Data-Driven Optimization Based Primary Users' Operational Privacy Preservation

Jingyi Wang, *Student Member, IEEE*, Sai Mounika Errapotu, *Student Member, IEEE*, Yanmin Gong, *Member, IEEE*, Lijun Qian, *Member, IEEE*, Riku Jäntti, *Senior Member, IEEE*, Miao Pan, *Member, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*—Recently opened spectrum within 3550–3700 MHz provides more accessing opportunities to secondary users (SUs), while it also raises concerns on the operational privacy of primary users (PUs), especially for military and government. In this paper, we propose to study the tradeoff between PUs' temporal privacy and SUs' network performance using the data-driven approach. To preserve PUs' temporal operational privacy, we develop an obfuscation strategy for PUs, which allows PUs to intentionally add dummy signals to change the distribution of temporal spectrum availability, and confuse the adversary. While generating the dummy signals for privacy, the PUs have to consider the utility of SUs and try their best to satisfy SUs' uncertain traffic demands. Based on the historical data, we employ a data-driven risk-averse model to characterize the uncertainty of SUs' demands. With joint consideration of frequency reuse in the cognitive radio network, PUs' privacy, and uncertain SUs' demands, we employ a conflict graph to characterize the interference relationship between SUs, and formulate the data-driven risk-averse stochastic optimization problem. We provide corresponding solutions and through numerical simulation, we show that the proposed scheme is effective in preserving PUs' temporal operational privacy while offering good enough spectrum resources to satisfy SUs' traffic demands.**

***Index Terms*—PUs' temporal operational privacy, SUs' traffic demands, data-driven modeling and optimization, obfuscation strategy.**

Manuscript received November 18, 2017; revised March 30, 2018; accepted May 5, 2018. Date of publication May 17, 2018; date of current version June 19, 2018. This work was supported in part by the U.S. National Science Foundation under grants U.S. CNS-1343361, CNS-1350230 (CAREER), CNS-1646607, CNS-1702850, U.S. MURI, NSF CNS-1717454, and CNS-1731424. The work of L. Qian is supported in part by the U.S. Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)) under agreement number FA8750-15-2-0119. The associate editor coordinating the review of this paper and approving it for publication was Y. Gao. *(Corresponding author: Miao Pan.)*

J. Wang, S. M. Errapotu, and M. Pan are with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77204 USA (e-mail: jwang86@uh.edu; mounika2392@gmail.com; mpan2@uh.edu).

Y. Gong is with the School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK 74078 USA (e-mail: yanmin.gong@okstate.edu).

L. Qian is with the Department of Electrical and Computer Engineering, Prairie View A&M University, Prairie View, TX 77446 USA (e-mail: lijun@hotmail.com).

R. Jäntti is with the Department of Communications and Networking, Aalto University, 02150 Espoo, Finland (e-mail: riku.jantti@aalto.fi).

Z. Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 002447, South Korea (e-mail: zhan2@uh.edu).

Digital Object Identifier 10.1109/TCCN.2018.2837876

I. Introduction

In RECENT years, the exploding increase of mobile wireless devices and the proliferation of wireless services have accelerated the growth in demand for radio spectrum [1]–[3]. With limited unlicensed spectrum, regulators are turning to dynamic spectrum sharing and looking for advanced techniques to improve spectrum utilization. As one promising technology, cognitive radio (CR) [4]–[6] allows secondary users (SUs) to access the idle spectrum in temporal and spatial domain opportunistically, when primary users (PUs) are not active. To further meet the ever-increasing demand for spectrum, Federal Communication Commission (FCC) and National Telecommunications and Information Administration (NTIA) have agreed to open up the 3550-3700 MHz band for unlicensed communications [7], [8]. Note that most frequencies within 3550-3700 MHz are traditionally used by government agencies, e.g., Department of Defense [8], [9], and the operational information (such as time of use, geographical locations, anti-jamming capability, and so on) of government facilities, e.g., military radars, are very sensitive or even classified. Therefore, maintaining the PUs' operational privacy while providing SUs' spectrum accessing opportunities poses great challenges.

A. Related Work

There are several pioneering works about PUs' privacy preservation in existing literature. For example, Clark and Psounis [10] discuss several attack models and PUs' obfuscation strategies, based on the assumption that all the information of PUs and SUs are stored in a database. The adversary might hack the database or compromise SUs' devices to infer PUs' location information. Robertson *et al.* [11] proposed to add false spectrum allocation entries into the database to prevent the adversary from learning the operational privacy of PUs. Bahrak *et al.* [12] use obfuscation methods to develop a pentagon-shaped contour, which envelops the PU's actual contour to hide PU's accurate location. Another approach is to perturb the output with noises to satisfy differential privacy, as proposed by Dwork [13]. Since simply adding noise signals may degrade the performance of collaborative sensing results, Gao *et al.* [14] further proposed a distributed dummy report injection protocol, which jointly prevents the pollution of the aggregation results and preserves location privacy of PUs. Based on attributed-based encryption

techniques, Liu *et al.* [15] developed the query policy for PUs' spectrum usage database to protect PUs' location privacy. In military communications, Fu *et al.* [16] proposed a method that hides traffic characteristics from eavesdroppers by padding the traffic with constant/variable interarrival times, to mitigate the traffic analysis attacks. In addition, there are some previous works related to the time-based traffic model. For instance, Bonald *et al.* [17] show that if the underlaying scheduler is fair, the flow-level (TCP) throughput and delay admit simple time based form, which is independent of the actual inter-arrival distribution between MAC layer packets. However, most existing schemes do not consider the privacy of temporal information such as the time of usage, which are critical for PUs. The temporal operations of PUs might include highly confidential or even classified information (e.g., the operational time of military radars). If such information is obtained by a malicious party, it may jeopardize national security and people's safety. In addition, most of the existing PUs' privacy preserving designs have limited consideration on creating more accessing opportunities to satisfy SUs' traffic demands and improve spectrum utilization, that is the sole purpose of opening up 3550-3700 MHz band for CR communications.

In addition, there are a lot of existing literature works on primary user activity modeling and primary user activity measurement campaigns. For instance, Chen and Oh [18] and Saleem and Rehmani [19] introduce various spectrum occupancy models which extract different statistical properties from the measured data, and discuss the spectrum occupancy prediction which employs moving-average models to predict the channel status at future time instants. Xing *et al.* [20] takes the survey of prediction technique in cognitive radio network (i.e., hidden Markov model-based prediction, multilayer perceptron neural-network-based prediction, etc.), and present that relevant open research challenges. Höyhtyä *et al.* [21] introduce a method to analyze spatial occupancy in location probability metric, and find optimal location for sampling by use of simulated annealing in the article.

From the aspect of the PU, if the PU could precisely predict SU's traffic demands, it can provide better obfuscation strategy. In this way, the PUs can intentionally add dummy signals to obfuscate the attackers[1] while trying their best to satisfy SUs' traffic demands. However, it is a challenging problem to characterize the uncertainty of SUs' traffic demands. Some previous efforts tried to employ robust optimization to address this issue. For instance, Lundén *et al.* [22] proposed a robust computationally nonparametric cyclic correlation estimator, which does not require the distribution information of users' traffic. Gong *et al.* [23] designed an algorithm to search the optimal detection bound considering signal uncertainty. However, the robust optimization approach can be very conservative, since its objective is to minimize the worst case cost or the worst case effectiveness. If PUs add too many dummy signals, according to the overly conservative analysis for privacy preservation, it would reduce the utility of SUs.

[1]It refers to the attackers either hacking into the spectrum usage database or employing multiple SUs to sense in order to learn the PUs' operational parameters [10].

