2013 IEEE 33rd International Conference on Distributed Computing Systems

Location Privacy Preserving Dynamic Spectrum Auction in Cognitive Radio Network

Sheng Liu, Haojin Zhu, Rong Du, Cailian Chen, Xinping Guan
Shanghai Jiao Tong University
Shanghai, China
Email: {liusheng,zhu-hj,durong,cailianchen,xpguan}@sjtu.edu.cn

***Abstract*—Dynamic spectrum auction offers the flexibility and capability for bidders to request and acquire unoccupied channels from spectrum license holders. Compared with the conventional auction, spectrum auction allows various buyers to utilize the same channel simultaneously based on their locations, which is denoted as spectrum reusability. In this paper, we consider a novel kind of attack, which could compromise location privacy of bidders by observing the bid items as well as bid price. To thwart this attack, we introduce a new Location Privacy Preserving Dynamic Spectrum Auction (LPPA) scheme which consists of two components: Privacy Preserving Bid Submission protocol (PPBS) and Private Spectrum Distribution protocol (PSD). Based on the prefix membership verification scheme, PPBS allows the auctioneer to construct the conflict relationship between different users and obtain the maximum value of bids on various channels without leaking users' location information. Furthermore, PSD is proposed to efficiently distribute the spectrum among bidders and securely charge the winners with the help of periodically available TTP (Trusted Third Party). To demonstrate the effectivenss of the proposed scheme, we implement our attack and scheme on data extracted from Google Earth Coverage Maps released by FCC. The experiment results show the efficacy and efficiency of our approach.**

Keywords – **Location Privacy, Dynamic Spectrum Auction, Prefix Membership Verification**

I. Introduction

Over the last decade, the ever increasing spectrum demand for emerging wireless applications has inspired the concept of cognitive radio (CR) [1], which is expected to improve the utilization of the precious natural resource, radio spectrum. Different from the conventional spectrum management paradigms in which most of the spectrum is allocated to primary users (PU) for exclusive use, a CR system allows secondary users (SU) or lower-priority users to exploit the unoccupied spectrum opportunistically. By reusing the waste spectrum of some primary spectrum holders, CR would partially address the spectrum shortage issue.

A promising and incentive method to re-distribute spectrum resources among PUs and SUs in CR network is dynamic spectrum auction. Through auction, SUs could obtain spectrum access in a cost-effective manner while PUs would receive compensation from SUs as the reward of contributing their spectrum resources to others. Unlike other traditional auction schemes, dynamic spectrum auction permits the well-separated bidders to utilize the same channel simultaneously, denoted as spectrum reusability. This characteristics require bidders to submit their location information to the auctioneer to construct the conflict constraints. Particularly, a typical dynamic spectrum auction process could be described as follows: 1) Through spectrum sensing or database query, SUs independently obtain the condition of spectrum and determine the bid price of each available channel based on the spectrum quality. 2) In the bidding phase, SUs submit their ID, location and bids for each channel to the auctioneer. 3) After collecting all the bids, the auctioneer would distribute the channels among the bidders and charge the winners.

Despite a large body of research works concentrating on how to efficiently and truthfully launch an auction [2], [4], [5], [7]–[9], few attention has been drawn to the security issues so far. In this paper, we introduce a new security threat, *Location Privacy Leakage*, arising from dynamic spectrum auction. As illustrated above, spectrum auction requires users to submit their location information to an untrusted auctioneer, which will inevitably leave SUs' position, or even the trace to unwanted parties. As studied by existing research [13], the contextual information attached to a trace implies much about the individuals' hobbies, habits, activities, and relationships, making them victims of location-based spams or unwanted advertisement. What's worse, our research shows that, in addition to compromising users' location privacy directly through location submission process, the adversary could also infer users' location information from the bidding items and price.

Unfortunately, the existing approaches cannot achieve location privacy preserving dynamic spectrum auction resulting from the following technical challenges. Firstly, spectrum reusability requires the auctioneer to construct bidder conflict graph. Thus, to protect users' location privacy, the proposed scheme should enable the untrusted auctioneer to determine if the distance of two SUs is larger than a predefined threshold without revealing the bidders' real positions. Secondly, our study demonstrates that the attacker could geo-locate users from their bid items and price. As a result, the auction scheme must keep the bid price secret from the auctioneer while permitting it to launch the auction transparently. Thirdly, the exact charging price of winner has to be known by the auctioneer, which would absolutely reveal some plaintext-ciphertext pairs. We must minimize the information leakage through winner charging process.

