entropy

MDPI

Article

Competitive Sharing of Spectrum: Reservation Obfuscation and Verification Strategies

Andrey Garnaev * and Wade Trappe

Wireless Information Network Laboratory (WINLAB), Rutgers University, North Brunswick, NJ 08901, USA; trappe@winlab.rutgers.edu

* Correspondence: garnaev@yahoo.com; Tel.: +1-848-932-6857

Received: 19 May 2017; Accepted: 11 July 2017; Published: 15 July 2017

Abstract: Sharing of radio spectrum between different types of wireless systems (e.g., different service providers) is the foundation for making more efficient usage of spectrum. Cognitive radio technologies have spurred the design of spectrum servers that coordinate the sharing of spectrum between different wireless systems. These servers receive information regarding the needs of each system, and then provide instructions back to each system regarding the spectrum bands they may use. This sharing of information is complicated by the fact that these systems are often in competition with each other: each system desires to use as much of the spectrum as possible to support its users, and each system could learn and harm the bands of the other system. Three problems arise in such a spectrum-sharing problem: (1) how to maintain reliable performance for each system-shared resource (licensed spectrum); (2) whether to believe the resource requests announced by each agent; and (3) if they do not believe, how much effort should be devoted to inspecting spectrum so as to prevent possible malicious activity. Since this problem can arise for a variety of wireless systems, we present an abstract formulation in which the agents or spectrum server introduces obfuscation in the resource assignment to maintain reliability. We derive a closed form expression for the expected damage that can arise from possible malicious activity, and using this formula we find a tradeoff between the amount of extra decoys that must be used in order to support higher communication fidelity against potential interference, and the cost of maintaining this reliability. Then, we examine a scenario where a smart adversary may also use obfuscation itself, and formulate the scenario as a signaling game, which can be solved by applying a classical iterative forward-induction algorithm. For an important particular case, the game is solved in a closed form, which gives conditions for deciding whether an agent can be trusted, or whether its request should be inspected and how intensely it should be inspected.

Keywords: spectrum sharing; signaling games; bayesian games

1. Introduction

Cognitive radio (CR) networks are being explored as a powerful tool to improve spectrum efficiency by allowing unlicensed (secondary) users (SUs) to use spectrum belonging to a licensed (primary) user (PU) as long as they do not cause interference. Towards this end, the concept of a spectrum server has been introduced to improve the sharing of spectrum [1–3]. Spectrum servers coordinate the sharing of spectrum between different wireless services by taking in resource requests (i.e., an amount of bands needed), and then allocating resource assignments to these services. Unfortunately, the open and dynamic nature of CR platforms and their software, which allow for opportunistic access to the licensed spectrum by potentially unknown users, makes the operation of CR networks and their associated dynamic spectrum access protocols vulnerable to exploitation and interference. In particular, transmission reservation protocols, by which services (or users)

request spectrum from a spectrum server and thereby support the opportunistic usage of spectrum by secondary users, assume that the entities involved in the protocols are honest. These protocols can fail if malicious services/users aim to undermine the rules and etiquette surrounding these protocols. Such malicious manipulation is unfortunately easy and, for this reason, CR security has attracted considerable research attention recently. A reader can find comprehensive surveys of such threats in [4–7].

A curious reader might also ask: if opportunistic access to licensed spectrum by unknown users can be dangerous to the network, why not to restrict such access? The issue is that such access, as pointed out in the the National Broadband Plan [8] and in the President's Council of Advisors on Science and Technology (PCAST) report [9], represents an important economic growth engine in the United States. In particular, this report recommended the sharing of underutilized federal spectrum and identified 1000 MHz of spectrum as part of an ambitious endeavor to create "the first shared-use spectrum superhighways". Consequently, it is very important to develop a foundational understanding of the interference implications associated with spectrum access, and how spectrum bands can be assigned so as to mitigate intentional interference caused by malicious participants exploiting the information shared in a spectrum assignment.

In many scenarios involving spectrum sharing, the underlying spectrum resources (which might be spectral bands, or spectro-temporal slots) might originally be assigned to one entity (as in the case of TV white space spectrum), and it is the role of a spectrum server to support the sharing of spectrum with a second untrusted entity. The spectrum server, which might be administered by the government or a neutral third party, receives resource requests from both a primary/incumbent entity as well as the second entity, and aims to re-assign the spectrum so as to support an improved, combined benefit for both entities. Since the entities do not trust each other, the sharing of spectrum inherently becomes a competitive scenario that encounters numerous security risks as each system desires to use as much spectrum as possible to support its users, and each system could learn and cause harm (interference) to the bands assigned to the other system. Consequently, there are three main problems that arise in such a spectrum sharing problem: (1) how to maintain reliable performance for each system-shared resource (licensed spectrum); (2) whether to believe the resource requests announced by each agent; and (3) if they do not believe, how much effort should be devoted to inspecting spectrum so as to prevent possible malicious activity. In this paper, we present analysis that is focused on improving the security and assurability of the spectrum sharing problem by applying the notion of decoy tasks, i.e., obfuscating spectrum resource requests. Through our analysis, we show that it is possible to determine the expected damage that might result from a potential malicious activity, and arrive at an estimate for the probability of detecting the malicious activity by employing "spectrum inspection". Based on these probabilities, we then formulate a signaling game that allows one to determine whether to believe the second agent or not, and then how to engage in spectrum inspection. Since this type of problem can arise in many different scenarios involving spectrum sharing, such as the sharing of spectrum in cognitive radio networks or the sharing of unlicensed bands between two wireless carriers/technologies or the sharing between radar and communication systems [10–12], we formulate the problem abstractly as one involving two agents and a set of spectrum bands.

When considering dynamic spectrum sharing in a potentially adversarial setting, there is an underlying competitive problem to consider: multiple users compete for the spectrum resources and, regardless of whether they are malicious or not, there may not be any incentive for them to communally cooperate and remain within the bands that have been assigned to them. Game theory is an appropriate tool to analyze such competitive problems. In [13], the readers can find a comprehensive overview of game theoretical techniques for dynamic spectrum sharing problems, which maps out the problem of primary users sharing spectrum with well-intentioned secondary users, with a focus on the auctioning of spectrum. An excellent reference book involving game theory for wireless and communication networks is [14]. Our work differs from the problems outlined in both of these surveys as our problem involves a secondary user that has two objectives (a beneficial and an adversarial

intent), and thus our formulation will involve adversarial rewards involving the harm inflicted upon the primary user. Since our work explores the sharing of information between different organizations while facing attacks, one of the most relevant examples game-theoretical methods to model security problems is [15], where a Cournot-type model based on a contest success function was suggested to model investments into information security technologies where the firms share information resources. While information sharing can, on one hand, can increase economic benefits, on the other hand, it also creates new possibilities for adversaries aimed to perform security threats such as cyber attacks. While this work considers many motivating scenarios for two firms exchanging information, it is specifically focused on cyber security threats originating from an external, third agent and the impact that third agent can have upon the sharing of information between two firms. Our problem, on the other hand, considers one of the two participants having both a beneficial and harmful objective, and consequently its models do not extend directly to our communication problem where the secondary user can inflict wireless interference. In [16], a signaling game was proposed to model defense against attacks in honeypot-enabled networks. In this game, the attacker may try to deceive the defender by employing different types of attacks, ranging from suspicious to seemingly normal activity, while the defender in turn can make use of honeypots as a deception tool to trap the attacker. In our paper, a spectrum server announces decoys as a means to protect the primary user from interference attacks from a secondary user that may or may not choose to attack, but these decoys are not used as a means to dupe the adversary into attacking. In [17], a repeated spectrum-sharing game with cheat-proof strategies was investigated. By using a punishment-based repeated game, users are incentivized to share the spectrum in a cooperative way; and through mechanism-design-based and statistics-based approaches, user honesty is further enforced. Our work differs from this paper in that the objective of the secondary user is two-fold: both to acquire an appropriate amount of channels to support its users, and to increase its ability to launch an interference attack against the primary user. In this regard, our work includes interference as a reward metric for the secondary user system. In [18], the authors explore the problem of a coalition of users communicating in the presence of an adversary that may apply different types of jamming strategies, and whether it is possible to learn the adversary type. A game-theoretical approach is used to show that it is possible to learn the adversary's strategy in a finite number of steps. This work involves a general fading channel and power allocation formulation and does not involve a spectrum server allocating channels, and the objective of the communicating nodes is to identify the adversary's strategy. In [19], using a fictitious game for analyzing the defense of cognitive radio networks against an unknown jamming attacker was proposed, and the defense strategy employed is to switch channels in order to evade the jammer. Our work differs in that their adversary is separate from the secondary users (as opposed to being a secondary user), and the primary user is considered apart from the conflict. In particular, they do not consider aspects related to sharing between the primary and secondary user, nor that secondary users may have malicious intentions against the primary user. In [20] a game, where a *SU* shares time between law-obedient message transmission and noise-transmission to jam the *PU*, was suggested. This work is similar to our work in that it considers a secondary user that has both a benevolent and an interference objective. However, this work differs in two key aspects: first, the overall objectives are to maximize data rates; and, second, the secondary user employs jamming (noise forwarding) not to harm the primary user, but to nudge the primary user to adjust its power allocation to allow the secondary user to achieve a minimum data rate. Our work, however, explicitly considers that the secondary user has an adversarial intent underlying the use of interference. In [21], the resilience of LTE networks against smart jamming attacks was modeled, and represents an important example of where spectrum sharing is being proposed. A one-time spectrum coexistence problem in dynamic spectrum access when the secondary user may be malicious was investigated in our prior work in [22]. While that work is similar to the work presented here, an important difference in the current work is that the current work includes the introduction of additional functions that legitimate agents can use to defend themselves against the false announcements and interference introduced by the adversary. In particular, the current work goes beyond the interference tradeoffs explored in [22],

to include in the game the potential for each agent to believe/dis-believe the information being shared, and to give the primary user the ability to inspect the spectrum activities of a secondary user. Notably, in the current work, the costs associated with inspecting and the fine/penalty for the secondary user to be caught making a fraudulent resource request are integrated into the interference formulation, leading to the determination of the equilibria with respect to the amount of channels being shared and underlying costs for both sides associated with protecting and attacking spectrum sharing.