B. Our Contribution

To address these issues, we propose a novel PUs' obfuscation strategy design by formulating the PUs' operational privacy preservation problem as a data-driven risk-averse optimization, and provide robust solutions. Our salient contributions are summarized as follows:

- We introduce a new privacy preserving framework for PUs' obfuscation strategy design, which jointly considers PUs' operational privacy in the temporal domain, the obfuscation cost of PUs, the uncertainty of SUs' demands, and SUs' traffic demand satisfaction under frequency reuse network. Under such a framework, when PUs add dummy signals to obfuscate the adversary, they also need to consider the trade-off between preserving PUs' temporal privacy and satisfying SUs' traffic requirements, and thus cannot arbitrarily generate dummy signals for privacy preserving purposes.
- Under the proposed framework, with abundant historical data of SUs' traffic demands, we allow the PUs to employ data-driven modeling to characterize the uncertainty of SUs' traffic demands. The PUs can build a reference SUs' demand distribution from the historical data, and generate the predicted SUs' demand distribution close to the reference distribution at a certain confidence level. To realize the spectrum reuse under the proposed network, we employ a conflict graph to characterize the transmission interference between SUs, mathematically describe the channel interference relationship between SUs, and employ approximation algorithm to find a sufficiently large number of maximal independent set.
- Based on the modeling of SUs' uncertain traffic demands and temporal operational privacy metrics, we formulate the PUs' temporal privacy preservation problem into a risk-averse two-stage stochastic optimization under spectrum reuse. We develop algorithms for robust solutions, and conduct simulations to verify our theoretical analysis.

The rest of paper is organized as follows. In Section II, we introduce the network model and introduce the related model in the system. In Section III, we formulate the PUs' and SUs' utility function, and an optimization problem to preserve PUs' operational privacy. In Section IV, we develop the solutions to the proposed problem. Simulation results and discussions are presented in Section V, and the conclusion remarks are drawn in Section VI.

II. System Description

A. Network Configuration

As shown in Fig. 1, we consider a CR network [24] consisting of N SU transmission pairs, $\mathcal{N} = \{1, 2, \ldots, i, \ldots, N\}$ and M radars (PUs) transmission pairs, $\mathcal{M} = \{1, 2, \ldots, j, \ldots, M\}$, transmitting over non-overlapping brands from 3550-3770 frequency range. Following the principles of overlay CR network communications [25]–[27], SUs can opportunistically use the band when the PU owning that band is not active, and SUs must evacuate if the PU comes back. Here, we assume each PU is licensed to use a dedicated band, and each SU can only

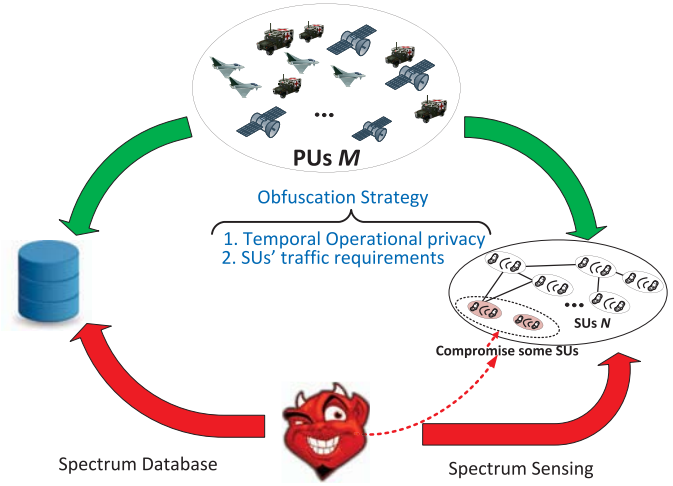


Fig. 1. System architecture and temporal operational attacks.

opportunistically access one band at a time. To preserve temporal operational privacy, PUs will send obfuscating dummy signals periodically, where the fixed period is denoted by $\mathcal{T}$. Let T_j represent the actual temporal spectrum availability for band j (i.e., available time for SUs' opportunistic spectrum accessing before PU j adds dummy signals), and y_j ($y_j \leq T_j$) be the transformed temporal spectrum availability for band j (i.e., the available time for SUs' opportunistic spectrum accessing after PU j adds dummy signals). Given the transmission rate, let a random variable $d_i(\xi)$ denote the required time to deliver the uncertain traffic demands of SU i within $\mathcal{T}$ corresponding to scenario ξ. For simplicity, we call $d_i(\xi)$ the demand of SU i in the rest of this paper, and let $\mathbb{P}_i$ be the distribution of $d_i(\xi)$. For instance, $\mathcal{T} = 60$ mins, and PU j is actively using band j for 20 mins, so that T_j is equal to 40 mins. After PU j executes obfuscation strategy, $y_j = 30$ mins, and the demand of SU i is $d_i(\xi) = 25$ mins.

B. Other Related Model in the System

1) SU's Transmission Range/Interference Range: When primary services are not active over a certain band, SUs can transmit with full power over that band. Suppose all SUs have the same full transmission power P. The power propagation gain [28] is

$$g_i = \gamma \cdot d_i^{-\alpha} \quad (i \in \mathcal{N}), \tag{1}$$

where α is the path loss factor, γ is an antenna related constant, and d_i is the distance between transmitter and receiver of SU pair i.[2] We assume that the data transmission is successful only if the received power at the SU pair's receiver exceeds the receiver sensitivity, i.e., a threshold P_{Tx}. Meanwhile, we assume interference becomes non-negligible only if it is over a threshold of P_{In} at the SU pair's receiver. Thus, the transmission range for a SU is $R_{Tx} = (\gamma P / P_{Tx})^{1/\alpha}$, which comes from $\gamma \cdot (R_{Tx})^{-\alpha} \cdot P = P_{Tx}$. Similarly, based on the interference threshold $P_{In} (P_{In} < P_{Tx})$, the interference range for a SU is $R_{In} = (\gamma P / P_{In})^{1/\alpha}$. It is obvious that $R_{In} > R_{Tx}$ since $P_{In} < P_{Tx}$. Typically, the interference range is 2 or 3 times of the transmission range [28], i.e., $\frac{R_{In}}{R_{Tx}} = 2$ or 3. These two ranges may vary with frequency. The conflict relationship between two SU pairs over the same frequency band can be determined by the specified interference range. In addition, if the interference range is properly set, the protocol model can be accurately transformed into the physical model.

[2]The capacity formulation is similar if we consider fading. The major procedure of proposed algorithms will not be changed.

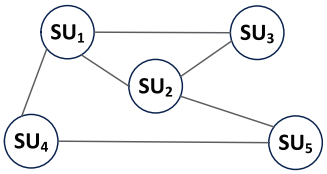


Fig. 2. A toy overall conflict graph observed by a PU.

2) Conflict Graph: We introduce a conflict graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$ to characterize the interference relationship between SUs in the CR network. Following the definitions in [29], we interpret the SU network as a two-dimensional resource space, with dimensions defined by the set of SUs, and the set of available bands. In $\mathcal{G}(\mathcal{V}, \mathcal{E})$, each vertex corresponds to a SU opportunistically accessing a certain band, i.e., a SU-band pair (i, k), where $i \in \mathcal{N}$ and $k \in \mathcal{M}$ [29]. Each SU i stands for a SU transmission pair, including a SU transmitter and a SU receiver from the same SU. Moreover, the distance between transmission pairs is much larger than the distance between transmitter and receiver of SU communication.

Similar to the interference conditions in [28], there is interference if either of the following conditions is true: (i) if two different SUs are using the same band, the receiver of one SU transmission pair is in the interference range of the transmitter in the other SU pair; (ii) a SU pair transmits over two or more bands at the same time. Here, the first condition represents co-band interference, and the second condition represents the radio interface conflicts of SU itself, i.e., the single radio of SU transmitter/receiver cannot support multiple transmissions over multiple bands simultaneously. If there are co-band interferences as shown in the toy conflict graph in Fig. 2, we connect two vertices in $\mathcal{V}$ with an undirected edge in $\mathcal{G}(\mathcal{V}, \mathcal{E})$.

Given $\mathcal{G}(\mathcal{V}, \mathcal{E})$, we describe the impact of vertex $i \in \mathcal{V}$ on vertex $j \in \mathcal{V}$ as follows,

$$\delta_{ik} = \begin{cases} 1, & \text{if there is an edge between vertex } i \text{ and } k, \\ 0, & \text{if there is no edge between vertex } i \text{ and } k, \end{cases} \tag{2}$$

where two vertices correspond to two SU-band pairs, respectively.

