IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Preserving Operation Frequency Privacy of Incumbents in CBRS

PRANAY AGARWAL[1], (Member, IEEE), ABHINAV KUMAR[1], (Senior Member, IEEE), AND RIE SHIGETOMI YAMAGUCHI[2], (Member, IEEE)

[1]Department of Electrical Engineering, Indian Institute of Technology Hyderabad, Hyderabad 502284, India
[2]Graduate School of Information Technology, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan

Corresponding author: Abhinav Kumar (e-mail: abhinavkumar@ee.iith.ac.in).

The authors express their sincere gratitude to Ministry of Electronics and IT, Govt. of India, for their financial support under Visvesvaraya PhD Scheme for Electronics and IT. The authors are also grateful to Japan International Cooperation Agency (JICA) for their financial support under Collaboration Kick-Starter Program (CKP).

ABSTRACT Citizens Broadband Radio Service (CBRS) is a novel service band in the United States, spanning 3550−3700 MHz, recently opened for commercial cognitive operations. The CBRS has a three tier hierarchical architecture, wherein, the topmost tier users (also called as incumbents) include military radars. The second and third tier facilitate licensed and unlicensed access to the band, respectively. The privacy of incumbents has been a major concern and different schemes have been proposed in the literature to preserve privacy of their location and operation time. However, the privacy of operation frequency of incumbents has not been suitably addressed. The operation frequency of incumbent is vulnerable to inference attacks from the adversary. For instance, an adversary can deduce the operation frequency of incumbent if a compromised device is asked to switch to another channel. Therefore, in this paper, we propose probabilistic usage of dummy incumbents on a channel and analyse the operation frequency privacy of incumbents for snapshot and time based models in the three tier CBRS system. The optimum dummy generation probability is obtained for the snapshot and time based models, varying capabilities of the adversary, and different system parameters. Finally, we verify the proposed results through simulations.

INDEX TERMS Citizens broadband radio service (CBRS), military radars, operation frequency privacy, preemptive resume priority queue, spectrum access system (SAS).

I. INTRODUCTION

THE mushrooming of smartphones and smart objects has augmented the volume of data flow across the globe. As a consequence, there is a dire requirement of additional spectrum to meet the ever-increasing demands for high data rates. The exploration of novel bands for wireless communications is a promising solution and researchers in industries and academia have been toiling hard for the same. Another possible strategy to combat spectrum dearth is to leverage the existing spectrum for boosting the capacity of wireless networks. The prioritized and dynamic spectrum access capabilities of cognitive radio networks (CRNs) can efficiently transform the spectrum holes into the transmission opportunities leading to the efficient utilization of the existing spectrum [1]. Motivated by this, the Federal Communications Commission (FCC) of United States has opened the Citizens Broadband Radio Service (CBRS) band, spanning 3550-3700 MHz, for commercial cognitive operations [2]. The CBRS has a three tier hierarchical architecture, wherein, the topmost tier users (also called as incumbents) are ship-borne or ground-based military radars and fixed-satellite-service earth stations [3]. The second tier, namely priority access license (PAL) tier, permits the wireless service providers to access the band in a licensed manner after purchasing the license via competitive bidding. The third tier, also known as the general authorized access (GAA) tier, permits unlicensed access to the spectrum. In this work, the devices operating in the second and third tiers are referred to as the PAL and GAA devices, respectively. The hierarchy of the tiers reflects the descending order of their priority of accessing the spectrum which implies that the lower tier devices have to regulate their transmissions or even vacate the spectrum if a higher tier device demands spectrum access. A centralised entity termed as spectrum access system (SAS) is responsible for allocating resources to the PAL and GAA devices while protecting the incumbents and PAL devices from any harmful interference.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access

The three-tier hierarchical architecture of CBRS is beneficial for wireless networks. For instance, the cellular base stations can use the CBRS spectrum as PAL devices for providing better quality-of-service to the associated end users. However, the advent of commercial devices into the CBRS spectrum has raised concerns regarding their penetration to the operation details of the incumbents. The adversary can infer the operation details of incumbents by sending multiple innocuous queries to the SAS through a compromised PAL or GAA device. This is a matter of grave concern as incumbents in CBRS include military radars and any loophole in the privacy of their location, operation time, or operation frequency can be detrimental to national security [4]. Different schemes have been proposed in the literature to ensure privacy of location and operation time of the incumbents in CBRS [5]- [10]. However, the privacy of operation frequency of incumbents has not been suitably addressed. The operation frequency of incumbents is vulnerable to inference attacks of the adversary. For instance, the adversary can infer the presence of incumbents on a channel, say C, if a compromised GAA device which has been operating on C is asked to switch to another channel. In our previous work, i.e., [11], we have proposed that SAS transmits dummy incumbent signals on any channel to preserve the privacy of operation frequency of incumbents. However, the scheme fails if the adversary compromises the SAS itself [10]. Moreover, the analysis presented in [11] is limited to only incumbents and GAA devices. Therefore, a holistic study of privacy of operation frequency of incumbents which incorporates the three tier hierarchical architecture of CBRS is required. This is the motivation for this work.

In this work, we propose that the military organization introduces dummy incumbents which transmits on any channel with some probability to preserve the operation frequency privacy of the real incumbents. *The key improvements in this work as compared to our previous work in [11] are as follows.* In our previous work, we have considered that the adversary has compromised a subset of GAA devices and has partial information on frequency relocation and suspension. Whereas, in this work, we consider that the adversary can compromise (i) a subset of GAA devices, (ii) all GAA devices, or (iii) the SAS. Therefore, we consider different capabilities of the adversary and study its impact on the operation frequency privacy of incumbents. Further, in this work, we study the privacy of incumbents while considering the activity of PAL devices. The PAL devices has higher priority of spectrum access than the GAA devices which implies that if an incumbent asks a PAL device to shift to another channel, the displaced PAL device can be accommodated by displacing a GAA device. In this work, we first compute the displacement and relocation probabilities for a PAL device which have not been computed in the previous work. Then, the probabilities of displacement and relocation of a GAA device are computed while considering the impact of activity of both incumbents and PAL devices. Whereas, in the previous work, we have computed the displacement and relocation probabilities of only GAA devices while considering the impact of activity of the incumbents. Thus, the analysis given in this work is holistic and more involved as compared to our previous work. Further, we also analyse the operation frequency privacy of incumbents in time-domain by employing queueing theory which has not been done in our previous work.

The key contributions of this work are as follows. We first consider a snapshot based model and propose that the military organization transmits dummy incumbent signals on a channel (not in use by real incumbent) with probability p. The probability of incorrect identification of the operation frequency of real incumbent by an adversary is analysed for different strategies and varying capabilities of the adversary. The optimum value of p is determined by solving the trade-off between operation frequency privacy of incumbents and availability of resources for PAL and GAA devices for different system parameters. We then extend the study to a time based model, wherein, we analyse the operation frequency privacy of incumbents while modeling the packet dynamics of incumbents (real and dummy) through a discrete two-class preemptive resume priority queue. An optimum packet arrival probability for dummy incumbents is obtained by studying the trade-off between privacy of incumbents and throughput of PAL and GAA devices. To the best of our knowledge, such time based model has not been explored in the existing literature of CBRS operation frequency privacy.

The paper is organised as follows. A brief overview of the existing literature is given in Section II. Section III provides the system model for both snapshot and time based model. The utility of incumbents, joint utility of PAL and GAA devices, and privacy communications trade-off is studied for snapshot and time based models in Section IV and V, respectively. Numerical results are given in Section VI. Section VII presents the concluding remarks and future works.

II. RELATED WORK

The adoption of CRNs has accelerated the efficient use of the existing spectrum. However, the consequential violation of the privacy of the operation parameters of primary and secondary users in CRNs has always been a matter of concern and several efforts have been made in the literature to preserve the same. The construction of a cloaking region around the secondary users (SUs) to preserve their location privacy has been proposed in [12]. The cryptographic tools have been employed in [13] to ensure that the fusion center cannot infer the locations of the SUs while aggregating their sensing reports. In [14], an additional entity named query server has been introduced between SUs and database to ensure that the database cannot record locations of the querying SUs. However, the query server can be the single point of failure. It has been proposed in [15] that the service providers generate cloaks with perturbed counts from the sensing data of their SUs to obscure the correlation between the sensing data and location of the SUs. The UMax protocol has been proposed in [16], wherein, both primary and secondary users

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access

simultaneously maximize their utilities while preserving the privacy of their locations. A scheme for ensuring the privacy of bids of SUs has been proposed in [17], wherein, the primary users allocate resources to the non-interfering SUs while maximizing their profit computed on the encrypted bids of the SUs.

The CBRS is a novel service band in the United States which the commercial cellular base stations can utilize for transmission in cognition with the incumbents of the band. The existing literature on privacy in traditional CRNs has paid more attention to the privacy of SUs. However, in CBRS, the incumbents include military radars, and hence, the privacy of their location, operation time, and operation frequency is crucial. Further, the schemes proposed in the existing literature for privacy of SUs in traditional CRNs cannot be directly extended to the privacy of incumbents in CBRS due to the technical dissimilarities between CBRS and traditional CRNs. For instance, CBRS has a centralized three-tier architecture with additional regulations on frequency reuse and allocation. Different schemes have been proposed in the literature to preserve the privacy of location and operation time of incumbents in CBRS. The addition of a non-positive random noise to the transmit power to be allocated to the SUs has been proposed in [5] to preserve the location privacy of incumbents. The addition of false locations of incumbents in the database, perturbation of the transmit power allocated to the SUs, and distortion of a-priori distribution of the locations of incumbents have been considered to preserve the location privacy of incumbents in [6]. In [7], the generation of multiple fake trajectories has been proposed to preserve the trajectory privacy of mobile incumbents. Differential privacy has been employed in [8] to preserve the privacy of the operation time of the incumbents. However, the algorithm proposed in [8] prevents any SU from transmission even when it is outside the protection zone of the incumbent. The addition of dummy signals on the channel of operation has been proposed to obfuscate the actual operation time of the incumbents in [9]. In [10], a generalized framework has been proposed to preserve the location and operation time of the incumbents, wherein, the inherent noise in the readings of environmental sensing capability (ESC) sensors, insertion of dummy entries of incumbents in database, and perturbation of resources to be allocated to the SUs add inaccuracy to the adversary's estimate of the distribution of these parameters of the real incumbents. However, the performance of the proposed framework has been evaluated only for the location privacy of the incumbents. Further, the proposed framework is not scalable to the dense network of incumbents and SUs. The cryptographic tools have been employed to preserve the privacy of parameters of incumbents in [18]- [20]. However, the proposed schemes introduce a third party for generation and distribution of security keys which can act as a single point of failure and levy additional computational overhead adding to the latency especially in processing batch requests.

The existing literature has emphasized on the privacy of location and operation time of the incumbents. The operation

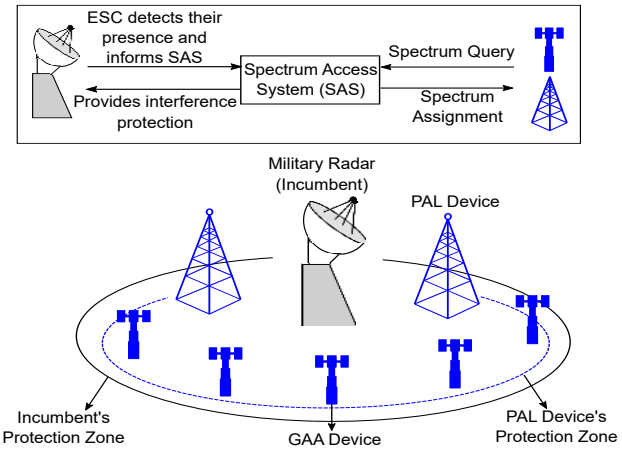


FIGURE 1: System Model.

frequency of incumbents is vulnerable to the inference attack of the adversary. For instance, the adversary can infer the presence of incumbents on a channel if a compromised PAL or GAA device is asked to switch to another channel. Therefore, an in-depth analysis of operation frequency privacy of incumbents is still required. In our previous work, i.e., [11], we have proposed that SAS transmits dummy incumbent signals on any channel to preserve the operation frequency privacy of incumbents. However, the proposed scheme fails if the adversary compromises the SAS itself [10]. Moreover, the analysis given in [11] has not considered the impact of the activity of the PAL devices. The existing works have focused mostly on the database inference models of the adversary. Whereas, in this work, we consider that the adversary aims to jam/eavesdrop a channel in use by the real incumbent. Further, the adversary can sense the spectrum and query the SAS for the same. Therefore, in this work, we first consider a snapshot based model, wherein, we propose that the military organisation transmits dummy incumbent signals on any channel with probability p and analyse the probability of incorrect identification of the operation frequency of real incumbent for different strategies and varying capabilities of the adversary. We then consider a time based model, wherein, we analyse the privacy of operation frequency of incumbents while modelling the packet dynamics of incumbents (real and dummy) via a discrete two-class preemptive resume priority queue. To the best of our knowledge, the time based model for analysing the privacy of incumbents in CBRS has not been explored in the existing literature. Next, we describe the system model for both snapshot and time based model.

III. SYSTEM MODEL

A. SNAPSHOT BASED MODEL

The Fig. 1 presents the system model which comprises of incumbents, PAL devices, and GAA devices. In this work, we consider that ESC sensors are deployed and exclusion zones are converted into protection zones [3], [21]. Let N denote the total number of real incumbents in the system. We use S and T to denote the total number of PAL and GAA devices in the system, respectively. Let $\mathcal{M}$ denote the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access

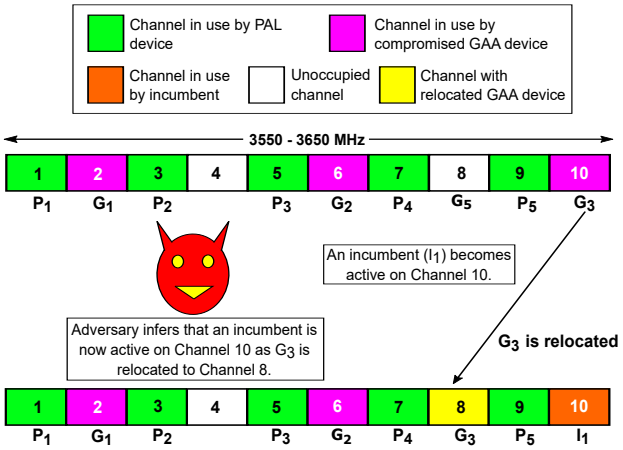


FIGURE 2: Adversary infers the operating frequency of the incumbent.