To address the above challenges, we introduce a novel *Location Privacy Preserving Dynamic Spectrum Auction* (LP-

1063-6927/13 $26.00 © 2013 IEEE
DOI 10.1109/ICDCS.2013.35

PA), which enables the dynamic spectrum auction launched without leaking SUs' position information. LPPA consists of two modules: *Privacy Preserving Bid Submission Protocol* (PPBS) and *Private Spectrum Distribution Protocol* (PSD). PPBS is build on prefix membership verification based privacy preserving range query protocol proposed by [11]. Through PPBS, SUs could submit their masked location information and bid price while the auctioneer could obtain the conflict relationship and the maximum value of bids on different channels without learning the exact user's position. Moreover, in order to permit the auctioneer to launch the auction, PSD introduces a greedy spectrum allocation algorithm to assign the channels among bidders and a pricing scheme to charge the winners securely with the help of TTP (Trust Third Party).

The contributions of our paper are summerized below:

- We identify a novel security threat in dynamic spectrum auction. Besides learning the buyers' positions directly from their submissions, the auctioneer can compromise the secondary users' location privacy according to their bid items and price. To the best of our knowledge, this paper is the first attempt to consider the location privacy leakage problem in dynamic spectrum auction.
- We propose a novel dynamic spectrum auction mechanism, LPPA, to thwart the location privacy leakage of secondary users. LPPA could prohibit the auctioneer from inferring the buyer's accurate position, meanwhile allowing spectrum auction launched efficiently.
- Simulation based on dataset released by FCC is conducted to validate the effectiveness of our attack and prove the efficacy of our scheme.

The rest of paper is organized as follows. In section II, we present our system model and attack model. In section III, the discovered attack is illustrated and in section IV and V, the two components PPBS and PSD of our approach LPPA are elaborated respectively in details. In section VI, we evaluate our scheme through extensive experiments. Section VII gives the description of the related works, which is followed by the summary in section VIII.

II. Preliminary

In this section, we give a brief introduction of dynamic spectrum auction and the fundamental of our bid submission scheme, prefix membership verification based privacy preserving range query protocol, followed by our adversary model and security assumptions.

A. Dynamic Spectrum Auction

We consider a typical dynamic spectrum auction in which one auctioneer auctions k channels among N bidders denoted as $SU_i, i \in \{1, ..., N\}, N > k$. These k channels may be owned by the auctioneer itself or some other spectrum owners. In the first case, the auctioneer itself is a spectrum license holder, while for the second case, it could be a third party delegated to launch the auction. We assume each spectrum is heterogeneous and has different available coverage due to the fact that the tower or base station of each PU is spatially diversified or different channels have various interference coverage. As a result, SUs from different locations may have various available channel sets which are denoted as $AS(i), i \in 1, ..., N$. For the ease of presentation, it is assumed that each buyer only pursue one channel for a short-term use (hours or days).

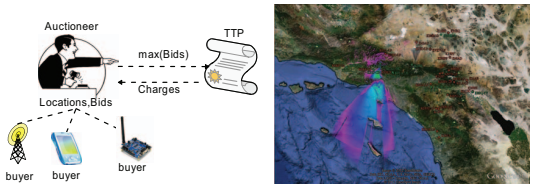
The spectrum auction procedure can be divided into the following four steps: (1) *Initial phase*: Through spectrum sensing or database query, a secondary user SU_i firstly obtains the condition of every channel independently and makes an evaluation. (2) *Bidding phase*: Each SU submits its ID i, location (loc_x^i, loc_y^i) and bids B_i on each channel to the auctioneer (the bid price will be zero if the spectrum is not available). Here, $B_i = \{b_1^i, ..., b_k^i\}$ is a vector representing the set of bids given by the SU_i. (3) *Allocation phase*: After collecting all the bids, the auctioneer carries out the spectrum allocation algorithm to decide who are the winners. (4) *Charging phase*: In this phase, the corresponding charge c_t of each winner would be determined by executing the pricing algorithm and published later.

B. Prefix Membership Verification Based Range Query

In this section, we review the privacy preserving range query protocol based on prefix membership verification scheme, proposed by [11]. At first, we introduce the prefix membership verification. The main idea of this scheme is to switch the verification of whether a figure is in a range to several checks of whether two numbers are equal. A prefix $\{0,1\}^s\{*\}^{w-s}$ with s leading 0s and 1s followed by $(w-s)$ $*$s is denoted as a s-prefix. Considering a w-bit binary number $t_1t_2...t_w$, we define the prefix family of this figure as the set of $w+1$ prefixes $\{t_1t_2...t_w, t_1t_2...t_{w-1}*, ..., t_1 * ...*, * * ...*\}$, where the ith prefix is $t_1t_2...t_{w-i+1}*...*$. The prefix family of x is denoted as $\mathcal{G}(x)$, where each prefix is a range containing figure x (i.e. $*$ represents either 1 or 0). For instance, the prefix family of 7 is {0111,011*,01**,0***,****}. Then, for any range $[y_1, y_2]$, we divide it to a set of prefixes, called $\mathcal{Q}([y_1, y_2])$. In fact, each prefix represents a subrange of $[y_1, y_2]$. For example, the prefixes set of range [6,14] is {011*,10**,110*,1110}.