It must be recognized that the objective behind an adversaries strategy depends significantly on the objective of the adversary, and such knowledge can lead to better defenses. For example, the detection of the intruder with uncertainty about the application being used was investigated in [23]. Packet-dropping attacks were studied in [24]. As further examples of game theory being applied to security and communication problems, we briefly mention [25] as a reference involving modeling malicious users in collaborative networks , [26] as a reference in which entities share information while engaged in information warfare, [27] for modeling attack-type uncertainty in a network, [28] for security threats involving multiple users in ad hoc networks, and [29] for resource attacks in networks using the ALOHA protocol. How secret communication can be affected by the fact that an adversary's capability to eavesdrop on a collection of communications from a base station to a set of users may be restricted and unknown to the transmitter was investigated in [30]. Problems related to spectrum scanning have been presented in [31,32], where the objective is to develop spectrum-scanning strategies that support the detection of a user illicitly using spectrum, and [33] for detecting attacks aimed at reducing the size of spectrum opportunities in a dynamic spectrum-sharing problem. [34] studied the interactions between a user and a smart jammer regarding their respective choices of transmit power in a general wireless setting, while [35,36] considered problems related to game theory and network security, While these references are not directly relevant to the spectrum allocation problem explored in this paper, these references help motivate the work that we present in this paper.

The organization of this paper is as follows: in Section 2 and in two its subsections, we introduce the tradeoff that exists between supporting the *PU*'s communication's reliability and the cost of such reliability. We formulate this tradeoff as two-step game and obtain an explicit solution to the game. In Section 2, we formulate and solve a signaling game that examines a different trade-off problem, namely, whether it is too costly/risky to believe the spectrum request originating from the potentially malicious *SU* and, if not, then to engage in verification of the *SU* request. In Section 4, conclusions are presented.

2. Trade off between Communication Reliability and Its Cost

We begin by presenting a general, universal dynamic access problem through which many practical coordinated spectrum sharing cases may be examined. Our universal dynamic spectrum access problem is depicted in Figure 1. In this scenario, there are n spectrum resources, which we shall refer to as bands (e.g., these may be actual frequency bands, or time-frequency slots in the context of radio resource scheduling) that are available for usage by two different players, the primary user (PU) and the secondary user (SU). These n bands are administered by a spectrum owner *SO*, whose objective is two-fold: first, it aims to support the improved usage of the n bands collectively by both the PU and SU; and, second, it is responsible for supporting the reliable communication of the *PU* in the presence of a *SU*, who might be malicious. The *PU* wants to reliably communicate with a set of n_P users using n_P bands, where the *PU* uses a single band for each user. The *SU*, similarly, must support reliable communication with a set of n_T users using n_T bands, where $n_T + n_P < n$ and n is the total number of bands available for sharing. The *SU*, similarly, needs to only use a single band for each of its users.

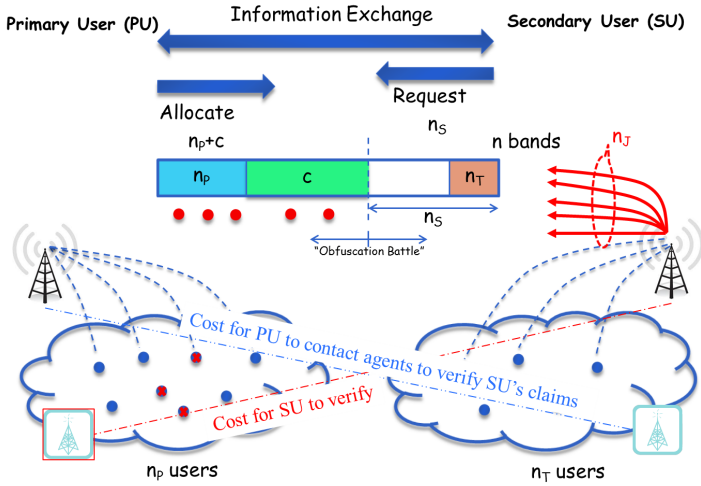

Figure 1. A universal spectrum access scenario that will be used to generically model the information obfuscation problem associated with spectrum sharing. Here, the coordination between a primary user (PU) and a secondary user (SU) is administered through a spectrum owner (SO) that acts as a spectrum server.

In the context of our problem, the SO may be thought of as a spectrum server that takes information related to each side's resource requests, and appropriately shares such information with other participants. The conduit of information being shared between the PU and the SO, and the SU and SO is an example of a spectrum underlay, and many practical approaches have been proposed for implementing such a spectrum coordination system. For example, in the context of coordinating between two different LTE providers aiming to share spectrum, the X2 interface is a peer-to-peer channel that supports inter-cell interference coordination (ICIC) in LTE, and one could propose extensions to X2 and ICIC standard that would support coordination between different LTE systems and a spectrum server. Alternatively, one could employ the operations, administration and management (OAM) interface that has been used as the basis for building a connection between self-organizing network controllers and eNB scheduling agent software to gain access to schedule and MAC layer functions. Similar approaches to cellular coordination have already been prototyped and validated using software-defined networking interfaces, such as that presented in [37]. The *SU* might be law-obedient (with probability q_0) and then he will use only the bands reserved for him, or he might be malicious (with probability $q_1 = 1 - q_0$) and, in this case he could try to harm the *PU*'s communication (e.g., by jamming). The *SO* has limited knowledge of the *SU*'s interference capabilities. To reflect this, the *SO* only knows that the *SU* can interfere with n_A signals. The *SO* has to reserve bands for use by the *PU* and the *SU*. The *SU* knows which bands are reserved for him and which are reserved for the *PU*. Without loss of generality we can assume that the *SO* reserves bands $[n - n_T + 1, n]$ for the *SU*'s communication. Thus, the *SO* has to reserve a set of bands for the *PU* within $[1, n - n_T]$ bands. The number of bands reserved for the *PU*'s usage should be larger than n_P in order to reduce the probability that the *SU* can interfere with the *PU*'s legitimate signals—in essence, the *PU*'s real allocation has been privacy-enhanced with the announcement of additional, decoy channels.

To reflect the fact that there might be a cost associated with introducing uncertainty in order to maintain communication reliability, we present a cost model that we will use in this paper for introducing uncertainty. We assume that when the *SO* reserves extra bands as decoys for the *PU* (beyond what it needs to support its users), such reservation costs C_U per band. The *SO* is thus faced with a dilemma: on one hand, more bands reserved for the *PU* increase communication reliability (it becomes harder for the *SU* to guess successfully interfere with actual communication signals). On the other hand, the costs associated with maintaining this higher level of communication reliability are increased. Thus, the *SO* has to make a tradeoff between the *PU* communication reliability and its

cost. We will formulate and solve this problem as a two-step game between the *SO* and the *SU* in the following two subsections.

2.1. First Step of the Game: To Make the Trade off between Communication's Reliability and Its Cost

In the first step of the game, to establish the tradeoff between communication reliability and the cost of obfuscation associated with increasing communication reliability, we assume the number of bands (decoys) c, reserved for increasing the domain of uncertainty, is fixed. Without loss of generality we can assume that bands $[1, n_P + c]$ are reserved for the *PU*, and the *SU* knows these bands. The *PU* has to support reliable communication with n_P users. The actual band assigned to each such user is fixed and known only to the *PU*. Without loss of generality we can assume that the bands for these n_P users are allocated within the bands $[1, n - n_T]$, and there is no way for the *SU* to ascertain whether an announced channel will be used or whether it will be a decoy channel. Further, we suppose that the *SU* is malicious and could try to interfere with the *PU*'s communication by using a jamming capacity of n_A signals, where each interference signal can reside in only a single band.

A (pure) strategy Y of the *SU* is a subset of n_A bands out of the set of $[1, n_P + c]$ bands reserved for the *PU*'s communication purposes, i.e., $|Y| = n_A$. Then, a (pure) strategy X of the *SO* is a subset of n_P bands from the bands $[1, n_P + c]$, i.e., $|X| = n_P$, which were assigned to the *PU* for transmitting communication signals. The payoff to the *SO* is the number of successfully transmitted (un-jammed)PU signals, i.e.,

$$v_{SO}(X, Y) = |X \backslash Y|, \tag{1}$$

namely bands that the *PU* employed that were not also selected by the SU. We look for a saddle point (an equilibrium strategy) [38], i.e., for a pair of strategies (X_*, Y_*) such that,

$$v_{SO}(X, Y_*) \leq v_{SO}(X_*, Y_*) \leq v_{SO}(X_*, Y), \tag{2}$$

where $v = v_{SO}(X_*, Y_*)$ is the value of the game.

Since $n_T + n_A < n$, for each *SU* strategy Y_* there is an *SO* strategy X such that $X \cap Y_*$ is the empty set. Thus, by (1) and (2), the value of the game is greater or equal to n_P. On the other hand, for each *SO* strategy X_* there is an *SU* strategy Y such that $X_* \cap Y$ is not empty. Thus, by (1) and (2), the value of the game is smaller than n_P. This implies that the game does not have an equilibrium involving pure equilibrium strategies, i.e., where specific sets are chosen. To solve for an equilibrium, we have to employ mixed strategies, which involves randomizing the selection of pure strategies. The following proposition gives the value of the game and equilibrium strategies.

