serve that determine a delivered price given by:

$$p_d = 1 - \sum_i x_i. \tag{6}$$

This corresponds to a market clearing price with a linear demand curve. Consumers also experience a latency cost for using SP i's spectrum given by $l_i = \frac{x_i}{w_i}$ so that the net service price that SP i can charge is given by

$$p_i = \tilde{\alpha}_i(p_d - l_i), \tag{7}$$

here we assume that customers only pay for the fraction of time that the spectrum is available (hence, the use of $\tilde{\alpha}_i$ in this expression). The net price can also be expressed as

$$p_i = \tilde{\alpha}_i \left(1 - x_i - x_{-i} - \frac{x_i}{w_i}\right). \tag{8}$$

For this model, it can be shown that in equilibrium, we have:[1]

$$\begin{aligned} p_i &= \frac{\tilde{\alpha}_i(w_i + 1)(w_{-i} + 2)}{3w_i w_{-i} + 4w_i + 4w_{-i} + 4}, \\ x_i &= \frac{w_i(w_{-i} + 2)}{3w_i w_{-i} + 4w_i + 4w_{-i} + 4}. \end{aligned} \tag{9}$$

Note that in these expressions, x_i does not depend on $\tilde{\alpha}_i$, while p_i is linear in this quantity. This means an attack will not change the quantity of customers an SP serves but will reduce its price.

Similar to [7], as long as x_i and p_i are non-increasing in q_i and if Q is small enough, the optimal strategy for the attacker is to attack only one of the SPs. In this case, $q_i \in \{0, Q\}$, which we assume in the following. In this case, we introduce the following lemma:

[1] We use the subscript $-i$ to denote a quantity corresponding to SP $j \neq i$.

Lemma 1. *Without any investment, the attacker would choose to attack SP i if the following condition is satisfied:*

$$\frac{(1-I_i)K_i}{(1-I_{-i})K_{-i}} > 1, \tag{10}$$

where K_i is defined as:

$$K_i = w_i(w_i+1)(w_{-i}+2)^2. \tag{11}$$

Proof. Assume there is an attack. Compare the revenue changes of two SPs:

$$\frac{\Delta R_i}{\Delta R_{-i}} = \frac{(\alpha_i - \tilde{\alpha}_i)K_i}{(\alpha_{-i} - \tilde{\alpha}_{-i})K_{-i}} = \frac{(1-I_i)K_i}{(1-I_{-i})K_{-i}}. \tag{12}$$

Under the condition assumed in the lemma, the potential revenue change $\Delta R_i > \Delta R_{-i}$, which means attacking the SP i is better for the attacker. □

Note if (10) is met with equality, the attacker is indifferent between attacking the two SPs. In this case, for convenience, we assume that it attacks SP1.

The following corollary to Lemma 1 characterizes the interplay of the SPs:

Corollary 1. *To incentivize the attacker to switch targets, the investment of a service provider i, denoted as I_i, must satisfy the following condition:*

$$\frac{1-I_i}{1-I_{-i}} < M_{i,switch} := \frac{K_{-i}}{K_i}. \tag{13}$$

Note that for each SP i, from (11), it follows that $M_{i,\text{switch}}$ is a constant dependent solely on the bandwidth allocations. Hence, the amount of investment needed to switch the attack is given by

$$I_{i,sw}(I_{-i}) = \max\left(0, 1 - M_{i,\text{switch}}(1-I_{-i})\right), \tag{14}$$

which depends on the amount of investment by the other SP.

Hence, an SP's investment can be to either protect itself against the attack or switch the attack to the other SP. First, we consider the case where an SP does not switch the attack, in which case, its investment will minimize the loss in (4), which can be rewritten as

$$R_{i,loss}(I_i, Q) = (1-I_i)Q\frac{x_i p_i}{\alpha_i} + c_i I_i^2. \tag{15}$$

The optimal investment for an SP to minimize this objective is given by

$$I_{i,best} = \min\left(\frac{Q x_i p_i}{2\alpha_i c_i}, 1\right). \tag{16}$$

SP i would only make this investment if it resulted in a lower loss, i.e., if

$$R_{i,loss}(I_{i,sw}(I_{-i}), 0) < R_{i,loss}(I_{i,best}(I_{-i}), Q). \tag{17}$$

Note if $I_{i,sw}(I_{-i}) < I_{i,best}$ this inequality is always satisfied. Similarly, the other SP can also try to switch the attack back. So, the strategic interaction between the SPs involves determining which SP is attacked as well as the defense level of that SP. Switching introduces a non-linearity in the SP's best responses, which in some cases prevents an equilibrium from existing.

Lemma 2. *If an equilibrium exists, then the following conditions must be satisfied if SP_i is attacked:*

- $I_i = I_{i,best}$.
- $I_{-i} = I_{-i,sw}(I_{i,best})$ *or* $I_{-i} = 0$.