Next, we propose the prefix numericalization function $\mathcal{O}(U)$ where U is an arbitrary prefix. Given a w-bit prefix $t_1...t_s * ...*$, the prefix numericalization function converts it to an unique $(w+1)$-bit number $t_1...t_s10..0$, which means we insert 1 between t_s and $*$ and then substitute 0 for all the $*$ (e.g. $\mathcal{O}(110*) = 11010$). Now, with the definition of prefix, we can conclude $x \in [y_1, y_2]$ if and only if $\mathcal{O}(\mathcal{G}(x)) \cap \mathcal{O}(\mathcal{Q}([y_1, y_2])) \neq \emptyset$ [11]. We take number 7 and range [6,14] as an example. The prefix numericalization set of range [6,14] is {01110,10100,11010,11101} and the prefix family of 7 is {01111,01110,01100,01000,10000}. There is a common number 01110 in both sets, thus 7∈[6,14].

Based on this scheme, privacy preserving range query protocol can be achieved as follows. Firstly, each original data processor transforms all its data to corresponding prefix numericalization families and encrypts the elements in every set using keyed-Hash Message Authentication Code (HMAC).



(a) (b)

Fig. 1. (a) The architecture of our auction scheme, (b) The coverage of channel KTBV-LD in Los Angeles.

After the masked data stored in an untrusted database, users would implement the same transformation and encryption on the range to set up a range query process. Due to the property of prefix membership issued above, the range query is switched into the checks of whether the couple of masked sets have common elements, with no data original value revealing. We would later elaborate how it works in our scenario in section IV.A and IV.B. Note that we choose this scheme as the foundation of our protocol because it provides significantly high level of security and could be efficiently extended to multi-dimensional data utilization [11].

C. Attack Model and Assumptions

We assume that the adversary's goal is to obtain the location of an SU, whose position is relatively fixed during one spectrum leasing time, by analyzing the bids from users. The attacker could either be the *curious-but-honest* auctioneer, who is stimulated to collect the location information of secondary users for marketing and sales strategies, or any external adversary who tries to infer the users' position by eavesdropping the spectrum auction process. The curious-but-honest model indicates that the auctioneer would honestly follow the protocol during the auction process but might attempt to compromise the SUs' location privacy passively. The general discussion on the motivation of service providers to collect mobile users' location information could be found in [13].

Note that the collusion between the attacker and some buyers is out of the scope of our paper [7]. Meanwhile, we presume the adversary has sufficient computation resource and spectrum condition information (available coverage of each channel and quality of spectrum in different positions) to perform a real-time analysis to geo-locate the users. It is also assumed that there exists a periodically available *trusted third party* (TTP) who is responsible to distribute the secret keys and help the auctioneer to decrypt the winner corresponding charge. Fig.1 (a) illustrates the entire architecture of our auction scheme.

III. Problem Formulation

In this section, we first introduce our basic location privacy compromising attack according to the bid channels of each buyer and then propose an advanced scheme by further exploiting the bid price of each spectrum.

A. Bid Channels Mining Attack

Obviously, the SUs would only bid the channels which are available to them all the time during the lease term, otherwise they might cause interference to the primary users. This fact indicates that SU must lie in the complement area of each corresponding PU's signal coverage. As a result, after obtaining each buyer's available channels set from their bids, the auctioneer could decrease the possible position range of the SU by intersecting the complements of different PUs' coverages. This is similar to the location privacy leakage issue in database-driven cognitive radio [19]. Through iteratively performing this operation, the attacker could acquire a relatively accurate estimation of SU's position if the cardinality of its available spectrum set is quite large.

To better qualify our problem, we divide the whole region into multiple cells and represent each cell by a pair of figures (m, n). m is the row number and n is the column one, respectively. We also denote the whole coverage of the map as A and the available communication range of each channel r as $C_r, r = 1, ..., k$ (i.e. the complement of PU signal coverage). Our basic attack algorithm is elaborated in Algorithm 1.

B. Bid Price Mining Attack

Most of the dynamic spectrum auction schemes proposed by existing research works [2] [4] [5] [7] are truthful (or strategy-proof), which means each buyer determines its bids according to the true value of the spectrum. The channel evaluation here is the estimation of the spectrum capacity or availability through spectrum sensing or database querying [5]. Although different SUs may have various bidding price according to the importance and urgency of their communication, their bids on each channel partly depend on the quality and characteristics of the spectrum which have a strong correlation with buyers' location. Consequently, after using BCM attack, the adversary could further narrow down the possible position range of each buyer by analysing the relation between bidding price and location.