Proposition 1. *The value of the first step of the considered game is,*

$$T^{n_P+c}_{n_P,n_A} = n_P \left(1 - \frac{n_A}{n_P + c}\right), \tag{3}$$

and a saddle point is $(X_{n_P,[1,n_T+c]}, Y_{n_A,[1,n_P+c]})$*, where,*

(1) $X_{n_P,[1,n_P+c]}$ *is a (mixed) strategy of the SO in which the SO chooses to assign to the PU* n_P *bands at random with equal probability from the total set of* $[1, n_P + c]$ *bands reserved for the PU's communication. There are* $\binom{n_P+c}{n_P}$ *subsets of* $n_P + c$ *bands consisting of* n_P *bands. Thus, the strategy* $X_{n_P,[1,n_P+c]}$ *chooses each such subset with probability* $1/\binom{n_P+c}{n_P}$*.* $(\binom{n}{p} = \frac{n!}{(n-p)!p!}$ *is the number of combinations of p objects selected out of n objects.)*

(2) $Y_{n_A,[1,n_P+c]}$ *is a (mixed) strategy of the SU that involves choosing at random* n_A *bands with equal probability from the full set of* $[1, n_P + c]$ *bands. There are* $\binom{n_P+c}{n_A}$ *subsets of* $n_P + c$ *bands consisting of* n_A *bands. Thus, the strategy* $Y_{n_A,[1,n_P+c]}$ *chooses each such subset with probability* $1/\binom{n_P+c}{n_A}$*.*

Also, we note that $X_{n_P,[1,n_P+c]}$ and $Y_{n_A,[1,n_P+c]}$ are equalizing strategies, i.e., for any SU's pure strategy Y and SO's pure strategy X the following equalities hold:

$$v_{SO}(X_{n_P,[1,n_P+c]}, Y) = v_{SO}(X, Y_{n_A,[1,n_P+c]}) = T^{n_P+c}_{n_P,n_A}. \tag{4}$$

The expected number of successfully interfered bands is,

$$H^{n_P+c}_{n_P,n_A} = \frac{n_A n_P}{n_P + c}.$$

Proof. Let the *SO* apply a mixed strategy $X_{n_P,[1,m]}$, where $m = n_P + c$ and the *SU* applies a (pure) strategy Y that involves assigning n_A fixed bands for the purpose of interfering with the *PU*. Then, the expected number of successfully transmitted signals is,

$$v_{SO}(X_{n_P,[1,m]}, Y) = \frac{\sum_{i=0}^{n_{PA}} (n_P - i) \binom{n_A}{i} \binom{m - n_A}{n_P - i}}{\binom{m}{n_P}}, \tag{5}$$

where $n_{PA} := \min\{n_P, n_A\}$.

Now, look at the *SU*. Let the *SO* apply a (pure) strategy X, i.e., a set of n_P bands for the *PU*'s transmission is fixed, and the *SU* apply a mixed strategy $Y_{n_S,[1,m]}$. Then, the expected number of successfully transmitted signals is,

$$v_{SO}(X, Y_{n_A,[1,m]}) = \frac{\sum_{i=0}^{n_{PA}} (n_P - i) \binom{n_P}{i} \binom{m - n_P}{n_A - i}}{\binom{m}{n_A}}. \tag{6}$$

Since,

$$\frac{\binom{n_A}{i} \binom{m - n_A}{n_P - i}}{\binom{m}{n_P}} = \frac{\binom{n_P}{i} \binom{m - n_P}{n_A - i}}{\binom{m}{n_A}}, \tag{7}$$

then,

$$v_{SO}(X_{n_P,[1,m]}, Y) = v_{SO}(X, Y_{n_A,[1,m]}) = T^{m}_{n_P,n_A}.$$

Now we prove (3) by induction by m. Let $n_A \leq n_P$. For $m = n_A$ the result is obvious. Let it hold for a $m \geq n_A$. We prove that then it also holds for $m + 1$. Since $\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1}$ for any k we have that,

$$\begin{aligned}
\sum_{i=0}^{n_A} (n_P - i) \binom{n_P}{i} \binom{m + 1 - n_P}{n_A - i} &= \sum_{i=0}^{n_A} (n_P - i) \binom{n_P}{i} \binom{m - n_P}{n_A - i} + \sum_{i=0}^{n_A - 1} (n_P - i) \binom{n_P}{i} \binom{m - n_P}{n_A - 1 - i} \\
&= (\text{ by induction's assumption}) \\
&= n_P \left(1 - \frac{n_A}{m}\right) \binom{m}{n_A} + n_P \left(1 - \frac{n_A - 1}{m}\right) \binom{m}{n_A - 1} \\
&= n_P \left(1 - \frac{n_A}{m + 1}\right) \binom{m + 1}{n_A},
\end{aligned}$$

and (3) follows. The case $n_A > n_P$ can be considered similarly. □

2.2. Second Step of the Game: To Make the Tradeoff between Communication's Reliability and Its Cost

In the second step of the game, to make the tradeoff between communication reliability and the cost of such reliability, the *SO*, knowing the equilibrium strategy for the first step, wants to

appropriately choose an appropriate amount of obfuscation, c, so as to specify the domain of uncertainty with the objective of maximizing the difference between reliable *PU* communication (i.e., unjammed communication signals) and the cost to maintain this reliability. Thus, by Proposition 1, the expected payoff to the *SO* is given as follows:

$$\begin{aligned} v_U(c) &= q_0(n_P - C_U c) + q_1\left(T_{n_P,n_S}^{n_P+c} - C_U c\right) \\ &= q_0(n_P - C_U c) + q_1\left(n_P\left(1 - \frac{n_A}{n_P + c}\right) - C_U c\right). \end{aligned}$$

The goal of the *SO* is to maximize his payoff $v_U(c)$, i.e., to find such c that,

$$c = \arg \max_{c \in \{0,\ldots,n-n_P-n_T\}} v_U(c).$$

Proposition 2. *In the second step of the game, to achieve the optimal trade-off between communication reliability and the cost of this reliability, the SO has to announce $n_P + c$ bands that are reserved for the PU's usage, where,*

$$c = \begin{cases} 0, & \frac{n_A}{n_P} < \frac{C_U}{q_1}, \\ A_-, & \frac{n_A n_P}{(n-n_T)^2} < \frac{C_U}{q_1} < \frac{n_A}{n_P}, v_U(A_-) > v_U(A_+) \\ A_+, & \frac{n_A n_P}{(n-n_T)^2} < \frac{C_U}{q_1} < \frac{n_A}{n_P}, v_U(A_-) < v_U(A_+) \\ n - n_T - n_P, & \frac{C_U}{q_1} < \frac{n_A n_P}{(n-n_T)^2} \end{cases}$$

with ($\lfloor \xi \rfloor$ and $\lceil \xi \rceil$ being the floor and ceiling functions mapping a real number to the largest previous to ξ or the smallest integer following ξ, respectively.)

$$A_- = \left\lfloor \sqrt{\frac{q_1 n_P n_A}{C_U}} - n_P \right\rfloor \text{ and } A_+ = \left\lceil \sqrt{\frac{q_1 n_P n_A}{C_U}} - n_P \right\rceil.$$

Proof. Note that,

$$\frac{dv_U(c)}{dc} = \frac{q_1 n_P n_A}{(n_P + c)^2} - C_U$$

and,

$$\frac{d^2 v_U(c)}{dc^2} = -\frac{2 q_1 n_P n_A}{(n_P + c)^3} < 0.$$

Thus, v_U is strictly a concave function, and it has a unique maximum in $[0, n - n_P - n_T]$ which is given as follows:

$$c = \begin{cases} 0, & \frac{q_1 n_A}{n_P} \leq C_U, \\ \sqrt{\frac{q_1 n_P n_A}{C_U}} - n_P, & \frac{q_1 n_A n_P}{(n-n_T)^2} < C_U < \frac{q_1 n_A}{n_P}, \\ n - n_P - n_T, & \frac{q_1 n_A n_P}{(n-n_T)^2} \geq C_U. \end{cases}$$

Since we have to maximize v_U only within integer points of the interval $[0, n - n_P - n_T]$, the result follows. □

Figure 2a illustrates how the number of bands reserved by the *SO* depends on the cost of uncertainty C_U and the number of user communications the *PU* has to maintain n_P, where the scenario and adversarial profile was set to $n_A = 30$, $n_T = 60$, $q_1 = 0.5$ and $n = 200$. Figure 2b,c illustrates how the number of extra reserved bands and the payoff to the *SO* depends on the cost for introducing uncertainty, C_U, and the probability q_1 that the *SU* is malicious when $n_P = 50$. This figure shows that in some cases there is a tradeoff between the cost of uncertainty and the probability of the threat, in which case it is possible to increase communication reliability.