To be more specific, in Fig. 2, vertices (SU 1) and (SU 2) stand for SU 1 and SU 2 observed by a PU. They are connected by an edge, which corresponds to the interferences discussed previously. Vertices SU 1 and SU 2 connected through an edge means SU 1 and SU 2 cannot transmit traffic over the spectrum of the PU simultaneously.

3) Maximal Independent Set: Provided that there is a vertex set $\mathcal{I} \subseteq \mathcal{V}$ and a SU-band pair $i \in \mathcal{I}$ satisfying $\sum_{k \in \mathcal{I}, k \neq i} \delta_{ik} < 1$, the transmission at SU-band pair i will be successful even

if all the other SU-band pairs in the set $\mathcal{I}$ are transmitting at the same time. If any $i \in \mathcal{I}$ satisfies the condition above, we can reuse the spectrum frequency, and allow the transmission over all these SU-band pairs in $\mathcal{I}$ to be active simultaneously. Such a vertex/SU-band pair set $\mathcal{I}$ is called an independent set. If adding any one more SU-band pair into an independent set $\mathcal{I}$ results in a non-independent one, $\mathcal{I}$ is defined as a maximal independent set (MIS) [29].

C. Attack Model

In this work, we consider passive adversaries, who may learn the operational time of PUs either from spectrum database or from collective spectrum sensing results of compromised SUs. The compromised SUs do not intercept or modify the messages sent by PUs. Specifically, the adversaries can either eavesdrop the communication between the spectrum database server and SUs, or send queries to the database to learn spectrum availability in the database-driven approach [10], [12], or compromise some SUs' devices and collect spectrum sensing[3] results to infer PUs' operational characteristics in the spectrum sensing approach [10], as shown in Fig. 1.

III. Obfuscation Strategy and Problem Formulation

A. Utility Functions of PUs and SUs

From the PU's perspective, to preserve the temporal operational privacy from passive attackers, the PU executes obfuscation strategy by generating dummy signals for a certain time period when it actually has no traffic. As a result, the adversary cannot distinguish dummy signals from true signals, by database or collective spectrum sensing. Thereafter, the adversary would obtain transformed temporal spectrum occupation of the PUs based on detected signals, which is a combination of the dummy and true signals. As long as the dummy signals are sent frequently, the PUs' true operations can be hidden in those signals and the operational privacy of PUs can be preserved. Thus, the utility function of PUs' operational privacy preservation can be written as

$$U_{PU_j}(y_j) = c(T_j - y_j), \tag{3}$$

where c is a temporal privacy coefficient, T_j is the actual spectrum availability, and y_j is the transformed spectrum availability after the PU j's obfuscation strategy is executed. We can see that if $(T_j - y_j)$ is sufficiently large, PUs' temporal operational privacy is preserved effectively.

From the SUs' perspective, they attempt to transmit on available spectrum to satisfy their own demand. Since SUs can only observe the transformed spectrum availability of PUs, i.e., the spectrum availability after PUs execute obfuscation strategy, we denote the transformed spectrum availability for SU i over spectrum band j as x_i^j. Assuming the SU's traffic can be perfectly split, we let $\sum_{j=1}^{M} x_i^j$ denote the total available time that SU i can transmit over all spectrum bands. We define $d_i(\xi)$ as the actual time needed to satisfy the traffic demand of SU i. Then, $\min(\sum_{j=1}^{M} x_i^j, d_i(\xi))$ represents the traffic delivery time of SU i. Specifically, when $d_i(\xi) < \sum_{j=1}^{M} x_i^j$, which indicates that the time for delivering the traffic demand is less than the transformed available spectrum supply. Then SU i will only in transmit $d_i(\xi)$ to meet its service demands. On the other hand, if transformed available spectrum supply for SU i is less than its real demand, i.e., $\sum_{j=1}^{M} x_i^j < d_i(\xi)$, then SU i will deliver in $\sum_{j=1}^{M} x_i^j$. The utility function of SU i is $U_{SU_i}(d_i(\xi)) = bE_{\mathbb{P}_i}(\min(\sum_{j=1}^{M} x_i^j \omega_i^j, d_i(\xi)))$. In the network model, the SUs who do not interfere with each other can deliver the traffic on the same spectrum simultaneously. Let ω_i^j denotes the accessing status of SU $i \in \mathcal{N}$ to band $j \in \mathcal{M}$, where $\omega_i^j = 1$ indicates that SU i is opportunistically transmitting over band k, otherwise 0. Given $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ constructed from conflict graph, suppose we can list all MISs as $\mathscr{I} = \{\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_q, \ldots, \mathcal{I}_Q\}$, where Q is $|\mathscr{I}|$, and $\mathcal{I}_q \subseteq \mathcal{V}$ for $1 \le q \le Q$. Based on the definitions, assumptions and mathematical representations of interference relationship among SUs above, the maximization optimization of utility of function of SUs can be formulated as follows.

$$\max_{x,\omega} \quad b\sum_{i=1}^{N} E_{\mathbb{P}_i}\left(\min\left(\sum_{j=1}^{M} x_i^j \omega_i^j, d_i(\xi)\right)\right), \tag{4}$$

$$\omega_i^j \in \{0,1\}, \qquad (i \in \mathcal{N}, j \in \mathcal{M}), \tag{5}$$

$$\sum_{j \in \mathcal{M}} \omega_i^j \le 1, \qquad (i \in \mathcal{N}), \tag{6}$$

$$\omega_i^j \cdot \omega_k^j = 0, \qquad (i,k \in \mathcal{N}, j \in \mathcal{M}, (i,j) \in \mathcal{I}_u, (k,j) \in \mathcal{I}_v, \mathcal{I}_u, \mathcal{I}_v \in \mathscr{I} \text{ and } u \ne v) \tag{7}$$

where ω_i^j is optimization variable, b is the SUs' traffic delivery coefficient when SU i is given, and traffic demand $d_i(\xi)$ follows the distribution $\mathbb{P}_i$. Here, binary value ω_i^j indicates the accessing status of SU i to band j, (6) means that SU i can only access one band at a time due to the radio interference, and (7) presents the SUs who interfere with each other cannot delivery traffic on same band simultaneously.

The optimization above is a mixed-integer linear programming, which is NP-hard to solve. Some previous work proposed random algorithm for MIS search and adopted in [30], which provides a framework to find more MISs with more computation rounds. However, random search algorithm is quite inefficient for a large size MR-MC network, and could result in redundant search (i.e., getting a MIS already found) with high chance. Li *et al.* [31] theoretically develop a polynomial heuristic algorithm to compute set of MISs to better cover the critical MISs in the conflict graph. Moreover, Li *et al.* [31] solve the multi-dimensional conflict graph in the network to maximize capacity, which is the same as our scenario (The PU needs to find MISs to make decision to

[3]Here, we assume SUs use energy detection for spectrum sensing.

accept/reject proposed SUs considering SUs' mutual interference and spectrum reuse). We employ the greedy algorithm in [31] to find out a large number of MISs (e.g., the number is $Z = 10000$) for approximation instead of finding out all the MIS of $\mathcal{G}(\mathcal{V}, \mathcal{E})$, whose complexity is $\mathcal{O}(M^4N^8)$. By employing Z MISs found in $\mathcal{G}$, we can solve the relaxed optimization in (4) by commercial solvers such as CPLEX.

