Protecting Operation-Time Privacy of Primary Users in Downlink Cognitive Two-Tier Networks

Xuewen Dong, Yanmin Gong, Jianfeng Ma, and Yuanxiong Guo

***Abstract*—Dynamic Spectrum Sharing (DSS) has a great potential in fully utilizing the scarce spectrum resources, and heterogeneous two-tier network has been regarded as one major solution for achieving it. Without privacy protection in operation-time, however, the primary users will be reluctant to share their spectrum with secondary users. In this paper, we present PriDSS in two-tier wireless networks, the first scheme for the administrator of a dynamic spectrum sharing system to select secondary users in a differentially operation-time private manner. First, we describe the operation-time inference attacks on the traditional secondary users auction without privacy. Then, we bring up a ranking metric to quantify the administrator's preference for secondary users. Moreover, based on the exponential mechanism, we calculate the probability of each secondary user being selected as a winner through the ranking metric. Finally, a truthful payment method is designed according to that probability. Extensively theoretical analysis and evaluations show that PriDSS can simultaneously achieve truthfulness, approximate social welfare maximization, and differential operation-time privacy.**

***Index Terms*—Dynamic spectrum sharing, operation-time privacy, truthful auction, social welfare maximization, differential privacy.**

I. Introduction

RADIO spectrum plays an important role as not only a technological innovation enabler in wireless communications, but also as an economic growth engine. The demand for radio frequency spectrum has greatly increased with the growth in quantity of mobile wireless devices. In order to meet the rising demands of those spectrum starving devices, governments try to explore the feasibility of dynamic spectrum sharing [1]–[3] among increasingly wide variety of applications. For example, in 2015, the Federal Communications Commission of United States issued a declaration that the spectrum band from 3550 MHz to 3700 MHz will be released to new spectrum applications by advanced spectrum sharing systems [4]. Heterogeneous two-tier architecture [5] has been identified as one key solution of spectrum sharing systems. The proposed systems must be guaranteed that a tier of primary users (PUs) must be protect from interference and meanwhile assign spectrum resources dynamically to the lower tier of secondary users (SUs).

Generally, spectrum assignments are decided based on a databases of spectrum management policy and spectrum usage information. However, before the databases of information are used for these sharing systems, primary users have raised concerns that there is a risk of privacy leakage in these systems. Different from the television white space system in which most of the PUs are television broadcasts, plenty of primary systems in 3550 Mhz–3700 MHz belong to government organization, such as, Department of Defense radars. The operation information which is used to assign spectrum resources by a spectrum sharing system, such as frequencies, locations, and operation-time, may be considered very sensitive by the primary users.

The accurate operation-time, the real timeslots that the PUs transmit messages, is very important in the PUs' opinion. Firstly, as pointed out in [6], the operation information, including transmitter identity, location, antenna parameters and operation-time, of primary users is very sensitive. When the primary users belong to federal government, especially military, then the leakage of sensitive information may result in a serious threat to the PUs' privacy. The operation-time privacy problem can be considered as a special case of a more general SAS (Spectrum Access System) privacy framework [7]. Secondly, assumed that there is an adversary who tries to prevent the transmission, if it does not know the accurate operation-time information of PUs, then the adversary has to keep its attacking actions for a long time. As we know that the adversary who launches those attacking actions takes the risk of being detected. The leakage of operation-time privacy of PUs leads to a higher chance for the adversary to prevent the transmission without being detected. Thirdly, if the adversary does not know which channel PUs are using, it has to constantly launch the attack against all PU channels, disrupting both valid and invalid communications. In

Manuscript received July 18, 2017; revised December 2, 2017 and January 22, 2018; accepted February 15, 2018. Date of publication February 21, 2018; date of current version July 16, 2018. This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB1400700, in part by the National High Technology Research and Development Program (863 Program) under Grants 2015AA016007 and 2015AA017203, in part by the Key Program of National Natural Science Foundation of China under Grant U1405255, in part by Shaanxi Science and Technology Coordination and Innovation Project under Grant 2016TZC-G-6-3, in part by the Key Program of NSFC-Guangdong Union Foundation under Grant U1135002, in part by the Fundamental Research Funds for the Central Universities under Grants BDZ011402 and JB180303, in part by the National Natural Science Foundation of China under Grants 61602364, 61602365, and 61602357, and in part by the Natural Science Foundation of Shaanxi Province under Grant 2017JM6083. The review of this paper was coordinated by Prof. J. Deng. *(Corresponding author: Xuewen Dong.)*

X. Dong and J. Ma are with the Shaanxi Key Laboratory of Network and System Security, School of Computer Science and Technology, Xidian University, Xi'an 710126, China (e-mail: xwdong@xidian.edu.cn; jfma@mail.xidian.edu.cn).

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

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2018.2808347

practice, the adversary has limited power and financial resources to perform a constant attack on all channels, then the operation-time information is important for the adversary to reduce the power and financial cost, for it only need to perform the attack when the target PU is transmitting messages. Fourthly, the timeslot, in which the PUs are not using the channel, also should be protected. If the adversary knows the timeslots in which the PU is not transmitting, then it can estimate a rough operation-time, which is the privacy of the PU. In this paper, we aim to protect the operation-time privacy of PUs, and prevent the adversary judging whether the PUs are transmitting messages with one channel in any timeslot or not.

There are a few works that have been conducted on the operation-time privacy of PUs. Bahrak *et al.* have discussed the operation-time inference problem and propose two countermeasures against this inference, including adding random buffer timeslots to forge a longer operation-time interval and grouping an PU's k continuous operation-time intervals into a single operation-time interval [6]. However these two countermeasures just add some simple noises and the adversary still can get the roughly operation-time of PUs. The traditional encryption method can be used to protect the data modification attack, however, it can not be used to protect the operation-time privacy well under a powerful adversary which compromises all the SUs. In that case, the adversary can know all the spectrum assignment results, and can infer the real operation-time of PUs, which we will give an inference attack example in detail in Section IV-B.

To formalize the definition of PUs' operation-time privacy clearly, we leverage the notion of differential privacy [8]–[10]. Differential operation-time privacy can be achieved if the change of an PU's status, whether it uses a channel in a timeslot or not, has limited impact on the final result. We also utilize the exponential mechanism [9] [10], a classic method to design differentially private schemes, to protect PUs' operation-time privacy.

In this paper, we propose a novel scheme PriDSS, in which the administrator can select spectrum-sharing secondary users in a differentially private manner. To our knowledge, this is the first paper which preserves the differential operation-time privacy of PUs in dynamic spectrum sharing system. Our main contributions in this paper are as follows. First, we analyze the SUs selection process without privacy in DSS system and formulate it as an auction problem. Second, under the previous formulation, we demonstrate two operation-time inference attacks. Third, based on exponential mechanism, we present our PriDSS scheme to provide differential operation-time privacy. Finally, we evaluate PriDSS thoroughly by theoretical analysis and simulation studies. Analysis and evaluation results show that PriDSS can achieve the following objectives simultaneously.

- *Differential operation-time privacy:* Through the proposed scheme, even if the adversary knows how the dynamic spectrum sharing scheme works and can obtain all the assignment results of SUs, the adversary can neither judge whether an PU is using a channel or not in a specific timeslot, nor judge which PU is it when it is told that one PU is not using the channel in a timeslot.
- *Approximate social welfare maximization:* PriDSS aims to approximately maximize the social welfare, which is the total valuation of the SUs in the winner set which are allowed to use the sharing channel of PUs.
- *Truthfulness:* Each PriDSS secondary user has no incentive to manipulate the bid value and lie about his valuations.

The remainder of this paper is organized as follows. In Section II, we briefly introduce the related works. The system model and adversary model are presented in Section III. In Section IV, we formulate the SUs selection problem and describe the inference attacks. In Section V, we bring up our PriDSS scheme with differential privacy and carry out performance analysis in Section VI. In Section VII, we thoroughly evaluate the performance of our PriDSS scheme via simulations. At last, we conclude the paper in Section VIII.

II. Related Works

In this section, we briefly introduce the relate works about the privacy protection techniques in cognitive radio networks. Spectrum sensing and spectrum sharing are the most two popular research topics in cognitive radio networks. Firstly, we will introduce some prior privacy protection works in these two topics. Secondly, we present some existing techniques about protecting privacy of PUs. Finally, we introduce some works about differential privacy.

About the privacy protection in spectrum sensing, some excellent schemes have been proposed to protect the location privacy of SUs in spectrum sensing systems [11]–[15]. Most of these schemes aims to protect the physical sensing location information and prevent the administrator from inferring it according to the submitted sensing reports. Gao *et al.* propose a collaborative spectrum sensing scheme with privacy preserving property, in which through cryptographic techniques the fusion center can acquire the aggregated results without leaking each secondary user's private value [12]. Moreover, it bring up a novel sensing data randomization technique which can provide differential location privacy for SUs. Based on differential privacy theory, Jin *et al.* propose a scheme PriCSS which aim of hiding sensing participants' locations in a spectrum-sensing auction [15].