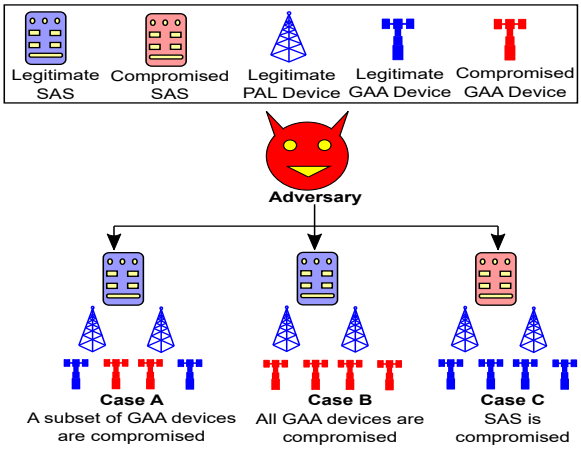


FIGURE 3: Different cases of adversary.

set of channels in CBRS, each spanning a bandwidth of W MHz. Then, $M = |\mathcal{M}|$ denotes the number of channels, i.e., cardinality of set $\mathcal{M}$. For the snapshot based model, we assume that only one of the incumbent, PAL device, or GAA device can be active on a channel at an instant of time. Further, we assume that a device (incumbent, PAL device, or GAA device) transmits on only one channel at an instant of time. Thus, $N \leq M$. Same holds for S and T. These assumptions are made for ease of analysis in snapshot based model. However, later in time based model, we relax these assumptions. The practical scenario relevant for the snapshot based model is as follows. The PAL and GAA devices are located within the protection zone of incumbents. It is a reasonable assumption as the incumbents have protection zones of radius 63 km and larger [22]. The GAA devices are located within the protection zone of PAL devices. It is a reasonable assumption as the protection zone of PAL devices has radius of 40 km [23]. Further, PAL and GAA devices are located in proximity of each other, corresponding to dense network deployment scenario. In accordance with the transmission precedence rules set by FCC [3], the PAL devices can transmit on a channel only in the absence of the incumbents and GAA devices can transmit only if any higher tier device is not active on the channel. This implies that lower tier device has to switch to another channel, if available, whenever a higher tier device requests the channel from the SAS. An adversary can use these events of frequency relocation (or suspension) of lower tier devices to infer the operation frequency of the incumbents, especially if the lower tier devices are compromised. For instance, consider an adversary which has compromised all the GAA devices. As illustrated in Fig. 2, the adversary can then infer the presence of an incumbent on Channel 10 as the compromised GAA device G_3, which has been operating on Channel 10, is now relocated to Channel 8. In our previous work, i.e., [11], we have proposed that SAS transmits dummy incumbent signals on any channel to preserve the operation frequency privacy of incumbents. However, this scheme is not robust against varying capabilities of the adversary as we discuss next.

In this work, we consider an adversary which aims to eavesdrop or jam the channel in use by an incumbent. However, it can attack only one channel at an instant of time due to the limited hardware available at its end. We consider the following cases of the adversary depending on its capabilities as illustrated in Fig. 3.

- **Case A:** The adversary compromises a subset of GAA devices or overhears the communication between SAS and a subset of GAA devices. Equivalently, it can also deploy its own small cell base stations or Wi-Fi access points as GAA devices for accessing the spectrum. Therefore, in this case, it has access to partial information on frequency relocation and suspension of GAA devices. However, it cannot differentiate between the transmissions of incumbents and transmissions of PAL and non-compromised GAA devices. This adversary case has been analysed in our previous work, i.e., [11], while only considering incumbents and GAA devices.
- **Case B:** The adversary compromises all the GAA devices or overhears the messages exchanged between SAS and all GAA devices. Therefore, in this case, it has access to complete information on frequency relocation and suspension for GAA devices. However, it cannot segregate the transmissions of incumbents and PAL devices. The scheme proposed in our previous work, i.e., [11], can preserve the operation frequency privacy of incumbents in this case. However, please note that this adversary case has not been analysed in our previous work, i.e., [11] and is novel to this work.
- **Case C:** This case corresponds to a smart adversary (SA) which can compromise the SAS or overhear the communication between SAS and ESC sensors [10]. Therefore, in this case, the adversary can prepare a list of channels in use by incumbents. The scheme proposed in our previous work, i.e., [11], fails to preserve the operation frequency privacy of incumbents in this case as the SAS itself is compromised. This case also encompasses the adversary which compromises all PAL and GAA devices or can differentiate between the transmissions

of incumbents and transmissions of PAL and GAA devices.

In all the aforementioned cases, we consider that the adversary cannot differentiate between the transmissions of real and dummy incumbents. Further, the adversary is aware of the privacy preserving strategy employed by the military organization. However, it neither knows the number of incumbents in the system nor their probability of being active on any channel. Given the aforementioned limitations and sources of information, the intent of the adversary is the correct identification of the operation frequency of a real incumbent. Therefore, we propose that the military organization transmits dummy incumbent signals on any channel (not in use by real incumbents) with probability p to preserve the operation frequency privacy of incumbents and analyse the probability of incorrect identification of the operation frequency of a real incumbent by the adversary as the privacy metric for incumbents.

B. TIME BASED MODEL

In this part, we consider that the time axis is discretized into slots [1]. Let N and D denote the total number of real and dummy incumbents in the system, respectively. We use M to denote the total number of channels. In each slot, we consider an incumbent (real or dummy) can transmit on a channel and a channel can be in use by only one incumbent. This implies $N \leq M$ and $D \leq M$. The packet arrival follows Bernoulli process with parameters λ_R and λ_D for real and dummy incumbents, respectively, which implies that a packet arrives in a slot with probability λ_R (respectively, λ_D) for a real (respectively, dummy) incumbent [24]. The packet length is considered as a geometric random variable with parameters μ_R and μ_D for real and dummy incumbents, respectively, and it specifies the number of slots a packet requires for transmission [24]. We also consider that the packet service starts at the beginning of the slot. We consider that the incumbents (real and dummy) stay on the same channel until the packet service is not complete and select a channel randomly whenever they have a fresh packet to transmit. Further, the dummy incumbents stay on the channel if the ongoing packet service is interrupted by a real incumbent and resume the packet service once the real incumbent departs.

We consider that the mobile network operators (MNOs) purchase the PAL license and use the CBRS spectrum to offload their traffic. The directional LTE macro evolved NodeBs (MeNBs) deployed by the MNO are considered as the PAL devices. The Tier 3 facilitates unlicensed access to the spectrum and is suitable for private LTE use case [25]. Therefore, we consider omnidirectional small cell evolved NodeBs (SeNBs) as GAA devices. We focus on the area within the protection zone of incumbents as the frequency privacy is most vulnerable in this zone. Thus, the PAL and GAA devices cannot transmit on the channel on which any incumbent is active. We consider the SA, i.e., Case C of the adversary. The adversary can enlist the channels in use by incumbents (real or dummy) in each slot but cannot differentiate between the transmissions of real and dummy incumbents. Further, it aims to eavesdrop/jam the channel in use by real incumbent but can attack only one channel in a slot. Therefore, we aim to analyse the probability of incorrect identification of the operation frequency of real incumbents by the adversary for each slot which is equivalent to the proportion of the time for which the adversary has successfully attacked the operations of the real incumbents out of the total time for which the incumbents are active. A comprehensive list of symbols used in this paper and their definition is given in Table 1. Next, we discuss the utility of incumbents, joint utility of PAL and GAA devices, and privacy communications trade-off for the snapshot based model.

[1]Please note that this slot is not same as the LTE slot.

IV. SNAPSHOT BASED MODEL: ANALYSIS

The arrival and departure of incumbents on any channel need not be pre-determined. The ESC sensors inform the SAS about the presence of incumbents on a channel and SAS asks the PAL and GAA devices transmitting on that channel to switch to another channel, if available, within 300 s [3]. This leads to the frequency relocation (or suspension) of a PAL and GAA device which can be used by an adversary to infer the operation frequency of the incumbent as illustrated in Fig. 2. Therefore, in order to study the impact of the frequency relocation (or suspension) on the privacy of incumbents, we first consider Case B of the adversary. We study the operation frequency privacy of incumbents in this part for a slot. Further, we assume that no incumbents are active initially for ease of analysis. Let η and θ denote the probabilities that a PAL and GAA device has data to transmit, respectively. We use s and t to denote the number of PAL and GAA devices which have data to transmit in the slot under consideration, respectively. Since no incumbents are active and PAL devices have higher spectrum access priority than GAA devices, the SAS allocates a channel each to the s PAL devices. Let $\mathcal{M}_s$ denote the set of channels assigned to the PAL devices. Now, the SAS can allocate a channel each to t GAA devices only if $|\mathcal{M} - \mathcal{M}_s| > t$. We use τ to denote the number of GAA devices that can be accommodated. Therefore,

$$\tau = \min(t, M - s)\ . \tag{1}$$

Let $\mathcal{M}_t$ denote the set of channels assigned to τ GAA devices. Thus, s PAL and τ GAA devices are actively transmitting on a channel each contained in the sets $\mathcal{M}_s$ and $\mathcal{M}_t$, respectively. We denote the set of unoccupied channels by $\mathcal{M}_v$ and $\mathcal{M}_v = \mathcal{M} - \mathcal{M}_s - \mathcal{M}_t$. Let v denote the number of unoccupied channels, i.e., $v = |\mathcal{M}_v|$, and $v = M - s - \tau$. Now, at some instant within the slot, the real incumbents become active and SAS accordingly relocates (or suspends) the PAL and GAA devices. Let n incumbents become active on $\mathcal{M}_n (\subseteq \mathcal{M})$ set of channels. Further, the military organization transmits dummy incumbent signals on d channels contained in the set $\mathcal{M}_d$ such that $d = |\mathcal{M}_d|$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access

TABLE 1: Symbols and Notations

Notation	Definition	Notation	Definition
$N(D)$	Total number of real (dummy) incumbents in the system	$\lambda_R(\lambda_D)$	Probability of packet arrival for real (dummy) incumbent in a slot
n	Number of active real incumbents	$\mu_R(\mu_D)$	Expected length of real (dummy) incumbent packet
q	Probability of a real incumbent being active on any channel	$\rho_R(\rho_D)$	Load offered by real (dummy) incumbent on a channel
p	Probability of transmission of dummy incumbent signals on any channel in snapshot based model	ρ_T	Total load offered by incumbents (real and dummy) on a channel
$S(T)$	Total number of PAL (GAA) devices in the system	$\mathcal{O}$	Set of MNOs
$\eta(\theta)$	Probability that a PAL (GAA) device has data to transmit	$\mathcal{B}_o$	Set of MeNBs of the MNO o
$s(t)$	Number of active PAL (GAA) devices	$\mathcal{U}_{b,o}$	Set of MUEs associated with the MeNB b of MNO o
τ	Number of GAA devices which can be accommodated	$\mathcal{J}$	Set of SeNBs
$n_s(n_t)$	Number of channels in use by real incumbents but were allocated to PAL (GAA) devices	$\mathcal{G}_j$	Set of SUEs associated with SeNB j
$s_p(\tau_p)$	Number of perturbed PAL (GAA) devices	$\mathbf{X}(\mathbf{Y})$	Binary channel allocation matrix for PAL (GAA) devices
$\tau_p^1(\tau_p^2)$	Number of GAA devices perturbed due to incumbents (PAL devices)	$r_{u,b,o}(r_{g,j})$	Link rate of an MUE (SUE)
$s_{pr}(\tau_{pr})$	Number of relocated PAL (GAA) devices	$\gamma^m_{u,b,o}(\gamma^m_{g,j})$	SINR of an MUE (SUE) on channel m
$s_{np}(\tau_{np})$	Number of non-perturbed PAL (GAA) devices	$P^m_{u,b,o}(P^m_{g,j})$	Transmit power allocated to an MUE (SUE) on channel m
s^v_{pr}	Number of PAL devices relocated on vacant channels	$h^m_{u,b,o}(h^m_{g,j})$	Channel gain of an MUE (SUE)
$\mathcal{M}(M)$	Set (number) of channels	ξ	Spectral efficiency in bits/symbol
$\mathcal{M}_n$	Set of channels in use by real incumbents	$\mathcal{M}_p$	Set of channels in use by real and dummy incumbents
$\mathcal{M}_d(d)$	Set (number) of channels on which dummy incumbent signals are transmitted	$\mathcal{M}_s(\mathcal{M}_t)$	Set of channels which were allocated to PAL (GAA) devices
$\mathcal{M}_v(v)$	Set (number) of channels which were unoccupied	$\mathcal{M}_{vp}$	Set of channels in use by incumbents but were unoccupied
$\mathcal{M}_{spr}$	Set of channels on which perturbed PAL devices are relocated	$\mathcal{M}_{tp}(\mathcal{M}^c_{tp})$	Set of channels in use by incumbents and PAL devices but were allocated to (compromised) GAA devices
$\mathcal{M}_{sp}(\mathcal{M}_{tp1})$	Set of channels in use by incumbents but were allocated to PAL (GAA) devices	n_v	Number of channels in use by real incumbents but were unoccupied
$v_p(v_{np})$	Number of channels occupied (not occupied) by incumbents which were unoccupied	κ	Number of channels available to accommodate perturbed PAL devices
ψ	Number of channels available to accommodate perturbed GAA devices	$\mathcal{Z}(Z)$	Set (number) of channels which an adversary infers as occupied by incumbents for snapshot based model
U_I	Utility of Incumbents	U_S	Joint utility of PAL and GAA devices
Γ	Threshold on the privacy of incumbents	$\omega_1(\omega_2)$	Weight factor for non-perturbed (relocated) PAL and GAA devices
$\tau^c(\tau^l)$	Number of compromised (non-compromised) GAA devices	$\mathcal{M}^l_{tpr}(\mathcal{M}^l_{tnp})$	Set of channels in use by non-compromised relocated (non-perturbed) GAA devices
τ^c_p	Number of compromised and perturbed GAA devices	$\lambda^{eff}_R(\lambda^{eff}_D)$	Effective probability of packet arrival for real (dummy) incumbents for a slot
W	Bandwidth of a channel in MHz	Υ	Number of slots in which atleast one channel is in use by incumbents
$\mathcal{E}(E)$	Set (number) of channels in use by incumbents (real or dummy) for time based model	ζ	Proportionality constant

and $\mathcal{M}_d \subseteq \mathcal{M} - \mathcal{M}_n$. Please note that real and dummy incumbent operations can happen on any channel, regardless of its occupancy status with respect to PAL and GAA devices. The set of channels belonging to incumbents (real or dummy) is denoted by $\mathcal{M}_p$ and $\mathcal{M}_p = \mathcal{M}_n \cup \mathcal{M}_d$. The SAS suspends the operations of PAL and GAA devices transmitting on $\mathcal{M}_s \cap \mathcal{M}_p$ and $\mathcal{M}_t \cap \mathcal{M}_p$ channels, respectively, and relocate them to unoccupied channels, if available. *We refer to these PAL and GAA devices as perturbed PAL and GAA devices, respectively, in the rest of paper.* In this context, we next compute the expected number of non-perturbed and perturbed but relocated PAL and GAA devices. It is then used to compute the joint utility of PAL and GAA devices which is characterised as the weighted sum of non-perturbed and relocated PAL and GAA devices.