To introduce our attack algorithm, we firstly define an estimated quality parameter $q_r^i, r \in AS(i)$ of each spectrum exploited by every user SU_i. This variable is computed as follows. By comparing all the bidding price of SU_i, the attacker finds out the maximum value b_{max}^i and corresponding channel r_{max} in the available channels set $AS(i)$. Next, regarding $q_{r_{max}}^i = 1$ as the reference, we compute other channels estimated quality parameter using the following equation:

$$q_r^i = \frac{b_r^i \times q_{r_{max}}^i}{b_{max}^i} = \frac{b_r^i}{b_{max}^i} \tag{1}$$

Algorithm 1: BCM Attack Algorithm

1: **Input**: the bid vector $B_i = \{b_1^i, ...b_k^i\}$ of SU_i.
2: **Output**: the possible location set P of SU_i.
3: **Initialization**: set $P = A$.
4: **for** Each component b_r^i of $B_i, r = 1, ..., k$ **do**
5: **if** $b_r^i > 0$ **then**
6: $P = P \bigcap C_r$
7: **end if**
8: **end for**

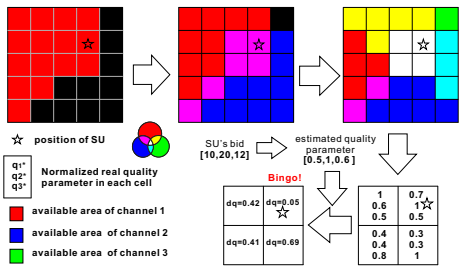


Fig. 2. An example of our attack

Apparently, a higher bid on the channel r implies a larger q_r^i, which means this spectrum has a higher quality. We assume the attacker has all the real quality statistics of each channel in each cell (it could obtain this information from a geo-location database), denoted as $q_r^*(m,n), r = 1,...,k$. Here, (m,n) represents the row and column number of the cell respectively.

Based on the buyer's bid, the adversary executes the basic attack algorithm to obtain the possible position set of SU_i and estimated quality parameter q_r^i at first. Then, it computes the distance $dq_{m,n}$ of every probable cell between estimated and real quality parameters as below:

$$dq_{m,n} = \sum_{r \in AS(i)} (q_r^i - \frac{q_r^*(m,n)}{q_{r_{max}}^*(m,n)})^2 \quad (2)$$

The attacker regards the cell with minimum distance dq^{min} as SU_i's position. Note that we normalized $q_r^*(m,n)$ by $q_{r_{max}}^*(m,n)$ because we define $q_{r_{max}}^i = 1$.

Fig.2 shows a simple instance of our BPM attack. After launching the basic attack, the attacker obtains the four-cell possible position set of buyer. According to user's bids, we could calculate the estimated quality parameter of each channel as $[0.5, 1, 0.6]$ and further obtain the dq value of every cell. Note that $dq(1,2) = 0.05$ is the minimum and thus the user is geo-located in cell (1,2) with real spectrum quality statistics $[0.7, 1, 0.5]$. The complete algorithm is shown in Algorithm 2.

Due to the fact that the performance of spectrum sensing is vulnerable to noise and channel fading, there may be a measurement discrepancy between the channel evaluation of secondary user and the real spectrum quality. Therefore, we choose multi-cells with the least values to be the output of our BPM attack for practical use. Note that, although this attack is more powerful for truthful auction, it still takes effect to general spectrum auction scheme because the bid price partly depends on the quality of spectrum. Moreover, in algorithm 2, we launch our BCM attack first to decrease the calculation work and make BPM attack more efficiently. However, even without our basic attack, BPM attack would still be set up by searching the whole possible cells and using the price of all the channels.

Algorithm 2: BPM Attack Algorithm

Input: the possible location set P of SU_i, its available channel set $AS(i)$ and the corresponding bid $b_r^i, r \in AS(i)$.
Output: the accurate position cell (x,y).
Initialization:$r_{max} = 0$, $b_{max}^i = 0$, $x = 0$, $y = 0$, $eq_{min} = MAXIMUM$.
for Each $r \in AS(i)$ **do**
  if $b_r^i > b_{max}^i$ **then**
    $r_{max} = r$, $b_{max}^i = b_r^i$.
  end if
end for
Set $q_{r_{max}}^i = 1$.
for Each $r \in AS(i)$ **do**
  $q_r^i = \frac{b_r^i}{b_{max}^i}$.
end for
for Each cell (m,n) in P **do**
  $dq_{m,n} = \sum_{r \in AS(i)} (q_r^i - \frac{q_r^*(m,n)}{q_{r_{max}}^*(m,n)})^2$
end for
for Each cell (m,n) in P **do**
  if $dq_{m,n} < dq_{min}$ **then**
    $x = m$, $y = n$,$dq_{min} = dq_{m,n}$.
  end if
end for