About the privacy protection in spectrum sharing, works focus on protecting the bid privacy of SUs. To solve the spectrum assignment problem while protecting bidders' bid privacy, Huang *et al.* bring up SPRING [16], which is the first privacy-preserving and strategy-proof spectrum auction scheme in noncooperative wireless networks. However, SPRING did not consider the spatial reusability of spectrum. Wu *et al.* design a both strategy-proof and privacy-preserving auction mechanisms for spatial reusable radio frequency spectrum in [17]. Neither of those two works consider the revenue gain of the auctioneer and the privacy of bidders together. By using the graph-partitioning technique and the differential privacy technique, Zhu *et al.* propose a strategy-proof, differentially private and approximate revenue maximization mechanism for spectrum auction in [18].

Only a few works have conducted on protecting the operation parameters privacy of primary users. From the view of PUs

and spectrum administrator, the operation parameter privacy of PUs is very important and the PUs will be reluctant to share their spectrum without operation parameter privacy protection. Considering that the central server is untrustworthy for preserving those sensitive operation data, authors in [19] present a centralized dynamic spectrum access (DSA) system with privacy-preserving property, which realized a complex spectrum assignment process of DSA through efficient secure multi-party computation and homomorphic encryption. Some work aim to protect the location privacy of PUs. Bahrak *et al.* [6] provide several methods to protect the location privacy of PUs, such as: a perturbative masking method, changing the shape of the protected contour, a k-anonymity method which combines protected contours of k PUs and a k-clustering algorithm. Clark and Psounis [20] discuss two obfuscation strategies for PUs' location privacy, including inserting false PU entries into the database and parameter randomization, and found out that the adversary could estimate the accurate locations of PUs after a long-term observation of the assignment results.

As to operation-time privacy of PUs to the best of our knowledge, only [6] has discussed this problem. Authors in [6] propose two countermeasures against operation-time inference, such as adding random buffer timeslots to forge a longer operation-time interval and grouping an PU's k continuous operation-time intervals into a single operation-time interval. Those two countermeasures just add some simple noises and can not provide rigorous privacy protection. The adversary still can infer the roughly operation-time of PUs. In this paper, we want to protect the operation-time privacy of PUs, even though the adversary knows all the assignment results by eavesdropping or some other means.

Recently, differential privacy [8]–[10] has been introduced into cognitive radio network research. The works in [18] and [21] try to combine differential privacy with spectrum auctions. Authors in [15] utilizes differential privacy in spectrum sensing field. By contrast, our work aim to design a dynamic spectrum sharing systems with differential operation-time privacy property.

In conclusion, there are three major differences between our proposed system and existing related works. Firstly, we focus on PUs' privacy instead of SUs' privacy in most literatures. Secondly, compared to a few papers on PUs' privacy, we aim to protect operation-time privacy instead of location privacy. Thirdly, we achieve rigorous privacy using differential privacy while all other works do not provide such guarantee.

III. System and Adversary Model

A. System Model

For simplicity of presentation, we only consider the case of operation-time privacy-preserving DSS for a single channel C in this paper. The major notations used in this paper are listed in Table I.

The PriDSS is run by a trustworthy spectrum administrator. The PriDSS administrator can accept registrations from PUs and answer the queries about spectrum-occupancy from SUs. It runs spectrum assignment algorithm to choose part of secondary users to use the channel C, and tries to maximize its utility from sharing the channel. In general, there are a large quantity of secondary users which compete to access the channel, so we formulate the spectrum assignment problem as an auction and use the social welfare as the utility function of the system administrator. It also acts as a trustworthy "seller" who tries to obtain the maximal social welfare from selling it, and as an auctioneer who selects part of the bidding SUs to use the channel, while guaranteeing that the accumulated interference of SUs to each primary user is less than the interference threshold of it.

TABLE I
Notation Definition

Notation	Definition
PU_m	the mth Primary User, $1 \le m \le M$
I_m^{th}	the interference threshold of PU_m, $1 \le m \le M$
SU_n	the nth Secondary User, $1 \le n \le N$
C	the channel that Primary users share with Secondary Users
v_n	the claimed valuation of SU_n' for the channel C
$\overline{v_n}$	the true valuation of SU_n' for the channel C
ϱ_n	the payment which SU_n makes to the administrator for C
SBS_n	the secondary base station serving SU_n, $1 \le n \le N$
p_n	the power of SBS_n, $1 \le n \le N$
$g_{n,m}$	the gain between SBS_n and PU_m
$d_{n,m}$	the distance between SBS_n and PU_m
$I_{n,m}$	the interference between SBS_n and PU_m, is also the indirect interference between SU_n and PU_m
$\beta_{n,m}$	the ratio of the indirect interference over claimed valuation
SP_m	the indicator of PU_m, PU_m =1 means PU_m is using C
SS_n	the indicator of SU_n, SU_n =1 means SU_n is a winner
I_m^a	the allowable interference of PU_m, $1 \le m \le M$
Ω	the candidate set of secondary users
ε	factors for exponential mechanism of differential privacy
$\triangle$	the maximum input difference for the input SP_m
γ	the maximum number of SUs in the winnerset

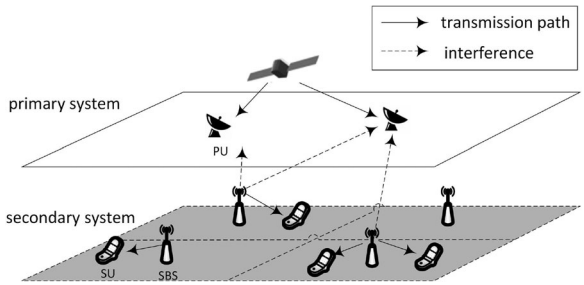

Fig. 1. Cognitive two-tier network model.

As shown in Fig. 1, the primary system and the secondary system of the cognitive two-tier network are located in the same area and we use two levels to describe them for clarity.

The primary system is using the 3550–3700 MHz band for downlinking data, which means transmitting data from the satellite to serval earth station receivers (primary users). There are *M* primary users, who share the single channel *C* in a cooperative way (e.g., TDMA). Each primary user has its interference threshold, which can not be exceeded when sharing the channel *C* with secondary users. The set of primary users is $\overrightarrow{PU} = \{\mathrm{PU}_1, \mathrm{PU}_2, \ldots, \mathrm{PU}_M\}$ with location set $L_{PU} = \{L_{\mathrm{PU}_1}, L_{\mathrm{PU}_2}, \ldots, L_{\mathrm{PU}_M}\}$ and interference threshold set

$I^{\text{th}} = \{I_1^{\text{th}}, I_2^{\text{th}}, \ldots, I_M^{\text{th}}\}$. The secondary system includes several downlink cognitive small-cell base stations (SBS). The SBSs serve the secondary users $\overrightarrow{SU} = \{\text{SU}_1, \text{SU}_2, \ldots, \text{SU}_N\}$ with location set $L_{SU} = \{L_{\text{SU}_1}, L_{\text{SU}_2}, \ldots, L_{\text{SU}_N}\}$, which are interested in the channel *C* and bid for it. Similar to [23], the SBS in each cell serves no more than one secondary user at the same time. Furthermore, the SBSs and the users are all equipped with single antenna. The first tier (the primary system) is unaware of the presence of the second tier, so the two tiers are exclusively independent to each other and there is no cross-tier cooperation between them.

The true valuation of SU_n for the channel C is $\overline{v_n}$, and the bid of SU_n is $b_n = (L_{\text{SU}_n}, v_n)$, where v_n is his claimed valuation to use the channel. We assume v_n is valued in the range of $[v_{\min}, v_{\max}]$, where $v_{\max}$ and $v_{\min}$ are reasonable maximum and minimum possible valuation, respectively. The SBS serving SU_n is denoted as SBS_n. The gain and distance between SBS_n and PU_m is denoted as $g_{n,m}$ and $d_{n,m}$ respectively. The transmitting power of SBS_n is p_n. Since the primary system of two-tier network shares the channel C in a cooperative way (e.g., TDMA) and also shares it with the secondary system, so any transmission between a pair of SBS and SU in the secondary system will produce interference to all the PUs. The interference between SBS_n and PU_m can be calculated as $I_{n,m} = p_n \cdot g_{n,m}$.

We consider the downlink transmission of secondary system, if SU_n is selected as a winner, there must exist a interference $I_{n,m}$ between SBS_n and PU_m. So we call interference $I_{n,m}$ is also the indirect interference between SU_n and PU_m.

It is noted that our system model allows multiple SUs in a cell competing the channel, however, for only one channel are considered to be shared, the SUs in a cell can only be served in a TDMA way. So the SBS in each cell serves no more than one secondary user at the same time. In one cell, if there are multiple SUs competing the only channel in a timeslot, then the indirect interferences between those SUs in that cell and a PU are the same, because the indirect inference between SU_n and PU_m is calculated as $p_n \cdot g_{n,m}$, where p_n is the transmitting power of SBS_n in that cell and $g_{n,m}$ is the gain between SBS_n and PU_m. So the SU with the highest bid in that cell will be chosen to participate the spectrum auction, and other SUs in that cell will be neglected for they have no chance to be allocated with the channel.

