Market Models of Spectrum Attacks 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. In additional to degrading service, attacks can influence the market interactions between competing service providers (SPs). This paper investigates these interactions by considering two SPs engaged in Cournot competition while utilizing both proprietary and shared spectrum, with shared spectrum available in either licensed or open-access forms. Additionally, we assume the presence of an attacker whose objective is to deny service to one or more of the shared bands for a fraction of the time, consequently reducing the overall total revenue. We analyze the optimal forms of attacks under different attacker objectives and their repercussions on the resulting market equilibrium. Utilizing these analyses, we compare the impacts of various spectrum sharing approaches (licensed and open access) and differing amounts of spectrum holdings of the two providers.**

***Keywords*—Game theory, resource allocation, network pricing.**

I. Introduction

Spectrum sharing provides a way of enabling new uses of a spectrum band without needing to relocate incumbent users. Recent examples include the Citizens Broadband Radio Service (CBRS) approach adopted in the 3.5 GHz band in the U.S. [1] and the Automated Frequency Coordination (AFC) approach used in the 6GHz band [2]. A potential issue with shared spectrum is that it may be more vulnerable to different security attacks compared to traditional exclusively licensed spectrum (e.g., see [3]). Attacks may degrade the services being offered in such a band and can also impact the competition between service providers operating in the band. In this paper, we seek to understand the market impacts of such attacks.

Our approach builds on the work in [4] that adopts a Cournot model for competition with shared spectrum that is intermittently available due to the spectrum use of incumbent users. In this model, wireless service providers (SPs) compete for a mass of non-atomic users. Each SP has access to its own proprietary spectrum that is not shared, as well as the band of shared spectrum. The SPs then compete by determining the quantity of customers served in each spectrum band, which determines the *delivered price* for service via a given demand function. The actual price an SP charges for service is given by the difference between this delivered price and a congestion cost, reflecting the quality of service obtained from that SP. The congestion cost, in turn, depends on the mass of customers an SP serves, the spectrum used, and the availability of the shared band.

We depart from the model in [4] by considering the presence of a single attacker that can reduce the availability of the shared spectrum through some type of denial-of-service (DoS) attack, such as a primary emulation attack [5], a jamming attack [6], or an attack on components of a spectrum management system [7]. The result of such an attack is to change the availability of the shared spectrum. We initially assume that this attacker's objective is to minimize the total revenue obtained in the market. It achieves this through two effects. First, it reduces the amount of spectrum available. Second, it can affect the competition among the SPs, for example, by reducing the market power of an SP by attacking it. One motivation for such attacks is financial gain for the attacker, i.e., the attacker could seek to extort the SPs to recover their lost revenue. If the SPs negotiate separately with the attacker, we show that the total revenue objective may not maximize the attacker's potential financial gain, leading us to introduce a second objective that better captures this.

Following [4], we explore two approaches for utilizing the shared band: licensed sharing and open access sharing. In licensed sharing, the band is divided into sub-bands, each licensed to a single SP, enabling exclusive spectrum use when the incumbent is inactive (similar to Priority Access in CBRS). The attacker can allocate attacks across these sub-bands, affecting spectrum availability differently for each SP. In open access sharing, the entire band is accessible to all SPs when not in use by the incumbent (similar to Generalized Authorized Access in CBRS). Attacks reduce availability uniformly for all SPs.

Our analysis is structured as a two-stage game. In the first stage, the attacker allocates attacks across the shared spectrum bands. In the second stage, the SPs determine user quantities to serve. We characterize the sub-game perfect Nash equilibrium. For licensed sharing, this involves optimizing the allocation of attacks across SPs. We find that the attacker targets only one SP to maximize its gain. We investigate how an SP's bandwidth holdings affect its vulnerability, revealing that an SP with less proprietary and more licensed shared bandwidth becomes a prime target for a weak attacker. In open access sharing, increasing attacker strength can shift which SPs utilize

This work was supported in part by the National Science foundation under grants CNS-1908807 and 2132700.

ISBN 978-3-903176-55-3 © 2023 IFIP

the open bandwidth. Numerical comparisons demonstrate that the preferred sharing form for welfare in the face of an attack depends on the attacker's strength.

In terms of related work, there has been a large body of work in addition to [4], studying market models for shared spectrum, e.g., [8], [9], [10], [11], [12], [13], [14]. Similar to our approach, these papers consider SPs competing using spectrum that is modeled as a congestible resource. However, in those works, the spectrum is always available, and there are no attackers present. There have also been several other papers that considered models with intermittently available shared spectrum, such as [15], but again attackers that influence this intermittence are not considered. There has also been a large body of work on different attack models for spectrum, see for example [3], [5], [6], [16], [17], [18]. Although attacks may take different forms, they ultimately affect specific properties of the band, such as availability or bandwidth allocation. Instead of focusing on individual attack models, our objective is to abstract these attacks and analyze their broader market implications. By employing this abstraction, we can better understand how these attacks impact the market dynamics.

II. Model with Licensed Shared Bandwidth

We begin with specifying our model for the case where the shared bandwidth is licensed. We consider a model with two SPs competing for a common pool of infinitesimal customers. Each SP i ($i \in \{1,2\}$) has b_i units of *proprietary bandwidth*, which is assigned exclusively to that provider. Additionally, each SP i has w_i units of *licensed shared spectrum*, which is available with probability α due to the activity of the incumbent user of that band. [1]

Additionally, we consider an attacker that can attack one or both of the SP's licensed shared bands to reduce their availability. We denote by q_i the reduction imposed on SP i's licensed shared band so that the availability of this band becomes $\alpha - q_i$. We further assume that the attacker is constrained so that

$$q_1 + q_2 \leq Q, \tag{1}$$

where Q denotes the total *attack power*. This constraint could arise due to the attacker's desire not to be identified or due to other technical considerations.[2] Note that the attacker can only target the shared band of spectrum and not the SPs' proprietary bands, modeling the fact that shared spectrum may be more susceptible to certain attacks.