IV. Privacy Preserving Bid Submission Protocol

In order to thwart the BCM and BPM attack, we propose a novel *Location Privacy Preserving Dynamic Spectrum Auction* (LPPA) which consists of two modules: *Privacy Preserving Bid Submission* protocol (PPBS) and *Private Spectrum Distribution* protocol (PSD). We would elaborate PPBS in this section and leave the description of PSD in next part. PPBS aims to enable the buyers to submit their encrypted positions and bid price, meanwhile permitting the auctioneer to transparently construct the conflict relationship and find out the maximum bid price. It can be divided into two components: *Private Location Submission* protocol and *Private Bid Submission* protocol. We first propose the location submission protocol and basic bid submission scheme based on the prefix membership verification scheme proposed in [11]. Then we further introduce several problems while utilizing the basic bid scheme and give the corresponding modifications.

A. Private Location Submission Protocol

1) System Parameter: Our location submission scheme is elaborated in this section. For simplicity, we regard the interference range of each user as a *square* with the same side length 2λ and a centroid in his own position. Furthermore, each SU_i's location is represented as (loc_x^i, loc_y^i) (this pair of numbers can be the latitude and longitude coordinates from GPS or other geo-location system). Without loss of generality, we consider all the location coordinates as non-negative integers because other kind of numbers could be easily transformed to non-negative integers. Considering hidden terminal problem, SU_i and SU_j has a conflict relationship if and only if $|loc_x^i - loc_x^j| < 2\lambda$ and $|loc_y^i - loc_y^j| < 2\lambda$.

2) Key Generation: The TTP generates a secret key g_0 for HMAC (keyed-Hash Message Authentication Code) and distributes it to the bidders. This key is only known by the

SUs and TTP.

3) Location Submission Procedure: The protocol is composed of the following steps:

i. Each secondary user SU_i computes the family prefix of its own location components (i.e. $\mathcal{G}(loc_x^i)$ and $\mathcal{G}(loc_y^i)$) and converts the interference range $[loc_x^i - 2\lambda, loc_x^i + 2\lambda]$ and $[loc_y^i - 2\lambda, loc_y^i + 2\lambda]$ to the corresponding range prefixes (i.e. $\mathcal{Q}([loc_x^i - 2\lambda, loc_x^i + 2\lambda])$ and $\mathcal{Q}([loc_y^i - 2\lambda, loc_y^i + 2\lambda])$).

ii. Then SU_i makes numericalization transform of all the prefixes, i.e. calculates $\mathcal{O}(\mathcal{G}(loc_x^i))$, $\mathcal{O}(\mathcal{G}(loc_y^i))$, $\mathcal{O}(\mathcal{Q}([loc_x^i - 2\lambda, loc_x^i + 2\lambda]))$ and $\mathcal{O}(\mathcal{Q}([loc_y^i - 2\lambda, loc_y^i + 2\lambda]))$.

iii. Utilizing the key g_0, each user calculates the HMAC value of each numericalized prefix. For the convenience of presentation, we denote the composite function $\mathcal{H}_{g_0}(x) = HMAC_{g_0}(\mathcal{O}(x))$. That is to say, the bidders calculate $\mathcal{H}_{g_0}(\mathcal{G}(loc_x^i))$, $\mathcal{H}_{g_0}(\mathcal{Q}([loc_x^i - 2\lambda, loc_x^i + 2\lambda]))$, $\mathcal{H}_{g_0}(\mathcal{G}(loc_y^i))$, and $\mathcal{H}_{g_0}(\mathcal{Q}([loc_y^i - 2\lambda, loc_y^i + 2\lambda]))$. Then they submit these values to the auctioneer.

iv. After collecting all the submitted location information, the auctioneer constructs the conflict relationship between two different users i and j by examining the following two conditions:

$$\mathcal{H}_{g_0}(\mathcal{G}(loc_x^i)) \bigcap \mathcal{H}_{g_0}(\mathcal{Q}([loc_x^j - 2\lambda, loc_x^j + 2\lambda])) \neq \emptyset$$

$$\mathcal{H}_{g_0}(\mathcal{G}(loc_y^i)) \bigcap \mathcal{H}_{g_0}(\mathcal{Q}([loc_y^j - 2\lambda, loc_y^j + 2\lambda])) \neq \emptyset$$

If the two conditions hold simultaneously, the auctioneer concludes these two users would interfere with each other, otherwise they may use the same channel at the same time.