In this paper, we discuss the downlink transmission not the uplink transmission of cognitive two-tier networks. The difference between downlink transmission and uplink transmission is that the transmitters (or the receivers) are different. In the secondary system, the transmitters of uplink transmission are the SUs, leading to a little more complicated system model and different computation of the interference, which will be discussed in my future works. The key idea of our proposed method can still be used to protected the operation-time privacy of PUs in uplink cognitive two-tier networks.

B. Adversary Model

In this paper, we try to maximize the ability of the adversary and aim to preserve the operation-time privacy of PUs, even if the adversary nearly has all background knowledge except the operation-time of PUs. In this case, if the adversary still can not deduce the operation-time of PUs from its knowledge and spectrum assignment results, then this PriDSS scheme can be called as an excellent operation-time privacy-preserving DSS system.

The adversary includes internal attackers and external attackers to PriDSS and they may also collude. An internal attacker refers to an SU or a SBS of PriDSS system. Internal attackers are assumed to be honest-but-curious (HBC) which means that they faithfully fulfill the spectrum auction, and will share their operation parameters and the spectrum assignment results with other attackers. The HBC assumption is commonly adopted to model the attackers in the literature, which is not carrying out denial-of-service attacks. On the contrary, an external attacker does not take part in PriDSS while trying to infer the operation-time information of PUs from public information.

By those internal attackers and external attackers, the adversary can maximize its ability. We assume the adversary has arbitrary knowledge about SUs and SBSs and try to infer the operation-time privacy of PUs. We consider a special case that all SUs and SBSs are attackers, so the adversary can know all the operation parameters including identities, locations and assignment results of the SUs and SBSs.

We also assume that the adversary knows about most of PUs' operation parameters, including the locations of PUs, the interference thresholds of the PUs and the channel C, but do not know the accurate operation-time of PUs which is what we want to protect. These assumptions are reasonable, because the locations of PUs are static and public in some cases. [20] also proves that the locations of PUs can be estimated from continuous observations of assignment results, so are the interference thresholds.

It is noted that the aim of our paper is not to prevent DoS attack, eavesdropping attack, and data modification attack, all of which have been analyzed by former researchers for a long time. Generally, it is really hard to prevent DoS attack and eavesdropping attack, and encryption method can be used to prevent data modification attack. All those attacks are about security, however, this paper focus on protect the operation-time privacy of PUs. Even though traditional encryption methods have been used to prevent data modification attack, and all SUs are truthful and follow normal communication protocol, the adversary still can infer the operation-time privacy of PUs, which will be proved in Section IV-B. So based on differential privacy theory, we will propose a new method to protect the operation-time privacy of PUs.

IV. Secondary Users Selection in DSS Without Privacy

A. Secondary Users Selection Problem Formulation

The administrator tends to maximize its utility (social welfare) by selecting the SUs using the channel. We use $\overrightarrow{SP} = \{SP_1, SP_2, \ldots, SP_M\}$ to denote the status set of PUs, which is also the input data, and SP_m is an indicator for PU_m:

$$SP_m = \begin{cases} 1, & \text{PU}_m \text{ is using the channel } C \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

We use $\overrightarrow{SS} = \{SS_1, SS_2, \ldots, SS_N\}$ to denote the status set of SUs after the selection, which is also the output data set after the auction, and SS_n is an indicator for SU_n:

$$SS_n = \begin{cases} 1, & \mathrm{SU}_n \text{ is selected into the winner set} \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

The utility of SU_n whose bid b_n is accepted is defined as "$u_n = (\overline{v_n} - \varrho_n) \cdot SS_n$", where ϱ_n is the payment which SU_n makes to the administrator. The utility and the payment are set to 0 if the secondary user is not a winner. We also assume that the SUs know the spectrum assignment algorithm and the payment computation method ahead of time. Each secondary user wants to maximize his own utility by choosing different strategies. So the claimed valuation v_n might not necessarily same to the true valuation $\overline{v_n}$ for each secondary user.

We want to design a truthful scheme in which SUs have no incentive to lie about their claimed valuation and formulate the secondary users selection in PriDSS as follows without considering operation-time privacy.

$$\max \quad \sum_{n=1}^{N} SS_n \cdot v_n$$

s.t.

$$\begin{cases} \sum_{n=1}^{N} p_n \cdot g_{n,m} \cdot SS_n \cdot SP_m \le I_m \mathrm{th}, & (1 \le m \le M) \\ SS_n = 0, 1 & (1 \le n \le N) \end{cases} \tag{3}$$

The objective of the formulation is to obtain the maximum social welfare, which refers to the total valuation of the SUs in the winner set. The first constraint above indicates that the accumulated interference between the SUs in the winner set and each PU is less than that PU's interference threshold. The second constraint means the value of SS_n equals 1 or 0 for all secondary users. $SS_n = 1$ when the nth secondary user is selected into the winner set, otherwise, $SS_n = 0$.

B. Operation-Time of PU is No Secret

Now we exemplify an attack to infer a PriDSS PU's operation-time privacy when a winner set is selected under the spectrum auction framework described in Section IV-A. The operation-time attack can be divided into two inference phases as follows. Based on the background and assignment results, can the adversary judge whether there exists one PU which is not using the channel in a timeslot or not? Moreover, if the adversary is told that there is one PU is not using the channel in a timeslot, can the adversary judge which PU it is? The operation-time privacy is important and sensitive in the PUs' opinion. If the adversary knows the accurate operation-time of PUs, it will have high chance to produce huge damage to the PUs without being detected.

Inference 1: whether there exist one PU which is not using the channel C.

The key insight for operation-time inference attack is that the assignment results will be different if only one PU's operation-time changed.

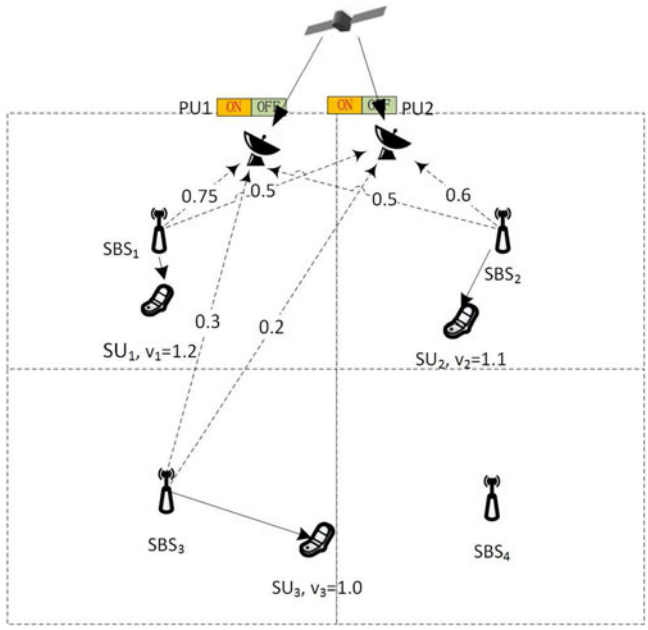

Fig. 2. A simple network with 2 PUs and 3 SUs.

According to the SUs selection problem formulated in Section IV-A, we compare the assignment results of two timeslots. If all the PUs are using the channel C in these two timeslots, and all the operation parameters of PUs and SUs, including locations, claimed valuations, interference thresholds and powers, are same, then the assignment results of these two timeslots should be same too. Therefore, if the assignment results of two timeslots are different, and the adversary with maximal ability can make sure that the all the operation parameters of PUs and SUs except the operation-time parameter are same, then the adversary can infer that not all the PUs are using the channel C in these two timeslots. In other words, the adversary can conclude that there exist one PU which is not using the channel C in one timeslot.

Inference 2: which PU is not using the channel C.

After the adversary concludes there is an PU which is not using the channel in one timeslot, can he infer which PU it is? We use an example to demonstrate the inference process. In Fig. 2, there are 2 PUs sharing the channel and 3 SUs bidding for it. In Fig. 2, all PUs' interference thresholds are same and equal to $I\mathrm{th} = 1.0$ and the decimal number on each dash line is the interference between the corresponding SBS and the PU. v_n is the SU_n's valuation for the channel and bid with it.

Each PU have two statuses in a timeslot: on or off, which means the PU is using the channel (called as an active PU) or not (called as an inactive PU) in that timeslot. Based on the secondary users selection formulation (3), when both PU_1 and PU_2 are using the channel, then the winner set is $winnerset1 = \{\mathrm{SU}_2, \mathrm{SU}_3\}$. For the other three different combinations of two PUs' statuses, there are two winner sets $winnerset2 = \{\mathrm{SU}_1, \mathrm{SU}_3\}$ and $winnerset3 = \{\mathrm{SU}_1, \mathrm{SU}_2, \mathrm{SU}_3\}$.

Now we will introduce a weaker adversary model than the adversary model in Section III-B. If the inference can attack

successfully under the weaker adversary model, it also can attack successfully under the more powerful adversary model in Section III-B. We assume the adversary does not know the locations of PUs and the value of interference threshold $I\text{th}$. So it does not know the real interferences on all dash lines. But it knows that there are two PUs and interference thresholds of them are same. It also knows the powers of SBSs are same and all operation parameters about SUs.