We consider a two-stage model in which the attacker moves first and determines its allocation of attack power across the two shared bands. In the second stage, the SPs engage in Cournot competition, which we describe next.[3]

[1]In our analysis, we assume uniform α values for all SPs to simplify the model. It is straightforward to extend the analysis to incorporate different α values for each SP.

[2]Depending on the attack type, additional constraints could be taken into account. For instance, the cost of an attack may vary based on the targeted amount of shared bandwidth. We leave such considerations to future research.

[3]One could also view this as a model in which the attacker first announces a threat to attack (possibly with a ransom demand to not launch this attack) and the firms then determine the impact this threat will have on the market.

A. Cournot Competition between SPs

In the second stage, each SP i specifies a quantity of customers it serves on its proprietary spectrum, x_{b_i}, and its shared spectrum, x_{w_i}. The total quantity of customers served by both SPs on both types of spectrum determines a market *delivered price* for service via a downward sloping inverse demand curve $P(y) = 1-y$, where $y = x_{b_1}+x_{b_2}+x_{w_1}+x_{w_2}$. The price that an SP charges for service on a band is given by the difference between the delivered price and a *congestion cost* for that band. Each SP seeks to maximize its profit given by the product of the price it charges and the number of customers served.

As in [4], we model the congestion cost for the proprietary band of SP i as

$$l_{b_i}(x_{b_i}, x_{w_i}) = (\alpha - q_i)\frac{x_{b_i}}{b_i} + (1 - \alpha + q_i)\frac{x_{b_i} + x_{w_i}}{b_i}.$$

The congestion cost for the licensed shared band of SP i is

$$\begin{aligned} &l_{w_i}(x_{b_i}, x_{w_1}, x_{w_2}) \\ &= (\alpha - q_i)\frac{x_{w_1} + x_{w_2}}{w_i} + (1 - \alpha + q_i)\frac{x_{b_i} + x_{w_i}}{b_i}. \end{aligned}$$

These congestion costs model a situation in which customers are sensitive to the average congestion they experience over time and, whenever the shared spectrum is not available, the customers allocated to that spectrum are served using the SP's licensed spectrum.

Similar to [4], this Cournot competition can equivalently be viewed in terms of a model in which each SP i allocates its total traffic of $x_i = x_{b_i} + x_{w_i}$ to a single band of T_i units of proprietary spectrum, where

$$T_i = b_i \frac{b_i + w_i}{b_i + (1 - (\alpha - q_i))\, w_i}. \tag{2}$$

Further, there is a unique Nash equilibrium to this competition in which the quantity served by each SP is given by

$$x_i = \frac{T_i T_{-i} + 2T_i}{3T_i T_{-i} + 4 + 4\,(T_i + T_{-i})} \tag{3}$$

where T_{-i} denotes the equivalent proprietary spectrum of SP $j \neq i$. The corresponding price offered by each provider is given by:

$$p_i = \frac{T_i T_{-i} + 2T_i + T_{-i} + 2}{3T_i T_{-i} + 4 + 4(T_i + T_{-i})}. \tag{4}$$

These characterize the outcome of the 2nd stage of our model.

From these expressions, it can be seen that

$$\frac{\partial x_i}{\partial T_i} > 0,\ \frac{\partial x_i}{\partial T_{-i}} < 0,\ \frac{\partial p_i}{\partial T_i} > 0,\ \frac{\partial p_i}{\partial T_{-i}} < 0. \tag{5}$$

In other words, an increase in a SP's equivalent bandwidth leads to an increase in its quantity served and its price, while an increase in its competitor's equivalent bandwidth leads to a reduction in both of these quantities. Note also from (2) that increasing the attack power on SP i will lead to a decrease in that SP's equivalent bandwidth, and thus decrease that SP's profit, while increasing the profit of the other SP.

ISBN 978-3-903176-55-3 © 2023 IFIP

B. Optimal attacker strategy

1) Attack on Total Revenue: As an initial attacker objective, we assume that the attacker seeks to minimize the total revenue earned by both SPs in the market. In other words, in the first stage of the model, the attacker seeks to specify (q_1, q_2) subject to (1) to minimize

$$R(x_1, x_2) = \sum_i x_i p_i \tag{6}$$

where x_i, p_i satisfies (3),(4). Additionally, we assume that $0 \leq q_i \leq \alpha$ for each SP i so that (2) is meaningful. As q_i approaches the upper limit of α, note that T_i approaches b_i, as in this case the SP essentially has no access to the shared spectrum.