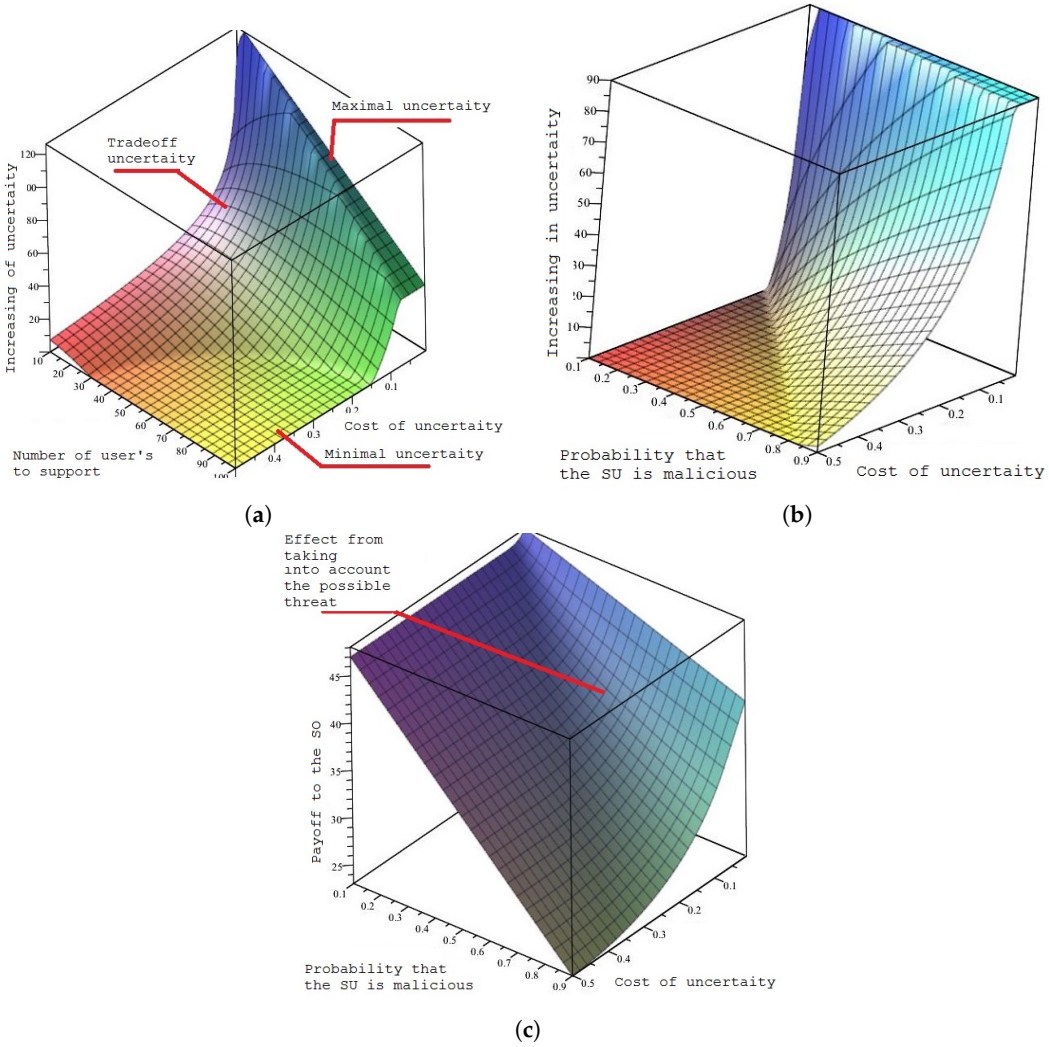

Figure 2. (**a**) Number of extra bands reserved for the *PU* as a function of the cost of uncertainty C_U and number of users the *PU* has to maintain (i.e., n_P); (**b**) number of extra reserved bands for the *PU*; and (**c**) the payoff to the *SO* as a function of the cost of uncertainty and the probability q_1 that the *SU* is malicious.

Finally, we note that, in this section, in Proposition 1, the basic formula for the expected number of jammed signals was derived in closed form. This allows one to find the tradeoff between communication reliability and the cost of such reliability if the SU might be malicious, which is maintained by means of introducing obfuscation. In the next section, we apply this formula to evaluate: (1) whether to believe in the announced purpose or size of the SU's requests for spectrum resources; and (2) if one does not believe the SU, the intensity with which one should employ inspection of his spectrum activity so as to prevent possible malicious activity.

3. Signaling Game: Whether It is Worth Believing the Potentially-Malicious *SU* or Not to Believe and Then Inspect His Request

The malicious *SU* requests bands that he will supposedly use for legitimate purposes, but in doing so faces a dilemma. On the one hand, by requesting more bands under the pretext of legitimate use, the *SU* will actually support his malicious activity by reducing the amount of bands available to the *SO* to use to obfuscate the *PU*'s actual channel need (and thus increase the likelihood that the *SU* will be able to interfere with the *PU*). On the other hand, requesting too many extra bands can make

the *SO* suspicious of the request, which might then lead to the *SO inspecting* the request by actively engaging additional resources (at a cost) to verify the truth of the request.

We now examine the scenario from the *SO* perspective. Since the *SO* is not sure about whether the *SU* is malicious, upon observing the *SU* request, the *SO* also faces a dilemma: either to believe or not believe the request. Not believing the request will then lead to the *SO* inspecting the veracity of the request to check whether the *SU* is trying to deceive. This can reduce the likelihood of possible *SU* malicious activity if the inspection detects the deception, but it also introduces an extra expense for the *SO*. In this section we formulate this problem as a *signaling game* [38], and then, to obtain insight into the problem, we give an explicit solution for a basic subcase in the next subsection.

Signaling games deal with the situation where one player knows some information that the other player does not. The first player (the sender), who possesses some private information, might try to manipulate the situation by sharing some altered version of that information to his rival. The first player may be motivated to deceive his rival, for example, in order to gain a higher payoff from the game. The second player (the receiver), who does not possess this private information, has to make a decision based on the information shared by the sender and, in particular, must decide how to take any actions given the potential that the information exchanged was false. We note that signaling games are widely employed for modeling different aspects of malicious activity in networks, for example, in multi-step attack-defense scenarios [39], for intrusion detection in wireless sensor networks [40], for cyber security [41], for intrusion detection in mobile ad hoc networks [42], for investigation of deception in network security [43], for honeypot selection in computer networks [44], for studying the impact of uncertain cooperation among well-behaved and socially selfish nodes on the performance of data forwarding [45], and for achieving an always best connected service in vehicular networks [46].

In the model we now consider, we assume that there is no cost associated with introducing uncertainty, i.e., $C_U = 0$, and in this case the *SO* will allocate the maximal domain of uncertainty based on the *SU*'s request, i.e., the *PU* bands will be $[1, n - n_T]$. We assume that $n_T \in \{1, \ldots, N_T\}$, where N_T corresponds to an upper bound on the possible bands the *SU* could request for legitimate purposes. We assume that the *SO* has knowledge of N_T, and that he has statistical knowledge characterizing the *SU*'s needs and behavior. Specifically, he knows that, with probability q_{0i}, the *SU* is law-obedient and $n_T = i$, and with probability q_{1i} the *SU* is malicious and $n_T = i$, where $i = 1, \ldots, N_T$.

The *SU* knows its own true n_T, and, having knowledge of n_T, can submit a reservation for either n_T or $n_T + 1, \ldots$, up to N_T bands if he is malicious. If the *SU* is law-obedient, he requests the correct number of bands. As noted earlier, requesting more bands is better for a malicious *SU*'s jamming objective, but the *SO* can choose to inspect the bands to see whether that band is actually in use (or historically has been in use). If the *SO* finds that some bands are not in use, then the *SU* is fined C_S per falsely-claimed, unused band. Meanwhile, however, we assume that there is an inspection cost C_P per band that is inspected by the *SO*. The payoff to the *SU* is the expected number of interfered users, weighted by R times the number of successful transmission minus the expected fine. The payoff for the *SO* is the expected number of successful transmissions by the *PU* minus inspection expenses. This situation is well-modeled by a *signaling game*, where the *SU* is the *sender*. The *SU* can be one of $2N_T$ types: type-$(1, i)$ which occurs with probability q_{1i} and occurs when the *SU* is malicious and must support $n_T = i$ users; or type-$(0, i)$ which occurs with probability q_{0i} and occurs when the *SU* is law-obedient and must support $n_T = i$ users, where $i = 1, \ldots, N_T$. Let b be the requested number of bands by the *SU*. The malicious *SU*, knowing its n_T, submits a reservation for at least n_T bands, and at most N_T bands. Of course, for $n_T = N_T$, (so, the *SU* has type-$(1, N_T)$), the only strategy he can apply is to request for N_T bands, but for $n_T < N_T$, he has $N_T - n_T + 1$ strategies, and thus he may request for either $b = n_T$ or $b = n_T + 1, \ldots$ or N_T bands to be reserved. The law-obedient *SU*, submits a reservation without deception, so type-$(0, i)$ *SU* has the only strategy to request $b = i$ bands, $i = 1, \ldots, N_T$.

Denote by $A_{SU}(t,\tau)$, the set of (pure) *SU*'s strategies of type-(t,τ). Thus,

$$A_{SU}(t,\tau) = \begin{cases} \{\tau\}, & t = 0, \\ \{\tau, \ldots, N_T\}, & t = 1. \end{cases}$$

The *SO* observes the request for b bands and must decide either to believe the *SU*, and thus supplies him with b reserved bands (denote it as a strategy B, for "believe"), or not to believe and thereby inspect the bands (denote it as a strategy I, for "inspect"). Thus, the set of (pure) strategies for the *SO* is $A_{SO}(b) = \{B, I\}$ for $b > 2$ and $A_{SO}(b) = \{B\}$ for $b = 1$.

We note that we implicitly assume that the inspection does not turn the malicious *SU* into a non-malicious *SU*. Rather, we assume that it might reduce the likelihood of his malicious activity being successful, and also reduces his payoff due to there being a fine for unused bands.

Of course, the result of the inspection depends on how the inspection protocol is being performed and the technical characteristics of the tools being employed (e.g., detection sensitivities, etc.). As a basic example of an inspection protocol we consider the following simple protocol where the *SO* starts by inspecting only one randomly chosen band out of the n_T requested bands. Let α_{k,n_T} be the detection probability of an unused band when there are k unused bands among n_T requested bands. It is clear that $\alpha_{k,n_T} = k/n_T$ in the case of perfect detection for inspection of an unused band. If an unused band is detected (and hence a false request is being made) then the total inspection of the remaining full set of requested band $n_T - 1$ is performed. Let C_P be the cost per an inspected band. Thus,

(1) If the *SU* is of type-$(0,1)$, he has only the strategy of requesting one band and the *SO* also has only the strategy of believing the request. Then, by Proposition 1, the payoff to the *SO* is $T^{n-1}_{n_P,0}$ and the payoff to the *SU* is R.

(2) If the *SU* is of type-$(0,i)$, $i \in \{2, \ldots, N_T\}$, he has one strategy for requesting i bands, while the *SO* has two strategies for each request of i bands (to believe or to inspect):

- if the *SO* believes, then the payoff to the *SO* is $T^{n-i}_{n_P,0}$ and the payoff to the *SU* is Ri,
- if the *SO* inspects, then the payoff to the *SO* is $T^{n-i}_{n_P,0} - C_P$ and the payoff to *SU* is Ri.