B. PUs' Operational Privacy Preserving Optimization

Based on the utility functions of PUs and SUs, we expect an obfuscation strategy jointly considering PUs' operational privacy preservation and the satisfaction of SUs' uncertain traffic demands. Regardless of the PU's power consumption, generating more dummy signals obviously better protects the PU's operational privacy but reduces the available opportunistic accessing time of the SUs, diminishing the SUs' traffic delivery. Considering the trade-off between PUs' privacy and SUs' utility, we formulate the PUs' obfuscation strategy design into an optimization, a classic two-stage stochastic programming (SP) problem, described as follows[4]:

$$\begin{aligned}\max_{y,x,\omega} \quad & \sum_{j=1}^{M} c\big(T_j - y_j\big) \\ & + b\sum_{i=1}^{N}\mathbb{E}_{\mathbb{P}_i}\left(\min\left(\sum_{j=1}^{M} x_i^j\omega_i^j, d_i(\xi)\right)\right), \qquad (8)\\ \text{s.t.} \quad & \textit{constraints } (5),\ (6), \textit{and } (7)\\ & T_j - y_j \geq \lambda, \qquad (9)\\ & \sum_{i=1}^{N} x_i^j\omega_i^j \leq y_j. \qquad (10)\end{aligned}$$

The function $\min(\cdot, \cdot)$ in (8) considers the influence of PUs' obfuscation strategy $(\sum_{j=1}^{M} x_i^j\omega_i^j)$ on the SUs' traffic delivery time utility. It is not accurate to just let $d_i(\xi)$ denote the SUs' traffic delivery time utility, since the total available time on PU's spectrum may be less than $d_i(\xi)$. The function $\min(\cdot, \cdot)$ in (8) returns the smaller value of $\sum_{j=1}^{M} x_i^j\omega_i^j$ and $d_i(\xi)$. The constraint (10) indicates that total transmission time for SUs over PU *j*'s spectrum should be less than the total transformed available spectrum supply of PU *j*. Besides, to preserve PU *j*'s operational privacy, the time period of the sent dummy signals, i.e., $T_j - y_j$, is then required to be larger than a certain predefined privacy threshold λ, which is a constant, as shown in (9).

Due to the ambiguity in demand, it is practically difficult to know the actual probability distribution of SUs' demands. In this paper, we employ a data-driven approach, i.e., the risk-averse stochastic optimization approach (RA-SP) allowing distribution ambiguity [32], to characterize the uncertainty of SUs' demands. Instead of deriving a true distribution for the unknown parameter ξ, this optimization approach constructs a confident set *D*, which allows the distribution ambiguity to be within *D* under a certain confidence level (e.g., 99%). With RA-SP, considering the worst-case distribution, we can reformulate the problem as follows.

$$\begin{aligned}\max_{y,x,\omega} \quad & \sum_{j=1}^{M} c\big(T_j - y_j\big) \\ & + \min_{\mathbb{P}_i\in D} \sum_{i=1}^{N} b\,\mathbb{E}_{\mathbb{P}_i}\min\left(\sum_{j=1}^{M} x_i^j\omega_i^j, d_i(\xi)\right),\\ \text{s.t.} \quad & \textit{constraints } (5),\ (6), \textit{and } (7)\\ & T_j - y_j \geq \lambda,\\ & \sum_{i=1}^{N} x_i^j\omega_i^j \leq y_j. \qquad (11)\end{aligned}$$

We use a distance measurement proposed in [33] and [34] to quantify the distance between two distributions. Specifically, a predefined distance measure $d(\mathbb{P}_i^0, \mathbb{P}_i)$ is constructed on confident set *D*, where $\mathbb{P}_i^0$ is the reference distribution estimated from historical data, and $\mathbb{P}_i$ is the ambiguous distribution of SU *i*. The distance *d* and confident set *D* can be defined as follows:

$$D = \Big\{\mathbb{P}_i : d_\zeta\Big(\mathbb{P}_i^0, \mathbb{P}_i\Big) \leq \theta\Big\}, \qquad (12)$$

$$d_\zeta\Big(\mathbb{P}_i^0, \mathbb{P}_i\Big) = \sup_{h\in\mathcal{H}}\left|\int_\Omega h d\mathbb{P}_i^0 - \int_\Omega h d\mathbb{P}_i\right|, \qquad (13)$$

where the distance under ζ-structure probability metric is denoted by $d_\zeta(\cdot, \cdot)$, the tolerance is denoted by θ, and $\mathcal{H}$ is a family of real-valued bounded measurable functions on Ω (the sample space on ξ). Tolerance θ is correlated to historical data size. It can be easily inferred that the more historical data that the PU can observe, the tighter *D* would be, and the closer the ambiguous distribution $\mathbb{P}_i$ would be to $\mathbb{P}_i^0$. More details of ζ-structure probability metric will be illustrated in the following section.

IV. Risk-Averse Stochastic Programming for Preserving Temporal Operational Privacy

This section is organized as follows. First, we illustrate the construction of the reference distribution $\mathbb{P}_i^0$ for SU *i*. Then we represent how to determine tolerance θ on the amount of historical data under ζ-structure. Finally we develop algorithms to solve the problem with respect to different probability distance metrics.

A. Reference Distribution

First, the reference distribution $\mathbb{P}_i^0$ is defined as follows:

$$\mathbb{P}_i^0(x \leq X) = \frac{1}{Q}\sum_{q=1}^{Q}\delta_{d_q^0(\xi)}(x). \qquad (14)$$

Suppose we use a set of historical data $\{d_1^0(\xi), d_2^0(\xi), d_3^0(\xi), \cdots, d_Q^0(\xi)\}$ to estimate the reference distribution $\mathbb{P}_0$. We utilize the empirical distribution of the historical data samples to construct $\mathbb{P}_0$. To be specific, the distribution in (14), the indicator variable $\delta_{d_k^0(\xi)}(x)$ is equal to 1 when $d_k^0(\xi) \leq x$,

[4]If consider operational privacy of primary user over different time period, it can be easily extend. Particularly, $y_t + \lambda_t = y_{t+1} + \lambda_{t+1}$.

and 0 otherwise. Then the reference distribution data can be represented by its mass probability p_k^0 which is the ratio of the number of historical data samples matching $d_i(\xi)$ and K, since the supporting space is discrete.

B. Converge Rate Under ζ-Probability Metrics

As described in Section IV, we employ three metrics and solve our problem under these constraints correspondingly. We define ρ (x, y) as the distance between two variables x and y, and n as the dimension of Ω. $\mathbb{P} = \mathcal{L}(x)$ represents random variables x following distribution $\mathbb{P}$. The metrics are derived as follows.

- *Kantorovich Metric:* denoted as $d_K(\mathbb{P}_i^0, \mathbb{P}_i)$, $\mathcal{H} = \{h\colon ||h||_L \leq 1\}$, where $||h||_L\colon = \sup\{h(x) - h(y)/\rho(x,y) : x \neq y \text{ in } \Omega\}$. By the Kantorovich-Rubinstein theorem. the Kantorovich metric is equivalent to the Wasserstein metric. In particular, when $\Omega = R$, let d_w denote the Wasserstein metric, then

$$d_w\Big(\mathbb{P}_i^0, \mathbb{P}_i\Big) = \int_{-\infty}^{+\infty} |F(x) - G(x)| dx, \tag{15}$$

  where F and G are the distribution function derived from $\mathbb{P}_i^0$ and $\mathbb{P}_i$ respectively.
- *Fortet-Mourier Metric:* denoted as $d_{FM}(\mathbb{P}_i^0, \mathbb{P}_i)$, $\mathcal{H} = \{h\colon ||h||_C \leq 1\}$, where $||h||_C\colon = \sup\{h(x) - h(y)/c(x,y)\colon x \neq y \text{ in } \Omega\}$ and $c(x,y) = \rho(x,y) max\{1, \rho(x,a)^{p-1}, \rho(y,a)^{p-1}\}$ for some $p \geq 1$ and $a \in \Omega$. Note that when $p = 1$, Fortet-Mourier metric is the same as Kantorovich metric. The Fortet-Mourier metric is usually utilized as a generalization of Kantorovich metric, with the application on mass transportation problems.
- *Uniform Metric:* denoted as $d_U(\mathbb{P}_i^0, \mathbb{P}_i)$, $\mathcal{H} = \{I_{(-\infty,t]}, t \in R^n\}$. According to the definition, we have $d_U(\mathbb{P}_i^0, \mathbb{P}_i) = \sup_t |\mathbb{P}_i^0(x \leq t), \mathbb{P}_i(x \leq t)|$.

From the definition of metrics and relationships between metrics under ζ-structure, we can derive the convergence property and convergence rate accordingly.

For the uniform metric, the convergence rate can be derived from the Dvoretzky-Kiefer-Wolfowitz inequality [35].