To summarize, the problem faced by the attacker is given by

$$\begin{aligned} &\min_{q_i} \sum_i x_i p_i \\ &s.t.\ (1)\ ,(2)\ ,(3)\ ,(4), 0 \leq q_i \leq \alpha, \forall i. \end{aligned} \tag{7}$$

Next, we consider solving (7). It can shown that the attacker's objective is non-decreasing in q_1 and q_2. Hence, at an optimal solution, the attacker's choices of q_1 and q_2 must either satisfy $q_1 + q_2 = Q$ or $q_i = \alpha$ for all i, as otherwise, the attacker could increase q_i for some i and decrease its objective. If $Q > 2\alpha$, then the only possible such solution is for $q_1 = q_2 = \alpha$, in which case neither SP has access to the shared spectrum. Hence, in the following, we focus on the more interesting case of $Q < 2\alpha$. In this case, let $q_1 = q$. Then, at optimality, it must be that $q_2 = Q - q$ and q must satisfy

$$\max(0, Q - q) \leq q \leq \min(\alpha, Q). \tag{8}$$

Hence, we can reformulate the attacker's problem in terms of the single optimization variable q. The resulting one-dimensional problem is not convex, but can be solved by a direct search over q to find the optimum value.

2) Attack for Gain: As we noted, one motivation for an attacker may be to seek financial gain from the SPs. The maximum amount that the SPs would be willing to pay to prevent an attack would be equal to the loss in total revenue they experience due to the attack. However, if the attacker negotiates separately with each SP, then the total revenue lost may not be a good indicator of what that attacker may gain. The reason for this is that the attack profile that minimizes the total revenue may be one that *increases* the revenue of one of the SPs. Essentially, making one SP more competitive can reduce the revenue of its competitor by a larger amount. In such a case, as we will show later, the attacker could recover more revenue from the competitor than indicated by the total revenue lost.

Based on the above, we next consider a different attackers objective, which we refer to as the attacker's *gain*. This directly accounts for the revenue lost from an attack that an attacker can recover. This is given by

$$G(x_1, x_2) = \sum_i (R_0(x_{i,0}) - R(x_i), 0). \tag{9}$$

Here, $R(x_i) = x_i p_i$ denotes the current revenue of SP i, while $R_0(x_{i,0}) = x_{i,0} p_{i,0}|_{Q=0}$ represents the initial revenue of SP i in the absence of an attack, where $x_{i,0}$ and $p_{i,0}$ denote the equilibrium quantity and price in the absence of an attack. The attacker's gain can be interpreted as the sum of only the revenue loss experienced by the SPs without considering any potential increase in revenue.

The problem the attacker now faces can be expressed as:

$$\begin{aligned} &\max_{q_i} \sum_i (R_0(x_{i,0}) - R(x_i), 0) \\ &s.t.\ (1)\ ,(2)\ ,(3)\ ,(4), 0 \leq q_i \leq \alpha, \forall i. \end{aligned} \tag{10}$$

This problem is also non-convex, but it remains one-dimensional and so can still be solved through a direct search over q. Additionally, we can use the structure of this problem to gain additional insights, as discussed next.

Assuming a small enough value for Q, we argue next that the attacker would target only one of the service providers (SPs), unless both SPs share identical parameters. In the latter case, the attack distribution does not impact the optimal attacker gain. As observed through 5, an attack on SP i results in a reduction of the equivalent bandwidth T_i, leading to a decline in consumer quantity and price. Consequently, this decreases the revenue for the targeted SP while increasing the revenue of the other SP. This outcome is intuitive, as it renders the attacked SP less competitive within the market. Thus, the optimal strategy for the attacker involves targeting only one of the SPs until its shared bandwidth is jammed, as any alternative strategy could be improved upon to achieve greater gains. This holds for any value of $Q < \alpha$; when the total attack power exceeds this, then the attacker may or may not benefit from attacking both SPs as we will show in Sect. IV.

To summarize, to solve (10) when $Q < \alpha$, the attacker's solution is simple: it uses all of its power to attack only one of the SPs.

III. Model with Open Access Sharing

In this section we turn to the case where the shared spectrum is open access, meaning that both SPs can utilize the entire shared spectrum with a bandwidth of $W = w_1 + w_2$. Again we assume that this band is available with probability α. In this case, we assume that the attacker can only attack the entire open shared band using its total attack power of Q so that the open bands' availability becomes $\alpha - Q$. This models a case in which the two SPs are either given access to the entire shared band or no access (e.g., this could be determined by a spectrum management system).[4]

Given an attack, the two SPs compete as in the previous section. The only difference here is how the congestion costs are determined for the traffic the SPs allocate to the open shared band, which we denote by $x_{W,i}$ for SP i. As in [4], we

[4]An extension of this that we leave for future work would be to consider models in which the shared band is divided into sub-bands, each of which is open access, and the attacker can then allocate its attacks across these sub-bands as in the licensed case.

ISBN 978-3-903176-55-3 © 2023 IFIP

model the congestion experienced by these customers when the open shared band is available by $\frac{x_{W,1}+x_{W,2}}{W}$. Note that in this case, each SP's customers experience congestion that depends on the aggregate traffic in the band, reflecting the open access. Using this, one can again determine average congestion costs accounting for the spectrum availability and traffic offloading when the shared spectrum is unavailable as in the licensed shared case.

We do not have a closed-form solution to the resulting Cournot competition with open spectrum. However, following [4], it can be shown that this model is a potential game, so the equilibrium among the SPs can be found by solving a system of linear equations that correspond to the first-order optimality conditions for the potential function. Adapting this to the case where the spectrum is attacked, we can numerically determine the equilibrium with open access shared spectrum.