Now we will present the detail inference attack process, through which the adversary can infer which PU is on or not based on the winnersets and its knowledge.

Inference Step 1: One scenario for $winnerset3$ is that both PU_1 and PU_2 are inactive, and there is at least one active PU when $winnerset1$ or $winnerset2$ happens.

Inference Step 2: According to $winnerset2$, the adversary knows that the sum inference of SBS_1 and SBS_3 to at least one active PU is less than interference threshold $I\text{th}$.

Inference Step 3: The bid value of SU_1 is 1.2, which is larger than that of SU_2. So when $winnerset1$ happens, the reason for choosing $\{\text{SU}_2, \text{SU}_3\}$ but not choosing $\{\text{SU}_1, \text{SU}_3\}$, is that the sum interference of SBS_1 and SBS_3 to at least one active PU is larger than the interference threshold $I\text{th}$.

Inference Step 4: Based on the result of Inference step 2 and Inference step 3, the adversary can infer that the sum inference of SBS_1 and SBS_3 to one PU is larger than its interference threshold $I\text{th}$, and calls it PU_a. It can also get the sum inference of SBS_1 and SBS_3 to the other PU is less than interference threshold $I\text{th}$, and calls that PU PU_b. Because the powers of SBSs are same and the gain is proportional to the distance between the transmitter and receiver, the adversary can conclude the PU_a is closer to SBS_1 and SBS_3 than PU_b.

The adversary can also infer that PU_a is active when $winnerset1$ happens, and PU_a is inactive when $winnerset2$ happens, which successfully infer the operation-time privacy of PU_a. Furthermore, if the SUs change the bid value, the adversary can infer PU_b's operation-time privacy by similar steps. For the weaker adversary model introduced before the Inference Steps, the adversary does not know the real identifications of the PUs (i.e., PU_1 and PU_2), so it can only name the PUs with other names (e.g., PU_a and PU_b), and it can still infer the operation-time privacy of PUs with these names. For the powerful adversary model defined in the Section III-B, the adversary can know that PU_a is PU_1 and PU_b is PU_2, and can infer the operation-time privacy of PU_1 and PU_2.

V. Secondary Users Selection With Differential Operation-Time Privacy

So far, we have formulated secondary users selection in PriDSS, and presented a few inference attacks under the formulation, which can seriously threaten the operation-time privacy of PriDSS primary users. In this section, we introduce some background about truthful auction and differential privacy theory. Then based on differential privacy, we present an advanced formulation for secondary users selection in the PriDSS system to achieve truthfulness, approximate social welfare maximization and differential operation-time privacy simultaneously.

A. Background

For better understanding of our scheme, we first introduce some background knowledge.

Definition 1: (Truthful Auction) An auction is truthful if and only if any bidder's (expected) utility of bidding its true valuation $\overline{v_n}$ is at least its (expected) utility of bidding any other value v_n [15] [24],

$$u_i(\overline{v_n}, v_{-n}) \geq u_i(v_n, v_{-n}), \tag{4}$$

where v_{-n} means other agents' bids.

Theorem 1: A decreasing output function admits a truthful payment scheme satisfying voluntary participation if and only if $\int_0^\infty x_i(v_{-n}, u)du \leq \infty$ for all n, v_{-n}. In this case, we can take the payments to be [25] [15]

$$\varrho_i(v_{-n}, v_n) = v_n x_n(v_{-n}, v_n) + \int_{v_n}^{\infty} x_n(v_{-n}, u)du \tag{5}$$

Differential privacy theory is a classic technique to provide statistical guarantee on privacy leakage. The core idea of it is that the outputs of the scheme are almost same if the inputs are two nearly identical data sets (different for a single element) [15]. The definition of differential privacy is formalized as follows [8].

Definition 2: (Differential Privacy) A randomized function M gives ϵ-differential privacy if for all data sets D_1 and D_2 differing on at most one element, and for all $S \subseteq Range(M)$,

$$Pr[M(D_1) \in S] \leq \exp(\epsilon) \times Pr[M(D_2) \in S]. \tag{6}$$

As we know, exponential mechanism [9] [10] is a powerful tool to realize differential privacy. We define a query function $q(A, r)$ which maps a pair of input A and candidate outcome r to a real valued "score". The score is higher, the performance that the mechanism achieved is better. Specifically, the score is defined as follows.

$$Pr[\varepsilon_q^\epsilon(A) = r] \propto \exp(\epsilon q(A, r)). \tag{7}$$

The exponential mechanism offers $2\epsilon\Delta$ differential privacy, where Δ is the is the upper-bound of difference of two data sets.

The following theorem means that the probability of a highly suboptimal output is exponentially low [27].

Theorem 2: The exponential mechanism, when used to select an output $r \in R$, gives $2\epsilon\Delta$-differential privacy, letting R_{OPT} be the subset of R achieving $q(A, r) = \max_r q(A, r)$, ensures that

$$Pr\left[q(A, \epsilon_q^\varepsilon(A)) < \max_r q(A, r) - \frac{\ln(|R|/|R_{OPT}|)}{\epsilon} - \frac{t}{\epsilon}\right] \leq \exp(-t). \tag{8}$$

B. Differentially Private Secondary Users Selection

Before we present the differentially private secondary users selection algorithm, we first bring up an approximation algorithm to solve the secondary users selection problem without considering privacy, then we will combine the differential privacy mechanism with the approximation algorithm to protect the operation-time privacy of primary users.

The secondary users selection problem in Section IV-A can be essentially treated as Knapsack problem which is knowingly NP-complete. Thus our secondary users selection problem is also NP-complete, and an iterative **approximation algorithm** are proposed to solve it as follows. First of all, we define the contributory welfare of an SU as his claimed valuation over the sum indirect interference to all the PUs. Then, in each iteration, a new SU with the maximum contributory welfare among the remaining SUs is selected into the winner set. At last, the algorithm terminates when one constraint will not be satisfied if selecting one more SU as a winner. One SU is called to outbid another when the latter is selected later than the former.

In order to protect the operation-time privacy of primary users, we bring up an approximate algorithm based the exponential mechanism, which achieves the desired approximate maximum social welfare and differential operation-time privacy .

In PriDSS, the administrator aims to choose part of SUs to use the shared spectrum, and the notation in the following algorithm can be referred in Section III.

We first carry out *PreProcess()* function to remove some invalid SUs and calculate some parameters. In Algorithm 1, the*PreProcess()* function has threefold functions. Firstly, it computes the indirect interference $I_{n,m}$ between each pair of SU_n and PU_m, and remove those SUs, whose indirect interferences between each of them and any PU are larger than that PU's interference threshold, from the candidate set Ω (line 2-7). Secondly, it calculates the sum indirect interference I_n for each SU in the candidate set (line 8), and sort all the sum indirect inferences in ascending order (line 11). Then we can get the maximum number of SUs γ in the winner set, if the administrator always select the SU with minimum indirect interference from the remaining candidate set Ω into the winner set (line 12). Thirdly, the ratio of the indirect interference between each pair of SU and PU over the valuation is denoted as β, e.g., $\beta_{n,m} = \frac{p_n \cdot g_{n,m}}{v_n}$. we computes the maximum β among the SUs the candidate set Ω and denotes it as $\beta_{\max}$ (line 13).

Then, a ranking metric is used to quantify the spectrum administrator's preference for SUs, which applies to $\mathrm{SU}_n\,(n \in [1, N])$:

$$r(\mathrm{SU}_n) = \frac{\sum_{m=1}^{M} p_n \cdot g_{n,m} \cdot SP_m}{v_n}. \tag{9}$$

The rationale of the ranking metric is as follows. As we know, the SU with the largest contributory welfare among the remaining SUs have a highest priority to be selected by the spectrum administrator. The contributory welfare of an SU is calculated by his claimed valuation over the sum interference to all the PUs. In each iteration, we calculate the ranking preference for each SU. Then for any remaining SU_n, which has not been selected as a winner, we compute a quality score as follows,

$$q(\mathrm{SU}_n, SS_n) = -r(\mathrm{SU}_n). \tag{10}$$

The "$-$" sign in the above equation is used to fit the exponential mechanism for choose the largest contributory welfare in each iteration. It is obvious that $r(\mathrm{SU}_n)$ is smaller, the quality score of SU_n is higher. During the process of winner selection the administrator tend to select the SU with higher quality score.

Algorithm 1: PreProcess() function.