Proof. The first condition directly follows (16). Then, if the one being attacked did switch the attack, $I_{-i} = I_{-i,\text{sw}}(I_{i,\text{best}})$. If the one being attacked did not switch the attack, then $I_{-i} = 0$, which gives the second condition. □

Taking Lemma 2 into account, the following proposition summarizes the competition model:

Proposition 1. *Assuming $w_1 > w_2$, which implies that SP1 is the larger provider, the following cases for equilibrium exist in the game:*

Case 1: If $R_{1,loss}(I_{1,best}, Q) < R_{1,loss}(I_{1,sw}(0), 0)$, then the equilibrium is $I_1 = I_{1,best}$ and $I_2 = 0$. In this case, the investment to switch the attack is not profitable for SP1 and, knowing this, SP2 has no incentive to invest.

Case 2: If

$$R_{1,loss}(I_{1,best}, Q) > R_{1,loss}(I_{1,sw}(I_{2,best}), 0),$$
$$R_{2,loss}(I_{2,best}, Q) < R_{2,loss}(I_{2,sw}(I_{1,sw}(I_{2,best})), 0),$$

then the equilibrium is $I_1 = I_{1,sw}(I_{2,best})$ and $I_2 = I_{2,best}$. In this case, SP1 switches the attack.

Proof. Both cases directly follow Corollary 1 and Lemma 2. There might be another case when SP1 has the incentive to invest higher than $I_{1,\text{best}}$ to switch the attack. SP2 estimated this switch and has the incentive to switch back. Then SP1 finally found it would be best for them only to invest $I_{1,\text{best}}$. Suppose this case exists and is noted as Case 3. The conditions are:

$$I_{1,\text{best}} > I_{1,\text{sw}}(0),$$
$$R_{2,\text{loss}}(I_{2,\text{sw}}(I_{1,\text{best}}), 0) < R_{2,\text{loss}}(I_{2,\text{best}}, Q),$$
$$R_{1,\text{loss}}(I_{1,\text{sw}}(I_{2,\text{sw}}(I_{1,\text{best}})), 0) > R_{1,\text{loss}}(I_{1,\text{best}}, Q),$$

However, It can be shown that the third inequality in Case 3 can be held only if $I_{1,best} > 1$, which is a contradiction to the definition given in 16. Thus, Case 3 is non-existent, preventing further iterative interplay between the SPs. Hence, the proposition is proven.

□

B. Social Planner

In this section, we consider a social planner that seeks to minimize the sum of the loss terms across the two SPs, i.e., its objective is[2]

$$\min_{I_1, I_2} \sum_i R_{i,loss}(I_i, q_i). \tag{18}$$

[2]Note that the planner is setting the investment levels but not the quantity of customers served by the two SPs, which is still determined via competition.

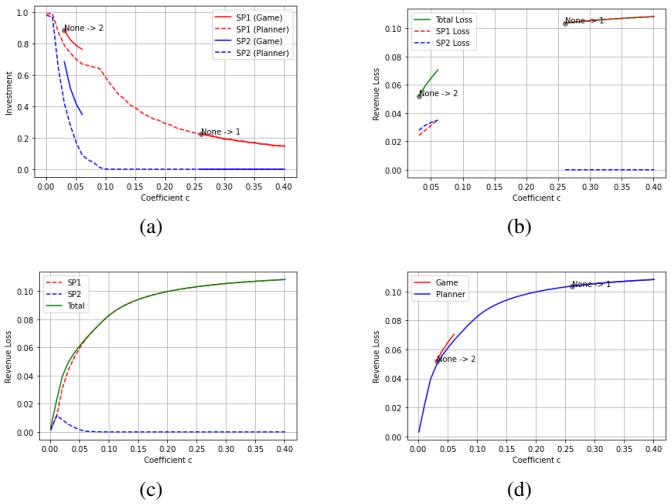
This problem can be formulated as the following mixed-integer nonlinear program:

$$\begin{aligned} min \ & \sum_{i=1}^{2} G(I_i) Q \frac{x_i p_i}{\alpha_i} y_i + C_i(I_i) \\ s.t. \ & I_1 > \left(1 - \frac{K_2}{K_1}(1 - I_2)\right) y_2 \\ & y_1 I_1 < 1 - \frac{K_1}{K_2}(1 - I_2) \\ & y_i \in \{0, 1\} \\ & \sum_i y_i = 1. \end{aligned} \tag{19}$$

Note here that the binary variables y_i are used to indicate which SP is attacked. In the following section, we will numerically compare the solution to this problem with the equilibrium outcome in the game.

IV. Numerical Results

We provide numerical examples showing the equilibrium outcome and the planner's decisions. These examples show that when c is small, the game has an equilibrium that falls into Case 2 in Proposition 1, while when c is large, a Case 1 equilibrium exists. For the intermediate value of c, an equilibrium does not exist. Also, it can be noted that the planner often decides on a lower level of investment compared to that in the game, suggesting that the strategic interaction of the SPs can lead to over-investment, resulting in a larger revenue loss, especially when the attack is relatively minor.