B. Basic Private Bid Submission Protocol

As is pointed out above, during the auction procedure, the auctioneer needs to find out the maximum value of a set of bids to determine the winner. In order to thwart the BCM and BPM attack, the bid submission protocol should keep the exact bid value secret while permitting the auctioneer to search *the largest price*. Similar to the location submission scheme, the basic bid submission protocol is also based on the prefix membership verification scheme. Next, we would introduce the *basic bid submission protocol* in details.

1) Protocol Initialization: We denote the upper bound of bid price as $bmax$ and assume the bids are non-negative integers. TTP generates the key gc, gb and delivers them to SUs. Here, gb is the key for HMAC and gc is the symmetric key of TTP. Also, these keys are kept secret from the auctioneer.

2) Bid Submission:

i. Each buyer SU_i firstly calculates the prefix conversion of all his spectrum bids $b_r^i, r = 1, ..., k$ and the corresponding range of $[b_r^i, bmax]$ utilizing the key gb (i.e. $\mathcal{H}_{gb}(\mathcal{G}(b_r^i))$, $\mathcal{H}_{gb}(\mathcal{Q}([b_r^i, bmax]))$). Then it submits these values and the encrypted bid price B_{gc}^i to the auctioneer.

ii. After collecting all the bids from buyers, the auctioneer tries to search a largest number b_{mx} in a group of bids

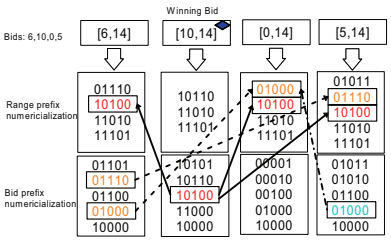


Fig. 3. An example of basic bid submission protocol

satisfying the following requirements for arbitrary bid b_a in the bid set.

$$\mathcal{H}_{gb}(\mathcal{G}(b_{mx})) \cap \mathcal{H}_{gb}(\mathcal{Q}([b_a, bmax])) \neq \emptyset \qquad (3)$$

Note that if equation (5) holds, $b_{mx} \geq b_a$. Therefore, we can conclude b_{mx} is the maximum value.

For instance, when four bidders bid {6,10,0,5} for one channel, they would submit the prefix family and range prefix as shown in Fig.3 (assuming $bmax$ is 14), respectively. After obtaining the encrypted bid price, the auctioneer checks whether there is a common number in each pair of different bids' prefix family and the range prefix. Here, 10's prefix family has the same number 10100 in both 6's, 0's and 5's range prefix set. As a result, we determine 10 is the largest bid. On the other hand, 6's prefix family has the common number 01110 with the range prefix of 5, but no equal figure in 10's, which indicates 6 is less than 10, but larger than 5. Note that prefix membership verification based encryption is a kind of order preserving encryption [12], as we can see in the above example.

C. Advanced Private Bid Submission Protocol

1) Insufficiency of Basic Bid Submission Scheme: Although the auctioneer cannot acquire the exact values of the bids, it can make the comparison operation directly on the encrypted price. This means, by omitting the minimum price (maybe zero) of the bids, the auctioneer could obtain the spectrum with positive bid price. Using these channels, the auctioneer can launch the BCM attack. This issue happens in the following *two phases*: (1) When one bidder submits his bid vector, the auctioneer would learn the available channel information of this user by neglecting his least bid component. (2) After collecting all the users' bids, the auctioneer would analyze all the bids on the same channel to find out the users with large bid price and conclude this spectrum unoccupied for him.

Meanwhile, it is apparent that the number of zero bid price is much larger than the amount of other values. Therefore, by filtering the encrypted figure with the largest showing frequency, the auctioneer may find out the zero bid price. What's more, although the number of prefixes in number prefix family is identical, the range prefix has different amount of elements (e.g. $[10, 14]$ has three prefixes while $[5, 14]$ has five, shown in Fig.3), which could be used to distinguish the price.

2) The Advanced Scheme: In this part, we would modify the basic bid submission scheme to address the above three problems. For the information leakage through one user's bid, we utilize the *different hash keys* to encrypt the bid

price on various channels. As a result, the auctioneer cannot compare the ciphertexts calculated by different HMAC. Then for the analysis of bids on one spectrum, we make zero price replaced by other non-zero numbers with certain probability. This implies we disguise zero price with the HMAC encryption of other numbers instead of itself. To maintain the performance of the auction system, for larger numbers, we set a smaller probability to have the substitution. Specifically, we denote the probability to substitute zero with number t as $p_t, t = 0, 1, ..., b(max)$ satisfying $p_1 \geq ... \geq p_{b(max)}$. Note that $b(max)$ is the maximum value of all the spectrum bid price for each user and zero has a probability p_0 to remain unchanged.