Input: Threshold set $I\mathrm{th}$, claimed valuation set v, power set p, gain set g, candidate set Ω, $\overrightarrow{PU}$, $\overrightarrow{SU}$ and PUs' status set $\overrightarrow{SP}$,

Output: Ω, the maximum number of winner set γ, the maximum β in the candidate set $\beta_{\max}$

1: calculate the sum of interference threshold $\widehat{I\mathrm{th}} \leftarrow \sum_{m=1}^{M} I_m^{\mathrm{th}}$
2: calculate the indirect interference $I_{n,m} = p_n \cdot g_{n,m}$ between each pair $(\mathrm{SU}_n, \mathrm{PU}_m)$
3: **for all** $\mathrm{SU}_n \in \Omega$ **do**
4: **if** exist $m \in [1, M]$ satisfies $I_{n,m} > I_m^{\mathrm{th}}$ **then**
5: $\Omega \leftarrow \Omega - \{\mathrm{SU}_n\}$
6: **end if**
7: **end for**
8: **for all** $\mathrm{SU}_n \in \Omega$ **do**
9: calculate $I_n = \sum_{m=1}^{M} I_{n,m}$
10: **end for**
11: sort all the I_n within Ω in ascending order
12: calculate γ, the maximum number of SUs in the winner set, assuring that the sum of first γ interference in the sorted interference set is less than $\widehat{I\mathrm{th}}$
13: calculate the maximum β of the SUs in the candidate set $\beta_{\max}$, which means $\beta_{\max} = \max_{1 \le m \le M, \mathrm{SU}_n \in \Omega} \beta_{n,m} = \max_{1 \le m \le M, \mathrm{SU}_n \in \Omega} \frac{p_n \cdot g_{n,m}}{v_n}$.

During the process of winner selection the administrator tend to select the SU with higher quality score.

The details of our assignment scheme is illustrated in Algorithm 2. Based on the exponential mechanism, we compute the probability of SU_n being selected into the winner set as

$$Pr[SS_n = 1] = \exp\left(-\varepsilon' \cdot r(\mathrm{SU}_n)\right), \tag{11}$$

where ε' is specified as $\frac{\varepsilon}{\triangle \cdot \beta_{\max} \cdot \gamma}$. $\triangle$ is the maximum input difference for the input SP_m, which equals $\max(SP_m) - \min(SP_m) = 1$. ε is a parameter to balance the privacy leakage and efficiency (social welfare maximization in our scenario). The probability of SU_n being selected can thus be derived considering all the unselected SUs in candidate set in line 8 of Algorithm 2. The probability are normalized by the overall SUs' selection probability. According to the selection probabilities in the candidate Ω, we assume that the winner being selected in this iteration is SU_n. Then We remove SU_n from Ω and add SU_n into the winner set W. Moreover, we modify each PU's remaining allowable interference I_m^a and remove those SUs, which interference between any of them and any PU is larger than that PU's remaining allowable interference, from Ω.

Based on Theorem 1, we can design a truthful payment method. The payment that each winner SU_n paid to the

Algorithm 2: Secondary Users Selection in PriDSS.

Input: Threshold set $I\text{th}$, claimed valuation set v, power set p, gain set g, PUs' status set SP, $\overrightarrow{PU}$ and $\overrightarrow{SU}$.
Output: Winner Set W, social welfare Wel.
1: Initialization:$W \leftarrow \emptyset, Wel \leftarrow 0$, candidate set $\Omega \leftarrow \overrightarrow{SU}$, allowable interference set $I^a \leftarrow I\text{th}$
2: PreProcess();
3: $\varepsilon' \leftarrow \frac{\varepsilon}{\triangle \cdot \beta_{\max} \cdot \gamma}$;
4: **for all** $\text{SU}_n \in \overrightarrow{SU}$ **do**
5: $r(\text{SU}_n) = \frac{\sum_{m=1}^{M} p_n \cdot g_{n,m} \cdot SP_m}{v_n}$;
6: **end for**
7: **for all** $\text{SU}_n \in \Omega$ **do**
8: $Pr[W \leftarrow W \cup \{\text{SU}_n\}] = \frac{\exp(-\varepsilon' \cdot r(\text{SU}_n))}{\sum_{\text{SU}_i \in \Omega} \exp(-\varepsilon' \cdot r(\text{SU}_i))}$;
9: **end for**
10: Select SU_n according to the computed probability distribution.
11: **if** SU_n is selected **then**
12: $\Omega \leftarrow \Omega - \{\text{SU}_n\}$;
13: $W \leftarrow W \cup \{\text{SU}_n\}$;
14: $Wel = Wel + v_n$;
15: $I_m^a = I_m^a - g_{n,m} \cdot p_n, m \in [1, M]$;
16: **for all** $\text{SU}_j \in \Omega$ **do**
17: **if** exist $m \in [1, M]$ satisfies $I_{j,m} > I_m^a$ **then**
18: $\Omega \leftarrow \Omega - \{\text{SU}_j\}$;
19: **end if**
20: **end for**
21: **end if**

administrator is

$$\begin{aligned}\varrho_n(v_{-n}, v_n) &= v_n(1 - x_n(v_{-n}, v_n)) + \int_{v_n}^{v_{\max}} (1 - x_n(v_{-n}, u))du \\ &= v_{\max} - v_n \cdot x_n(v_{-n}, v_n) - \int_{v_n}^{v_{\max}} x_n(v_{-n}, u)du \end{aligned} \quad (12)$$

where $x_n(v_{-n}, v_n)$ stands for the probability of SU_n being selected as a winner, when SU_n's claimed valuation is v_n and others' claimed valuation vector is v_{-n}.

VI. Performance Analysis

Till now, we have proposed our scheme PirDSS detailedly. In this section, we will prove how PriDSS achieves the three desired objectives:differential operation-time privacy, approximate social welfare maximization, and truthfulness.

A. Differential Operation-Time Privacy

Theorem 3: PriDSS preserves $(e-1)\varepsilon$-differential operation-time privacy.

Proof: In two successive auction rounds, we assume that there are two neighboring status sets of PUs $\overrightarrow{SP} = \{SP_1, SP_2, \ldots, SP_M\}$ and $\overrightarrow{SP'} = \{SP'_1, SP'_2, \ldots, SP'_M\}$ in which only the lth index elements of these two status sets are different. $SP_m = SP'_m$ for all $m \in [1, M]$ except $m = l$. Differential privacy requires that taking these two neighboring status sets as input, the probabilities that the winner set is W or W' are almost the same. The reason of our proof is that according to the two ordered winner sets W and W', we can get an upper-bound for $Pr[W = \{w_1, w_2, \ldots, w_k\}]/Pr[W' = \{w_1, w_2, \ldots, w_k\}]$. Thereinto, for any $j > i$, w_j is selected before w_j. For simplicity of description, we use the notations p_i and v_i to denote the power and valuation of SU_{w_i} separately. The formal proofs are as follows.

$$\begin{aligned}&\frac{Pr[W = \{w_1, w_2, \ldots, w_k\}]}{Pr[W' = \{w_1, w_2, \ldots, w_k\}]} \\ &= \prod_{i=1}^{k} \frac{\frac{\exp\left(-\varepsilon' \sum_{m=1}^{M} g_{i,m} \cdot SP_m \cdot p_i / v_i\right)}{\sum_{j \in \Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m} \cdot SP_m \cdot p_j / v_j\right)}}{\frac{\exp\left(-\varepsilon' \sum_{m=1}^{M} g_{i,m} \cdot SP'_m \cdot p_i / v_i\right)}{\sum_{j \in \Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m} \cdot SP'_m \cdot p_j / v_j\right)}} \\ &= \prod_{i=1}^{k} \frac{\exp\left(-\varepsilon' \sum_{m=1}^{M} g_{i,m} \cdot SP_m \cdot \frac{p_i}{v_i}\right)}{\exp\left(-\varepsilon' \sum_{m=1}^{M} g_{i,m} \cdot SP'_m \cdot \frac{p_i}{v_i}\right)} \\ &\quad \cdot \prod_{i=1}^{k} \frac{\sum_{j \in \Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m} \cdot SP'_m \cdot \frac{p_j}{v_j}\right)}{\sum_{j \in \Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m} \cdot SP_m \cdot \frac{p_j}{v_j}\right)} \quad (13) \\ &= \exp\left(\varepsilon' \sum_{i=1}^{k} g_{i,l} \cdot (SP'_l - SP_l) \cdot \frac{p_i}{v_i}\right) \\ &\quad \cdot \prod_{i=1}^{k} \frac{\sum_{j \in \Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m} \cdot SP'_m \cdot \frac{p_j}{v_j}\right)}{\sum_{j \in \Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m} \cdot SP_m \cdot \frac{p_j}{v_j}\right)}, \quad (14)\end{aligned}$$

where Ω_1 is the candidate set Ω after $PreProcess()$ is carried out and Ω_i is the candidate set Ω before $w_i (i > 1))$ is selected into winner set.