We consider n as a binomial random variable with parameters (N, q), where, q denotes the probability of a real incumbent being active on a channel. The probability mass function (PMF) of n, denoted by $\mathbb{P}(n = n_0)$, is given as

$$\mathbb{P}(n = n_0) = \binom{N}{n_0} q^{n_0}(1-q)^{N-n_0} . \tag{2}$$

Similarly, given n, d is a binomial random variable with parameters $(M - n, p)$. Likewise, we consider that s and t are binomial random variables with parameters (S, η) and (T, θ), respectively. Then, the PMFs of s and t, denoted by $\mathbb{P}(s = s_0)$ and $\mathbb{P}(t = t_0)$, respectively, are given as

$$\mathbb{P}(s = s_0) = \binom{S}{s_0} \eta^{s_0}(1-\eta)^{S-s_0} , \tag{3}$$

$$\mathbb{P}(t = t_0) = \binom{T}{t_0} \theta^{t_0}(1-\theta)^{T-t_0} . \tag{4}$$

We can see from (1) that τ is deterministic if s and t are known. Same applies for v as $v = M - s - \tau$. We characterize the joint utility of PAL and GAA devices as the expected number of devices which are actively transmitting on the band. This requires the expected number of non-perturbed GAA devices and in turn the expected number of GAA devices which can be accommodated. Therefore, using (3) and (4), the expected value of τ, denoted by $\mathbb{E}(\tau)$, is given by

$$\mathbb{E}(\tau) = \sum_{s_0=0}^{S} \sum_{t_0=0}^{T} \tau \, \mathbb{P}(t = t_0)\mathbb{P}(s = s_0) . \tag{5}$$

Let n_s (respectively n_t) denote the number of channels currently being used by the real incumbents but were allocated to PAL (respectively GAA) devices. Thus, $n_s = \mathcal{M}_n \cap \mathcal{M}_s$ (respectively $n_t = \mathcal{M}_n \cap \mathcal{M}_t$). Similarly, n_v denotes the number of channels currently being used by the real incumbents but were unoccupied and $n_v = \mathcal{M}_n \cap \mathcal{M}_v$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access

Given $n = n_0$ and $s = s_0$, the conditional PMF of n_s, denoted by $\mathbb{P}(n_s = \alpha | n_0, s_0)$, is given by

$$\mathbb{P}(n_s = \alpha | n_0, s_0) = \frac{\binom{s_0}{\alpha}\binom{M-s_0}{n_0-\alpha}}{\binom{M}{n_0}} . \quad (6)$$

Let d_s denote the number of channels chosen as dummy but were allocated to PAL devices. Then, $d_s = \mathcal{M}_d \cap \mathcal{M}_s$. This implies that given n_s, d_s is a binomial random variable with parameters $(s - n_s, p)$. We use s_p to denote the number of perturbed PAL devices. Then, $s_p = |\mathcal{M}_p \cap \mathcal{M}_s| = n_s + d_s$. Given $n = n_0$, $s = s_0$, and $n_s = \alpha$, the conditional PMF of s_p, denoted by $\mathbb{P}(s_p = x | \alpha, n_0, s_0)$, is given by

$$\mathbb{P}(s_p = x | \alpha, n_0, s_0) = \binom{s_0-\alpha}{x-\alpha} p^{x-\alpha}(1-p)^{s_0-x} . \quad (7)$$

We use $\mathbb{P}(s_p = x)$ and $\mathbb{E}(s_p)$ to denote the PMF and expected value of s_p, respectively. Using (2), (3), (6), and (7), we obtain

$$\begin{aligned}\mathbb{P}(s_p{=}x) &= \sum_{n_0=0}^{N}\sum_{s_0=0}^{S}\sum_{\alpha=0}^{\min(n_0,s_0)} \binom{s_0-\alpha}{x-\alpha} p^{x-\alpha}(1-p)^{s_0-x} \\ &\quad \mathbb{P}(n_s{=}\alpha|n_0,s_0)\mathbb{P}(s{=}s_0)\,\mathbb{P}(n{=}n_0) , \text{ and} \\ \mathbb{E}(s_p) &= \sum_{x=0}^{S} x\,\mathbb{P}(s_p = x) . \quad (8)\end{aligned}$$

Let τ_p^1 denote the number of GAA devices perturbed due to incumbents (real or dummy), i.e., $\tau_p^1 = n_t + d_t$. Then, $\tau_{np}^1 = \tau - \tau_p^1$, where, τ_{np}^1 denotes the number of GAA devices not perturbed due to incumbents. We use v_p to denote the number of channels which incumbents are using but were unoccupied. Then, $v_{np} = v - v_p$, where, v_{np} denotes the number of channels which are still unoccupied. Let $\mathbb{P}(\tau_p^1 = y | n_t)$ denote the conditional PMF of τ_p^1 given n_t. Similarly, we use $\mathbb{P}(v_{np} = \epsilon | n_v)$ to denote the conditional PMF of v_{np} given n_v. Then,

$$\mathbb{P}(\tau_p^1 = y | n_t) = \binom{\tau-n_t}{y-n_t} p^{y-n_t}(1-p)^{\tau-y} , \text{ and} \quad (9)$$

$$\mathbb{P}(v_{np} = \epsilon | n_v) = \binom{v-n_v}{v-\epsilon-n_v} p^{v-\epsilon-n_v}(1-p)^{\epsilon} . \quad (10)$$

The number of channels available to relocate the perturbed PAL devices, denoted by κ, is then given by $\kappa = \tau_{np}^1 + v_{np}$. We use s_{pr} to denote the number of relocated PAL devices. Then, $s_{pr} = \min(s_p, \kappa)$. The PMF of s_{pr}, denoted by $\mathbb{P}(s_{pr} = x)$, is given by

$$\begin{aligned}\mathbb{P}(s_{pr} = x) &= \mathbb{P}(s_p \geq x, \kappa = x) + \mathbb{P}(s_p = x, \kappa \geq x) - \\ &\quad \mathbb{P}(s_p = x, \kappa = x) . \quad (11)\end{aligned}$$

Given n, s, and t, n_s, n_t, and n_v are correlated since $n_s + n_t + n_v = n$. Therefore, given $n = n_0$, $s = s_0$, and $t = t_0$, the joint conditional PMF of n_s, n_t, and n_v, denoted by $\mathbb{P}(n_s, n_t, n_v | n_0, s_0, t_0)$, is given by

$$\mathbb{P}(n_s, n_t, n_v | n_0, s_0, t_0) = \frac{\binom{s_0}{n_s}\binom{\tau}{n_t}\binom{v}{n_v}}{\binom{M}{n_0}} . \quad (12)$$

Using (2)-(4), (7), (9)-(10), and (12), we have

$$\begin{aligned}\mathbb{P}(s_p{=}x, \kappa{=}x) &= \sum_{n_0,s_0,t_0}\sum_{n_s,n_t,n_v} \mathbb{P}(s_p = x|n_s) \\ &\quad \sum_{y=n_t}^{\tau} \mathbb{P}(\tau_p^1 = y|n_t)\mathbb{P}(v_{np} = \epsilon|n_v) \times \\ &\quad \mathbb{P}(n_s, n_t, n_v|n_0, s_0, t_0)\mathbb{P}(t = t_0) \times \\ &\quad \mathbb{P}(s = s_0)\mathbb{P}(n = n_0) , \quad (13)\end{aligned}$$

where, $\epsilon = x - (\tau - y)$. Similarly,

$$\begin{aligned}\mathbb{P}(s_p{\geq}x, \kappa{=}x) &= \sum_{n_0,s_0,t_0}\sum_{n_s,n_t,n_v}\sum_{\chi=x}^{s_0} \mathbb{P}(s_p = \chi|n_s) \\ &\quad \sum_{y=n_t}^{\tau} \mathbb{P}(\tau_p^1 = y|n_t)\mathbb{P}(v_{np} = \epsilon|n_v) \\ &\quad \times\mathbb{P}(n_s, n_t, n_v|n_0, s_0, t_0)\mathbb{P}(t = t_0) \\ &\quad \times\mathbb{P}(s = s_0)\mathbb{P}(n = n_0) . \quad (14)\end{aligned}$$

Likewise,

$$\begin{aligned}\mathbb{P}(s_p{=}x, \kappa{\geq}x) &= \sum_{n_0,s_0,t_0}\sum_{n_s,n_t,n_v}\sum_{\chi=x}^{\kappa_{max}}\sum_{y=n_t}^{\tau} \mathbb{P}(s_p{=}x|n_s) \\ &\quad \mathbb{P}(\tau_p^1 = y|n_t)\mathbb{P}(v_{np} = \epsilon|n_v) \times \\ &\quad \mathbb{P}(n_s, n_t, n_v|n_0, s_0, t_0)\mathbb{P}(t = t_0) \times \\ &\quad \mathbb{P}(s = s_0)\mathbb{P}(n = n_0) , \quad (15)\end{aligned}$$

where, $\epsilon = \chi - (\tau - y)$ and $\kappa_{max} = v + \tau - n_t - n_v$. Substituting (13)-(15) into (11), we obtain $\mathbb{P}(s_{pr} = x)$. The expected value of s_{pr}, denoted by $\mathbb{E}(s_{pr})$, is given by

$$\mathbb{E}(s_{pr}) = \sum_x x\,\mathbb{P}(s_{pr} = x) . \quad (16)$$

Some perturbed PAL devices are relocated by perturbing GAA devices (not perturbed by incumbents) and some perturbed PAL devices are relocated on unoccupied channels. Let τ_p^2 denote the number of GAA devices perturbed to relocate PAL devices. We use s_{pr}^v to denote the number of PAL devices relocated on the unoccupied channels. Then, $s_{pr} = \tau_p^2 + s_{pr}^v$. We denote the total number of perturbed GAA devices by τ_p. Then, $\tau_p = \tau_p^1 + \tau_p^2$. Using (2)-(4), (9)-(10), and (12), we have

$$\begin{aligned}\mathbb{P}(\tau_p{=}x) &= \sum_{n_0,s_0,t_0}\sum_{n_s,n_t,n_v}\sum_{y=n_t}^{t_0}\sum_{\epsilon=0}^{v-n_v}\sum_{\delta=0}^{\beta+\epsilon} \mathbb{P}(\tau_p^1{=}y|n_t) \\ &\quad \mathbb{P}(\tau_p^2 = \alpha, s_{pr}^v = \phi|\delta, \beta, \epsilon)\mathbb{P}(s_{pr} = \delta|\beta, \epsilon) \\ &\quad \mathbb{P}(v_{np} = \epsilon|n_v)\mathbb{P}(n_s, n_t, n_v|n_0, s_0, t_0) \\ &\quad \mathbb{P}(t = t_0)\mathbb{P}(s = s_0)\mathbb{P}(n = n_0) , \quad (17)\end{aligned}$$

where, $\mathbb{P}(\tau_p = x)$ denotes the PMF of τ_p, $\alpha = x - y$, $\phi = \delta - \alpha$, and $\beta = \tau - y$. Given $\tau_{np}^1 = \beta$ and $v_{np} = \epsilon$, the conditional PMF of s_{pr}, denoted by $\mathbb{P}(s_{pr} = \delta|\beta, \epsilon)$, is given by (18). Given $s_{pr} = \delta$, $\tau_{np}^1 = \beta$, and $v_{np} = \epsilon$, the joint conditional PMF of τ_p^2 and s_{pr}^v, denoted by $\mathbb{P}(\tau_p^2 = \alpha, s_{pr}^v = \phi|\delta, \beta, \epsilon)$, is given by (19). Substituting (18)-(19) into (17), we obtain

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access

$$\mathbb{P}(s_{pr}=\delta|\beta,\epsilon)=\begin{cases}\binom{s_0-n_s}{\delta-n_s}\,p^{\delta-n_s}(1-p)^{s-\delta} & \text{if } \delta<\beta+\epsilon\,,\\ \sum_{\chi=\beta+\epsilon}^{s}\binom{s_0-n_s}{\chi-n_s}\,p^{\chi-n_s}(1-p)^{s-\chi} & \text{if } \delta=\beta+\epsilon\,,\\ 0 & \text{otherwise}\,.\end{cases} \tag{18}$$

$$\mathbb{P}(\tau_p^2=\alpha,s_{pr}^v=\phi|\delta,\beta,\epsilon)=\begin{cases}\frac{\binom{\beta}{\alpha}\binom{\epsilon}{\phi}}{\binom{\beta+\epsilon}{\delta}} & \text{if } \delta,\beta,\epsilon,\alpha>0\;||\;\alpha\leq\beta||\alpha\leq\delta\;||\;\phi\leq\epsilon\,,\\ 0 & \text{otherwise}\,.\end{cases} \tag{19}$$

$\mathbb{P}(\tau_p=x)$. The expected value of τ_p, denoted by $\mathbb{E}(\tau_p)$, is given by

$$\mathbb{E}(\tau_p)=x\,\mathbb{P}(\tau_p=x)\,. \tag{20}$$

Let τ_{pr} denote the number of perturbed GAA devices which are relocated. The number of channels which are unoccupied after allocation of incumbents and relocation of PAL devices is denoted by ψ, where, $\psi = v_{np}-s_{pr}^v$. Then, $\tau_{pr}=\min(\tau_p,\psi)$. The PMF of τ_{pr}, denoted by $\mathbb{P}(\tau_{pr}=x)$, is given by

$$\begin{aligned}\mathbb{P}(\tau_{pr}=x) \;=\; &\mathbb{P}(\tau_p\geq x,\psi=x)+\mathbb{P}(\tau_p=x,\psi\geq x)-\\ &\mathbb{P}(\tau_p=x,\psi=x).\end{aligned} \tag{21}$$

Using (2)-(4), (9)-(10), (12), and (18)-(19), we have

$$\begin{aligned}\mathbb{P}(\tau_p{=}x,\psi{=}x) \;=\; &\sum_{n_0,s_0,t_0}\sum_{n_s,n_t,n_v}\sum_{y=n_t}^{\tau}\sum_{\epsilon=0}^{v-n_v}\\ &\mathbb{P}(\tau_p^2=\alpha,s_{pr}^v=\phi|\beta,\epsilon)\\ &\mathbb{P}(s_{pr}{=}\delta|\beta,\epsilon)\mathbb{P}(\tau_p^1{=}y|n_t)\\ &\mathbb{P}(v_{np}{=}\epsilon|n_v)\mathbb{P}(n_s,n_t,n_v|n_0,s_0,t_0)\\ &\mathbb{P}(t{=}t_0)\mathbb{P}(s{=}s_0)\mathbb{P}(n{=}n_0)\,,\end{aligned} \tag{22}$$

where, $\alpha=x-y$, $\phi=\epsilon-x$, $\beta=\tau-y$, and $\delta=\alpha+\phi$. Similarly,

$$\begin{aligned}\mathbb{P}(\tau_p{\geq}x,\psi{=}x) \;=\; &\sum_{n_0,s_0,t_0}\sum_{n_s,n_t,n_v}\sum_{y=n_t}^{\tau}\sum_{\epsilon=0}^{v-n_v}\sum_{\varpi=\alpha}^{\beta}\\ &\mathbb{P}(\tau_p^2=\varpi,s_{pr}^v=\phi|\beta,\epsilon)\\ &\mathbb{P}(s_{pr}{=}\delta|\beta,\epsilon)\mathbb{P}(\tau_p^1{=}y|n_t)\\ &\mathbb{P}(v_{np}{=}\epsilon|n_v)\mathbb{P}(n_s,n_t,n_v|n_0,s_0,t_0)\\ &\mathbb{P}(t{=}t_0)\mathbb{P}(s{=}s_0)\mathbb{P}(n{=}n_0)\,.\end{aligned} \tag{23}$$

Likewise,

$$\begin{aligned}\mathbb{P}(\tau_p{=}x,\psi{\geq}x) \;=\; &\sum_{n_0,s_0,t_0}\sum_{n_s,n_t,n_v}\sum_{y=n_t}^{\tau}\sum_{\epsilon=0}^{v-n_v}\sum_{\varpi=0}^{\phi}\\ &\mathbb{P}(\tau_p^2=\alpha,s_{pr}^v=\varpi|\beta,\epsilon)\\ &\mathbb{P}(s_{pr}{=}\delta|\beta,\epsilon)\mathbb{P}(\tau_p^1{=}y|n_t)\\ &\mathbb{P}(v_{np}{=}\epsilon|n_v)\mathbb{P}(n_s,n_t,n_v|n_0,s_0,t_0)\\ &\mathbb{P}(t{=}t_0)\mathbb{P}(s{=}s_0)\mathbb{P}(n{=}n_0)\,,\end{aligned} \tag{24}$$

Substituting (22)-(24) into (21). we obtain $\mathbb{P}(\tau_{pr}=x)$. The expected value of τ_{pr}, denoted by $\mathbb{E}(\tau_{pr})$, is given by

$$\mathbb{E}(\tau_{pr})=\sum x\,\mathbb{P}(\tau_{pr}=x)\,. \tag{25}$$

Next, we present the joint utility of PAL and GAA devices.