(3) If the *SU* is of type-$(1,i)$, $i \in \{1, \ldots, N_T\}$, he has $N_T - i + 1$ strategies to request:

- if $i = 1$ and the *SU* requests one band, the *SO* also has only the strategy to believe the request. Then the payoff to the *SO* is $T^{n-1}_{n_P,n_A}$ and the payoff to the *SU* is $R + H^{n-1}_{n_P,n_A}$;
- if either $i = 1$ and the *SU* requests $b > 1$ bands, or $i > 1$, then the *SO* has two strategies (to believe or to inspect):
  - if the *SU* believes then the payoff to the *SO* is $T^{n-b}_{n_P,n_A}$ and the payoff to the *SU* is $Ri + H^{n-b}_{n_P,n_A}$,
  - if the *SU* inspects then the payoff to the *SO* is equal to,

$$\alpha_{b-i,b} T^{n-i}_{n_P,n_A} + \bar{\alpha}_{b-i,b} T^{n-b}_{n_P,n_A} - C_P - C_P(b-1)\alpha_{b-i,b}$$

and the payoff to the *SU* is equal to,

$$Ri + \alpha_{b-i,b} H^{n-i}_{n_P,n_A} + \bar{\alpha}_{b-i,i} H^{n-b}_{n_P,n_A} - \alpha_{b-i,b} C_S(b-i).$$

Denote the payoff to the *SU* and the *SO* by $v_{SU}(t,\tau;b,a)$ and $v_{SO}(t,\tau;b,a)$ if circumstances are such that the *SU* is of type-(t,τ), the *SU* has chosen $b \in A_{SU}(t,\tau)$ bands (messages) to request for its own reservation, while the *PU* has selected strategy $a \in A_{SO}(b)$.

We look for a perfect Bayesian equilibrium (PBE) in this signaling game [38]. A PBE is a pair $(b^*(t,\tau), a^*(b))$ of strategies such that:

(1) For each type-$(1,\tau)$, the malicious *SU*'s request (message) $b^*(1,\tau)$ has to maximize the *SU*'s payoff, i.e.,

$$b^*(1,\tau) = \arg \max_{b \in A_{SU}(1,\tau)} u_{SU}(1,\tau; b, a^*(b)).$$

(2) For each message b, the *SO*'s strategy $a^*(b)$ has to maximize the expected *SO*'s payoff, given his posterior beliefs $\mu(\cdot|b)$ about which type could have sent the request (message) b, i.e.,

$$a^*(b) = \arg \max_{a \in A_{SO}(b)} \sum_{t=0,1,\tau=1,\ldots,N_T} \mu(t,\tau|b) u_{SO}(t,\tau; b, a).$$

with the posterior *SO* beliefs $\mu(\cdot|b)$ given by Bayes's rule,

$$\mu(t,\tau|b) = \frac{q_{t\tau}\text{Prob}(b(t,\tau) = b)}{\sum_{t',\tau'} q_{t'\tau'}\text{Prob}(b(t',\tau') = b)}$$

for,

$$\sum_{t',\tau'} q_{t'\tau'}\text{Prob}(b(t',\tau') = b) > 0.$$

This is a signaling game with a finite sets of (pure) strategies, and generally to solve it randomized strategies have to be employed. To deal numerically with such problem an iterative forward induction algorithm for solving signaling games based on a rationalizability approach suggested in [47] can be used. An alternative approach is to use the Gambit software package [48] for solving signaling games. To obtain insight into the problem and to see how the solution explicitly depends the parameters associated with the scenario, in the next section, we directly find the solution for a particular baseline case.

Explicit Solution for a Basic Case, $N_T = 2$

In this section to get insight of the problem we present explicit solution for a particular case $N_T = 2$. Let $\alpha = \alpha_{1,2}$ be the detection probability of an unused band when there is one unused band among two requested bands. Note that, since $N_T = 2$, if an unused band is detected (and hence a false request is being made) then there is no need to engage the full set of bands in an inspection. In Figure 3, the diagram for making decisions in this signaling game is presented.

To describe the main result, let us introduce the following notations:

- Let $\boldsymbol{b} = \boldsymbol{b}(\tau, b)$ be the probability that the malicious *SU* of type-$(1,\tau)$ requests b bands.
- Let $\boldsymbol{a}(i,\xi)$ be the conditional probability that the *SO* employs strategy ξ when observing a request for i bands.

Thus, $\boldsymbol{b}$ and $\boldsymbol{a}$ can be interpreted as randomized behaviour strategies for the malicious *SU* and for the *SO*.

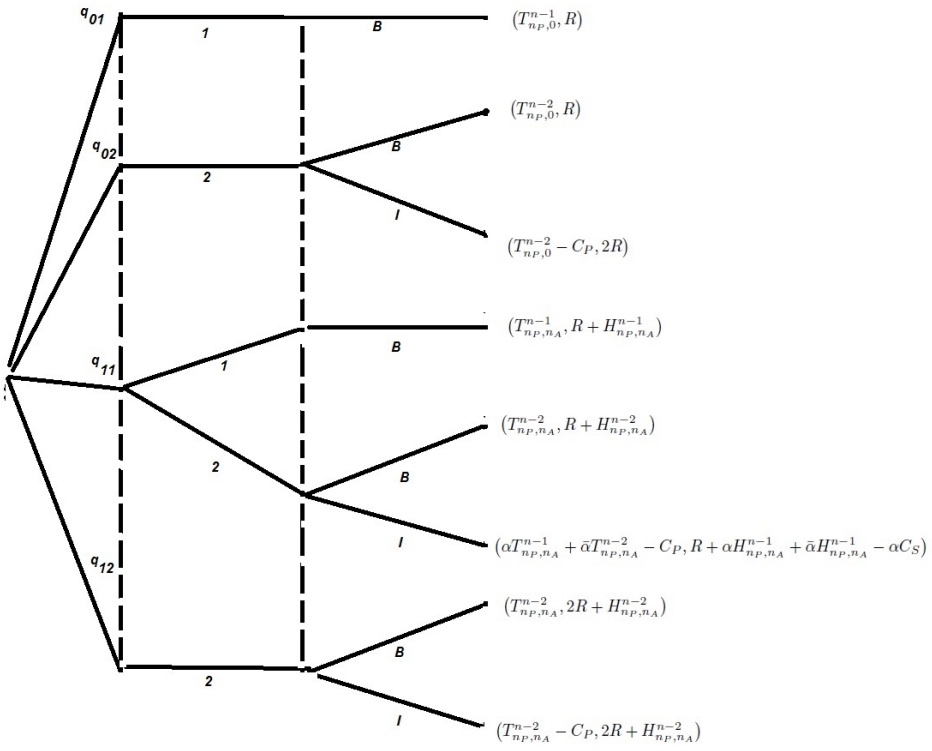

Figure 3. Diagram for how decisions are made.

Proposition 3. *(a) If the cost associated with inspecting a band is high,*

$$C_P \geq \frac{q_{11}\alpha(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A})}{q_{02} + q_{12} + q_{11}},$$

then the equilibrium strategy for the SO is to always believe (i.e., strategy B), while the equilibrium strategy for the SU is always to request two bands.

(b) If the inspection cost is small,

$$C_P < \frac{q_{11}\alpha(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A})}{q_{02} + q_{12} + q_{11}},$$

then two subcases arise:

(b_1) if the fine is small,

$$C_S < (H^{n-2}_{n_P,n_A} - H^{n-1}_{n_P,n_A})(1-\alpha)/\alpha,$$

then, the equilibrium strategy for the SU is always to request two bands, and the SO always should inspect;

(b_2) if the fine is large,

$$C_S > (H^{n-2}_{n_P,n_A} - H^{n-1}_{n_P,n_A})(1-\alpha)/\alpha,$$

then in equilibrium both rivals apply mixed strategies, namely:

$$
\begin{aligned}
\boldsymbol{b}(1,1) &= \frac{\alpha q_{11}(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A}) - C_P(q_{02}+q_{12}+q_{11})}{q_{11}\left(\alpha(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A}) - C_P\right)},\\
\boldsymbol{b}(1,2) &= \frac{C_P(q_{02}+q_{12})}{q_{11}\left(\alpha(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A}) - C_P\right)},\\
\boldsymbol{b}(2,1) &= 0,\\
\boldsymbol{b}(2,2) &= 1,\\
\boldsymbol{a}(1,B) &= 1,\\
\boldsymbol{a}(1,I) &= 0,\\
\boldsymbol{a}(2,B) &= \frac{\alpha C_S - (1-\alpha)(H^{n-2}_{n_P,n_A} - H^{n-1}_{n_P,n_A})}{\alpha(C_S + H^{n-2}_{n_P,n_A} - H^{n-1}_{n_P,n_A})},\\
\boldsymbol{a}(2,I) &= \frac{H^{n-2}_{n_P,n_A} - H^{n-1}_{n_P,n_A}}{\alpha(C_S + H^{n-2}_{n_P,n_A} - H^{n-1}_{n_P,n_A})}.
\end{aligned}
$$

Proof. Since $\boldsymbol{b} = \boldsymbol{b}(\tau, b)$ is the probability that the malicious *SU* of type-$(1,\tau)$ requests b bands, it is clear that $\boldsymbol{b}(2,2) = 1$ and $\boldsymbol{b}(1,1) + \boldsymbol{b}(1,2) = 1$. Thus, the *SU*'s strategy $\boldsymbol{b}$ can be uniquely defined by using only one of its components $\boldsymbol{b}(1,2)$.