Proposition 1: The convergence rate of the uniform metric for a single dimension case is (i.e., n= 1),

$$\mathbb{P}\Big(d_U\Big(\mathbb{P}_i^0, \mathbb{P}_i\Big) \leq \theta\Big) \geq 1 - \exp\Big(-\frac{\theta^2 Q}{2}\Big). \tag{16}$$

In [32], the converge rate of the Kantorovich metric is shown below.

Proposition 2: For a general dimension case (i.e., $n \geq 1$).

$$\mathbb{P}\Big(d_K\Big(\mathbb{P}_i^0, \mathbb{P}_i\Big) \leq \theta\Big) \geq 1 - \exp\Big(-\frac{\theta^2 Q}{2\varnothing^2}\Big). \tag{17}$$

Therefore we have $\mathbb{P}(d_K(\mathbb{P}_i^0, \mathbb{P}_i) \leq \theta) \geq 1 - \exp(-\frac{\theta^2}{2\varnothing^2} Q) = \eta$, and $\theta = \varnothing\sqrt{2log(1/(1-\eta))/Q}$.

From the relation between the Fortet-Mourier metric and Kantorovich metric, with Proposition 2, we can easily derive the convergence rate of other metrics.

Corollary 1: For a general dimension (i.e., $n \geq 1$), we have

$$\mathbb{P}\Big(d_{FM}\Big(\mathbb{P}_i^0, \mathbb{P}_i\Big) \leq \theta\Big) \geq 1 - \exp\Big(-\frac{\theta^2 Q}{2\varnothing^2 \Lambda^2}\Big). \tag{18}$$

With the convergence rate in (16)-(18), we can calculate the tolerance θ accordingly. For instance, in the Kantorovich metric, we assume the confidence level is η. Therefore, $\mathbb{P}(d_u(\mathbb{P}_i^0, \mathbb{P}_i) \leq \theta)) \geq 1 - \exp(-\frac{\theta^2}{2\varnothing^2} Q) = \eta$ according to (16), and $\theta = \varnothing\sqrt{2log(1/(1-\eta)/Q)}$. After that, we explore how to solve the problem in (11). The sample space is $\Omega = \{\xi^1, \xi^2, \ldots, \xi^Q\}$. The formulation can be simplified as:

$$\begin{aligned}
\max_{y,x,\omega} \quad & \sum_{j=1}^{M} c\big(T_j - y_j\big) \\
& + \min_{p_i^k} \sum_{i=1}^{N}\sum_{k=1}^{K} b p_i^k \min\left(\sum_{j=1}^{M} x_i^j \omega_i^j, d_i(\xi)\right), && (19)\\
\text{s.t.} \quad & (5),\ (6),\ (7), \\
& T_j - y_j \geq \lambda, && (20)\\
& \sum_{i=1}^{N} x_i^j \omega_i^j \leq y_j, && (21)\\
& \sum_{k=1}^{K} p_i^k = 1, \forall i = 1, \ldots, N, && (22)\\
\max_{h_k} \quad & \sum_{k=1}^{K} h_k p_i^{k0} - \sum_{k=1}^{K} h_k p_i^k \leq \theta, \forall h_k : ||h||_\zeta \leq 1, && (23)
\end{aligned}$$

where $|h||_\zeta$ is defined according to different metrics. For the Kantorovich metric and the Bounded-Lipschits metric, $|h_x - h_y| \leq \rho(\zeta^x, \zeta^y)$. For the Fortet-Mourier metric, $|h_x - h_y| \leq \rho(\zeta^x, \zeta^y) \max\{1, \rho(\zeta^x, a)^{p-1}, \rho(\zeta^y, a)^{p-1}\}$. The constraints in (22)-(23) can be summarized as $\sum_k a_{kl} h_k \leq b_{kl}, l = 1, \ldots, L$. To reformulate the constraints, we consider the following problem:

$$\begin{aligned}
\min_{h} \quad & \sum_{k=1}^{K} h_k p_i^{k0} - \sum_{k=1}^{K} h_k p_i^k, && (24)\\
\text{s.t.} \quad & \sum_{k=1}^{K} a_{kl} h_k \leq b_{kl}, l = 1, \ldots, L. && (25)
\end{aligned}$$

The dual problem can be formulated as:

$$\begin{aligned}
\min_{u} \quad & \sum_{l=1}^{L} b_l u_l, && (26)\\
\text{s.t.} \quad & \sum_{l=1}^{L} a_{kl} u_l \geq p_i^{k0} - p_i^k, \forall k = 1, \ldots, V, && (27)
\end{aligned}$$

where u is the dual variable. Accordingly, the problem can be reformulated as follows:

$$\begin{aligned}
\max_{y} \quad & \sum_{j=1}^{M} c\big(T_j - y_j\big) \\
& + \min_{p_i^k} \sum_{i=1}^{N}\sum_{k=1}^{K} b p_i^k \min\left(\sum_{j=1}^{M} x_i^j \omega_i^j, d_i(\xi)\right), && (28)
\end{aligned}$$

Algorithm 1 Algorithm for Obfuscation Strategy

1: **Input:** Historical data $d_1^0(\xi)$, $d_2^0(\xi)$, $d_3^0(\xi)$ from true distribution. Set η as the confident level of *D*.
2: **Output:** Objective value of the added time period of dummy signals.
3: Obtain the reference distribution $\mathbb{P}_0^i(x)$ and tolerance θ based on the historical data.
4: Use the reformulation (SP-M) or (SP-U) to solve the problem.
5: Output the solution.

$$\text{(SP-M) s.t.} \quad (5),\ (6),\ (7),$$

$$T_j - y_j \geq \lambda, \tag{29}$$

$$\sum_{i=1}^{N} x_i^j \omega_i^j \leq y_j \tag{30}$$

$$\sum_{k=1}^{K} p_i^k = 1, \sum_{l=1}^{L} b_l u_l \leq \theta, \tag{31}$$

$$\sum_{l=1}^{L} a_{il} u_l \geq p_i^{k0} - p_i^k, \forall i = 1, \ldots, N. \tag{32}$$

For the Uniform metric, we can have the reformulation from the Uniform metric definition:

$$\max_{y,x,\omega} \quad \sum_{j=1}^{M} c\big(T_j - y_j\big) + \min_{p_i^k} \sum_{i=1}^{N} \sum_{k=1}^{K} b p_i^k \min\left(\sum_{j=1}^{M} x_i^j \omega_i^j, d_i(\xi)\right), \tag{33}$$

$$\text{(SP-U) s.t.} \quad (5),\ (6),\ (7),$$

$$T_j - y_j \geq \lambda, \tag{34}$$

$$\sum_{i=1}^{N} x_i^j \omega_i^j \leq y_j, \tag{35}$$

$$\sum_{k=1}^{K} p_i^k = 1, \forall i = 1, \ldots, N, \tag{36}$$

$$\left|\sum_{k=1}^{l} \left(p_i^{k0} - {p_i}^k\right)\right| \leq \theta, \forall l = 1, \ldots, L. \tag{37}$$

The formulation SP-M and SP-U can be solved by CPLEX, etc. We also summarize the algorithm for the problem in Algorithm 1, and the detailed description of notation is in Table I.