To prevent the auctioneer from filtering zero price, we let each user add an offset rd on all their bids and map the price zero to [0,rd] with the same probability. That is to say, when the bidder bids zero, it has a probability $\frac{1}{rd+1}$ to bid a price in range [0,rd]. Meanwhile, this change would not affect the result of the auction. To appropriately choose the value of rd and keep it secret, we would prohibit the auctioneer from finding out the zero price according to the bid distribution. For the different cardinality of range prefix family, we randomly choose the values out of the domain of HMAC output but with the same message length to fill in the set up to $(2w-2)$ [15] elements (w is the bit length of bid).

Next, we show the detailed steps of our advanced scheme. We assume TTP generates the HMAC keys $\{gb_1, gb_2, ..., gb_k\}$ and the value of rd and cr (described later in section V.B). These keys are shared to the bidders but hidden to the auctioneer.

i. Each buyer SU_i adds an offset rd to all its bids. Then it determines the sets of zero (here already becomes rd) replaced by different numbers, denoted as $V_0, ..., V_{b(max)}$, according to the probability $p_t, t = 0, 1, ..., b(max)$. For $0 \in V_0$, it maps them to the range $[0, rd]$ with the same probability $\frac{1}{rd}$.
ii. Then each bidder multiply his bid price by cr and randomly map the price x to the range $[cr \cdot x, cr \cdot (x+1) - 1]$ at uniform probability. The reason for this modification would be elaborated at the pricing algorithm in the next section.
iii. This step is similar to the phase 1 in basic bid submission scheme but using different HMAC keys. Moreover, for zero $\in V_t, t = 1, ..., b(max)$, we replace their encryption with number t's, which would make the auctioneer regards some zeros as positive integers. Meanwhile, we fill each range prefix to a $(2w-2)$-element set. Note that here we only change the HMAC outputs of zero price, but keep the ciphertext using key gc (TTP's symmetric key) unaltered.
iv. The scheme for auctioneer remains the same as basic approach.

3) Discussion on Tradeoff between Security Level and Auction Performance: The zero-replace probabilities are selected independently by each user according to its own privacy protection requirements. To prevent the auctioneer from isolating their available spectrum, the user could decrease p_0 while increasing $p_t (t \geq 1)$. Unfortunately, this would result in auction performance drop, because zero bid may occasionally win the auction. As a result, users should carefully select the value of p_t based on their demand for both privacy protection and spectrum utilization. To better quantify this tradeoff, we give three theorems below. Here, for the simplicity of presentation, we assume each bidder's zero price could be independently replaced by any number $r \in [0, bmax]$ with the probability p_r.

Theorem 1: *Given all the N SU's bids $b_1, b_2, ..., b_N$ on one channel (Without loss of generality, we suppose $b_1 \leq b_2 \leq ... \leq b_N$) and the total number of zero price m, the probability p_t with which zero price would not win the auction is:*

$$p_f = \frac{(1 - \sum_{r=1+b_N}^{bmax} p_r)^{m+1} - (1 - \sum_{r=b_N}^{bmax} p_r)^{m+1}}{(m+1)p_{b_N}} \quad (4)$$

Proof: The consequence zero price would not win could be resulted from the following two circumstances: (1) all the numbers replacing zero are less than b_N; (2) though some zero may be substituted by b_N, the original b_N is randomly chosen to be the winner. The probability of the first condition is $(1 - \sum_{r=b_N}^{bmax} p_r)^m$ and the one of the second is $\sum_{k=1}^{m} \frac{1}{k+1} \binom{m}{k} p_{b_N}^k (1 - \sum_{r=b_N}^{bmax} p_r)^{m-k}$. The sum of this two formulas could be simplified to the result shown above.

Theorem 2: *Given one channel bid $b_1, b_2, ..., b_N$ and the total number of zero price m, assuming the auctioneer would select the t-largest price and judge this spectrum available to the corresponding users ($m > t$ and for simplicity, we select t users, not all users bidding t-largest values), the probability p_f of no location information leakage would be:*

$$p_f = \sum_{k=t}^{m} [\binom{m}{k} (\sum_{r=1+b_N}^{bmax} p_r)^k (\sum_{r=0}^{b_N} p_r)^{m-k}] + \sum_{k=0}^{t-1} \{\binom{m}{k} \cdot (\sum_{r=1+b_N}^{bmax} p_r)^k [\sum_{j=t-k}^{m-k} \frac{j-1}{j} \binom{m-k}{j} (\sum_{r=0}^{b_N-1} p_r)^{m-k-j} p_{b_N}^j]\}$$

Proof: No location information leakage means the t-largest price are in fact all zeros. The results can also be divided into two conditions: (1) there are more than t zeros substituted by numbers larger than b_N; (2) there are more than t zeros replaced by numbers not less than b_N (including b_N) but the original b_N has not been randomly selected. The probability of the first circumstance is the former item of the formula and the second is the latter one. Note that in second formula, j represents the number of zeros replaced by b_N. Next, we consider the circumstance providing the best location privacy protection, which means $p_0 = p_1 = ... = p_{bmax} = p = \frac{1}{1+bmax}$.