If $SP'_l > SP_l$, the second product is smaller than 1, then

$$\begin{aligned}&\frac{Pr[W = \{w_1, w_2, \ldots, w_k\}]}{Pr[W' = \{w_1, w_2, \ldots, w_k\}]} \\ &< \exp\left(\varepsilon' \sum_{i=1}^{k} g_{i,l} \cdot (SP'_l - SP_l) \cdot \frac{p_i}{v_i}\right) \\ &= \exp\left(\frac{\varepsilon}{\Delta \cdot \beta_{\max} \cdot \gamma} \cdot \sum_{i=1}^{k} g_{i,l} \cdot (SP'_l - SP_l) \cdot \frac{p_i}{v_i}\right) \quad (15)\end{aligned}$$

In Algorithm 1, γ is the maximum number of winner set and $\beta_{\max}$ is the maximum β in the candidate set, so $\gamma \geq k$ and $\beta_{\max}$ is larger or equals than any $\beta_i = \frac{p_i \cdot g_{i,l}}{v_i}$, so $\sum_{i=1}^{k} g_{i,l} \cdot \frac{p_i}{v_i} \leq \beta_{\max} \cdot \gamma$. And as we know $SP'_l - SP_l = \Delta = 1$, then

$$\begin{aligned}&\frac{Pr[W = \{w_1, w_2, \ldots, w_k\}]}{Pr[W' = \{w_1, w_2, \ldots, w_k\}]} \\ &< \exp\left(\frac{\varepsilon}{\triangle \cdot \beta_{\max} \cdot \gamma} \cdot \sum_{i=1}^{k} g_{i,l} \cdot (SP'_l - SP_l) \cdot \frac{p_i}{v_i}\right) \\ &< \exp(\varepsilon) \quad (16)\end{aligned}$$

If $SP'_l < SP_l$, the first product is smaller than 1. Then we denote that $\alpha_m = SP_m - SP'_m$, therefor,

$$\begin{aligned}
&\frac{Pr[W=\{w_1,w_2,\ldots,w_k\}]}{Pr[W'=\{w_1,w_2,\ldots,w_k\}]} \\
&< \prod_{i=1}^{k} \frac{\sum_{j\in\Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m}\cdot SP'_m \cdot \frac{p_j}{v_j}\right)}{\sum_{j\in\Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m}\cdot SP_m \cdot \frac{p_j}{v_j}\right)} \\
&= \prod_{i=1}^{k} \left[\frac{\sum_{j\in\Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m}\cdot SP'_m \cdot \frac{p_j}{v_j}\right)}{\sum_{j\in\Omega_i} \exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m}\cdot \alpha_m \cdot \frac{p_j}{v_j}\right)} \right. \\
&\quad \left. \cdot \frac{1}{\exp\left(-\varepsilon' \sum_{m=1}^{M} g_{j,m}\cdot SP'_m \cdot \frac{p_j}{v_j}\right)} \right] \\
&= \prod_{i=1}^{k} \mathbb{E}_{j\in\Omega_i} \left[\exp\left(\varepsilon' \cdot \sum_{m=1}^{M} g_{j,m}\cdot \alpha_m \cdot \frac{p_j}{v_j} \right) \right] \\
&= \prod_{i=1}^{k} \mathbb{E}_{j\in\Omega_i} \left[\exp\left(\varepsilon' \cdot g_{j,l}\cdot \alpha_l \cdot \frac{p_j}{v_j} \right) \right] \qquad (17)
\end{aligned}$$

where $\alpha_l = 1$, $\varepsilon' = \frac{\varepsilon}{\triangle\cdot\beta_{\max}\cdot\gamma}$.

We know γ is the maximum number of winner set and $\beta_{\max}$ is the maximum β in the candidate set, so $\beta_{\max}$ is larger or equals than any $\beta_j = \frac{p_j\cdot g_{j,l}}{v_j}$.Note that for all $\eta \le 1, e^\eta \le 1 + (e-1)\eta$, therefor,

$$\begin{aligned}
&\frac{Pr[W=\{w_1,w_2,\ldots,w_k\}]}{Pr[W'=\{w_1,w_2,\ldots,w_k\}]} \\
&\le \prod_{i=1}^{k} \mathbb{E}_{j\in\Omega_i} \left[1 + (e-1)\left(\varepsilon' \cdot g_{j,l}\cdot \alpha_l \cdot \frac{p_j}{v_j} \right) \right] \\
&\le \exp\left((e-1)\cdot\varepsilon' \cdot \sum_{i=1}^{k} \mathbb{E}_{j\in\Omega_i} \left(g_{j,l}\cdot\alpha_l\cdot\frac{p_j}{v_j} \right) \right) \\
&= \exp\left(\frac{(e-1)\cdot\varepsilon}{\triangle\cdot\beta_{\max}\cdot\gamma} \cdot \sum_{i=1}^{k} \mathbb{E}_{j\in\Omega_i} \left(g_{j,l}\cdot\alpha_l\cdot\frac{p_j}{v_j} \right) \right) \\
&\le \exp((e-1)\varepsilon) \qquad (18)
\end{aligned}$$

From (16) and (18), we prove PriDSS preserves $(e-1)\varepsilon$-differential operation-time privacy.

B. Approximate Social Welfare Maximization

Theorem 4: With the probability of at least $1 - 1/N^{\mathcal{O}(1)}$, PriDSS can assign channel C to a set of winners with a social welfare of at least $\frac{\tau\cdot OPT}{\widehat{I\text{th}}} - \mathcal{O}(\ln(N))$, where OPT denotes the optimal (maximum) social welfare, N is the number of secondary users, τ is the minimum sum indirect interference from an SU to all the PUs and $\widehat{I\text{th}}$ is the sum of PUs' interference thresholds.

Proof: The winner set with the maximum social welfare is denoted as W_{OPT}, and an arbitrary winner set is denoted as W. The winners in W is numbered according to the selection order, i.e., $W = \{w_1, w_2, \ldots, w_l\}$.

We construct a set W_i for each $i \in W$, under constraints $(\forall j \in W_i)$ as follows:

1) $j \in W_{OPT}$;
2) $j \in \Omega$ before i is selected;
3) j will be removed from Ω after i is selected.

The above constraints means the reason for secondary user j not being selected into W is that there is a secondary user i competing the channel with secondary user j, and i wins. In addition, secondary user j will be removed from Ω for its indirect interference exceed PUs' remaining allowable interference I^a.

It is notable that the q function in (8) refers to the unified quality scores in our scenario. So, by taking $t = \mathcal{O}(\ln(N))$, we have

$$\begin{aligned}
&-\frac{I_i}{v_i} \ge -\frac{I_j}{v_j} - \mathcal{O}(\ln(N)) \\
&\text{i.e.} \\
&v_j \le \frac{I_j\cdot v_i}{I_i} + \mathcal{O}(\ln(N)) \\
&\quad \le \frac{I_j\cdot v_i}{\tau} + \mathcal{O}(\ln(N)) \qquad (19)
\end{aligned}$$

with a probability of at least $1 - 1/N^{\mathcal{O}(1)}$, where $I_i = \sum_{m=1}^{M} p_i \cdot g_{i,m} \cdot SP_m, \tau = \min_{1\le i\le N}(I_i)$.

We denote $\widehat{I\text{th}} = \sum_{m=1}^{M} I_m\,\text{th}$, so $\widehat{I\text{th}} \ge \sum_{j\in W_{OPT}} I_j$. Summing all $j(j \in W_i)$ together, we can get

$$\begin{aligned}
\sum_{j\in W_i} v_j &\le \left(\frac{v_i}{\tau} + \mathcal{O}(\ln(N)) \right) \cdot \sum_{j\in W_i} I_j \\
&\le \frac{\widehat{I\text{th}}}{\tau}\cdot v_i + \mathcal{O}(\ln(N)) \qquad (20)
\end{aligned}$$

with a probability of at least $1 - 1/N^{\mathcal{O}(1)}$.

By summing all $i(i \in W)$, we get

$$\begin{aligned}
\sum_{j\in W_{OPT}} v_j &= \sum_{j\in W_{OPT}-W} v_j + \sum_{j\in W_{OPT}\cap W} v_j \\
&= \sum_{i\in W-W_{OPT}} \left(\sum_{j\in W_i} v_j \right) + \sum_{j\in W_{OPT}\cap W} v_j \\
&= \sum_{i\in W-W_{OPT}} \left(\sum_{j\in W_i} v_j \right) + \sum_{i\in W_{OPT}\cap W} v_i \\
&\le \frac{\widehat{I\text{th}}}{\tau} \cdot \sum_{i\in W} v_i + \mathcal{O}(\ln(N)) \qquad (21)
\end{aligned}$$

with a probability of at least $1 - 1/N^{\mathcal{O}(1)}$.

From (21) we can get

$$\sum_{i\in W} v_i \ge \frac{\tau\cdot OPT}{\widehat{I\text{th}}} - \mathcal{O}(\ln(N)) \qquad (22)$$

with a probability of at least $1 - 1/N^{\mathcal{O}(1)}$.

C. Truthfulness

Now we prove that PriDSS is truthful. According to Theorem 1, we need to prove that the selection process of PriDSS is monotone decreasing.

Lemma 5: In PriDSS, for each secondary user i, $1 - x_i(v_{-i}, v_i)$ is monotone decreasing, which is equivalent to that $x_i(v_{-i}, v_i)$, the probability of SU_i being selected as a winner, is monotone increasing with his claimed valuation v_i.