Additionally, it can be shown that only SP 2 will utilize the open spectrum if and only if the following condition holds:

$$b_1 \geq 2W + 2b_2 + 2 + \frac{4\,(1-\alpha+Q)\,W}{b_2}. \tag{11}$$

In other words, if SP 1 has a large enough amount of proprietary spectrum, it will not allocate any traffic to the open shared spectrum in equilibrium. In the case that (11) holds, let

$$\gamma = \left[4\left(1+\frac{1}{b_1}\right)\left(1+\frac{1}{b_2}\right)-1\right]\left(1+\frac{b_2}{W}\right) - \frac{4(\alpha-Q)}{b_2}\left(1+\frac{1}{b_1}\right). \tag{12}$$

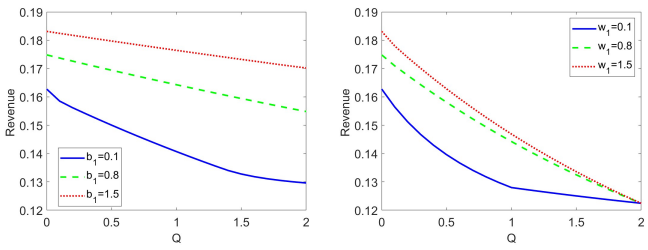
The resulting equilibrium can then be written as

$$\begin{aligned} x_{W,1} &= 0, \\ x_{W,2} &= \frac{1+\frac{2}{b_1}}{\gamma}, \\ x_{b_1} &= \frac{1+\frac{2(1-\alpha+W)}{b_2}+\frac{b_2}{W}+\frac{2}{W}}{\gamma}, \\ x_{b_2} &= \frac{b_2}{W}x_{W,2}. \end{aligned} \tag{13}$$

From (12), it can be seen that γ is increasing in Q and so from (13), it follows that in such an equilibrium, the traffic served by the weaker SP (SP 2) will decrease as Q increases, while the traffic served by the stronger SP (SP 1) can be shown to be increasing in Q. Hence, in this case, an attack on the open spectrum will increase the market share of the stronger SP. Intuitively, since this SP is not using the shared spectrum, an attack on the shared spectrum makes its service more desirable to customers compared to SP 2. Also note that the right-hand side of (11) has a term that is linearly increasing in Q. Hence, in some cases, the presence of an attacker can cause the stronger SP to begin using the open spectrum when in the absence of an attack, it would not.

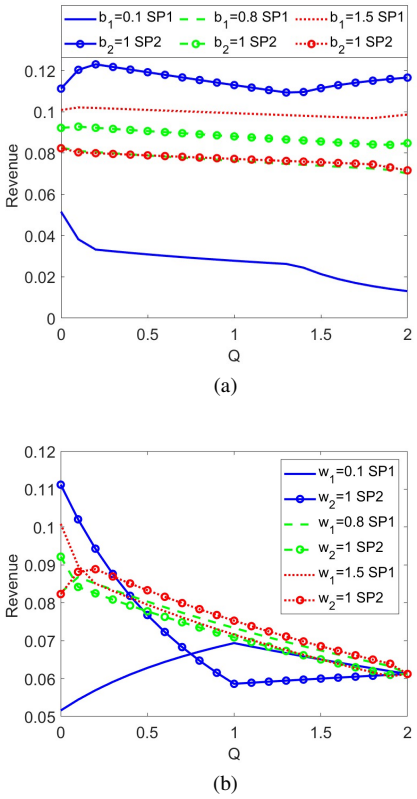
IV. Numerical Results

Next, we show some numerical examples with different amounts of bandwidth and total attack power.



(a) (b)

Fig. 1. Total revenue versus Q for (a) different values of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1, when $w_2 = 1, b_1 = b_2 = 0.5$, attacking on total revenue.



(a)

(b)

Fig. 2. The revenue of each SP versus Q for (a) different values of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1 when $w_2 = 1, b_1 = b_2 = 0.5$, attacking on total revenue.

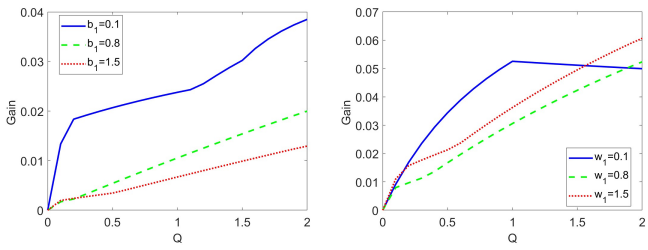
A. Licensed Shared Bandwidth

First, we present a set of examples where the shared bandwidth is licensed. In all these examples, the availability of the licensed bandwidth is set to $\alpha = 1$. In this section, we give results for two scenarios: one where the attacker aims to minimize the total revenue and another where it seeks to optimize its gain.

1) Attack on Total Revenue: In Fig. 1, we show the impact of varying Q on the total SP revenue (summed across the two SPs). In Fig. 1(a), this is shown for different values of b_1, where $b_2 = 1$ and $w_1 = w_2 = 0.5$.

As expected, the total revenue in each case is decreasing in

ISBN 978-3-903176-55-3 © 2023 IFIP



(a) (b)

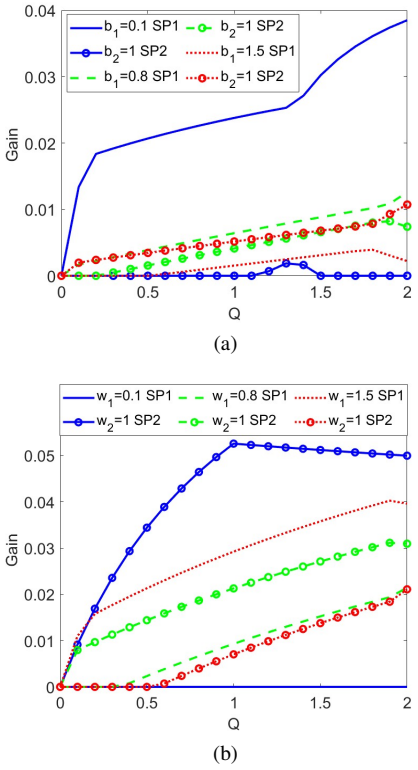
Fig. 3. The total gain versus Q for (a) different values of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1 when $w_2 = 1, b_1 = b_2 = 0.5$, attacking on total revenue.

the attack power and revenue is larger when the proprietary spectrum allocated to SP 1 increases.