(a) (b) (c) (d)

Fig. 1. Equilibrium outcome: (a) Investment decisions (b) Revenue loss in the game (c) Revenue loss by the planner (d) Revenue loss compare. Constants: $Q = 0.8,\ \alpha_1 = \alpha_2 = 1,\ w_1 = 5,\ w_2 = 1.$

V. Conclusions

We presented an initial study of how shared licensed spectrum might influence security investment decisions by strategic competing service providers. These investments serve two roles: to reduce the damage of an attack and to redirect an attacker to the other SP, leading to intricate strategic interactions. Numerical results show that, in some cases, this competition can result in no equilibrium and over-investment in security compared to that of a social planner. Possible future directions include considering other spectrum sharing models and other attack models.

References

[1] Federal Communications Commission, "Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band", FCC 15-47 Report and order and second further notice of proposed rule-making, April 2015.

[2] Federal Communications Commission, "FCC Requests 6 GHz Automated Frequency Coordination Proposals", FCC-21-100 Public Notice, September 2021.

[3] S. Bhattarai, J.-M. J. Park, B. Gao, K. Bian, W. Lehr, "An Overview of Dynamic Spectrum Sharing: Ongoing Initiatives, Challenges, and a Roadmap for Future Research", *IEEE Transactions on Cognitive Communications and Networking*, vol. 2, no. 2, pp. 110–128, 2016.

[4] M. Clark, K. Psounis, "Can the privacy of primary networks in shared spectrum be protected", *in IEEE INFOCOM*, pp. 1–9, 2016.

[5] J.-M. Park, V. Kumar, T. Oyedare, "Policy Enforcement in Dynamic Spectrum Sharing", *Spectrum Sharing: The Next Frontier in Wireless Networks*, pp. 341–359, 2020.

[6] R. Berry, M. Honig, T. Nguyen, V. Subramanian, R. Vohra, "The value of sharing intermittent spectrum", *Management Science*, vol. 66, no. 11, pp. 5242–5264, 2020.

[7] Z. Xie, R. A. Berry, "Market Models of Spectrum Attacks with Shared Spectrum", *International Symposium on Modeling and Optimization in Mobile, Ad-Hoc and Wireless Networks*, 2023.

[8] Z. Jin, S. Anand, K. P. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks", *IEEE International Conference on Communications*, 2009.

[9] Y. E. Sagduyu, R. A. Berry, A. Ephremides, "Jamming games in wireless networks with incomplete information", *IEEE Communications Magazine*, 2011.

[10] A. Hayrapetyan, Éva Tardos, T. Wexler, "A network pricing game for selfish traffic", *in Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing*, pp. 284–291, 2005.

[11] Y. Zhu, R. A. Berry, "Contracts as Investment Barriers in Unlicensed Spectrum", *in IEEE INFOCOM*, pp. 1925–1933, 2018.

[12] A. Ghosh, R. A. Berry, "Competition with Three-Tier Spectrum Access and Spectrum Monitoring", *in Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 241–250, 2019.

[13] A. Ghosh, R. Berry, "Entry and investment in CBRS shared spectrum", *in 2020 18th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT)*, pp. 1–8, 2020.

[14] G. Saha, A. A. Abouzeid, "Optimal Spectrum Partitioning and Licensing in Tiered Access Under Stochastic Market Models", *IEEE ACM Transactions on Networking*, 2021.

[15] D. Yang, G. Xue, J. Zhang, J. Zhang, A. W. Richa, X. Fang, "Coping with a Smart Jammer in Wireless Networks: A Stackelberg Game Approach", *IEEE Transactions on Wireless Communications*, 2013.

[16] L. Xiao, T. Chen, T. Chen, T. Chen, J. Liu, H. Dai, "Anti-Jamming Transmission Stackelberg Game With Observation Errors", *IEEE Communications Letters*, 2015.

[17] Y. Gao, Y. Xiao, M. Wu, M. Xiao, J. Shao, "Game Theory-Based Anti-Jamming Strategies for Frequency Hopping Wireless Communications", *IEEE Transactions on Wireless Communications*, 2018.

[18] A. Garnaev, A. P. Petropulu, W. Trappe, H. V. Poor, "A Jamming Game With Rival-Type Uncertainty", *IEEE Transactions on Wireless Communications*, 2020.

[19] A. Pourranjbar, G. Kaddoum, K. Aghababaiyan, "Deceiving-Based Anti-jamming against Single-Tone and Multi-Tone Reactive Jammers", *IEEE Transactions on Communications*, 2022.

[20] L. Jia, N. Qi, F. Chu, S. Fang, X. Wang, S. Ma, S. Feng, "Game-Theoretic Learning Anti-Jamming Approaches in Wireless Networks", *IEEE Communications Magazine*, 2022.