Proof: Due to the randomized selection property of PriDSS, we only need to prove that the probability of SU_i being selected as winner is increasing, when his claimed valuation v_i increases in each round.

$$\begin{aligned} &Pr(W \leftarrow W \cup \{\mathrm{SU}_i\}) \\ &= \frac{\exp\left(-\varepsilon' \cdot r(\mathrm{SU}_i)\right)}{\sum_{j\in\Omega} \exp(-\varepsilon' \cdot r(\mathrm{SU}_j)} \\ &= \frac{\exp(-\varepsilon' \cdot r(\mathrm{SU}_i))}{\exp(-\varepsilon' \cdot r(\mathrm{SU}_i) + \sum_{j\in\Omega\setminus\{\mathrm{SU}_i\}} \exp(-\varepsilon' \cdot r(\mathrm{SU}_j)} \\ &= 1 - \frac{\sum_{j\in\Omega\setminus\{\mathrm{SU}_i\}} \exp(-\varepsilon' \cdot r(\mathrm{SU}_j)}{\exp(-\varepsilon' \cdot r(\mathrm{SU}_i) + \sum_{j\in\Omega\setminus\{\mathrm{SU}_i\}} \exp(-\varepsilon' \cdot r(\mathrm{SU}_j)} \end{aligned} \tag{23}$$

In the above equation, $r(\mathrm{SU}_i)$ will decreases if v_i rises. Then $\exp(-\varepsilon' \cdot r(\mathrm{SU}_i)$ will increases, leading to the total equation value to increase. This means that assuming SU_i not being selected in previous rounds, if we increase the value of v_i, the probability of SU_i being selected in the winner set W increases in every round.

Thus the following theorem is established:

Theorem 6: PriDSS is truthful.

VII. Performance Evaluation

In this section, we will evaluate whether PriDSS can achieve differential operation-time privacy and approximate social welfare maximization by simulations in Matlab.

In the simulation, a square urban area of 10 km by 10 km is divided into cells. The length of each cell is 500 meters, so there are 400 cells in this area. The PriDSS administrator manages the PUs sharing a single channel $C = 3.6 \times 10^9$Hz with SUs. The number of PUs M varies from 2 to 10 and the number of SUs N varies from 100 to 400. PUs are uniformly distributed located in the area. SUs are randomly located in the different cells, and there is one SU at most in each cell. The valuation of SUs v are uniformly distributed in the valuation range $[v_{\min}, v_{\max}]$. We set the valuation range $[v_{\min}, v_{\max}]$ to [100, 2000] and then normalize it to [0, 1].

Similar to [20], we also opt for a simple two-ray ground propagation model for the mean channel gain between any SU and any PU. The antenna heights of PUs and SUs are 100 m and 2 m separately. The powers of SBSs p are set to be 23 dBm, and the interference thresholds $I\mathrm{th}$ of PUs are set to be -80 dBm. We set the value of the privacy parameter ε to 0.5 or 5.0. The simulations are performed in MATLAB, and each result stands for the average value of 100 runs.

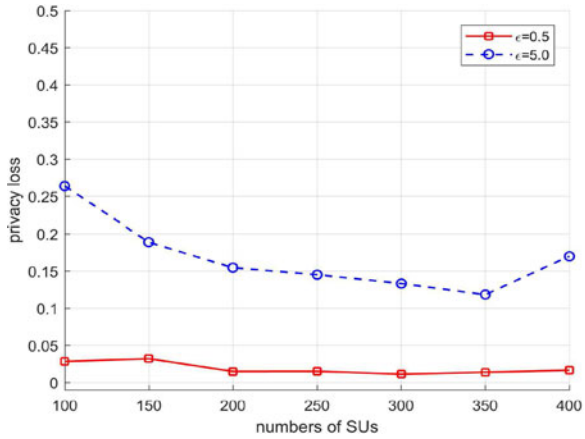

Fig. 3. Privacy loss for 3 PUs .

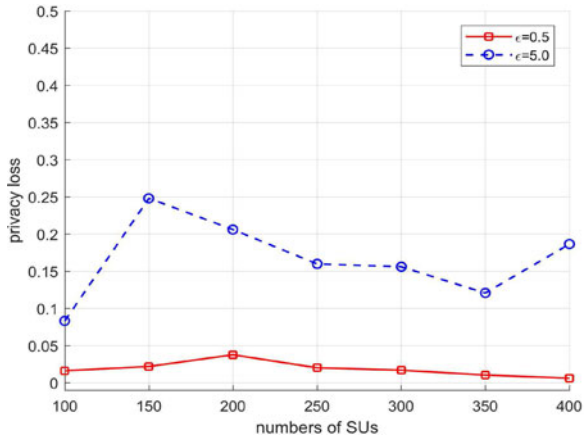

Fig. 4. Privacy loss for 8 PUs.

During the simulation process, we used two metrics to evaluate the performance of PriDSS. The first metric is the privacy loss, which is defined according to Definition 2,

$$\epsilon = \max_{S} \quad \ln \frac{Pr(M(D_1) \in S)}{Pr(M(D_2) \in S)}, \tag{24}$$

where D_1 and D_2 correspond to two PUs' status sets $\overrightarrow{SP}$s which only one element of them are different. We can get that ε is smaller, the impact that the change of a single status of PU on the final auction results is less, and thus each PU enjoys more operation-time privacy. The second metric we used is the social welfare of administrator (or total valuation of winners), which is expected to be as high as possible. In order to comparison, we demonstrate the social welfare of PriCSS and the approximation algorithm without considering privacy demonstrated in Section IV-A.

Firstly, we evaluate the operation-time privacy loss in PriDSS. We have proved that PriDSS preserves $(e-1)\varepsilon$-differential operation-time privacy in Section VI. We set $\varepsilon = 0.5$ or 5.0 in the simulations. Figs. 3 and 4 show the achievable privacy losses in PriDSS with three PUs and eight PUs, and the privacy losses in simulations are lower than the theoretical privacy loss value. We can find that when $\varepsilon = 0.5$, all privacy losses are less than 0.05, which is much lower than the theoretical privacy loss

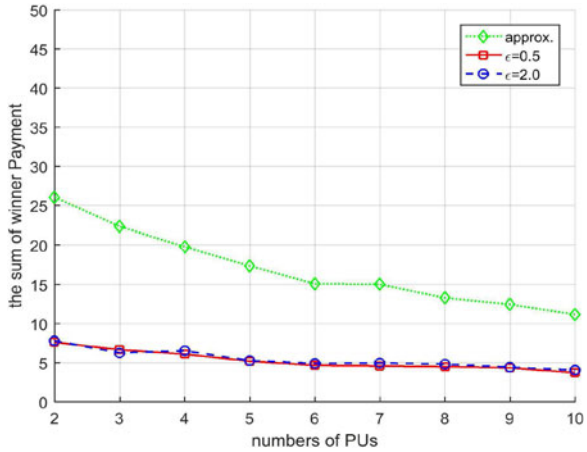

Fig. 5. Social welfare for 150 SUs.

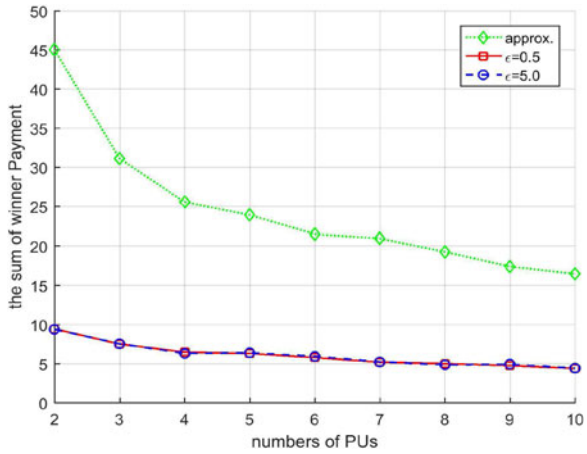

Fig. 6. Social welfare for 350 SUs.

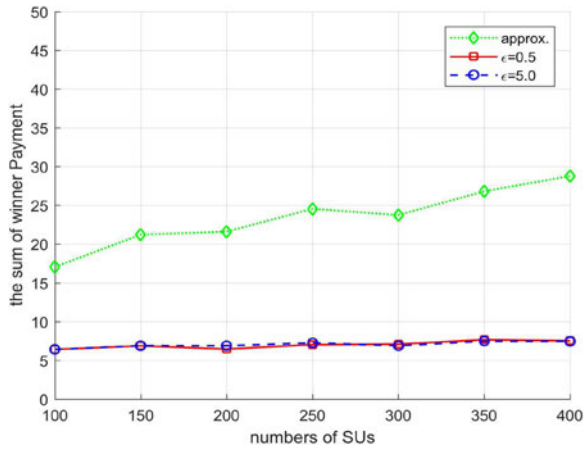

Fig. 7. Social welfare for 3 PUs.

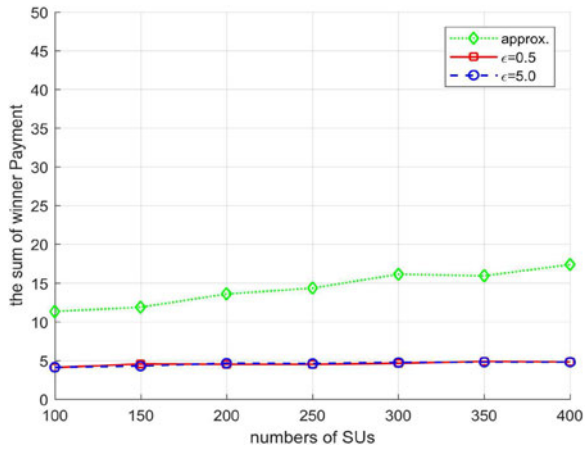

Fig. 8. Social welfare for 8 PUs.