TABLE I
THE LIST OF NOTATIONS

Symbol	Definition
$\mathcal{N}$	Sets of SUs
$\mathcal{M}$	Sets of PUs
T_j	Actual temporal spectrum availability for band j
y_i	Transformed temporal spectrum availability for band j
$d_i(\xi)$	Required time to deliver the uncertain traffic demand of SU i
$\mathcal{G}$	Conflict Graph to characterize the interference relationship among SUs
$\mathcal{V}$	Vertex set in conflict graph $\mathcal{G}$
$\mathcal{E}$	Edge set in conflict graph $\mathcal{G}$
$\mathcal{I}$	Independent set in conflict graph $\mathcal{G}$
ω_i^j	binary variable which indicates if SU i deliver traffic on spectrum j
U	Utility of PUs' operational privacy preservation
b	Traffic delivery coefficient
c	Coefficient of temporal privacy coefficient
x_i^j	Transformed spectrum availability for SU i over spectrum band j
$d_i(\xi)$	Actual traffic time demand for SU i corresponding to scenario ξ
$\mathbb{P}_i$	Real distribution of SU i traffic time demand
$\mathbb{P}_i^0$	Reference distribution of SU i traffic time demand
d_ζ	Distance of two distribution under metric ζ
$\mathcal{D}$	Confidence set
η	Confidence level
θ	Tolerance of the distance between two distributions
Ω	The sample space of ξ
$\varnothing$	The dimension of Ω
x_i^j	transformed spectrum availability for SU i over spectrum band j
ω_i^j	binary variable which indicates if SU_i transmit on PU_j

V. PERFORMANCE EVALUATION

For ease of illustration, in the simulations, we consider a CR network of 1 PU and $|\mathcal{N}| = 20$ SUs, where 20 nodes are randomly deployed in a 1000x1000 m^2 area. Considering the AWGN channel, we assume the noise power σ^2 is 10^{-10} W at all transmitters and receivers. Moreover, we set the path loss factor $\alpha = 4$, the antenna parameter $\gamma = 3.90625$, the receiver sensitivity $P_T = 100\sigma^2 = 10^{-8}$ W and the interference threshold $P_T = 6.25 \times 10^{-10}$ W. We set Z = 10000 as a sufficiently large number for the MISs.

The actual available time of the PU's spectrum is $T = 30$ mins in a particular period $\mathcal{T} = 60$ mins. We set the utility parameter for measuring operational privacy level c to be 3, and the utility parameter for SUs' traffic delivery b to be 5. We assume that traffic demand of all SUs follows a discrete distribution with two scenarios: 10 mins and 20 mins with probabilities 0.4 and 0.6, respectively. We use this distribution to generate the historical data set for simulations.

First, we set the confidence level η to be 98% and the size of historical data varying from 100 to 300, to study the impact of the size of historical data. We also consider two strategies while evaluating performance: with privacy obfuscating strategy ($\lambda = 15$ min) and without obfuscating strategy ($\lambda = 0$). First, considering only one SU in cognitive network, the results are reported in Fig. 3. From the figure, we can observe that the utility of network increases as the size of historical data increases, irrespective of the kind of metric. The intuition behind the results incurs the value θ decreases as the size of historical data increases. Therefore, the optimized problem in (11) becomes less conservative. We can also see that when sample size is 300, the gaps between system

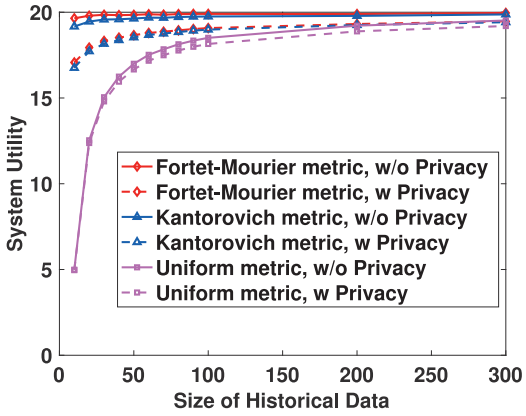


Fig. 3. Impact of size of historical data on system utility (One SU).

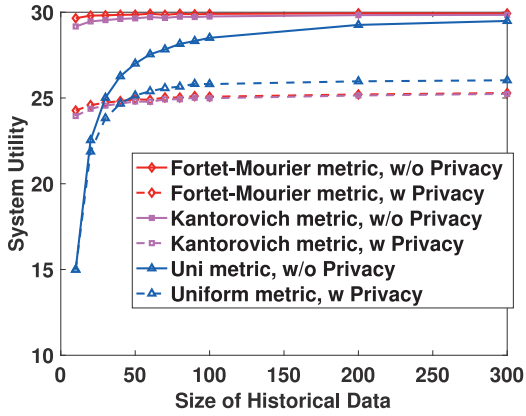


Fig. 5. Impact of historical data on system utility (One SU) under different distribution.

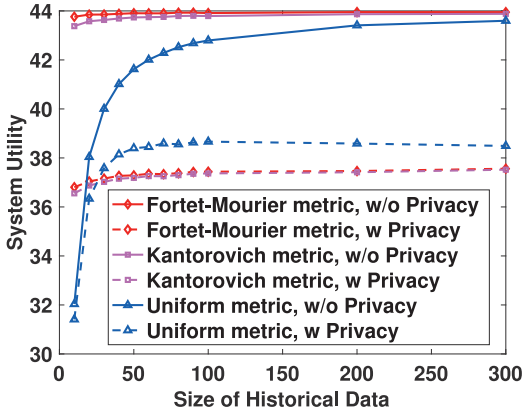


Fig. 4. Impact of size of historical data on system utility (One SU) under different coefficient $c = 1$, $b = 4$.

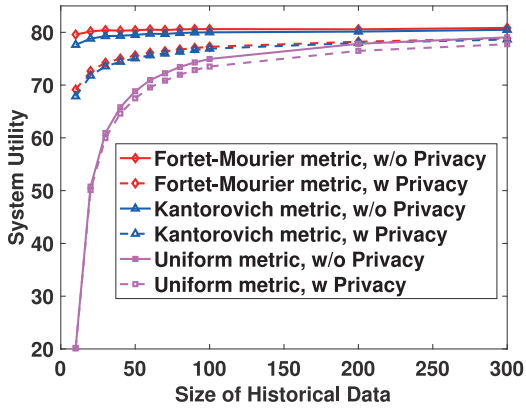


Fig. 6. Impact of historical data on system utility (10 SUs).

utility values are small under all metrics. Moreover, we study the performance under preserving privacy scheme. We set $\lambda = 15$ mins, which indicates that there is at least 15-minute gap between the transformed PUs' spectrum available time and the actual unoccupied period of the PU's spectrum. It can be observed that in Fig. 3, the total utility decreases after employing preservation privacy strategy since the PU's operational privacy preservation is at the cost of reducing accessing opportunities for SUs. We can observe that, as the size of historical data increases, the system utility tends to increase under all metric we use. It is because the value of tolerance θ decreases as the number of historical data sample increases, therefore, the risk-averse stochastic problem becomes less conservative. It is shown that the performance under uniform metric is most influenced by the size of historical data, and the performance under Fortet-Mourier metric is always has the highest system utility in the simulation results. In reality, if PUs are very conservative in the predicted distribution of SUs' traffic demand, it should employ uniform metric. On the other hand, the PUs could employ Fourtet-Mourier or Kantorovich Metric to predict the total system utility. To learn the impact on data set and parameter, we set the different value of coefficient ($c = 1$ and $b = 4$), and the different distribution (10 mins and 20 mins with probabilities 0.2 and 0.8). The result is shown in Fig. 4 and 5. We also have some insights of the system utility under multiple SUs, $|\mathcal{N}| = 10$ in Fig. 6. We can see that the system utility is much higher after considering frequency reuse in the CR network. To be specific, we compare the system utility under uniform metric for different numbers of SUs in Fig. 7. We find that the system utility increases as the number of SUs increases. In Fig. 8, we learn the impact of different numbers of SUs under different metrics. It is shown that as the number of SUs increases, the system utility increases, since the size of maximal independent set is larger when more SUs are in the network. Compared to the situation without privacy preserving, the system utility is always lower with privacy preservation scheme under all metrics. Moreover, the system utility under uniform metric has the worst performance.

In addition, we explore the impacts of dummy signals' time period on the system utility. The total number of historical samples is 300, and λ is set from 10 mins to 20 mins, and the results are shown in Fig. 9. We observe the dummy signal time period increases, the overall system utility under all metrics decreases for chosen PU's privacy coefficient c, SUs' utility coefficient b, and confidence level. The reason is that the contribution of PU's privacy preservation is less important than the deduction of the denied SUs' traffic demands to current system. Also, from Fig. 10, we can see that the system utility with more SUs ($|\mathcal{N}| = 5$) in the network is always higher than the system utility with less SUs ($|\mathcal{N}| = 3$) under the same dummy signals time period. However, for a more

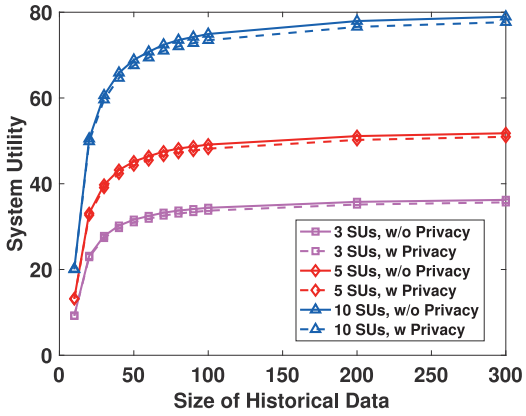


Fig. 7. Impact of size of historical data and different number of SUs under Uniform metric.