A. JOINT UTILITY OF PAL AND GAA DEVICES

Let initially the SAS allocated one channel each to s PAL and τ GAA devices. However, s_p PAL devices are perturbed due to incumbents. The τ_p GAA devices are perturbed due to incumbents and relocation of PAL devices. Then, s_{pr} PAL and τ_{pr} GAA devices are relocated on the available set of channels. Let s_{np} and τ_{np} denote the number of non-perturbed PAL and GAA devices, respectively. Then, $s_{np}=s-s_p$ and $\tau_{np}=\tau-\tau_p$. We use s_{ps} (respectively τ_{ps}) to denote the perturbed PAL (respectively GAA) devices which could not be relocated and have to defer their transmission until the availability of an unoccupied channel. Thus, $s_{ps}=s_p-s_{pr}$ and $\tau_{ps}=\tau_p-\tau_{pr}$. We consider the maximal contribution from the non-perturbed devices as their transmissions are unaffected by the presence of incumbents. We also consider the contribution of relocated devices since they continue to transmit after switching to another channel. However, switching delay and signaling overhead for switching can be considered as an additional cost borne by relocated devices as compared to non-perturbed devices. Thus, we characterize the joint utility of PAL and GAA devices as the number of actively transmitting PAL and GAA devices which simplifies to the number of non-perturbed and relocated PAL and GAA devices. Thus, the joint utility of PAL and GAA devices, denoted by U_S, is given by

$$U_S=\omega_1\left(s_{np}+\tau_{np}\right)+\omega_2\left(s_{pr}+\tau_{pr}\right)\,, \tag{26}$$

where, ω_1 (respectively ω_2) is the weight assigned to non-perturbed (respectively relocated) PAL and GAA devices and $\omega_1\geq\omega_2$.

We aim to maximize the joint utility of PAL and GAA devices. The maximization of the number of non-perturbed and relocated devices inherently controls the number of suspended devices since the number of PAL and GAA devices actively transmitting, i.e., s and τ, respectively, is fixed for the slot under consideration. Therefore, the utility of PAL and GAA devices only account for the non-perturbed and relocated devices. Further, the weight assigned for relocated devices can be less than or equal to the weight assigned for non-perturbed devices, depending on whether the network designer incorporates the switching delay and signaling overhead as a performance penalty for relocated devices. Using

(5), (8), (16), (20), (25), and (26), the expected joint utility of PAL and GAA devices, denoted by $\mathbb{E}(U_S)$, is given by

$$\mathbb{E}(U_S)=\omega_1(\mathbb{E}(s_{np})+\mathbb{E}(\tau_{np}))+\omega_2(\mathbb{E}(s_{pr})+\mathbb{E}(\tau_{pr}))\,, \quad (27)$$

where, $\mathbb{E}(s_{np}) = S\eta - \mathbb{E}(s_p)$ and $\mathbb{E}(\tau_{np}) = \mathbb{E}(\tau) - \mathbb{E}(\tau_p)$. Please note that the utility of PAL and GAA devices does not change with the adversary case under consideration. Next, we present the utility of incumbents.

B. UTILITY OF INCUMBENTS

We first present the utility of incumbents for the Case B, wherein, the adversary has compromised all the GAA devices. This implies that the adversary knows the status of channels contained in $\mathcal{M}_t$. The adversary can query SAS to find if a channel is unoccupied [26]. We consider that SAS replies a channel as unoccupied if it is not in use by any device. The channels contained in $\mathcal{M}_s$ are either occupied by incumbents (real or dummy) or PAL devices. Since the adversary in Case B cannot differentiate between the transmissions of incumbents and PAL devices, it cannot segregate the channels occupied by incumbents and PAL devices, and hence, it infers the channels occupied by PAL devices also as belonging to the incumbents. Let $\mathcal{M}_{vp}$ denote the set of channels which are now in use by incumbents but were unoccupied, i.e., $\mathcal{M}_{vp} = \mathcal{M}_v \cap \mathcal{M}_p$. We use $\mathcal{M}_{spr}$ to denote the set of channels on which perturbed PAL devices are relocated. The set of channels which were allocated to GAA devices but are now in use of incumbents and PAL devices is denoted by $\mathcal{M}_{tp}$. Let $\mathcal{M}_{tp1} \subseteq \mathcal{M}_{tp}$ denote the set of channels which are now in use by incumbents but were allocated to GAA devices. Then, the adversary can infer the channels contained in $\mathcal{M}_{spr}$, $\mathcal{M}_{tp1}$, and $\mathcal{M}_{vp}$ as belonging to incumbents in addition to $\mathcal{M}_s$. We use $\mathcal{Z}$ to denote the set of channels on which the adversary can infer the presence of incumbents. Then, for the Case B of the adversary, we have

$$\mathcal{Z} = \mathcal{M}_s \cup \mathcal{M}_{spr} \cup \mathcal{M}_{tp1} \cup \mathcal{M}_{vp}\,. \quad (28)$$

The aim of adversary is to identify one channel in use by real incumbent. Then, the adversary can adopt two potential strategies which are as follows.

- **Strategy 1:** The adversary randomly selects one channel from $\mathcal{Z}$ given by (28).
- **Strategy 2:** The adversary randomly selects a channel from $\mathcal{M}_{tp}$ if $\tau_p > 0$, and from $\mathcal{Z}$ given by (28), otherwise.

The likelihood of incorrectly detecting the channel in use by PAL device as the channel in use by incumbent is higher in Strategy 1 as compared to Strategy 2. This is because $\mathcal{Z}$ contains $\mathcal{M}_s$ and $\mathcal{M}_{spr}$ which contains non-perturbed and relocated PAL devices, respectively. However, in Strategy 2, incorrect identification can happen due to the channels which were allocated to GAA devices but are now in use by PAL devices, when $\tau_p > 0$. If $\tau_p^1 > 0$ but $\tau_p^2 = 0$, the only source of obfuscation are the dummy incumbent channels since no GAA device is perturbed to relocate any PAL device. Thus, intuitively, Strategy 2 appears to be of interest of the adversary as it offers less probability of incorrect identification as compared to Strategy 1. This claim is validated through numerical results in Section V.

Now, we compute the expected utility of incumbents for Strategy 1 for the Case B of the adversary. In Strategy 1, the adversary randomly selects a channel from $\mathcal{Z}$. Therefore, the utility of incumbents, denoted by U_I, is given by

$$U_I = \zeta\left(1-\frac{n}{Z}\right)\,, \quad (29)$$

where, ζ is the proportionality constant and

$$Z = |\mathcal{Z}| = s + s_{pr} + \tau_p^1 + v_p\,. \quad (30)$$

We use $\mathbb{P}(Z = z|n_0)$ to denote the conditional PMF of Z (30), given $n = n_0$. Using (3)-(4), (9)-(10), (12), and (18), we have

$$\begin{aligned}\mathbb{P}(Z=z|n_0) \;=\; & \sum_{n_0,s_0,t_0}\sum_{n_s,n_t,n_v}\sum_{y=n_t}^{\tau}\sum_{\epsilon=0}^{v-n_v}\mathbb{P}(s_{pr}=\delta|\beta,\epsilon)\\ & \mathbb{P}(\tau_p^1=y|n_t)\mathbb{P}(v_{np}=\epsilon|n_v)\times\\ & \mathbb{P}(n_s,n_t,n_v|n_0,s_0,t_0)\times\\ & \mathbb{P}(t=t_0)\mathbb{P}(s=s_0)\,, \end{aligned} \quad (31)$$

where, $\delta = z - y - (v - \epsilon) - s_0$ and $\beta = \tau - y$. Using (2), (29), and (31), $\mathbb{E}(U_I)$ for Strategy 1 is given by

$$\mathbb{E}(U_I)=\sum_{n_0=0}^{N}\sum_{z=n_0}^{M}\zeta\left(1-\frac{n_0}{z}\right)\mathbb{P}(Z=z|n_0)\mathbb{P}(n=n_0). \quad (32)$$

Let us now compute the expected utility of incumbents for the Strategy 2 of the adversary. The utility of incumbents for the Strategy 2 of the adversary, denoted by U_I, is given as

$$U_I = \begin{cases}\zeta\left(1-\frac{n_t}{\tau_p}\right) & \text{if } \tau_p > 0\,,\\ \zeta\left(1-\frac{n}{Z}\right) & \text{otherwise.}\end{cases} \quad (33)$$

We use $\mathbb{P}(Z = z|n_0, \tau_p = 0)$ to denote the conditional PMF of Z, given $n = n_0$ and $\tau_p = 0$. Using (3)-(4), (9)-(10), (12), and (18)-(19), $\mathbb{P}(Z = z|n_0, \tau_p = 0)$ is given by

$$\begin{aligned}\mathbb{P}(Z=z|n_0,\tau_p=0) \;=\; & \sum_{s_0,t_0}\sum_{n_s,n_t,}\sum_{\epsilon=0}^{v-n_v}\\ & \mathbb{P}(\tau_p^2=\alpha,s_{pr}^v=\phi|\beta,\epsilon)\\ & \mathbb{P}(s_{pr}=\delta|\beta,\epsilon)\mathbb{P}(\tau_p^1=0|n_t)\\ & \mathbb{P}(v_{np}=\epsilon|n_v)\\ & \mathbb{P}(n_s,n_t,n_v|n_0,s_0,t_0)\\ & \mathbb{P}(t=t_0)\mathbb{P}(s=s_0)\,, \end{aligned} \quad (34)$$

where, $\alpha = 0$, $\phi = \delta$, $\delta = z - s_0 - (v - \epsilon)$, and $\beta = \tau$. We denote the expected utility of incumbents by I_1 when $\tau_p = 0$. Using (2), (33), and (34), we obtain

$$I_1=\sum_{n_0=0}^{N}\sum_{z=n_0}^{M}\zeta\left(1-\frac{n_0}{z}\right)\mathbb{P}(Z=z|n_0,\tau_p=0)\mathbb{P}(n=n_0). \quad (35)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access

Let I_2 be the expected utility of the incumbents when $\tau_p > 0$. Using (2)-(4), (9)-(10), (12), (18)-(19), and (33), I_2 is given by

$$\begin{aligned} I_2 \quad = \quad & \sum_{n_0,s_0,t_0} \sum_{n_s,n_t,n_v} \sum_{\tau_p=n_t}^{\tau} \sum_{y=n_t}^{\tau_p} \sum_{\epsilon=0}^{v-n_v} \sum_{\delta=0}^{\beta+\epsilon} \zeta\left(1-\frac{n_t}{\tau_p}\right) \\ & \mathbb{P}(\tau_p^2=\alpha, s_{pr}^v=\phi|\delta,\beta,\epsilon)\mathbb{P}(s_{pr}=\delta|\beta,\epsilon) \\ & \mathbb{P}(\tau_p^1=y|n_t)\mathbb{P}(v_{np}=\epsilon|n_v)\mathbb{P}(n_s,n_t,n_v|n_0,s_0,t_0) \\ & \mathbb{P}(t=t_0)\mathbb{P}(s=s_0)\mathbb{P}(n=n_0)\ , \end{aligned} \tag{36}$$

where, $\alpha = \tau_p - y$, $\phi = \delta - \alpha$, and $\beta = \tau - y$. Using (35) and (36), the expected utility of incumbents for Strategy 2 of the adversary, denoted by $\mathbb{E}(U_I)$, is given as

$$\mathbb{E}(U_I) = I_1 + I_2\ . \tag{37}$$

Let us now consider the Case A of the adversary, wherein, the adversary has compromised a subset of GAA devices. Let τ^c and τ^l denote the compromised and non-compromised GAA devices, respectively, such that $\tau^c + \tau^l = \tau$. In this case, we consider that the adversary cannot differentiate between the transmissions of incumbents, PAL devices, and non-compromised GAA devices. This implies that the adversary can infer the presence of incumbents on the channels which are actually in use by non-compromised GAA devices. We use $\mathcal{M}_{tp}^c$ to denote the channels which were allocated to the compromised GAA devices but are now in use by incumbents or PAL devices such that $\mathcal{M}_{tp}^c \subseteq \mathcal{M}_{tp}$. We denote the channels in use by the relocated and non-perturbed non-compromised GAA devices by $\mathcal{M}_{tpr}^l$ and $\mathcal{M}_{tnp}^l$, respectively. Then, for the Case A of the adversary, we have

$$\mathcal{Z} = \mathcal{M}_s \cup \mathcal{M}_{spr} \cup \mathcal{M}_{tp1} \cup \mathcal{M}_{vp} \cup \mathcal{M}_{tpr}^l \cup \mathcal{M}_{tnp}^l\ . \tag{38}$$

Similar to the Case B, the adversary can adopt two potential strategies to select a channel in this case as well which are slightly modified versions of Strategy 1 and 2, mentioned as follows.

- **Strategy 3:** The adversary randomly selects one channel from $\mathcal{Z}$ given by (38).
- **Strategy 4:** The adversary randomly selects a channel from $\mathcal{M}_{tp}^c$ if $\tau_p^c > 0$, and from $\mathcal{Z}$ given by (38), otherwise.