In Fig. 1(b), we show curves for different values of w_1, when $w_2 = 1$ and $b_1 = b_2 = 0.5$. Again, these curves are decreasing in the attack power and increase in the amount of shared spectrum allocated in SP 1. One distinct feature to note is that when $b_1 = 0.1$ (or $w_1 = 0.1$) so that SP 1 has much less proprietary (shared) spectrum than SP 2, then as shown in Fig. 1, the total revenue decreases more quickly compared to the more balanced cases. To better understand this, in Fig. 2, we plot the individual revenues of the two SPs under the same parameters. As be seen in Fig. 2(a) for $b_1 = 0.1$, the revenue of the larger SP (SP 2) initially improves for small values of Q, compensating for the loss from SP 1, which keeps the total revenue from dropping too much. Also, we note from Fig. 2(b) that when the SPs have different amounts of licensed shared spectrum, which SP obtains the largest revenue can depend on the total attack power. For example, when $w_1 = 0.1$ and $w_2 = 1$, SP 2 obtains more revenue than SP 1 when Q is small but less revenue when Q is large. Intuitively, when Q is small, SP 2 benefits from having more spectrum, but when Q is large, it suffers due to attracting more spectrum attacks, as we will show next.

In Fig. 3 and Fig. 4, we plot the gain from (9), still assuming that the attacker is targeting the total revenue. We observe that the gain from the attack generally increases with the total power Q. Note that for the case of $b_1 = 0.1$ in Fig. 3 that the gain for small values of Q is clearly larger than the drop in total revenue as shown in Fig. 1. Also note that, the rate of increase in the gain may vary as the distribution of attack power differs depending on the specific situation. Additionally, we note that further attacks when $Q > \alpha$ can result in even lower gains, suggesting that the attacker may not be inclined to continue the attack once one of the SP's shared bandwidths becomes entirely unusable.

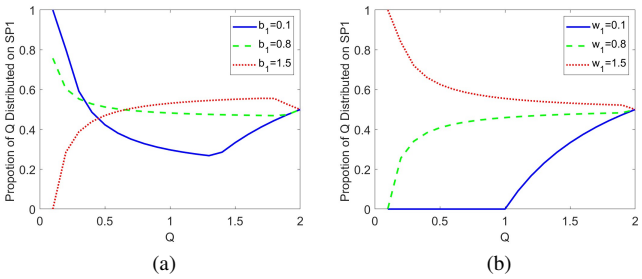
In Fig. 5, we show the optimal attack parameters for the same settings as in the previous figures. Namely, we plot the fraction q/Q of attack power allocated to SP 1's licensed shared spectrum. Note that from Fig. 5(a), when Q is small enough, the attacker will allocate 100% of its attack power to the smaller SP. However, in some cases, when Q is large



(a)

(b)

Fig. 4. The gain from each SP versus Q for (a) different values of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1 when $w_2 = 1, b_1 = b_2 = 0.5$, attacking on total revenue.



(a) (b)

Fig. 5. The fraction q/Q of attack power allocated to SP 1 versus Q for (a) different value of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1 when $w_2 = 1, b_1 = b_2 = 0.5$, attacking on total revenue.

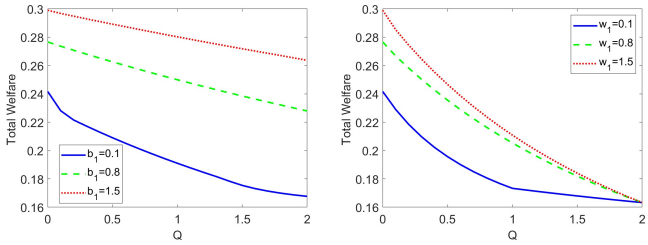
enough it may allocate more of its power to the larger SP. This is consistent with the individual revenue shown in Fig. 2(a).

From Fig. 5(b), it can be seen that when Q is small, the attacker will allocate all of its power to the larger SP, and in this case, will always allocate a larger percentage of its power to that SP, which is consistent with our explanation of the individual revenue in Fig. 2(b).

In Fig. 7, we show the consumer welfare versus the total attack power Q, for the same settings as in Fig. 1. Here, consumer welfare is given by $(1/2)y^2$, where y is the total amount of customers served in the market. Note that the trends in total consumer welfare are very similar to those for revenue.