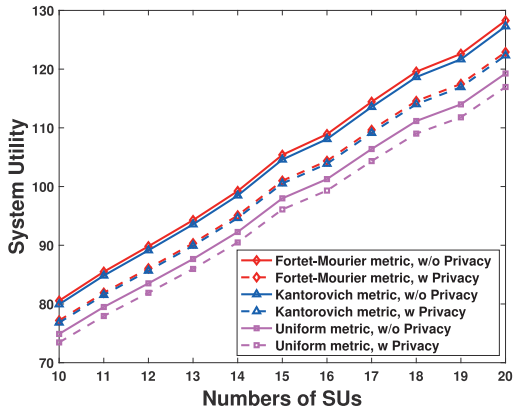


Fig. 8. Impact of different number of SUs on system utility under different metrics.

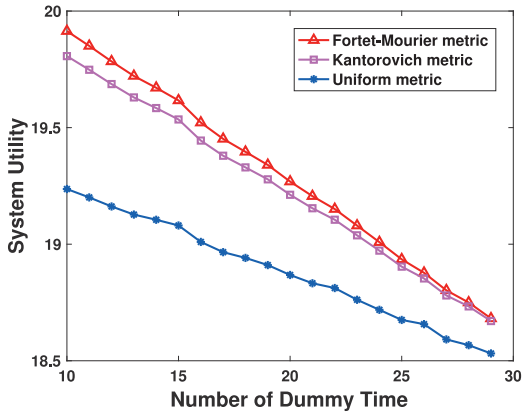


Fig. 9. PU temporal operational privacy and system utility tradeoff, $|\mathcal{N}| = 1$.

PU's privacy oriented system (e.g., $c \gg b$), the system utility may increase while adding more dummy signals. For given PUs' and SUs' utility parameters, the proposed scheme can provide a design guideline for such a CR network considering the trade-off between PUs' temporal operational privacy and SUs' performance.

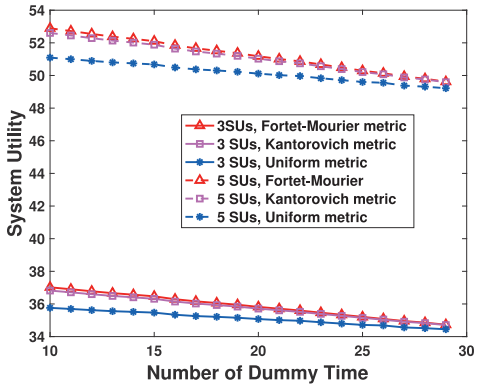


Fig. 10. Temporal operational privacy and system utility tradeoff, $|\mathcal{N}| = 3$ and $|\mathcal{N}| = 5$.

VI. Conclusion

In this paper, we have proposed a novel obfuscation strategy for PUs within 3550-3700 MHz, which has a joint consideration of PUs' temporal operational privacy preservation and SUs' uncertain traffic demands satisfaction under frequency reuse in a cognitive network communication. We have characterized the interference transmission relationship of SUs by constructing conflict graph, and approximation algorithm to find MISs. Moreover we have employed the data-driven risk-averse model in our scheme to characterize SUs' uncertain demand based on the historical data. With such a model, we have formulated the PUs' temporal operational privacy preservation problem into a risk-averse two-stage stochastic optimization. Since the formulated problem is NP-hard to solve, we have relaxed the integer variable and developed a robust algorithm for solutions. Our simulation results to show the effectiveness of the proposed scheme preserving PUs' temporal operational privacy and satisfying SUs' traffic demands. In the future, the research can also be extended as follows. In our current work we considered the assumption that each SU has only one radio interface, hence each SU transmission pair can only access one PU. In the future, we can study the network model with several radio interfaces for each SU transmission pair. Therefore, each SU can deliver traffic on different spectrums simultaneously. Moreover, by considering a much more complicated distribution of SUs' traffic demand, we are interested in achieving the system utility that better meets the practical circumstances. Finally, we can consider the temporal operational privacy in full duplex communication for CRN according to [36] and [37].

Acknowledgment

The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)) or the U.S. Government.

REFERENCES

[1] C. Xu *et al.*, "Efficiency resource allocation for device-to-device underlay communication systems: A reverse iterative combinatorial auction based approach," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 348–358, Sep. 2013.

[2] S. Bregni and L. Jmoda, "Accurate estimation of the hurst parameter of long-range dependent traffic using modified allan and Hadamard variances," *IEEE Trans. Commun.*, vol. 56, no. 11, p. 2224, Nov. 2008.

[3] W. Zhang *et al.*, "Energy-optimal mobile cloud computing under stochastic wireless channel," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4569–4581, Sep. 2013.

[4] A. Rabbachin, T. Q. S. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 480–493, Feb. 2011.

[5] Z. Wang and W. Zhang, *Opportunistic Spectrum Sharing in Cognitive Radio Networks*. Cham, Switzerland: Springer, 2015.

[6] F. Wang, M. Krunz, and S. Cui, "Price-based spectrum management in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 74–87, Feb. 2008.

[7] Y.-C. Liang, K.-C. Chen, G. Y. Li, and P. Mahonen, "Cognitive radio networking and communications: An overview," *IEEE Trans. Veh. Technol.*, vol. 60, no. 7, pp. 3386–3407, Sep. 2011.

[8] S. Zarrin and T. J. Lim, "Throughput-sensing tradeoff of cognitive radio networks based on quickest sensing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[9] Y. Zeng, Y.-C. Liang, A. T. Hoang, and R. Zhang, "A review on spectrum sensing for cognitive radio: Challenges and solutions," *EURASIP J. Adv. Signal Process.*, vol. 2010, no. 1, Dec. 2010, Art. no. 381465.

[10] M. Clark and K. Psounis, "Can the privacy of primary networks in shared spectrum be protected?" in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, San Francisco, CA, USA, Apr. 2016, pp. 1–6.

[11] A. Robertson, J. Molnar, and J. Boksiner, "Spectrum database poisoning for operational security in policy-based spectrum operations," in *Proc. IEEE Military Commun. Conf.*, San Diego, CA, USA, Nov. 2013, pp. 382–387.

[12] B. Bahrak *et al.*, "Protecting the primary users operational privacy in spectrum sharing," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw.*, McLean, VA, USA, Apr. 2014, pp. 236–247.

[13] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.*, Springer, 2008, pp. 1–19.

[14] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Commun.*, vol. 19, no. 6, pp. 106–112, Dec. 2012.

[15] J. Liu, C. Zhang, H. Ding, H. Yue, and Y. Fang, "Policy-based privacy-preserving scheme for primary users in database-driven cognitive radio networks," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–6.

[16] X. Fu, B. Graham, R. Bettati, and W. Zhao, "On effectiveness of link padding for statistical traffic analysis attacks," in *Proc. 23rd Int. Conf. Distrib. Comput. Syst.*, May 2003, pp. 340–347.

[17] T. Bonald, L. Massoulié, A. Proutière, and J. Virtamo, "A queueing analysis of max–min fairness, proportional fairness and balanced fairness," *Queueing Syst.*, vol. 53, nos. 1–2, pp. 65–84, 2006.

[18] Y. Chen and H.-S. Oh, "A survey of measurement-based spectrum occupancy modeling for cognitive radios," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 848–859, 1st Quart., 2016.

[19] Y. Saleem and M. H. Rehmani, "Primary radio user activity models for cognitive radio networks: A survey," *J. Netw. Comput. Appl.*, vol. 43, pp. 1–16, Aug. 2014.