In Strategy 3, the adversary draws a channel randomly from a larger set, i.e., $\mathcal{Z}$ (38), containing the channels in use by incumbents, PAL devices, and non-compromised GAA devices. Whereas, in Strategy 4, the adversary selects a channel randomly from $\mathcal{M}_{tp}^c$ which only contains the channels in use by incumbents and PAL devices, whenever $\tau_p^c > 0$. The adversary selects a channel from $\mathcal{Z}$ if $\tau_p^c = 0$. Therefore, the instances of selecting a channel randomly from $\mathcal{Z}$ are less in Strategy 4 as compared to the Strategy 3. This implies that the likelihood of making an incorrect selection is higher in Strategy 3 as compared to the Strategy 4. We validate this claim through numerical results in Section V. The expected utility of incumbents for both Strategy 3 and 4 can be analysed by combining the approach presented in this work and our previous work, i.e., [11]. In this work, we only present the numerical results for the expected utility of incumbents for Strategy 3 and 4 of Case A of the adversary.

We now consider the SA, i.e., Case C of the adversary. An SA has a list of channels exclusively occupied by incumbents which implies that the channels on which dummy incumbent signals are transmitted are the only source of ambiguity. Thus, for Case C of the adversary, i.e., SA, we have

$$\mathcal{Z} = \mathcal{M}_{sp} \cup \mathcal{M}_{tp1} \cup \mathcal{M}_{vp} = \mathcal{M}_p\ , \tag{39}$$

where, $\mathcal{M}_{sp}$ denotes the set of channels which were allocated to the PAL devices but are now in use of incumbents, i.e., $\mathcal{M}_{sp} = \mathcal{M}_s \cap \mathcal{M}_p$. Then, $Z = s_p + \tau_p^1 + v_p = n + d$. Given $n = n_0$, d is a binomial random variable with parameters $(M - n_0, p)$. Then, the conditional PMF of Z, given $n = n_0$, is given by

$$\mathbb{P}(Z = z|n_0) = \binom{M}{n_0} p^{z-n_0}(1-p)^{M-z}\ . \tag{40}$$

Since $\mathcal{Z}$ in (39) contains the channels in use by either real or dummy incumbents, no scope remains for further filtration, and hence, the adversary has a strategy to attack on the channel in use by real incumbent which is random selection of a channel from $\mathcal{Z}$. Thus, the utility of incumbents is as defined in (29) and the expected utility of incumbents can be obtained by substituting (40) into (32) in place of (31). Please note that the $\mathbb{E}(U_I)$ for an SA is independent of S, T, η, and θ. Next, we discuss the trade-off between utility of incumbents and joint utility of PAL and GAA devices.

C. PRIVACY COMMUNICATIONS TRADE-OFF

The military organization transmits dummy incumbent signals on any channel with probability p. Thus, more obfuscation is achieved with increase in the number of dummy channels. This implies $\mathbb{E}(U_I)$ increases as p increases. However, for larger values of p, the number of non-perturbed and relocated PAL devices reduces as the number of dummy channels increases. Thus, $\mathbb{E}(U_S)$, given by (27), is a decreasing function of p. Therefore, a trade-off exists between the operation frequency privacy of incumbents and availability of resources for PAL and GAA devices. We consider a stringent bound on the privacy of incumbents for the incumbents consist of military radars. Thus, we aim to achieve the optimum value of p which maximizes $\mathbb{E}(U_S)$ while simultaneously satisfying $\mathbb{E}(U_I) \geq \Gamma$, where, Γ denotes the lower bound on the probability of incorrect identification of the operating frequency of a real incumbent by the adversary. Then, the privacy communications trade-off problem is framed as

$$\max_p\ \mathbb{E}(U_S) \text{ s.t. } \mathbb{E}(U_I) \geq \Gamma \text{ and } 0 \leq p \leq 1\ . \tag{41}$$

Let p^* denote the optimum value of p which satisfies (41). It is non-trivial to simplify $\mathbb{E}(U_I)$ and $\mathbb{E}(U_S)$ in closed-form. Hence, p^* is obtained by evaluating (41) numerically for different system parameters. Next, we discuss the utility of incumbents, joint utility of PAL and GAA devices, and privacy communications trade-off for the time based model.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access

V. TIME BASED MODEL: ANALYSIS

We consider that the incumbents stay on the same channel until the packet service is complete. Further, the incumbents having a fresh packet to transmit in a slot randomly select a channel not already in use by the other incumbents in that slot. We observe here that the behaviour of incumbents is homogeneous across the channels. Let us consider only the real incumbents and the case when $N = M$. We can approximate the occupancy of a channel by tagging it to an incumbent which implies that the packet arrival happens on a channel with probability λ_R. This approximation can then be extended to the case $N < M$ by considering that the arrival of a packet happens on a channel with probability $\frac{\lambda_R N}{M}$. Similar approximation holds for the dummy incumbents. Further, the dummy incumbents stay on a channel if the ongoing packet service is interrupted by a real incumbent and resume the service once the real incumbent departs. Thus, the packet dynamics on any channel form a discrete two-class preemptive resume priority queue, wherein, the packets of real and dummy incumbents form higher and lower traffic classes, respectively [27]. Then, the effective arrival rate of packets of real and dummy incumbents, denoted by λ_R^{eff} and λ_D^{eff}, respectively, are given by

$$\lambda_R^{eff} = \frac{\lambda_R N}{M} \text{ and } \lambda_D^{eff} = \frac{\lambda_D D}{M} . \tag{42}$$

We denote the load offered by the real and dummy incumbents on a channel by ρ_R and ρ_D, respectively. Using (42), ρ_R and ρ_D are given by [27]

$$\rho_R = \frac{\lambda_R^{eff}}{\mu_R} \text{ and } \rho_D = \frac{\lambda_D^{eff}}{\mu_D} . \tag{43}$$

Let ρ_T denote the total load offered by the incumbents (real and dummy) on a channel. Using (43), ρ_T is computed as [27]

$$\rho_T = \rho_R + \rho_D . \tag{44}$$

In this context, we next discuss the utility of incumbents.

A. UTILITY OF INCUMBENTS

The set of channels in use by incumbents (real or dummy) in a slot is denoted by $\mathcal{E}$. We consider that an adversary intends to eavesdrop/jam a channel in use by real incumbents in each slot and can adopt two potential strategies for selecting a channel in each slot which are as follows.

- **Strategy 5:** The adversary selects a channel randomly from $\mathcal{E}$.
- **Strategy 6:** The adversary continues to attack the channel it attacked in the previous slot if it is in use by incumbents in the current slot, and makes a random selection from $\mathcal{E}$, otherwise.

A channel is in use by an incumbent (real or dummy) in any slot with probability ρ_T given by (44) [27]. Let E denote the number of channels in use by incumbents, i.e., $E = |\mathcal{E}|$. Then, E is a binomial random variable with parameters (M, ρ_T) and the PMF of E, denoted by $\mathbb{P}(E = e)$, is given by

$$\mathbb{P}(E = e) = \binom{M}{e} \rho_T^e \left(1 - \rho_T\right)^{M-e} . \tag{45}$$

A channel can be occupied by the real incumbent with probability ρ_R given by (43). Given a channel is occupied by an incumbent (real or dummy), the probability that it is occupied by a real incumbent is ρ_R/ρ_T. Let K denote the number of channels occupied by the real incumbents in any slot. The conditional PMF of $K = k$, given $E = e$, is denoted by $\mathbb{P}(K = k|E = e)$ and is given by

$$\mathbb{P}(K = k|E = e) = \binom{e}{k} \left(\frac{\rho_R}{\rho_T}\right)^k \left(1 - \frac{\rho_R}{\rho_T}\right)^{e-k} . \tag{46}$$

In Strategy 5, the adversary selects a channel randomly from $\mathcal{E}$. Given $E = e$ and $K = k$, the adversary makes a correct identification with probability k/e. Then, using (45) and (46), the probability of correct identification of operation frequency of real incumbent in a slot, denoted by I_3, is given by

$$I_3 = \sum_{e=1}^{M} \sum_{k=0}^{K} \frac{k}{e} \, \mathbb{P}(K = k|E = e)\mathbb{P}(E = e) . \tag{47}$$

Using (47), the probability of incorrect identification of the operation frequency of a real incumbent by the adversary in a slot, denoted by $\mathbb{E}(U_I)$, is given by

$$\mathbb{E}(U_I) = 1 - (1 - \rho_T)^M - I_3 , \tag{48}$$

where, $(1 - \rho_T)^M$ is the probability that no channel is in use by incumbents (real or dummy) in a slot, i.e., $\mathbb{P}(E = 0)$. We use Υ to denote the number of slots for which $E > 0$, i.e., atleast one channel is in use by incumbents (real or dummy). In this work, we only present the numerical results for Strategy 6 of the adversary. Next, we discuss the joint utility of PAL and GAA devices.

B. JOINT UTILITY OF PAL AND GAA DEVICES

Let $\mathcal{O}$ denote the set of MNOs and $\mathcal{B}_o$ denote the set of MeNBs of the MNO $o \in \mathcal{O}$. We denote the set of macro user equipments (MUEs) associated with the MeNB b of the MNO o by $\mathcal{U}_{b,o}$. We use $\mathcal{J}$ and $\mathcal{G}_j$ to denote the set of SeNBs and the set of the small cell user equipments (SUEs) associated to the SeNB $j \in \mathcal{J}$, respectively. The SAS allocates the channels to the MNOs and SeNBs and all the MeNBs can simultaneously use the channels assigned to the MNO. Let $\mathbf{X} = [X_o^m]$ and $\mathbf{Y} = [Y_j^m]$ denote the binary channel allocation matrices for MNOs and SeNBs, respectively. $X_o^m = 1$ (respectively $Y_j^m = 1$) if the channel $m \in \mathcal{M}$ is allocated to the MNO o (respectively SeNB j). We consider that a channel is uniquely assigned to an MNO. Two SeNBs can coexist on same channel if the distance between them is larger than the twice of their coverage radius [28]. A SeNB shares a channel with an MNO if its distance from all the MeNBs of the MNO is larger than the coverage radius of an MeNB. Further, the channel fading is assumed

TABLE 2: Modulation and coding scheme [29].

SINR Threshold (dB)	-6.5	-4	-2.6	-1	1	3	6.6	10	11.4	11.8	13	13.8	15.6	16.8	17.6
Efficiency (bits/symbol)	0.15	0.23	0.38	0.60	0.88	1.18	1.48	1.91	2.41	2.73	3.32	3.9	4.52	5.12	5.55

to be flat. The MUEs and SUEs associate to the MeNB and SeNB, respectively, which provides the maximum signal-to-interference-plus-noise ratio (SINR). The link rate achieved by the MUE u associated with the MeNB b of the MNO o is denoted by $r_{u,b,o}$. Similarly, $r_{g,j}$ denotes the link rate achieved by the SUE $g \in \mathcal{G}_j$ associated with the SeNB j. Then, $r_{u,b,o}$ and $r_{g,j}$ are given by

$$r_{u,b,o} = \frac{1}{|\mathcal{U}_{b,o}|} \frac{SC_{OFDM} SY_{OFDM}}{T_{sc}} \sum_{m \in \mathcal{M}} \xi(\gamma^m_{u,b,o}) \,, \quad (49)$$

$$r_{g,j} = \frac{1}{|\mathcal{G}_j|} \frac{SC_{OFDM} SY_{OFDM}}{T_{sc}} \sum_{m \in \mathcal{M}} \xi(\gamma^m_{g,j}) \,. \quad (50)$$

Here, we consider that each MeNB (respectively SeNB) allocates equal time to the associated MUE (respectively SUE), and hence, $1/|\mathcal{U}_{b,o}|$ (respectively $1/|\mathcal{G}_j|$) is the time fraction assigned. SC_{OFDM}, SY_{OFDM}, and T_{sc} denote the number of subcarriers per channel, number of symbols per subcarrier, and time fraction of a subframe, respectively. $\xi(\gamma^m_{u,b,o})$ (respectively $\xi(\gamma^m_{g,j})$) computes the spectral efficiency of the MUE (respectively SUE) in bits/symbol using the adaptive and modulation coding scheme given in Table 2 for various ranges of SINR [29]. The SINR of the MUE and SUE on the channel m, denoted by $\gamma^m_{u,b,o}$ and $\gamma^m_{g,j}$, respectively, are given by

$$\gamma^m_{u,b,o} = \frac{P^m_{u,b,o} h^m_{u,b,o}}{\sum_{\hat{b} \in \mathcal{B}_o \setminus b} P^m_{u,\hat{b},o} h^m_{u,\hat{b},o} + \sum_{j \in \mathcal{J}} P^m_{u,j} h^m_{u,j} + \sigma^2} \,,$$

$$\gamma^m_{g,j} = \frac{P^m_{g,j} h^m_{g,j}}{\sum_{o \in \mathcal{O}} \sum_{b \in \mathcal{B}_o} P^m_{g,b,o} h^m_{g,b,o} + \sum_{\hat{j} \in \mathcal{J} \setminus j} P^m_{g,\hat{j}} h^m_{g,\hat{j}} + \sigma^2} \,.$$

Here, $h^m_{u,b,o}$ (respectively $h^m_{g,j}$) denotes the channel gain for an MUE (respectively SUE) and σ^2 denotes the noise power. $P^m_{u,b,o}$ and $P^m_{g,j}$ denotes the transmission power for an MUE and SUE on a channel m, respectively, and are given by

$$P^m_{u,b,o} = \frac{P_S X^m_o}{3 \sum_m X^m_o} \text{ and } P^m_{g,j} = \frac{P_T Y^m_j}{\sum_m Y^m_j} \,,$$

where, P_S and P_T denote the total transmission power of an MeNB and SeNB, respectively. We consider that MeNB and SeNB distribute power equally among the channels allocated. Further, we have a multiplicative factor of $1/3$ as MeNB allocates equal power to the three sectors.

In this work, we characterize the joint utility of PAL and GAA devices as the sum of the average throughput achieved by an MUE and SUE computed using (49)-(50). The MUEs and SUEs transmit on all the channels allocated to the associated MeNBs and SeNBs, respectively, for the assigned time fraction. Thus, the allocation is required from SAS to the MeNBs and SeNBs. Since all MeNBs can simultaneously use the channels assigned to the MNOs, we need to determine the appropriate $\mathbf{X}$ and $\mathbf{Y}$ matrices specifying the channels allocated by SAS for MNOs and SeNBs, respectively, and we follow the approach given in [30] for the same. We construct a conflict graph, wherein, a vertex is denoted as $(Q, \mathcal{C})$, where, Q denotes a node (either an MNO or SeNB) and $\mathcal{C}$ denotes a set of channels which can be assigned to Q. The set $\mathcal{C}$ for any node Q should satisfy (i) the number of channels assigned to an MNO cannot exceed the number of licenses it holds, (ii) the number of channels assigned to an SeNB cannot exceed the number of channels it requests, (iii) a channel can be assigned to the MNO only if it is within $3550-3650$ MHz, and (iv) a channel cannot be assigned to an MNO and SeNB if it is in use by any incumbent. The weight of a vertex $(Q, \mathcal{C})$ is calculated using the *log-reward* function used in [30] which is $log(1 + |\mathcal{C}|)$. An edge exists between two vertices $(Q_1, \mathcal{C}_1)$ and $(Q_2, \mathcal{C}_2)$ if either $Q_1 = Q_2$ and $\mathcal{C}_1 \neq \mathcal{C}_2$ violating the one assignment per node or atleast a channel is common in $\mathcal{C}_1$ and $\mathcal{C}_2$ when (i) Q_1 and Q_2 are two MNOs, (ii) Q_1 and Q_2 are two conflicting SeNBs, or (iii) Q_1 and Q_2 is a pair of conflicting MNO and SeNB. We then obtain the binary matrices $\mathbf{X}$ and $\mathbf{Y}$ as the maximum weighted independent set of the constructed conflict graph. Let $\mathbb{E}(U_S)$ denote the expected joint utility of PAL and GAA devices obtained after averaging over different locations of eNBs and UEs. Next, we discuss the trade-off between the privacy of operation frequency of incumbents and throughput of PAL and GAA devices.