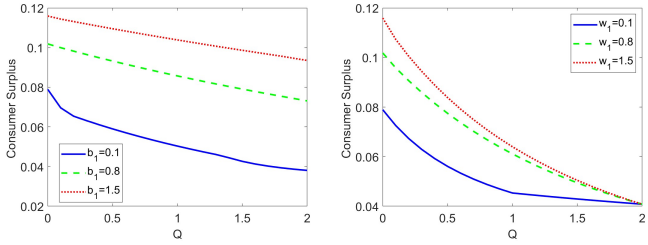
Finally, in Fig. 6, we plot the total welfare in the market,

ISBN 978-3-903176-55-3 © 2023 IFIP



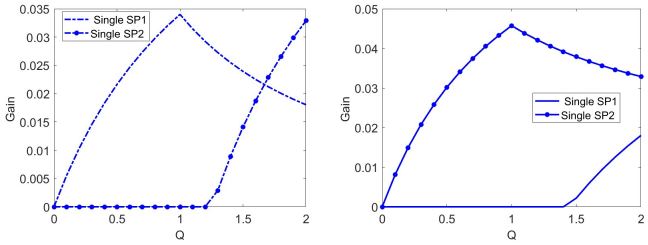
(a) (b)

Fig. 6. Total Welfare versus Q for (a) different values of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1 when $w_2 = 1, b_1 = b_2 = 0.5$, attacking on total revenue.



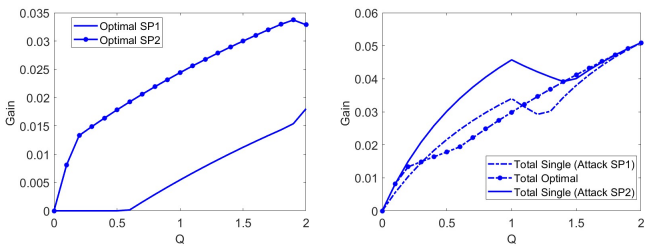
(a) (b)

Fig. 7. Consumer welfare versus Q for (a) different values of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1 when $w_2 = 1, b_1 = b_2 = 0.5$, attacking on total revenue.



(a) (b)

Fig. 8. Comparison of attack gains for single attacks when $b_1 = b_2 = 0.5, w_1 = 0.7, w_2 = 1$; attack power is first allocated entirely to (a) SP 1 or (b) SP 2



(a) (b)

Fig. 9. (a) Gain from both SPs during the optimal total revenue attack (b) Comparison between the optimal attack and the single attacks when $b_1 = b_2 = 0.5, w_1 = 0.7, w_2 = 1$

given by the sum of the consumer welfare and the total revenue, for the same sets of parameters. The behavior here is again very similar to the revenue and consumer welfare plots.

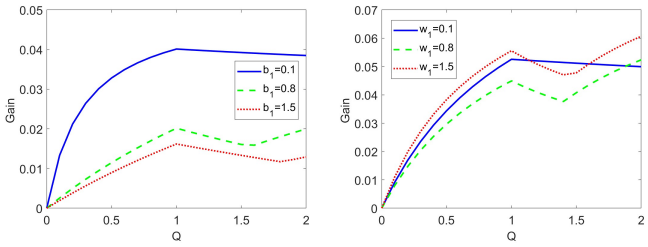
2) Attack for Gain: In the previous section, we argued that a single targeted attack is optimal for achieving the greatest gain before one of the SPs exhausts all shared bandwidth. In this section, we show the impact of such attacks and also consider cases where the attacker has sufficient power to jam both SPs to determine whether this is a viable strategy. Namely, in Fig. 8(a), we plot the attacker gain from each SP when it first allocates all attack power to SP 1 and then begins attacking SP 2, once $Q > 1$. Fig. 8(b) show an analogous plot when attacking SP 2 first. This shows that when Q is slightly greater than 1, attacking the other SP leads to a loss in the total gain. Also by comparing these two plots, one can see that for $Q < 1$, attacking the smaller SP (SP 2) first gives the attacker the larger gain.

Next, in Fig. (9) we illustrate the contrast between a single attack and the optimal total revenue attack. As shown in Fig. (9)(b), it is possible for the single attack to yield either better or worse gains based on the choice of the target. When the weaker SP (SP 2) is the target, then this single attack leads to a larger gain than that obtained with the optimal total revenue attack, consistent with our previous observations.

Next we consider the attack for the optimal gain as in (10), which we find through using a direct line search. As we will see, for $Q < 1$, this is consistent with our earlier claim that attacker should focus its attack only on the weaker SP.

In Fig. 10, we show the total gain versus Q for the same set of parameters as in Fig. 3. Compared to Fig. 3, the curves in this figure rise smoothly before reaching $Q = \alpha$. Upon surpassing this threshold, we observe a marked decrease in the gain, as the attacker requires additional power to counteract the previous increase brought on by the less competitive market. Once a certain point is reached, at $Q \approx 1.5$, the curve under the $w_1 = 0.1$ and $w_1 = 1.5$ cases in Fig.(10)(b) begins to rise again. This suggests that the attacker is sufficiently strong to reduce the other SP's revenue. We can see this trend more clearly in Fig. 11, which shows the gain obtained from each SP separately for the same scenarios.

In Fig. 12, we present the optimal attack parameters for



(a) (b)

Fig. 10. The total gain versus Q for (a) different values of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1 when $w_2 = 1, b_1 = b_2 = 0.5$, attacking for gain.