[20] X. Xing, T. Jing, W. Cheng, Y. Huo, and X. Cheng, "Spectrum prediction in cognitive radio networks," *IEEE Wireless Commun.*, vol. 20, no. 2, pp. 90–96, Apr. 2013.

[21] M. Höyhtyä *et al.*, "Spectrum occupancy measurements: A survey and use of interference maps," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2386–2414, 4th Quart., 2016.

[22] J. Lundén, S. A. Kassam, and V. Koivunen, "Robust nonparametric cyclic correlation-based spectrum sensing for cognitive radio," *IEEE Trans. Signal Process.*, vol. 58, no. 1, pp. 38–52, Jan. 2010.

[23] S. Gong, P. Wang, W. Liu, and W. Zhuang, "Performance bounds of energy detection with signal uncertainty in cognitive radio networks," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 2238–2246.

[24] L. Zhang, M. Xiao, G. Wu, S. Li, and Y.-C. Liang, "Energy-efficient cognitive transmission with imperfect spectrum sensing," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1320–1335, May 2016.

[25] F. Akhtar, M. H. Rehmani, and M. Reisslein, "White space: Definitional perspectives and their role in exploiting spectrum opportunities," *Telecommun. Policy*, vol. 40, no. 4, pp. 319–331, 2016.

[26] M. Monemi, M. Rasti, and E. Hossain, "On characterization of feasible interference regions in cognitive radio networks," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 511–524, Feb. 2016.

[27] M. Monemi, M. Rasti, and E. Hossain, "Characterizing feasible interference region for underlay cognitive radio networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 7603–7608.

[28] Y. T. Hou, Y. Shi, and H. D. Sherali, "Spectrum sharing for multi-hop networking with cognitive radios," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 146–155, Jan. 2008.

[29] J. Tang, S. Misra, and G. Xue, "Joint spectrum allocation and scheduling for fair spectrum sharing in cognitive radio wireless networks," *Comput. Netw. Elsevier J.*, vol. 52, no. 11, pp. 2148–2158, Aug. 2008.

[30] K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qiu, "Impact of interference on multi-hop wireless network performance," in *Proc. Mobile Comput. Netw. (Mobicom)*, San Diego, CA, USA, Sep. 2003, pp. 66–80.

[31] H. Li, Y. Cheng, C. Zhou, and P. Wan, "Multi-dimensional conflict graph based computing for optimal capacity in MR-MC wireless networks," in *Proc. Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Genoa, Italy, Jun. 2010, pp. 774–783.

[32] C. Zhao and Y. Guan, "Data-driven risk-averse two-stage stochastic program with ζ-structure probability metrics," *Optim. Online*, vol. 2, no. 5, p. 9, 2015.

[33] G. C. Calafiore, "Ambiguous risk measures and optimal robust portfolios," *SIAM J. Optim.*, vol. 18, no. 3, pp. 853–877, Oct. 2007.

[34] D. Klabjan, D. Simchi-Levi, and M. Song, "Robust stochastic lot-sizing by means of histograms," *Product. Oper. Manag.*, vol. 22, no. 3, pp. 691–710, Feb. 2013.

[35] A. Dvoretzky, J. Kiefer, and J. Wolfowitz, "Asymptotic minimax character of the sample distribution function and of the classical multinomial estimator," *Ann. Math. Stat.*, vol. 27, no. 3, pp. 642–669, 1956.

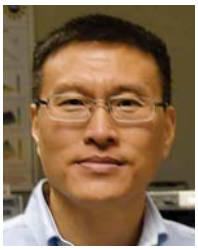
[36] A. N. Kadhim, F. Hajiaghajani, and M. Rasti, "On selecting duplex-mode and resource allocation strategy in full duplex D2D communication," in *Proc. Iran. Conf. Elect. Eng. (ICEE)*, Tehran, Iran, May 2017, pp. 1640–1645.

[37] M. Amjad, F. Akhtar, M. H. Rehmani, M. Reisslein, and T. Umer, "Full-duplex communication in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2158–2191, 4th Quart., 2017.

Jingyi Wang (S'16) received the B.S. degree in physics from Nankai University, China, in 2012 and the M.S. degree in electrical and computer engineering from Auburn University, Auburn, AL, USA, in 2015. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA. Her research interests include privacy preservation of cognitive radio networks, distributed spectrum trading, and wireless big data privacy. She was a recipient of the Best Paper Award in Globecom 2017 for her work on operational PU's privacy.

Sai Mounika Errapotu (S'14) received the B.Tech. degree in electronics and communication engineering from Jawaharlal Nehru Technological University, Hyderabad, India, in 2013. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA. Her research interests include security and privacy in wireless networks and cyber physical systems, differentially private data analysis, privacy in IoT and mobile crowd sourcing applications.

Yanmin Gong (S'10–M'14) received the B.Eng. degree in electronics and information engineering from the Huazhong University of Science and Technology, China, in 2009, the M.S. degree in electrical engineering from Tsinghua University, China, in 2012, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2016. She has been an Assistant Professor with the School of Electrical and Computer Engineering, Oklahoma State University since 2016. Her research interests include information security and privacy and mobile and wireless security and privacy, such as security in Internet-of-Things and privacy-preserving big data analytics. She has served as the Technical Program Committee Member for several conferences, including IEEE INFOCOM, CNS, and ICC. She is a member of ACM.



Lijun Qian received the B.S. degree from Tsinghua University, China, the M.S. degree from the Technion-Israel Institute of Technology, and the Ph.D. degree from Rutgers University. He was a Technical Staff Member with the Networks and Systems Research Department, Bell-Labs, Murray Hill, NJ, USA. He is an AT&T Endowed Professor with the Department of Electrical and Computer Engineering, Prairie View A&M University, a member of the Texas A&M University System. He is also the Director of the Center of Excellence in Research and Education for Big Military Data Intelligence (CREDIT Center) and the Wireless Communications Laboratory. He is a Visiting Professor with Aalto University, Finland. His research interests are in the area of big data processing, wireless communications and mobile networks, network security and intrusion detection, and computational and systems biology.

Riku Jäntti (M'02–SM'07) received the M.Sc. degree (with Distinction) in electrical engineering and the D.Sc. degree (with Distinction) in automation and systems technology from the Helsinki University of Technology (TKK), in 1997 and 2001, respectively. In 2006, he joined the Aalto University School of Electrical Engineering, Finland (formerly known as TKK), where he is an Associate Professor (Tenured) in communications engineering and the Head of the Department of Communications and Networking. He was a Professor pro tem with the Department of Computer Science, University of Vaasa. He is an Associate Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He is also an IEEE VTS Distinguished Lecturer (Class 2016). His research interests include radio resource control and optimization for machine type communications, cloud-based radio access networks, spectrum and co-existence management, and RF inference.

Miao Pan (S'07–M'12) received the B.Sc. degree in electrical engineering from the Dalian University of Technology, China, in 2004, the M.A.Sc. degree in electrical and computer engineering from the Beijing University of Posts and Telecommunications, China, in 2007, and the Ph.D. degree in electrical and computer engineering from the University of Florida in 2012. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Houston. He was an Assistant Professor in computer science with Texas Southern University from 2012 to 2015. His research interests include cognitive radio networks, cyber-physical systems, and cybersecurity. He was a recipient of the Best Paper Awards in Globecom 2015 and Globecom 2017. He is currently an Associate Editor of the IEEE INTERNET OF THINGS JOURNAL.

Zhu Han (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an Assistant Professor at Boise State University, ID, USA. Currently, he is a John and Rebecca Moores Professor in the Electrical and Computer Engineering Department as well as in the Computer Science Department at the University of Houston, TX, USA. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid.

Dr. Han received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the *Journal on Advances in Signal Processing* in 2015, IEEE Leonard G. Abraham Prize in the field of communications systems (Best Paper Award in IEEE JSAC) in 2016, and several best paper awards in IEEE conferences. Currently, he is an IEEE Communications Society Distinguished Lecturer. He is a 1% highly cited researcher 2017 according to Web of Science.