C. PRIVACY COMMUNICATIONS TRADE-OFF

The arrival of a fresh packet of a dummy incumbent in any slot is more likely as λ_D increases which implies that the likelihood of a dummy incumbent being active on a channel increases with λ_D. This in turn leads to more events of incorrect identification of the operation frequency of real incumbent by an adversary in any slot, and hence, $\mathbb{E}(U_I)$, given by (48), is an increasing function of λ_D. However, as λ_D increases, the incumbents occupy more channels reducing the number of channels available for PAL and GAA devices. As a consequence, the throughput of the PAL and GAA devices drop which implies that $\mathbb{E}(U_S)$ is a decreasing function of λ_D. Thus, there is a trade-off between the privacy of operation frequency of incumbents and throughput of PAL and GAA devices. The privacy communication trade-off problem formulated in the snapshot based model, given by (41), focuses primarily on the operation frequency privacy of incumbents by ensuring that the probability of incorrect identification of operation frequency of real incumbents is never less than a pre-specified threshold. Alternatively, we can jointly focus on the operation frequency privacy of incumbents and throughput of PAL and GAA devices, and hence, we maximise the objective function, denoted by $f(\lambda_D)$, characterized by the product of $\mathbb{E}^*(U_I)$ and $\mathbb{E}^*(U_S)$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access

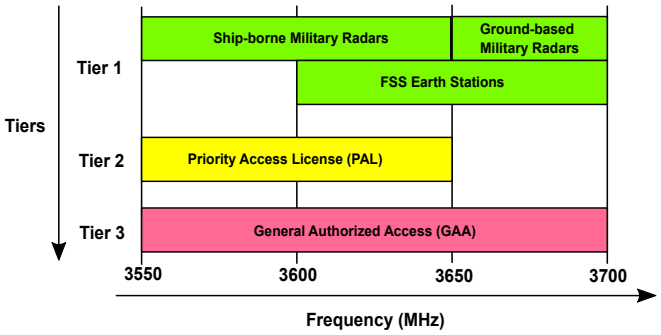


FIGURE 4: Regulation for frequency assignment in CBRS.

which is proportionally fair [31]. Here, $\mathbb{E}^*(U_I)$ and $\mathbb{E}^*(U_S)$ denotes the normalized values of $\mathbb{E}(U_I)$ and $\mathbb{E}(U_S)$, respectively. Thus, the privacy communications trade-off problem for this part is formulated as

$$\max_{\lambda_D} f(\lambda_D) = \mathbb{E}^*(U_I)\mathbb{E}^*(U_S) \text{ s.t. } \lambda_D \in [0, 1) \ . \qquad (51)$$

Please note that $\rho_T < 1$ is a strict requirement for the stability of the queue which determines the maximum permissible value of λ_D [27]. The $\mathbb{E}(U_S)$ is obtained by solving a combinatorial resource allocation problem, and hence, it is non-trivial to obtain the closed-form expression for $\mathbb{E}(U_S)$. Therefore, we next determine the optimum value of λ_D, denoted by λ_D^*, which solves the trade-off problem formulated in (51) numerically.

VI. NUMERICAL RESULTS

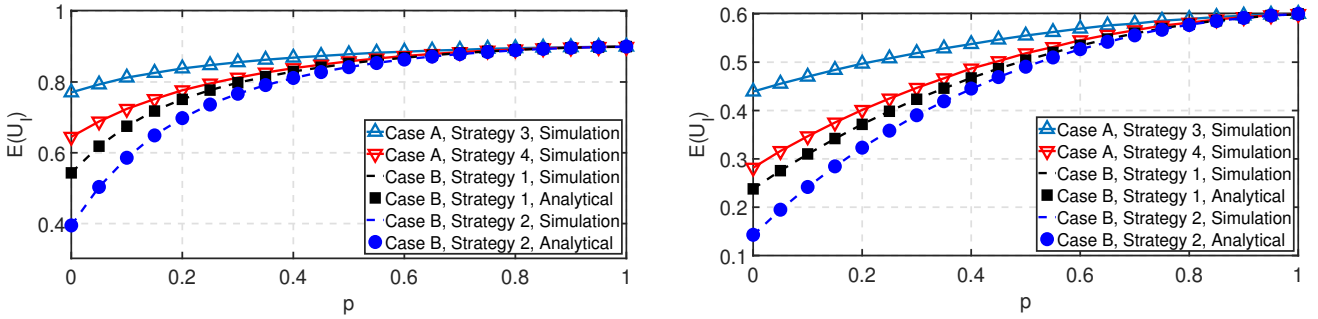
In this section, we first present the numerical results for the snapshot based model obtained via Monte-Carlo simulations performed using MATLAB. The results are averaged over 10^6 iterations. In each iteration, the random instances of number of active real incumbents, dummy incumbents, PAL devices, and GAA devices, i.e., n, d, s, and t, respectively, are generated and relocation of PAL and GAA devices is performed while selecting channels randomly for each real and dummy incumbent. The privacy of military radars is more crucial than that of fixed-satellite-service earth stations which only receive and do not transmit. Therefore, in this work, we only consider military radars as incumbents. Fig. 4 depicts the regulations imposed by the FCC on the assignment of frequencies to the incumbents, PAL devices, and GAA devices. The military ship-borne radars and PAL devices are permitted to operate only within $3550 - 3650$ MHz, as observed from Fig 4 [3]. Further, only one 10 MHz channel can be assigned for a license to a PAL device at an instant of time [3]. Therefore, we consider $M = 10$ and $W = 10$, corresponding to the $3550 - 3650$ MHz band [30]. Thus, τ in (1) corresponds to the number of GAA devices accommodated within $3550 - 3650$ MHz band. The remaining GAA devices can be considered as operating in the $3650 - 3700$ MHz band. We consider that the relocation of the perturbed PAL and GAA devices happen only within the $3550 - 3650$ MHz band. For PAL devices, it is in agreement with the regulations imposed by the FCC. However, we extend this consideration to GAA devices also for ease of analysis. The physical scenarios which validate the relevance of this consideration are as follows. The ground-based radars located at radio location sites mentioned in [3] and grandfathered wireless broadband licensees operate in $3650 - 3700$ MHz with protection radius of 80 and 150 km each [3], [23]. Hence, if they are active in the band, GAA devices located within their protection zone cannot transmit in the band. Some interfering GAA devices can also be actively transmitting in the $3650 - 3700$ MHz band. The number of non-compromised GAA devices, i.e., τ^c, for each iteration is selected as a binomial random variable with parameters (τ, ε), where, ε is selected uniformly randomly distributed within $\{0, ..., 1/\tau, ..., 1\}$ [11]. Table 3 provides details on simulation parameters.

TABLE 3: Simulation Parameters

Snapshot based Model			
N	5	S	7
T	10 [11]	M	10
W	10 [30]	q	0.1
η	0.6	θ	0.6 [11]
ζ	1	Γ	0.9 [11]
Time based Model			
N	5	D	10
M	15	λ_R	0.05
μ_R	0.2	μ_D	0.2
P_S	46 dBm	P_T	30 dBm
σ^2	-99 dBm	SC_{OFDM}	600
T_{sc}	1 ms [29]	SY_{OFDM}	14 [29]

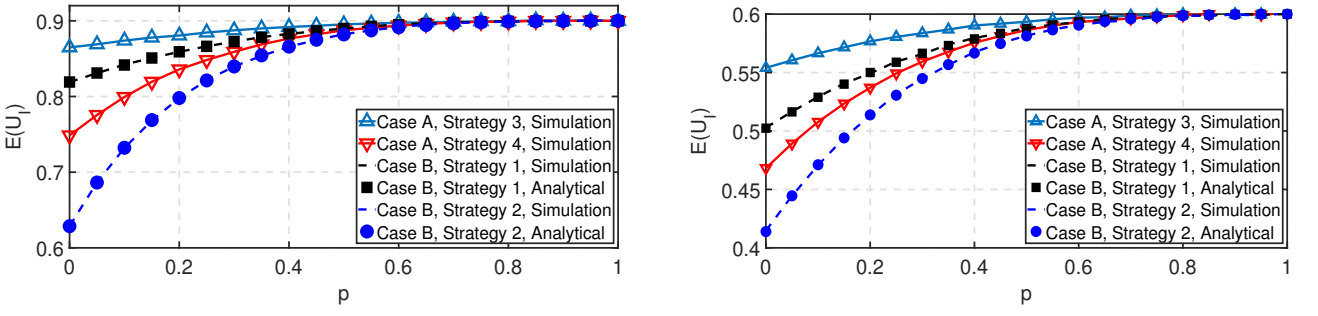
Fig. 5 presents the variation of $\mathbb{E}(U_I)$ for Strategy 1 and 2 of Case B and Strategy 3 and 4 of Case A of the adversary against different values of p at $\eta = 0.2$ for $q = 0.2$ and $q = 0.8$ in Fig. 5a and Fig. 5b, respectively. Similarly, Fig. 6 presents the variation of $\mathbb{E}(U_I)$ for Strategy 1 and 2 of Case B and Strategy 3 and 4 of Case A of the adversary against different values of p at $\eta = 0.6$ for $q = 0.2$ and $q = 0.8$ in Fig. 6a and Fig. 6b, respectively. We observe from Fig. 5 and Fig. 6 that the probability of incorrect identification is less for Strategy 2 (respectively Strategy 4) than Strategy 1 (respectively Strategy 3) for all values of p, q, and η for Case B (respectively Case A) of the adversary, as claimed in Section IV-B. In Case B of the adversary, Strategy 2 benefits the adversary by not accounting the channels in use by all non-perturbed and some relocated PAL devices, and hence, outperforms the Strategy 1. Whereas, in Case A of the adversary, Strategy 4 reduces the instances of deciding the channels in use by non-compromised GAA devices as belonging to the incumbents which leads to lower probability of incorrect identification as compared to the Strategy 3. However, as p increases, the number of dummy channels increases which in turn reduces the number of non-perturbed or relocated PAL devices and non-compromised GAA devices. This limits the benefit of the Strategy 2 (respectively Strategy 4) to the adversary for higher values of p for Case B (respectively Case A). Further, we observe from Fig. 5 and Fig. 6 that the $\mathbb{E}(U_I)$ is higher for Case A of the adversary as compared to the Case B for a fixed value of p, q, and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access



(a) (b)

FIGURE 5: Variation of expected utility of incumbents, $\mathbb{E}(U_I)$, for Strategy 1 and 2 of Case B and Strategy 3 and 4 of Case A of adversary against different values of p at $\eta = 0.2$ for $q = 0.2$ and $q = 0.8$ in (a) and (b), respectively.



(a) (b)

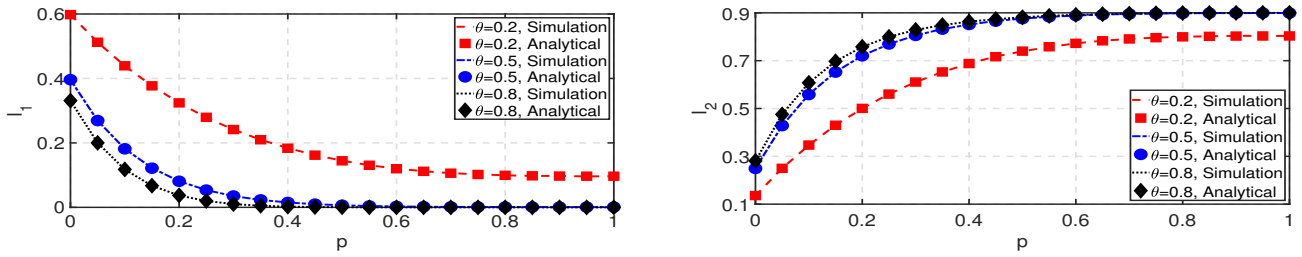
FIGURE 6: Variation of expected utility of incumbents, $\mathbb{E}(U_I)$, for Strategy 1 and 2 of Case B and Strategy 3 and 4 of Case A of adversary against different values of p at $\eta = 0.6$ for $q = 0.2$ and $q = 0.8$ in (a) and (b), respectively.

η. The Case B corresponds to a stronger adversary which has compromised all the GAA devices as compared to the Case A. Unlike Case A, Case B of the adversary does not infer the channels in use by GAA devices as belonging to the incumbents which reduces its probability of incorrect identification of the operation frequency of a real incumbent.

Fig. 7 presents the variation of I_1 (35) and I_2 (36) for different values of p and θ in Fig. 7a and Fig. 7b, respectively. Fig. 8 presents the variation of $\mathbb{E}(U_I)$ for Strategy 2 (37), and $\mathbb{E}(U_I)$ for Strategy 1 (32) for the Case B of the adversary and different values of p and θ in Fig. 8a and Fig. 8b, respectively. In Strategy 2, the adversary selects a channel from $\mathcal{M}_{tp}$ if $\tau_p > 0$, and from $\mathcal{Z}$ (28), otherwise. The event $\tau_p = 0$ implies that no GAA device is perturbed either due to incumbents or PAL devices. The number of active GAA devices increases with increase in θ, and hence, the likelihood of the $\tau_p = 0$ decreases. Thus, $\mathbb{P}(\tau_p = 0)$, given by (17), decreases with increase in θ. This implies I_1 decreases with increase of θ as observed from Fig. 7a. However, as θ increases, τ increases which leads to increase in τ_p and in turn I_2, as observed from Fig. 7b. Since, $\mathbb{E}(U_I)$ for Strategy 2 is a sum of an increasing and decreasing function of θ, we observe from Fig. 8a that $\mathbb{E}(U_I)$ is relatively constant for higher values of θ. At $\theta = 0.2$, $\mathbb{E}(\tau) = 1.9881$. This implies that channels in use by GAA devices are less, and hence, $\mathbb{P}(\tau_p = 0)$ is non-negligible even for larger values of p. This results in slower decay and rise of I_1 and I_2 in Fig. 7a and Fig. 7b, respectively, and also explains slightly different behaviour of $\mathbb{E}(U_I)$ in Fig. 8a. Further, as θ increases, τ increases, and hence, v decreases as $v = M - s - \tau$. Thus, τ_p increases and v_p decreases with increase in θ which results in constant $\mathbb{E}(U_I)$ for Strategy 1 with respect to θ, as observed from Fig. 8b.