Then, by the definition of $\boldsymbol{b}$, the marginal probability γ_i of observing a request for i bands is given as follows:

$$
\begin{aligned}
\gamma_1 &= \boldsymbol{b}(1,1)q_{11} + q_{01} = q_{01} + q_{11}(1 - \boldsymbol{b}(1,2)),\\
\gamma_2 &= \boldsymbol{b}(1,2)q_{11} + \boldsymbol{b}(2,2)q_{12} + q_{02} = q_{02} + q_{12} + q_{11}\boldsymbol{b}(1,2).
\end{aligned}
$$

The *SO* can build his belief about the *SU* based on the *SU*'s request by considering the conditional probability $\mu(t,\tau|j)$ that the *SU* of type-(t,τ) requests j bands, as follows:

$$
\begin{aligned}
\mu(0,1|1) &= \frac{q_{01}}{q_{01} + q_{11}(1 - \boldsymbol{b}(1,2))},\\
\mu(0,2|1) &= 0,\\
\mu(1,1|1) &= \frac{q_{11}(1 - \boldsymbol{b}(1,2))}{q_{01} + q_{11}(1 - \boldsymbol{b}(1,2))},\\
\mu(1,2|1) &= 0,\\
\mu(0,1|2) &= 0,\\
\mu(0,2|2) &= \frac{q_{02}}{q_{02} + q_{12} + q_{11}\boldsymbol{b}(1,2)},\\
\mu(1,1|2) &= \frac{q_{12}}{q_{02} + q_{12} + q_{11}\boldsymbol{b}(1,2)},\\
\mu(1,2|2) &= \frac{q_{11}\boldsymbol{b}(1,2)}{q_{02} + q_{12} + q_{11}\boldsymbol{b}(1,2)}.
\end{aligned}
\tag{8}
$$

Let $E^b u_{SO}(\xi, \boldsymbol{b})$ be the expected payoff for the *SO* when the *SU* applies strategy $\boldsymbol{b}$ and the *SO* employs strategy ξ and observes a request for b bands. Then,

$$\begin{aligned} E^1 u_{SO}(B, \boldsymbol{b}) &= T^{n-1}_{n_P,0}\mu(0,1|1) + T^{n-1}_{n_P,n_A}\mu(1,1|1), \\ E^2 u_{SO}(B, \boldsymbol{b}) &= T^{n-2}_{n_P,0}\mu(0,2|2) + T^{n-2}_{n_P,n_A}\mu(1,1|2) + T^{n-2}_{n_P,n_A}\mu(1,2|2), \\ E^2 u_{SO}(I, \boldsymbol{b}) &= (T^{n-2}_{n_P,0} - C_P)\mu(0,2|2) + (\alpha T^{n-1}_{n_P,n_A} + \bar{\alpha} T^{n-2}_{n_P,n_A} - C_P)\mu(1,1|2) \\ &\quad + (T^{n-2}_{n_P,n_A} - C_P)\mu(1,2|2). \end{aligned} \tag{9}$$

For a fixed *SU* strategy, the best response *SO* strategy is $\mathrm{BR}^b_{SO}(\boldsymbol{b}) = \arg_{\xi} \max E^b u_{SO}(\xi, \boldsymbol{b})$. By (8) and (9), we have that,

$$\mathrm{BR}^1_{SO}(\boldsymbol{b}) = B, \tag{10}$$

$$\mathrm{BR}^2_{SO}(\boldsymbol{b}) \begin{cases} = B, & C_P > \Xi, \\ \in \{B, I\}, & C_P = \Xi, \\ = I, & C_P < \Xi, \end{cases} \tag{11}$$

with,

$$\Xi = \alpha(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A})\mu(1,1|2) = (\text{by } (8)) = \frac{q_{11}\boldsymbol{b}(1,2)\alpha(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A})}{q_{02} + q_{12} + q_{11}\boldsymbol{b}(1,2)}.$$

Note that, for

$$C_P \geq \frac{q_{11}\alpha(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A})}{q_{02} + q_{12} + q_{11}}, \tag{12}$$

the following inequality holds for any $\boldsymbol{b}(1,2) \in [0,1]$:

$$C_P > \Xi. \tag{13}$$

Thus, if (12) holds, then $\mathrm{BR}^2_{SO}(\boldsymbol{b}) = B$. Since (10) also holds, (12) implies that the *SO* equilibrium strategy is to believe independent on the *SU*'s request. Then, the *SU* equilibrium strategy is always to request two bands.

Let us now suppose that (12) does not hold. Thus,

$$C_P < \frac{q_{11}\alpha(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A})}{q_{02} + q_{12} + q_{11}}. \tag{14}$$

Note that,

$$\boldsymbol{b}(1,2) = \frac{C_P(q_{02} + q_{12})}{q_{11}\left(\alpha(T^{n-1}_{n_P,n_A} - T^{n-2}_{n_P,n_A}) - C_P\right)} \tag{15}$$

is the unique root by $\boldsymbol{b}(1,2)$ of the equation,

$$C_P = \Xi.$$

Then, (14) implies that $\boldsymbol{b}(1,2)$ given by (15) is within $(0,1)$. Thus, by (11), if (14) holds, then (15) defines a *SU* strategy that is indifferent to the beliefs of the *SO* and his best response, and thus it is another possible candidate for the *SU* equilibrium strategy.

Since $\boldsymbol{a}(i,\xi)$ is the conditional probability that the *SO* employs strategy ξ when observing a request for i bands, it is clear that $\boldsymbol{a}(1,B) = 1$, $\boldsymbol{a}(1,I) = 0$ and $\boldsymbol{a}(2,B) + \boldsymbol{a}(2,I) = 1$. Then $\boldsymbol{a}$ is uniquely defined by its one component $\boldsymbol{a}(2,B)$.

If $\boldsymbol{a}$ is such that the payoff to the *SU* of type-(1,1) is insensitive to all of his requests, then $\boldsymbol{a}$ is the equilibrium. This condition is met when the expected values at the end of branches in the decision tree (Figure 3) are equal, i.e.,

$$\begin{aligned}\left(R + H^{n-2}_{n_P,n_A}\right)\boldsymbol{a}(2,B) + \left(R + \alpha H^{n-1}_{n_P,n_A} + \bar{\alpha} H^{n-2}_{n_P,n_A} - \alpha C_S\right)\boldsymbol{a}(2,I) \\ = (R + H^{n-1}_{n_P,n_A})\boldsymbol{a}(1,B) = R + H^{n-1}_{n_P,n_A}.\end{aligned} \tag{16}$$

Solving the last equation by $\boldsymbol{a}(2,B)$ yields:

$$\boldsymbol{a}(2,B) = \frac{\alpha C_S + \bar{\alpha}(H^{n-1}_{n_P,n_A} - H^{n-2}_{n_P,n_A})}{(C_S - H^{n-1}_{n_P,n_A} + H^{n-2}_{n_P,n_A})\alpha}.$$

Thus, if $C_S \geq (H^{n-2}_{n_P,n_A} - H^{n-1}_{n_P,n_A})(1-\alpha)/\alpha$ then $\boldsymbol{a}(2,B) \in [0,1]$. Then, this $\boldsymbol{a}$ jointly with $\boldsymbol{b}$ given by (15) give an equilibrium.

If $C_S > (H^{n-2}_{n_P,n_A} - H^{n-1}_{n_P,n_A})(1-\alpha)/\alpha$ then, instead of equality (16), the following inequality holds for any $\boldsymbol{a}$:

$$\left(R + H^{n-2}_{n_P,n_A}\right)\boldsymbol{a}(2,B) + \left(R + \alpha H^{n-1}_{n_P,n_A} + \bar{\alpha} H^{n-2}_{n_P,n_A} - \alpha C_S\right)\boldsymbol{a}(2,I) > R + H^{n-1}_{n_P,n_A}.$$

The left side of this inequality obtains its minimum for $\boldsymbol{a}(2,B) = 0$ and $\boldsymbol{a}(2,I) = 1$. Also, by (14) and (11), the best response to $\boldsymbol{b}(1,2) = 1$ is to inspect. Thus, in this situation, requesting two bands and inspecting the request combine to give the equilibrium, and this implies the result. □

Thus, we have shown in Proposition 3 that the game has either a pooling or a mixed equilibrium. The pooling equilibrium assumes that all the malicious *SU* types request the same number of bands. In our particular case this corresponds to two bands. In the pooling equilibrium the *SO* learns nothing from the *SU*'s request.

Figure 4 illustrates threshold lines for switching between the equilibrium strategies as a function of the number of bands with $\alpha = 0.5$.

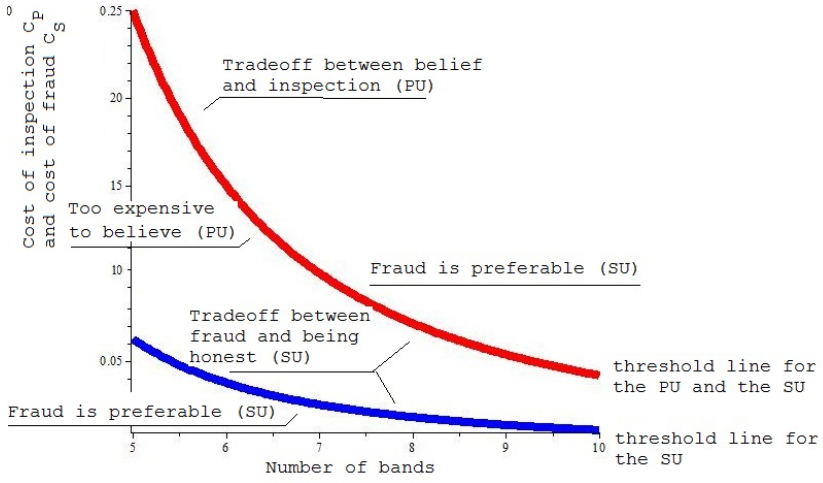

Figure 4. Threshold lines for switching between the equilibrium strategies as a function of the number of bands.