ISBN 978-3-903176-55-3 © 2023 IFIP

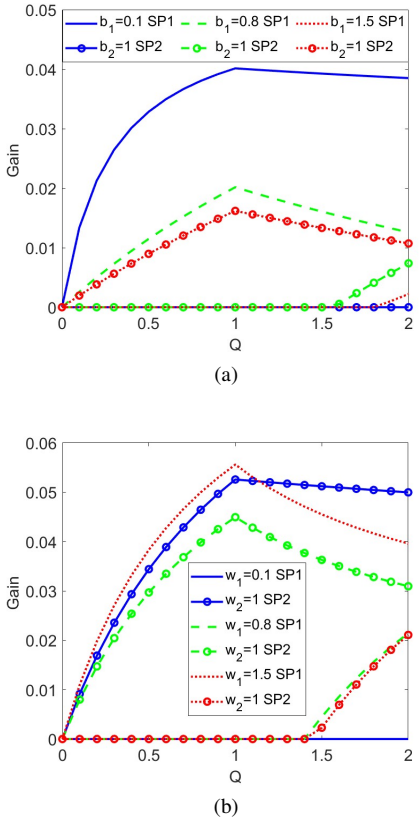


Fig. 11. The gain from each SP versus Q for (a) different values of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1 when $w_2 = 1, b_1 = b_2 = 0.5$, attacking for gain.

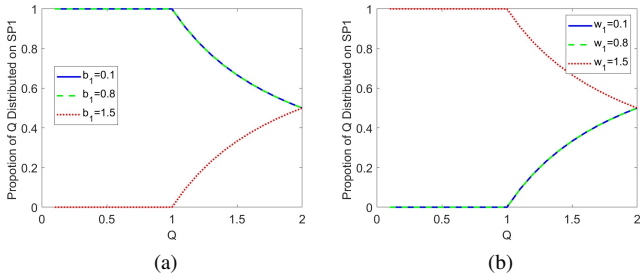


Fig. 12. The fraction q/Q of attack power allocated to SP 1 versus Q for (a) different value of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$ and (b) different values of w_1 when $w_2 = 1, b_1 = b_2 = 0.5$, attacking for gain.

the same settings as in Fig. 10. The results corroborate our earlier analysis and observations, indicating that the attacker will choose to target only one of the SPs with a single attack. This holds true for all tested parameters until $Q > \alpha$. After depleting one SP's shared bandwidth, we set the attacker to target the other SP. However, as we observed in Fig. 11, the attacker may not have an incentive to pursue this course of action as it may lead to a lower gain.

B. Open Access Shared Bandwidth

Next, we consider the open shared bandwidth case and compare it to the case with licensed shared bandwidth. The

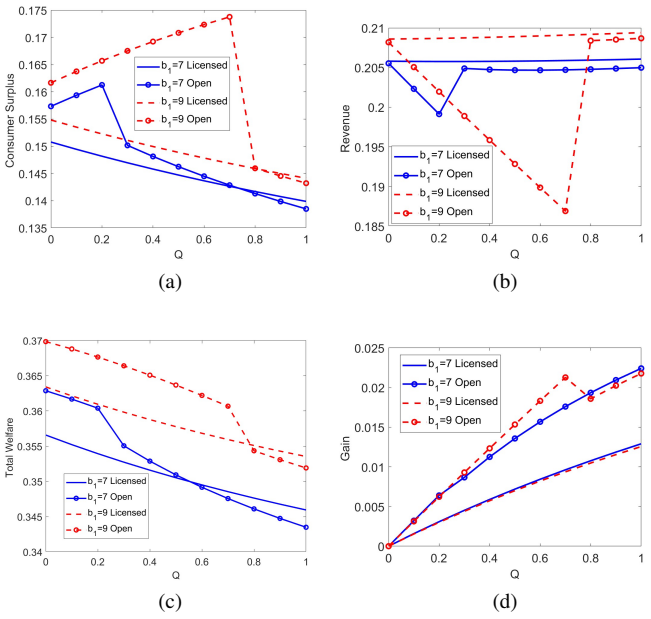


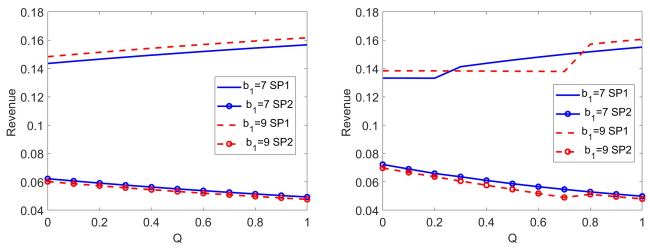
Fig. 13. Comparison of consumer welfare (a), total revenue (b), total welfare (c), and gain (d) for different values of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$.

availability of the shared bandwidth is again set to be $\alpha = 1$. The attacker's objective in the licensed shared bandwidth case is set to maximize its gain.

In Fig. 13, we compare the consumer welfare, total revenue, total welfare and attacker gain between open access sharing and licensed sharing for two different values of b_1. Here, we choose large enough values of b_i so that the condition in (11) is satisfied when $Q = 0$. As seen in Fig. 13(a), for small values of Q, increasing Q can improve consumer welfare with open access (while it always leads to lower consumer welfare with licensed shared access). These are exactly the cases in which the larger SP is not using the open shared band for small Q, and so larger Q values lead to it serving more customers. From Fig. 13(b), it can be seen that in this range, total revenue with open access is decreasing, and from Fig. 13(c), this decrease is enough so that the total welfare also decreases. It can also be seen that with open spectrum, these trends can abruptly change. This corresponds to the point where (11) no longer holds so that both SPs are using the open band. In Fig. 13(d), it is evident that an open shared bandwidth scenario yields a larger gain for the attacker. Additionally, we can observe a decrease in the gain as Q increases, which is again attributable to the condition in (11) no longer holding.