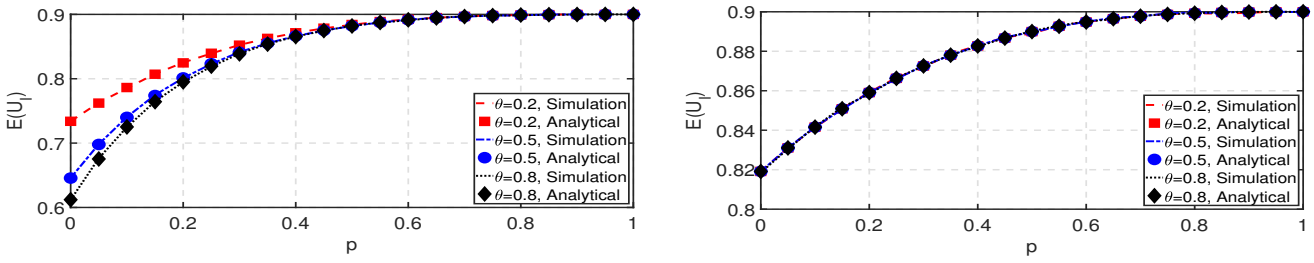
Fig. 9 presents the variation of p^* against different values of η and q for $N = 1$, $S = 7$, and Case A, B, and C of the adversary. Similarly, Fig. 10 presents the variation of p^* against different values of S and q for $N = 2$, $\eta = 0.6$, and Case A, B, and C of the adversary. Please note that the privacy constraint cannot be met for $q > 0.5$ for $N = 2$. Thus, the numerical results are limited to $q \leq 0.5$ in Fig. 10. In Fig. 9, since $N = 1$, either none or only one incumbent can be active at an instant of time. However, as q increases, the likelihood of the presence of the real incumbent on a channel increases and so does the likelihood of the correct identification of the real incumbent's operation frequency by the adversary. More dummy channels are then required to maintain the privacy of real incumbent frequency above the required threshold. Thus, p^* increases with increase in q for a fixed value of η, as observed in Fig. 9. However, as N changes from 1 to 2 in Fig. 10, the number of real incumbent channels increases which in turn increases the probability of correct identification of real incumbent frequency. Thus, we observe an increase in p^* in Fig. 10 as compared to Fig. 9 for Case C of the adversary. We can also observe increase

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access



(a) (b)

FIGURE 7: Variation of I_1 and I_2 for various values of p and θ in (a) and (b), respectively.



(a) (b)

FIGURE 8: Variation of expected utility of incumbent, $\mathbb{E}(U_I)$ for Strategy 2 (37) and expected utility of incumbent, $\mathbb{E}(U_I)$ for Strategy 1 (32) for the Case B of the adversary and various values of p and θ in (a) and (b), respectively.

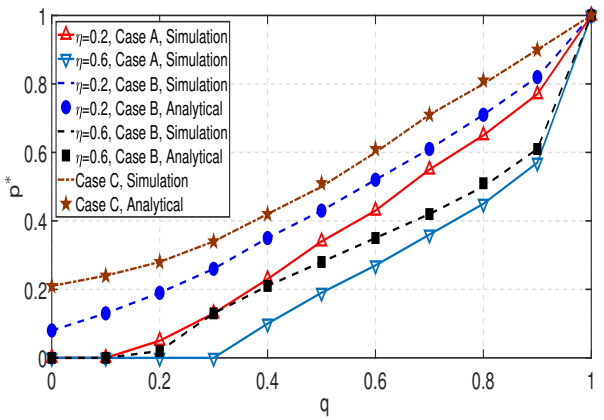


FIGURE 9: Variation of optimum value of p, p^*, against different values of η and q for $N = 1$, $S = 7$, and Case A, B, and C of the adversary.

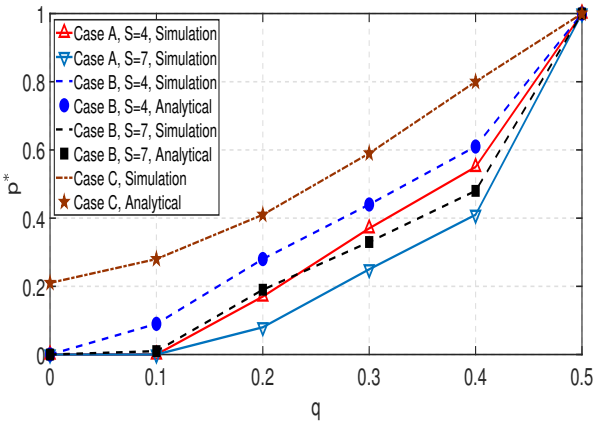
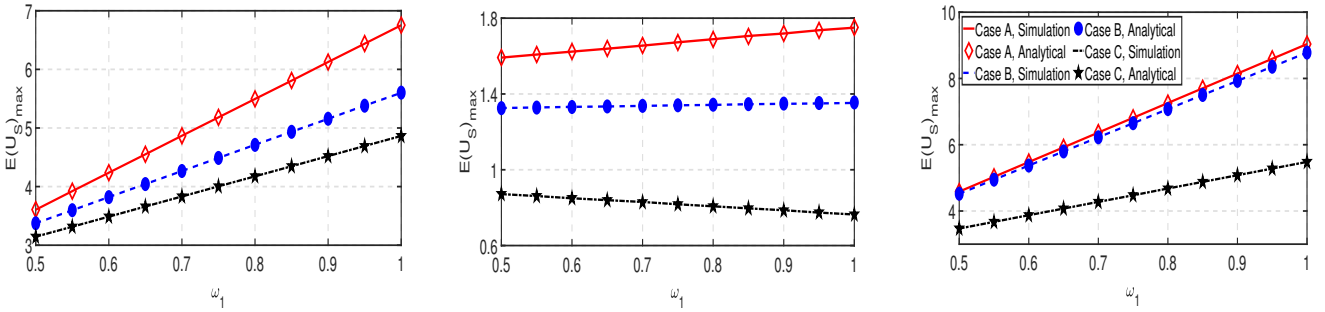


FIGURE 10: Variation of optimum value of p, p^*, against different values of S and q for $N = 2$, $\eta = 0.6$, and Case A, B, and C of the adversary.

in p^* for Case A and B of the adversary for $\eta = 0.6$ and $S = 7$ in Fig. 9 and 10. In Case C of the adversary, the channels on which dummy incumbent signals are transmitted are the only source of ambiguity in the identification of the real incumbent frequency by the adversary which implies that more dummy channels are required to maintain the operation frequency privacy above the required threshold. Thus, p^* is higher for Case C as compared to Case A and B of the adversary. Further, the channels in use by non-compromised GAA devices in Case A add an extra layer of obfuscation in the correct identification of the real incumbent frequency by the adversary as compared to the Case B. This results in higher p^* for Case B than Case A, as observed in Fig. 9 and 10. The number of active PAL devices increases as η increases for a fixed value of S. This leads to the increase in the proportion of relocated PAL devices on the channels which have been allocated to the GAA devices which in turn contributes to the obfuscation of the operation frequency of incumbents. Thus, p^* decreases as η increases for a fixed value of q, as observed in Fig. 9. Same explanation holds for the decrease of p^* with increase in S in Fig. 10. Further, we observe that p^* is zero for smaller values of q and larger values of η (respectively S) in Fig. 9 (respectively Fig. 10) for Case A and B of the adversary. This is because smaller values of q and p result in higher likelihood of $\tau_p = 0$ (respectively $\tau_p^c = 0$) and in turn selection of a channel randomly from $\mathcal{Z}$,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access



(a) (b) (c)

FIGURE 11: Variation of maximum value of $\mathbb{E}(U_S)$, i.e., $\mathbb{E}(U_S)_{max}$, obtained at p^* and $N = 1$, against different values of ω_1 for $q = 0.2$ and $\eta = 0.2$ in (a), $q = 0.8$ and $\eta = 0.2$ in (b), and $q = 0.2$ and $\eta = 0.6$ in (c), respectively. The legends for (a) and (b) are same as in (c).

given by (28) (respectively (38)), by the adversary in Case B (respectively Case A). Thus, the channels in use by PAL and non-compromised GAA devices lead to higher probability of incorrect identification of real incumbent frequency and in turn $p^* = 0$ for Case A and B of the adversary.

Fig. 11 presents the variation of maximum value of $\mathbb{E}(U_S)$, denoted by $\mathbb{E}(U_S)_{max}$, obtained at p^* and $N = 1$, against different values of ω_1 ($\omega_2 = 1 - \omega_1$) for $q = 0.2$ and $\eta = 0.2$ in Fig. 11a, $q = 0.8$ and $\eta = 0.2$ in Fig. 11b, and $q = 0.2$ and $\eta = 0.6$ in Fig. 11c, respectively. The weights ω_1 and ω_2 are assumed to be normalized. Further, we do not consider $\omega_1 < \omega_2$ as we could not identify a scenario, where, relocated devices add more to the system performance than the non-perturbed devices. Thus, we limit our study to $\omega_1 \geq 0.5$ since $\omega_1 \geq \omega_2$ and $\omega_1 + \omega_2 = 1$. The number of channels available for PAL and GAA devices reduces as p increases which in turn reduces their utility. Since p^* is highest for Case C and least for Case A, the $\mathbb{E}(U_S)_{max}$ is maximum for Case A and least for Case C, as observed from Fig. 11. Further, p^* increases as q increases, and hence, $\mathbb{E}(U_S)_{max}$ decreases for each case as q increases from 0.2 in Fig. 11a to 0.8 in Fig. 11b. Similarly, $\mathbb{E}(U_S)_{max}$ increases as η increases from 0.2 in Fig. 11a to 0.6 in Fig. 11c because p^* decreases with η.

We now present the numerical results for the time based model obtained for a total simulation area of 4 km^2. We only consider the military ship-borne radars as incumbents in this work. The packet dynamics of the real and dummy incumbents are simulated via MATLAB for 10^5 slots. Further, we consider two MNOs such that the first and second MNO hold 4 and 3 licenses which implies that they cannot be assigned more than 4 and 3 channels within 3550 − 3650 MHz, respectively. The MeNBs are deployed using the Poisson point process (PPP) with intensity of 5 MeNBs per km^2 for each MNO. The SeNBs are deployed using PPP with the intensity of 10 SeNBs per km^2. We consider that each SeNB requests 2 channels implying that it cannot be assigned more than 2 channels [30]. The coverage radii of MeNB and SeNB are calculated using the received power of −96 dBm and interference power of −80 dBm for a channel of 10 MHz [3]. We consider slot has the duration same as the

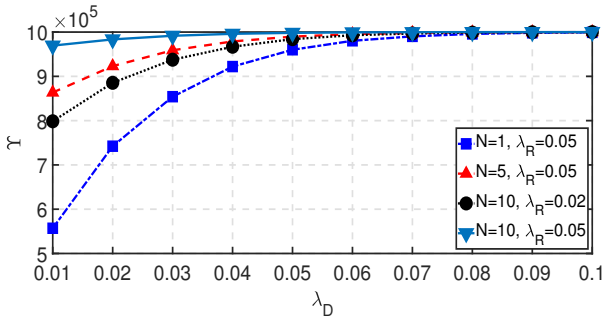


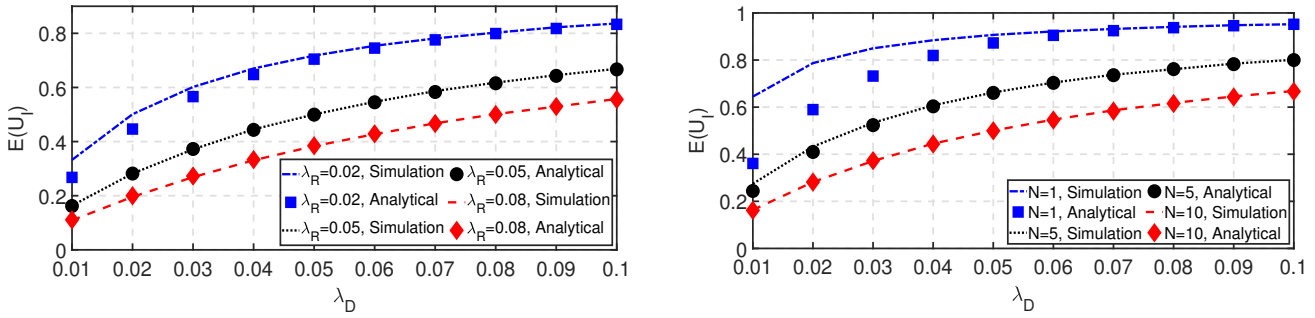
FIGURE 12: Variation of Υ against different values of λ_D for different values of N and λ_R.

subframe in LTE, i.e., 1 ms. [2] The complexity of computation of the link rates for an MUE and SUE over multiple channels for 10^5 slots is high. Therefore, we make the following simplifications for numerical results. (i) The throughput for PAL devices is the average of the throughput of the MUEs associated with an MeNB (nearest to the origin) for each MNO, where, the MUEs are distributed within the central area of 1 km^2 using PPP with intensity of 100 MUEs per km^2. (ii) The throughput of GAA devices is the average of the throughput of SUEs associated with the SeNBs. We consider 5 SUEs per SeNB deployed randomly within the coverage radius of an SeNB calculated using the SINR threshold of −6.5 dB. (iii) We consider that the SeNBs do not share a channel with MNO but can operate on the entire spectrum, i.e., 3550 − 3700 MHz. (iv) The appropriate $\mathbf{X}$ and $\mathbf{Y}$ matrices are obtained using the greedy maximum weighted independent set algorithm [30]. (v) The numerical results of the throughput for MUEs and SUEs are averaged over 5 different realizations of PPP. The urban macro and micro path loss models and directional antenna gain models specified in [32] are used. The channel gain for an MUE and SUE is computed using (2) in [29].

Fig. 12 presents the variation of Υ against different values

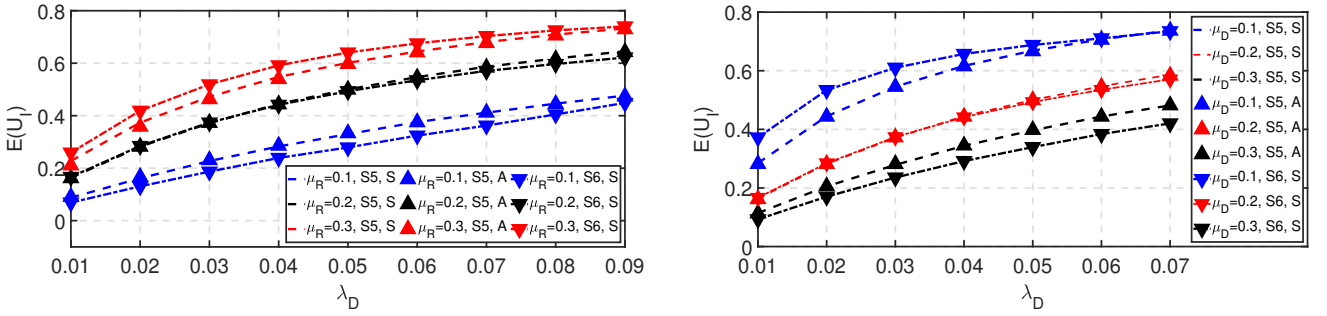
[2]Since the MUEs and SUEs are not mobile in this work, they will experience expected rate (averaged over multiple fading realizations), and hence, the numerical results can be obtained for any slot duration in the similar manner.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access



(a) (b)

FIGURE 13: Variation of expected utility of incumbents for Strategy 5, i.e., $\mathbb{E}(U_I)$, given by (48), against different values of λ_D for $N = 10$ and varying λ_R in (a) and $\lambda_R = 0.05$ and varying N in (b).