$(e-1)\varepsilon \approx 0.8$. We can get similar conclusions when $\varepsilon = 5.0$. This means that the change of s any PU's status has limited impact on the final auction result. Then differential privacy mechanism guarantees that arbitrary adversary can not infer the PUs' operation-time by performing the inference attacks introduced in Section IV-B or any other attack actions.

In Figs. 5 and 6, we also show the social welfare when there are 150 and 350 SUs. As expected, the social welfare of approximate algorithm decrease as the number of PUs rises. The reason of that is when there are more PUs, more SUs including many welfare-superiority SUs are removed from candidate set for the interference threshold. However, the decreasing trend was greatly depressed with PriDSS for both $\varepsilon = 0.5$ and $\varepsilon = 5.0$ cases. The exponential mechanism requires that every SU is selected based on a probability and can balance the influence of more PUs.

We illustrate the social welfare in PriDSS and the approximate algorithm without privacy (denoted as approx.) when there are three and eight PUs in Figs. 7 and 8. We find that the social welfare of the approximate algorithm tends to increase as the number of SUs increases because of more SUs competing the channel. However, the trend to increase can not be observed with PriDSS for both $\varepsilon = 0.5$ and $\varepsilon = 5.0$. This is mainly because the advantage of welfare-superiority SUs, which claim larger contributory welfare and hope to have more chance of being selected, is weakened due to increased number of SUs in PriDSS. That is to say, when the number of SUs increases, the ranking metrics of welfare-superiority SUs play less significant roles.

VIII. Conclusion

In this paper, we proposed PriDSS, a novel scheme in which the administrator can select spectrum-sharing SUs in a differentially operation-time private manner. After thorough privacy proving and efficiency analysis, we evaluate the performance of PriDSS extensively. Analysis and evaluation results shows that PriDSS can achieve three design objectives simultaneously: truthfulness, approximate social welfare maximization and differential operation-time privacy.

References

[1] 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.

[2] C. Zhai, J. Liu, and L. Zheng, "Cooperative spectrum sharing with wireless energy harvesting in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5303–5316, Jul. 2016.

[3] M. Xia and S. Aissa, "Modeling and analysis of cooperative relaying in spectrum-sharing cellular systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9112–9122, Nov. 2016.
[4] Federal Communications Commission, "Report and Order and Second Further Notice of Proposed Rulemaking," *Fed. Commun. Commiss.* 15-47 GN Docket No. 12-354, Apr. 2015.
[5] U. Siddique, H. Tabassum, E. Hossain and D. I. Kim, "Channel-Access-Aware user association with interference coordination in two-tier downlink cellular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5579–5594, Jul. 2016.
[6] B. Bahrak *et al.*, "Protecting the primary users' operational privacy in spectrum sharing," in *Proc. IEEE Int. Symp. Dyn. Spectrum Access Netw.*, McLean, VA, USA, Apr. 2014, pp. 236–247.
[7] A. Robertson *et al.*, "Spectrum database poisoning for operational security in policy-based spectrum operations," in *Proc. IEEE Mil. Commun. Conf.*, Nov. 2013, pp. 382–C387.
[8] C. Dwork, "Differential privacy," in *Proc. Int. Colloq. Automata, Lang. Program.*, Jul. 2006, pp. 1–12.
[9] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci.*, Oct. 2007, pp. 94–103.
[10] Z. Huang and S. Kannan, "The exponential mechanism for social welfare:private, truthful, and nearly optimal," in *Proc. 53rd Annu. IEEE Symp. Found. Comput. Sci.*, Oct. 2012, pp. 140–149.
[11] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen, "Location privacy preservation in collaborative spectrum sensing," in *Proc. IEEE Conf. Comput. Commun.*, Mar. 2012, pp. 729–737.
[12] Z. Gao, H. Zhu, S. Li, and S. Du, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 106–112, Dec. 2012.
[13] 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.
[14] H. To, G. Ghinita, and C. Shahabi, "A framework for protecting worker location privacy in spatial crowdsourcing," *Proc.VLDB Endowment*, vol. 7, no. 10, pp. 919–930, Jun. 2014.
[15] X. C. Jin and Y. C. Zhang, "Privacy-Preserving crowdsourced spectrum sensing," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2016, pp. 1–9.
[16] Q. Huang, Y. Tao and F. Wu, "SPRING: A strategy-proof and privacy preserving spectrum auction mechanism," in *Proc. IEEE Conf. Comput. Commun*, 2013, pp. 827–835.
[17] F. Wu, Q. Huang, Y. Tao, and G. Chen, "Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks," *IEEE/ACM Trans. Netw.*, vol. 23, no. 4, pp. 1271–1285, Aug. 2015.
[18] R. H. Zhu and K. G. Shin, "Differentially private and strategy-proof spectrum auction with approximate revenue maximization," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2015, pp. 918–926.
[19] Y. Z. Dou *et al.*, "P2-SAS: Preserving users' privacy in centralized dynamic spectrum access systems," in *Proc. 17th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Jul. 2016, pp. 321–330.
[20] M. Clark and K. Psounis, "Can the privacy of primary networks in shared spectrum be protected?," in *Proc. IEEE Conf. Comput. Commun 2016, 35th Annu. IEEE Int. Conf. Comput. Commun.*, San Francisco, CA, USA, 2016, Apr. 2016, pp. 1–9,
[21] R. H. Zhu, Z. J. Li, F. Wu, K. G. Shin, and G. H. Chen, "Differentially private spectrum auction with approximate revenue maximization," in *Proc. 15th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Aug. 2014, pp. 185–194.
[22] J. M. Peha, "Sharing spectrum through spectrum policy reform and cognitive radio," *Proc. IEEE*, vol. 97, no. 4, pp. 708–719, Apr. 2009.
[23] M. Maso, M. Debbah and L. Vangelista, "A distributed approach to interference align in OFDM-based two-tiered networks," *Trans. Vech. Technol.*, vol. 62, no. 5, pp. 1935–1949, Jun. 2013.
[24] J. Jia, Q. Zhang, Q. Zhang, and M. Liu, "Revenue generation for truthful spectrum auction in dynamic spectrum access," in *Proc. 10th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, May 2009, pp. 3–12.
[25] A. Archer and E. Tardos, "Truthful mechanisms for one-parameter agents," in *Proc. 42nd IEEE Symp. Found. Comput. Sci.*, Oct. 2001, pp. 482–491.
[26] V. Vazirani, *Approximation Algorithms*. New York, NY, USA: Springer, 2001.
[27] A. Gupta, K. Ligett, F. McSherry, A. Roth, and K. Talwar, "Differentially private combinatorial optimization," in *Proc. 21st Annu. ACM-SIAM Symp. Discrete Algorithm*, Jan. 17–19, 2010, pp. 1106–1125.
[28] M. Clark and K. Psounis, "Efficient resource scheduling for a secondary network in shared spectrum," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2015, pp. 1257–1265.

Xuewen Dong received the B.E., M.S., and Ph.D. degrees in computer science and technology from Xidian University, Xi'an, China, in 2003, 2006, and 2011, respectively. From 2016 to 2017, he was a Visiting Scholar with Oklahoma State University, Stillwater, OK, USA. He is currently an Associate Professor with the School of Computer Science, Xidian University, Xi'an, China. His research interests include cognitive radio network, wireless network security, and big data privacy.

Yanmin Gong received the B.Eng. degree in electronics and information engineering from Huazhong University of Science and Technology, Wuhan, China, in 2009, the M.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2012, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2016. Since August 2016, she has been an Assistant Professor with the School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK. 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 was the Technical Program Committee members for several conferences including IEEE INFOCOM and CNS. She is a member of ACM.

Jianfeng Ma received the B.S. degree in mathematics from Shaanxi Normal University, Xi'an, China, in 1985, and the M.E. and Ph.D. degrees in computer software and communications engineering from Xidian University, Xi'an, China, in 1988 and 1995, respectively. From 1999 to 2001, he was a Research Fellow with the Nanyang Technological University of Singapore, Singapore. He is currently a Professor with the School of Computer Science, Xidian University, Xi'an, China. His current research interests include distributed systems, computer networks, and information and network security.

Yuanxiong Guo received the B.Eng. degree in electronics and information engineering from Huazhong University of Science and Technology, Wuhan, China, in 2009, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2012 and 2014, respectively. Since 2014, he has been an Assistant Professor with the School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK. His current research interests include resource management and cybersecurity for networked systems including cyber-physical systems, Internet of things, wireless networks, and cloud/edge networks. He is a recipient of the Best Paper Award in the IEEE Global Communications Conference 2011. He is a member of the ACM.