Figure 5a,b illustrates the probability of believing in the request for two bands $\boldsymbol{a}(2,B)$ and the probability for requesting two bands, if only one legitimate communication has to be supported, i.e., $\boldsymbol{b}(1,2)$, as functions of the number of bands n and the probability that the malicious *SU* is of type-$(1,1)$ with scenario parameters: $C_P = 0.005$, $C_S = 0.7$, $n_A = 10$, $n_P = 30$, $\alpha = 0.5$, $q_{01} = 0.1$, $q_{02} = 0.3$ and

$q_{11} + q_{12} = 0.6$. Figure 5c illustrates how taking into account information about the nature of the *SU* can improve the *SO*'s payoff. Also, it is very interesting to note that the optimal strategy for the *SO*, as well as its payoff, are discontinuous in the information describing the *SU*.

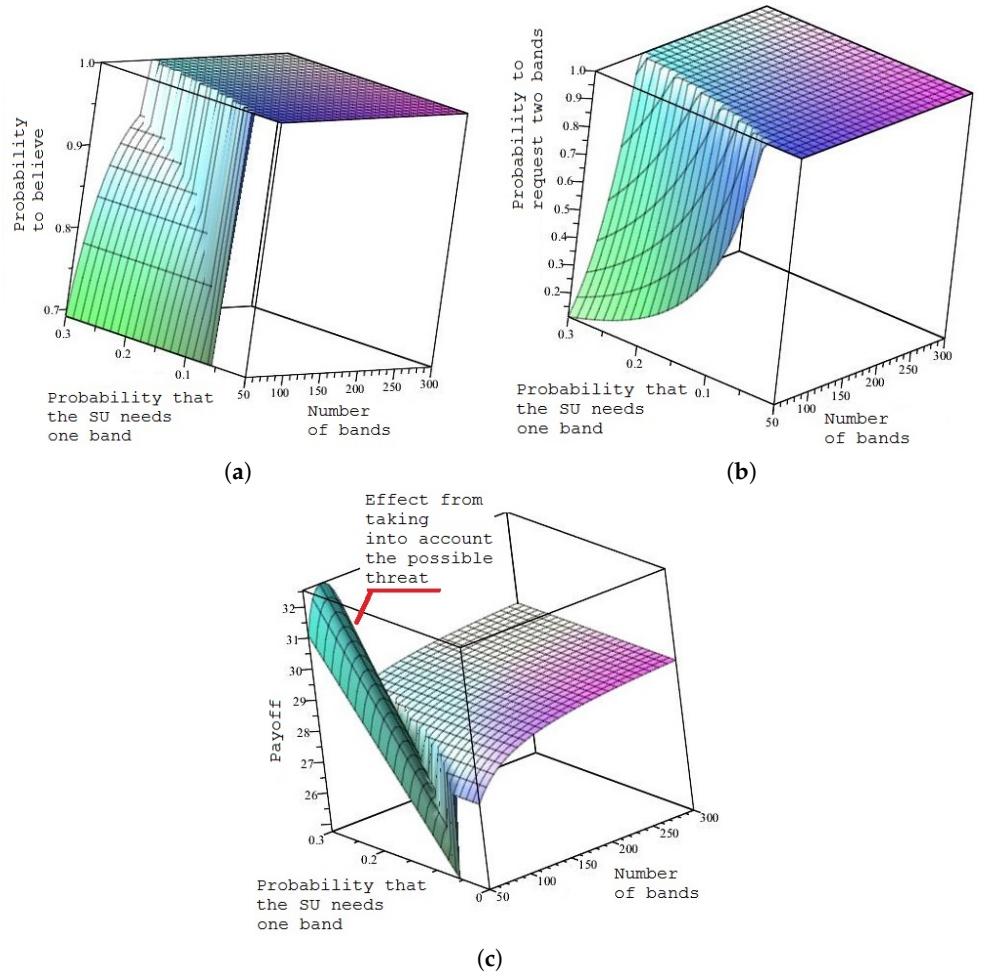

Figure 5. (**a**) Probability of believing in the request of two bands, $\boldsymbol{a}(2, B)$; (**b**) probability of requesting two bands, if only one connection has to be supported, $\boldsymbol{b}(1, 2)$; and (**c**) the payoff to the *SO* as functions of the number of bands n and the probability that the malicious *SU* is of type-$(1, 1)$.

4. Conclusions

In this paper, we have presented a new game-theoretic framework that can be useful in designing a dynamic spectrum access channel management protocol when there is the potential of an untrustworthy secondary participant. The new framework incorporates statistical information describing whether the *SU* is malicious and intends to interfere with primary communications. Using two Bayesian game-theoretical models, we have shown that such a paradigm can lead to protocols that can improve communication reliability. We have noted the interesting observation that the optimal strategy for the *SO*, as well as its payoff in this model, can be discontinuous in the statistical information describing the behavior characteristics of the *SU*. This implication of this discontinuity means that having precise knowledge of the statistical characterization of the *SU* is important since in some regimes there is a threshold behavior in the communication reliability, while in other situations the characterization produces only a minimal impact on the decisions being made. In particular, the practical interpretation of our analysis reveals that if one is operating in a channel-limited scenario, then using obfuscation (i.e., decoy channels) detracts too much from the objective of improving the combined performance (notably, obfuscation will impact the SU's legitimate performance). On the

other hand, if the SU cannot afford to engage in verifying whether the announced schedule is accurate (e.g., such verification would involve deploying infrastructure that is too costly), then the PU should maximize its use of a decoy strategy while meeting its own needs.

Acknowledgments: This material is based upon work supported by DARPA contract HR0011-13-C-0082. The views expressed are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government. Distribution Statement "A" (Approved for Public Release, Distribution Unlimited).

Author Contributions: Andrey Garnaev and Wade Trappe jointly conceived the problem formulation and the derivation of the solutions. Both authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations and notations are used in this manuscript:

CR	Cognitive Radio
PU	Primary User
SO	Spectrum Owner
SU	Secondary User
n	Number of bands
n_P	Number of users the *PU* wants to reliably communicate with
n_T	Number of users the *SU* wants to reliably communicate with
n_A	Number of signals the *SU* can interfere with
q_0	The probability that *SU* might be law-obedient
q_1	The probability that *SU* might be malicious
C_U	The reservation cost for a decoy
c	The number of decoys
X	The pure strategy of the *SO*
Y	The pure strategy of the *SU*
$v_{SO}(X,Y)$	The payoff to the *SO* on the first step
$X_{n_P,[1,n_P+c]}$	A (mixed) strategy for the *SO*
$Y_{n_S,[1,n_P+c]}$	A (mixed) strategy for the *SU*
$H_{n_P,n_A}^{n_P+c}$	The expected number of successfully interfered bands
$T_{n_P,n_A}^{n_P+c}$	The expected number of non-interfered bands
v_U	The expected payoff to the *SO* on the second step
N_T	The upper bound on the possible bands the *SU* could request for legitimate purposes
$A_{SU}(t,\tau)$	The set of (pure) *SU*'s strategies of type-(t,τ)
C_P	Inspection cost per band
C_S	Fine/penalty per falsely-claimed, unused band
$\alpha_{s,t}$	The detection probability of an unused band when there are s unused bands among t requested bands
R	The *SU* reward per successful requested communication
$\boldsymbol{b}(\tau,b)$	The probability that the malicious *SU* of type-$(1,\tau)$ requests b bands
$\boldsymbol{a}(i,\xi)$	The conditional probability that the *SO* employs strategy ξ when observing a request for i bands
$\mu(t,\tau\|j)$	The conditional probability that the *SU* of type-(t,τ) requests j bands
$q_{t,\tau}$	The probability that the *SU* has type-(t,τ)
$E^b u_{SO}(\xi,\boldsymbol{b})$	The expected payoff for the *SO* when the *SU* applies strategy $\boldsymbol{b}$ and the *SO* employs strategy ξ and observes a request for b bands
γ_i	The marginal probability of observing a request for i bands

References

1. Raman, C.; Yates, R.D.; Mandayam, N.B. Scheduling variable rate links via a spectrum server. In Proceedings of the First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), Baltimore, MD, USA, 8–11 November 2005; pp. 110–118.