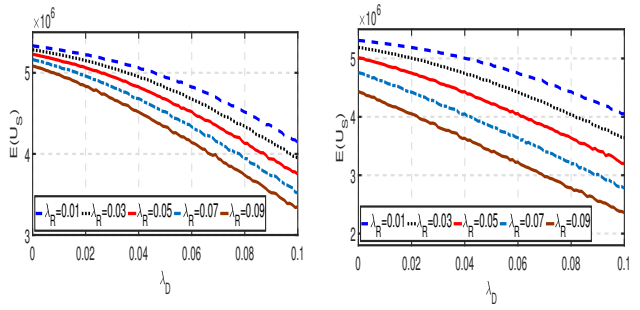
(a) (b)

FIGURE 14: Variation of expected utility of incumbents, i.e., $\mathbb{E}(U_I)$, for Strategy 5 and 6 of the adversary against different values of λ_D for different μ_R and μ_D in (a) and (b), respectively. The acronyms 'S5' and 'S6' in legends of both (a) and (b) denote Strategy 5 and Strategy 6, respectively. The acronyms 'S' and 'A' in legends of both (a) and (b) denote the Simulation and Analytical results, respectively.

of λ_D for different N and λ_R. Fig. 13 presents the variation of $\mathbb{E}(U_I)$, given by (48), for Strategy 5 of the adversary against different values of λ_D for $N = 10$ and varying λ_R in Fig. 13a and $\lambda_R = 0.05$ and varying N in Fig. 13b. The numerical results in Fig. 13 and Fig. 12 are obtained after simulating the packet dynamics of incumbents for 10^6 slots. The ρ_T given by (44) increases as λ_D increases. This in turn reduces the probability of no channel being occupied by incumbents (real or dummy), i.e., $(1 - \rho_T)^M$. Thus, we observe from Fig. 12 that Υ increases with λ_D. Similar holds for the increase of Υ with N and λ_R, as observed from Fig. 12, for ρ_T is an increasing function of N and λ_R for fixed values of λ_D, μ_R, and μ_D. The analytical results in Fig. 13 compute the instances of incorrect identification over the total number of slots, i.e., 10^6. Whereas, the simulation results in Fig. 13 compute the instances of incorrect identification over Υ slots. Thus, we observe a mismatch between analytic and simulation results in Fig. 13 for low-load regime, wherein, Υ is significantly less than 10^6 as illustrated in Fig. 12. The likelihood of the occupancy of a channel by dummy incumbent increases as λ_D increases which in turn increases the uncertainty in the operation frequency of real incumbent for an adversary. Thus, $\mathbb{E}(U_I)$ increases with λ_D as observed in Fig. 13. The packet arrival for real incumbent in a slot is more likely as λ_R increases implying that the probability of a real incumbent being active on a channel increases with λ_R. This leads to more instances of correct identification of real incumbents operation frequency by the adversary, and hence, $\mathbb{E}(U_I)$ decreases as λ_R increases. Similar explanation holds for the decrease of $\mathbb{E}(U_I)$ with N as observed in Fig. 13b.

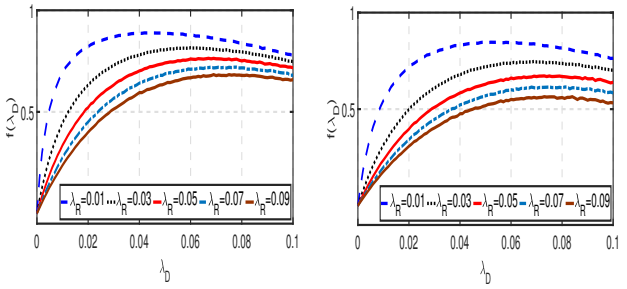
Fig. 14 presents the variation of $\mathbb{E}(U_I)$ for Strategy 5 and 6 of the adversary against different values of λ_D for different μ_R and μ_D in Fig. 14a and Fig. 14b, respectively. The expected packet length of the real incumbent decreases with μ_R which implies that the real incumbent stays on a channel for less number of slots for a packet service as μ_R increases. This decreases the likelihood of correct identification of the operation frequency of real incumbent, and hence, $\mathbb{E}(U_I)$ increases as μ_R increases for both Strategy 5 and 6 of the adversary. The reverse holds for the dummy incumbents, i.e., $\mathbb{E}(U_I)$ decreases with increase in μ_D for both Strategy 5 and 6 of the adversary as the probability of departure of a packet of dummy incumbent in a slot increases with μ_D. Consider the case when $\mu_R = 0.3$ and $\mu_D = 0.2$ as illustrated in Fig. 14a. In this case, the dummy incumbents stay on a channel for longer duration than the real incumbents. In Strategy 6, the adversary continues to attack a channel as long as it is observed to be in use by an incumbent (real or dummy). Whereas, in Strategy 5, the adversary randomly selects a channel in a slot irrespective of its occupancy history. Thus,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3120718, IEEE Access



(a) (b)

FIGURE 15: Variation of expected utility of PAL and GAA devices, i.e., $\mathbb{E}(U_S)$, against different values of λ_D and λ_R for $N = 5$ and $N = 10$ in (a) and (b), respectively.



(a) (b)

FIGURE 16: Variation of objective function $f(\lambda_D)$, (51), against different values of λ_D and λ_R for $N = 5$ and $N = 10$ in (a) and (b), respectively.

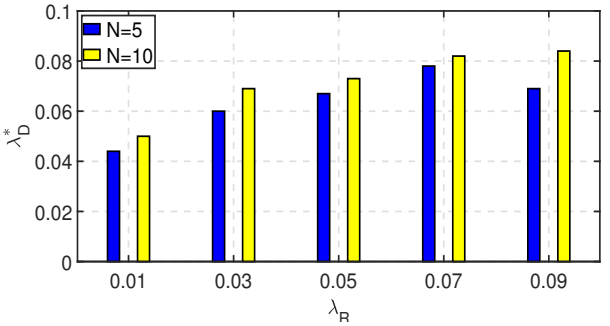


FIGURE 17: Variation of optimum value of λ_D, λ_D^* against different values of λ_R for different values of N.

the random selection in each slot in Strategy 5 benefits the adversary by relatively reducing the instances of incorrect identification than Strategy 6. A similar reasoning can be developed for the mixed trend of Strategy 5 and 6 for the remaining cases in Fig. 14a and Fig. 14b.

Fig. 15 presents the variation of $\mathbb{E}(U_S)$ against different values of λ_D and λ_R for $N = 5$ and $N = 10$ in Fig. 15a and Fig. 15b, respectively. The likelihood of arrival of a packet for real (respectively dummy) incumbents increases as λ_R (respectively λ_D) increases. This implies that the number of channels in use by incumbents (real and dummy) increases and in turn the channels available for the PAL and GAA devices decreases with λ_R and λ_D. Therefore, the throughput of PAL and GAA devices drops as λ_R and λ_D increases. Similarly, we observe $\mathbb{E}(U_S)$ decreases as N increases from 5 in Fig. 15a to 10 in Fig. 15b as the number of channels in use by real incumbents increases with N. Fig. 16 presents the variation of $f(\lambda_D)$, given by (51), against different values of λ_D and λ_R for $N = 5$ and $N = 10$ in Fig. 16a and Fig. 16b, respectively. Fig. 17 presents the variation of λ_D^* for different values of λ_R and N. We observe from Fig. 16 and Fig. 17 that a unique λ_D^* exists which maximises the $f(\lambda_D)$ solving the privacy communication trade-off for different values of λ_R and N. The number of channels in use by real incumbents increases with N which in turn increases the instances of correct identification of the operation frequency of real incumbents. Thus, more channels need to be occupied by the dummy incumbents to boost the probability of incorrect identification of operation frequency of the real incumbent by the adversary, and hence, we observe higher λ_D^* for $N = 10$ than $N = 5$ in Fig. 17.

VII. CONCLUSION AND FUTURE WORK

In this paper, we have studied the operation frequency privacy of the incumbents for a three-tier hierarchical architecture of CBRS. We have proposed that the military organization introduces dummy incumbents on a channel with some probability. The probability of incorrect identification of operation frequency of the real incumbent by the adversary has been analysed for different strategies and varying capabilities of the adversary for the snapshot based model. The operation frequency privacy of incumbents has also been analysed for the time based model while modeling the packet dynamics of real and dummy incumbents via a discrete two-class preemptive resume priority queue. The optimum dummy generation probability has been shown to exist which solves privacy communications trade-off for both snapshot and time based models and different system parameters. In future, we plan to extend the snapshot based model analysis to a more practical scenario by exploiting the spatial relations within the PAL and GAA devices.

REFERENCES

[1] M. R. Hassan et al., "Exclusive use of spectrum access trading models in cognitive radio networks: a survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2192–2231, 2017.

[2] *Report and Order and Second Further Notice of Proposed Rulemaking, Amendment of Commission's Rules With Regard to Commercial Operations in* 3550 − 3650 *MHz Band*, document 12-354, Federal Communication Commission, Apr. 2015.

[3] Electronic Code of Federal Regulations, "Part 96: Citizens' Broadband Radio Service," *Electronic Code for Federal Regulation (eCFR)*, 2019 [Online]. Available: *https://www.ecfr.gov/cgi-bin/text-idx?node=pt47.5.96&rgn=div5*.

[4] *CBRS Operational Security*, WINNF-TS-0071, Version V1.0.0, Wireless Innovation Forum, Jul. 2017.

[5] S. Bhattarai et al., "Thwarting location inference attacks in database-driven spectrum sharing," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 2, pp. 314–327, Jun. 2018.

[6] M. A. Clark and K. Psounis, "Trading utility with privacy in shared spectrum access systems," *IEEE/ACM Trans. Netw.*, vol. 26, no. 1, pp. 259–273, Feb. 2018.

[7] X. He et al., "Camouflaging mobile primary in database driven cognitive

radio networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 21–24, Jun. 2018.

[8] X. Dong et al., "Protecting operation time privacy of primary users in downlink cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6561–6572, Jul. 2018.

[9] J. Wang et al., "Data-driven optimization based primary users' operational privacy preservation," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 2, pp. 357–367, Jun. 2018.

[10] M. A. Clark and K. Psounis, "Optimizing primary user privacy in spectrum sharing systems," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 533–546, Apr. 2020.

[11] P. Agarwal et al., "Privacy preserving scheme for operating frequency of incumbents in citizens broadband radio service," in *Proc. IEEE DySPAN*, Newark, USA, Nov. 2019, pp. 1–10.

[12] L. Xing et al., "An optimized algorithm for protecting privacy based on coordinates' mean value for cognitive radio networks," *IEEE Access*, vol. 6, pp. 21971–21979, May 2018.

[13] Y. Mao et al., "Towards privacy preserving aggregation for collaborative spectrum sensing," *IEEE Trans. Inf. Forensics Security*, vol.12 no. 6, pp. 1483–1493, Jun. 2017.

[14] M. Grissa et al., "Location privacy preservation in database-driven wireless cognitive radios through encrypted probabilistic data structures," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 2, pp. 255–266, Jun. 2017.

[15] W. Wang and Q. Zhang, "Privacy preserving collaborative spectrum sensing with multiple service providers," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1011–1019, Feb. 2015.

[16] Z. Zhang et al., "Bilateral privacy preserving utility maximization protocol in database driven cognitive radio networks," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 236–247, Apr. 2020.

[17] S. M. Errapotu et al., "Bid privacy preservation in matching based in multiradio multichannel spectrum trading," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8336–8347, Sep. 2018.

[18] H. Li et al., "PeDSS: Privacy enhanced and database-driven dynamic spectrum sharing," in *Proc. IEEE INFOCOM*, Paris, France, May 2019, pp. 1477–1485.

[19] Y. Dou et al., "P^2-SAS: privacy-preserving centralized dynamic spectrum access system," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 1, pp. 173–187, Jan. 2017.

[20] Q. Cheng et al., "Preserving honest/dishonest users' operational privacy with blind interference calculation in spectrum sharing systems," *IEEE Trans. Mobile Comput.*, vol. 19, no. 12, pp. 2874–2890, Dec. 2020.

[21] M. Troglia et al., "FaIR: Federated incumbent detection in CBRS band," in *Proc. DySPAN*, Newark, USA, Nov. 2019, pp. 1–6.

[22] E. Drocella et al., "3.5 GHz exclusion zone analyses and methodology," U. S. Department of Commerce, National Telecommunication and Information Administration, USA, NTIA Technical Report 15-517, March 2016. [Online]. Available: https://www.its.bldrdoc.gov/publications/details.aspx?pub=2805

[23] *Requirements for commercial operation in the U.S. 3550-3700 MHz citizens broadband radio service band*, WINNF-TS-0112, Version V1.6.0, Wireless Innovation Forum, Oct. 2018.

[24] A. Azarfar et al., "Delay analysis of multichannel opportunistic spectrum access MAC protocols," *IEEE Trans. Mobile Comput.*, vol. 15, no. 1, pp. 92–106, Jan. 2016.

[25] G. Brown, "Private LTE Networks," Qualcomm/Heavy Reading, White Paper, 2017. [Online]. Available: https://www.qualcomm.com/media/documents/files/private-lte-networks.pdf

[26] *Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS) - Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification*, WINNF-TS-0016, Version V1.2.1, Jan. 2018.

[27] J. Walraevens et al., "Performance analysis of a G1-Geo-1 with a preemptive resume priority scheduling discipline," *European Journal of Operations Research*, vol. 157, no. 1, pp. 130–151, Aug. 2004.

[28] *CBRS Coexistence Technical Specifications*, document CBRSA-TS-2001, V3.1.0, CBRSA, Jul. 2020.

[29] Y. Ramamoorthi and A. Kumar, "Resource allocation for CoMP in cellular networks with base station sleeping," *IEEE Access*, vol. 6, pp. 12620–12633, Mar. 2018.

[30] X. Ying et al., "SAS-assisted coexistence-aware dynamic channel assignment in CBRS band," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6307–6320, Sep. 2018.

[31] A. Kumar and C. Rosenberg, "Energy and throughput trade-offs in cellular networks using base station switching," *IEEE Trans. Mobile Comput.*, vol. 15, no. 2, pp. 364–376, Feb. 2016.

[32] *3GPP Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects (Release 9)*, document TR 36.814, version 9.2.0, Mar. 2017.