It is also worth noting that the plot in Fig. 13 suggests that an optimal attack for maximizing other objectives with open shared spectrum may not necessarily utilize the entire attack budget Q as depicted in these plots. In instances where attacking with $q = Q$ results in increased consumer welfare, a counter-intuitive outcome arises: to minimize consumer welfare, the optimal attack would involve setting $q = 0$. In other words, the open spectrum would deter a sufficiently weak attacker from initiating an attack in these cases.

ISBN 978-3-903176-55-3 © 2023 IFIP



(a) (b)

Fig. 14. Comparison of individual revenue between licensed shared spectrum (a) and open shared spectrum (b) for different choices of b_1 when $b_2 = 1, w_1 = w_2 = 0.5$.

Comparing the open access and licensed cases, in Fig. 13, it can be seen that for small values of Q, open access leads to greater consumer welfare and greater total welfare compared to licensed shared access. However, for large values of Q, licensed shared access has higher consumer welfare and total welfare. Total revenue is always greater with licensed shared access, and hence the gain for the attacker is worse. Intuitively, open access increases competition, which benefits consumer welfare and total welfare. However, open access also increases the attacker's ability by enabling it to attack both firms, which increases its gain.

Finally, in Fig. 14, we compare the individual revenues between licensed and open sharing for the same two values of b_1 as in Fig. 13. Comparing the two cases, note that the large SP (SP 1) always obtains more revenue with licensed sharing. However, the smaller SP (SP 2) may benefit when the spectrum is open access, especially for small values of Q. Also note that with licensed sharing, SP 1 always has a large revenue with the larger values of b_1. However, this may not be the case with open access sharing, depending upon the attack power Q. And at a certain time point, as depicted in Fig. 14(b), an attacker may not benefit from increasing its attack power (after $Q = 0.7$).

V. Conclusions

We studied the market implications of attacks on the shared spectrum in a basic model where an attacker seeks to disrupt the market and minimize total revenue. Two service providers (SPs) compete for customers via Cournot competition, considering the attacker's decisions. We determined the optimal attack allocation for licensed shared spectrum and characterized the impact of an attack with open access shared spectrum. We then numerically compared the impact of different bandwidth allocations and access regimes for shared spectrum.

Our results demonstrated that for licensed shared spectrum, an attacker tends to target the SP with more shared and less proprietary spectrum to achieve the best gain. However, this may not hold with sufficient attack power. The attacker's gain can be better when the bandwidth is open access, while consumer welfare may also be higher, suggesting that the choice of access regimes may involve a balance between deterring attacks and improving consumer welfare.

Future extensions to these models include considering additional objectives for the attacker, such as consumer welfare, and exploring scenarios with faster decision-making time scales, requiring proactive anticipation and response from service providers. Incorporating scenarios where the attacker lacks complete market information and examining mixed settings of licensed and open access shared spectrum are also of interest. Finally, considering potential defense strategies for the SPs is another potential direction.

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] J.-M. Park, J. H. Reed, A. Beex, T. C. Clancy, V. Kumar, B. Bahrak, "Security and enforcement in spectrum sharing", *Proceedings of the IEEE*, vol. 102, no. 3, pp. 270–281, 2014.

[4] 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.

[5] Z. Jin, S. Anand, K. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks", *in 2009 IEEE International Conference on Communications*, pp. 1–5, IEEE, 2009.

[6] Y. E. Sagduyu, R. A. Berry, A. Ephremides, "Jamming games in wireless networks with incomplete information", *IEEE Communications Magazine*, vol. 49, no. 8, pp. 112–118, 2011.

[7] S. Shi, Y. Xiao, W. Lou, C. Wang, X. Li, Y. T. Hou, J. H. Reed, "Challenges and new directions in securing spectrum access systems", *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6498–6518, 2021.

[8] P. Maillé, B. Tuffin, J.-M. Vigne, "Competition between wireless service providers sharing a radio resource", *in International Conference on Research in Networking*, pp. 355–365, Springer, 2012.

[9] F. Zhang, W. Zhang, "Competition between wireless service providers: Pricing, equilibrium and efficiency", *in 2013 11th International Symposium on Modeling & Optimization in Mobile, Ad Hoc & Wireless Networks (WiOpt)*, pp. 208–215, 2013.

[10] T. Nguyen, H. Zhou, R. Berry, M. Honig, R. Vohra, "The Cost of Free Spectrum", *Operations Research*, vol. 64, no. 6, pp. 1217–1229, 2016.

[11] C. Liu, R. A. Berry, "Competition with shared spectrum", *in 2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, pp. 498–509, 2014.

[12] X. Wang, R. A. Berry, "Market competition between LTE-U and WiFi", *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 765–779, 2021.

[13] M. Muthuswamy, R. Berry, M. Honig, T. Nguyen, V. Subramanian, R. Vohra, "Spectrum Pooling with Competitive Service Providers", *in 2021 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2021.

[14] G. Saha, A. A. Abouzeid, "Optimal spectrum partitioning and licensing in tiered access under stochastic market models", *IEEE/ACM Transactions on Networking*, vol. 29, no. 5, pp. 1948–1961, 2021.

[15] 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.

[16] A. Garnaev, W. Trappe, Y. T. Hou, W. Lou, "Spectrum attacks aimed at minimizing spectrum opportunities", *in 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2092–2096, 2017.

[17] M. Li, I. Koutsopoulos, R. Poovendran, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks", *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1119–1133, 2010.

[18] 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*, vol. 17, no. 8, pp. 5314–5326, 2018.

ISBN 978-3-903176-55-3 © 2023 IFIP