2. Buddhikot, M.M.; Kolodzy, P.; Miller, S.; Ryan, K.; Evans, J. DIMSUMnet: New directions in wireless networking using coordinated dynamic spectrum. In Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, Taormina-Giardini, Naxos, Italy, 13–16 June 2005; pp. 78–85.
3. Raychaudhuri, D.; Baid, A. NASCOR: Network Assisted Spectrum Coordination Service for Coexistence between Heterogeneous Radio Systems. *IEICE Trans. Commun.* **2014**, *E97-B*, 251–260.
4. Park, J.-M.; Reed, J.H.; Clancy, T.C. Security and Enforcement in Spectrum Sharing. *Proc. IEEE* **2014**, *102*, 270–281.
5. Bhattacharjee, S.; Sengupta, S.; Chatterjee, M. Vulnerabilities in Cognitive Radio Networks: A Survey. *Comput. Commun.* **2013**, *36*, 1387–1398.
6. El-Hajj, W.; Safa, H.; Guizani, M. Survey of Security Issues in Cognitive Radio Networks. *J. Internet Technol.* **2012**, *12*, 181–198.
7. Khare, A.; Saxena, M.; Thakur, R.S.; Chourasia, K. Attacks and Preventions of Cognitive Radio Network-A Survey. *Int. J. Adv. Res. Comput. Eng. Technol.* **2013**, *2*, 1002–1006.
8. Federal Communications Commission (FCC). National Broadband Plan: Connecting America. 2010. Available online: http://www.broadband.gov/plan/ (accessed on 11 December 2013).
9. President's Council of Advisors on Science and Technology (PCAST). Report to the President Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth. 2012. Available online: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_spectrum_report_final_july_20_2012.pdf (accessed on 11 December 2013).
10. Lackpour, A.; Luddy, M.; Winters, J. Overview of interference mitigation techniques between WiMAX networks and ground based radar. In Proceedings of the 20th Annual Wireless and Optical Communications Conference, Newark, NJ, USA, 15–16 April 2011; pp. 1–5.
11. Sanders, F.H.; Sole, R.L.; Carroll, J.E.; Secrest, G.S.; Allmon, T.L. *Analysis and Resolution of RF Interference to Radars Operating in the Band 2700–2900 MHz from Broadband Communication Transmitters*; NTIA Technical Report TR-13-490; United States Department of Commerce: Washington, DC, USA, 2012.
12. Khawar, A.; Abdel-Hadi, A.; Clancy, T.C. Spectrum sharing between S-band radar and LTE cellular system: A spatial approach. In Proceedings of the IEEE International Symposium on Dynamic Spectrum Access Networks, McLean, VA, USA, 1–4 April 2014; pp. 7–14.
13. Ji, Z.; Liu, K.J.R. Dynamic Spectrum Sharing: A Game Theoretical Overview. *IEEE Commun. Mag.* **2007**, *45*, 88–94.
14. Han, Z.; Niyato, D.; Saad, W.; Basar, T.; Hjrungnes, A. *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*; Cambridge University Press: New York, NY, USA, 2012.
15. Hausken, K. Information sharing among firms and cyber attacks. *J. Account. Public Policy* **2007**, *26*, 639–688.
16. La, Q.D.; Quek, T.Q.S.; Lee, J.; Jin, S.; Zhu, H. Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things. *IEEE Internet Things J.* **2016**, *3*, 1025–1035.
17. Wu, Y.; Wang, B.; Liu, K.J.R.; Clancy, T.C. Repeated Open Spectrum Sharing Game with Cheat-Proof Strategies. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 1922–1933.
18. Garnaev, A.; Liu, Y.; Trappe, W. Anti-jamming Strategy versus a Low-Power Jamming Attack When Intelligence of Adversary's Attack Type is Unknown. *IEEE Trans. Signal Inf. Process. Netw.* **2016**, *2*, 49–56.
19. Meamari, E.; Afhamisisi, K.; Shahhoseini, H.S. An Analysis on Interactions among Secondary User and Unknown Jammer in Cognitive Radio Systems by Fictitious Play. In Proceedings of the 10th International ISC Conference on Information Security and Cryptology (ISCISC 2013), Yazd, Iran, 29–30 August 2013; pp. 1–6.
20. Khalil, K.; Ekici, E. Multiple Access Game with a Cognitive Jammer. In Proceedings of the 46th Asilomar Conference on Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA, USA, 4–7 November 2012; pp. 1383–1387.
21. Aziz, F.M.; Shamma, J.S.; Stuber, G.L. Resilience of LTE Networks against Smart Jamming Attacks. In Proceedings of the IEEE Global Communications Conference (GLOBECOM 2014), Austin, TX, USA, 8–12 December 2014; pp. 734–739.
22. Garnaev, A.; Trappe, W. One-time Spectrum Coexistence in Dynamic Spectrum Access When the Secondary User may be Malicious. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1064–1075.

23. Garnaev, A.; Trappe, W. A Bandwidth Monitoring Strategy Under Uncertainty of the Adversary's Activity. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 837–849.
24. Estiri, M.; Khademzadeh, A. A Game-Theoretical Model for Intrusion Detection in Wireless Sensor Networks. In Proceedings of the 23rd Canadian Conference on Electrical and Computer Engineering (CCECE 2010), Calgary, AB, Canada, 2–5 May 2010; pp. 1–5.
25. Theodorakopoulos, G.; Baras, J.S. Game Theoretic Modeling of Malicious Users in Collaborative Networks. *IEEE J. Sel. Areas Commun.* **2008**, *26*, 1317–1327.
26. Hamilton, S.N.; Miller, W.L.; Ott, A.; Saydjari, O.S. *Challenges to Applying Game Theory to the Domain of Information Warfare*; 4th Information Survivability Workshop: Vancouver, BC, Canada, 2002.
27. Garnaev, A.; Baykal-Gursoy, M.; Poor, H.V. Security Games with Unknown Adversarial Strategies. *IEEE Trans. Cybern.* **2016**, *46*, 2291–2299.
28. Liu, Y.; Comaniciu, C.; Mani, H. *A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks*; Workshop on Game Theory for Communications and Networks (GameNets): Pisa, Italy, 2006.
29. Sagduyu, Y.E.; Ephremidess, A. A Game-theoretic Analysis of Denial of Service Attacks in Wireless Random Access. *J. Wirel. Netw.* **2009**, *15*, 651–666.
30. Garnaev, A.; Trappe, W. Secret Communication When the Eavesdropper Might Be an Active Adversary. In *Multiple Access Communications*; Lecture Notes in Computer Science; Jonsson, M., Vinel, A., Bellalta, B., Belyaev, E., Eds.; Springer: Halmstad, Sweeden, 2014; Volume 8715, pp. 121–136.
31. Garnaev, A.; Trappe, W. Stationary Equilibrium Strategies for Bandwidth Scanning. In *Multiple Access Communcations*; Lecture Notes in Computer Science; Jonsson, M., Vinel, A., Bellalta, B., Marina, N., Dimitrova, D., Fiems, D., Eds.; Springer: Vilnius, Lithuania, 2013; Volume 8310, pp. 168–183.
32. Garnaev, A.; Trappe, W.; Kung, C.-T. Optimizing Scanning Strategies: Selecting Scanning Bandwidth in Adversarial RF Environments. In Proceedings of the 8th International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM 2013), Washington, DC, USA, 8–10 July 2013; pp. 148–153.
33. Garnaev, A.; Trappe, W. Bandwidth Scanning when Facing Interference Attacks Aimed at Reducing Spectrum Opportunities. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1916–1930.
34. Xiao, L.; Liu, J.; Mandayam, N.B.; Poor, H.V. Prospect Theoretic Analysis of Anti-jamming Communications in Cognitive Radio Networks. In Proceedings of the IEEE Global Communications Conference (GLOBECOM 2014), Austin, TX, USA, 8–12 December 2014; pp. 746–751.
35. Nguyen, K.C.; Alpcan, T.; Basar, T. Stochastic games for security in networks with interdependent nodes. In Proceedings of the International Conference on Game Theory for Networks (GAMENETS 2009), Istanbul, Turkey, 13–15 May 2009; pp. 697–703.
36. Calinescu, G.; Kapoor, S.; Qiao, K.; Shin, J. Stochastic Strategic Routing Reduces Attack Effects. In Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM 2011), Houston, Texas, USA, 5–9 December 2011; pp. 1–5.
37. Jin, X.; Li, L.E.; Vanbever, L.; Rexford, J. SoftCell: Scalable and Flexible Cellular Core Network Architecture. In Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies (CoNEXT 2013), Santa Barbara, CA, USA, 9–12 December 2013; ACM: New York, NY, USA, 2013; pp. 163–174.
38. Fudenberg, D.; Tirole, J. *Game Theory*; MIT Press: Boston, MA, USA, 1991.
39. Lin, J.; Liu, P.; Jing, J. Using Signaling Games to Model the Multi-step Attack-Defense Scenarios on Confidentiality. In *Decision and Game Theory for Security*; Lecture Notes in Computer Science; Grossklags, J., Walrand, J., Eds.; Springer: Budapest, Hungary, 2012; Volume 7638, pp. 118–137.
40. Estiri, M.; Khademzadeh, A. A Theoretical Signaling Game Model for Intrusion Detection in Wireless Sensor Networks. In Proceedings of the International Telecommunications Network Strategy and Planning Symposium (Networks), Warsaw, Poland, 27–30 September 2010; pp. 1–6.
41. Casey, W.; Morales, J. A.; Nguyen, T.; Spring, J.; Weaver, R.; Wright, E.; Metcalf, L.; Mishra, B. Cyber Security via Signaling Games: Toward a Science of Cyber Security. In *Distributed Computing and Internet Technology*; Lecture Notes in Computer Science; Natarajan, R., Ed.; Springer: Bhubaneswar, India, 2014; Volume 8337, pp. 34–42.
42. Patcha, A.; Park, J.-M. *A Game Theoretic Approach to Modeling Intrusion Detection in Mobile Ad Hoc Networks*; IEEE Workshop on Information Assurance and Security (WIAS): West Point, NY, USA, 2004; pp. 30–34.
43. Carroll, T.E.; Grosu, D. A Game Theoretic Investigation of Deception in Network Security. *Secur. Commun. Netw.* **2011**, *4*, 1162–1172.

44. Pibil, R.; Lisy, V.; Kiekintveld, C.; Bosansky, B.; Pechoucek, M. Game Theoretic Model of Strategic Honeypot Selection in Computer Networks. In *Decision and Game Theory for Security*; Lecture Notes in Computer Science; Grossklags, J., Walrand, J., Eds.; Springer: Budapest, Hungary, 2012; Volume 7638, pp. 201–220.
45. Xia, F.; Jedari, B.; Yang, L.T.; Ma, J.; Huang, R. A Signaling Game for Uncertain Data Delivery in Selfish Mobile Social Networks. *IEEE Trans. Comput. Soc. Syst.* **2016**, *3*, 100–112.
46. Mabrouk, A.; Kobbane, A.; Sabir, E.; Ben-Othman, J.; El Koutbi, M. A Signaling Game-Based Mechanism to Meet Always Best Connected Service in VANETs. In Proceedings of the IEEE Global Communications Conference (GLOBECOM 2015), San Diego, CA, USA, 6–10 December 2015; pp. 1–5.
47. Battigalli, P. Rationalization in Signaling Games: Theory and Applications. *Int. Game Theory Rev.* **2006**, *8*, 67–93.
48. McKelvey, R.D.; McLennan, A.M.; Turocy, T.L. Gambit: Software Tools for Game Theory, Version 16.0.0. 2010. Available online: http://www.gambit-project.org (accessed on 11 December 2013).