Theorem 3: *Given one channel bid $b_1, b_2, ..., b_N$ and the total number of zero price m, assuming the auctioneer would select the t-largest price, we define μ as the number of non-zero bid price (plaintext) chosen by auctioneer. Then the*

expectation value $E[\mu]$ *is:*

$$E[\mu] = \sum_{\mu=1}^{t} \mu p^m \{ \binom{bmax - b_{N-\mu} - \mu}{t-\mu} \sum_{j=t-\mu}^{m} [\binom{m}{j} \cdot \sum_{i=0}^{j-t+\mu} \binom{j}{i} \binom{i+\mu-1}{\mu-1} \binom{j-i-1}{t-\mu-1} (1+b_{N-\mu})^{m-j}] \}$$

Proof: Note that here unlike the theorem 2, we select all the users bidding t largest price. We first consider the circumstance that μ non-zero bids are selected by the auctioneer. This means only $t-\mu$ values substituting zero are larger than $b_{N-\mu}$ and the amount of all possible combinations is $\binom{bmax-b_{N-\mu}-\mu}{t-\mu}$. Here, we regard the problem of replacing $j, t-\mu \leq j \leq m$ zeros by t values as the equivalent question of placing j balls into t drawers. Note that, here, $t-\mu$ drawers should have at least one ball in each drawer while μ drawers can contain any number of balls. The number of these combinations is $\sum_{j=t-\mu}^{m}[\sum_{i=0}^{j-t+\mu}\binom{j}{i}\binom{i+\mu-1}{\mu-1}\binom{j-i-1}{t-\mu-1}]$. Therefore, the probability that μ true bids are selected by the auctioneer is shown above. From the theorem above, we can observe the location privacy preserving level depends on the value of zero changing probability and the number of largest price the auctioneer selects.

4) Impact on Communication Cost: In order to protect the location privacy, our protocol utilizes the prefix membership verification to converse a number into a set of prefix, which definitely increase the communication volume. To quantify this cost, we give theorem 4 as below:

Theorem 4: *Given the length w of the bid number and the ratio h of the HMAC output length to the original prefix length, the total transmission cost of our advanced bid submission protocol is $h \cdot k \cdot N(3w-1)(w+1)$.*

Proof: The prefix family of each bid has $(w+1)$ elements and the cardinality of range prefix is at most $(2w-2)$ [15]. Meanwhile, each prefix is a $(w+1)$-bit number. Therefore, the total bits transmitted during one auction is $h \cdot k \cdot N(3w-1)(w+1)$ where k is the number of spectrum. As we can see, our total communication cost is linear to the user number N. Meanwhile, due to the low computational complexity of hash function, the system resource needed for our security scheme is quite small.

V. Private Spectrum Distribution Protocol

In this section, we introduce the *Private Spectrum Distribution protocol* (PSD) which permits the auctioneer to transparently launch the auction. PSD contains a greedy *spectrum allocation algorithm* to assign the spectrum among bidders and a *charging algorithm* to securely determine the winning bids with the help of TTP (trusted third party). Next, we introduces the protocols in Algorithm 3.

A. Spectrum Allocation Algorithm

Existing spectrum auctions either only consider the spectrum with uniform characteristics [2], [4], or require available channels information to deal with the spatial heterogeneity of spectrum [5], [8]. As a result, to assign the channels among bidders without revealing their available spectrum set, we give a greedy algorithm *Spectrum Allocation Algorithm*.

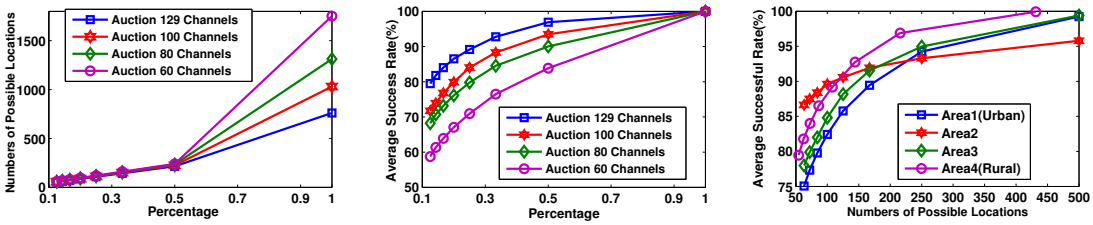
Algorithm 3: Spectrum Allocation Algorithm

1: **Input**: the bid table T of all the users.
2: **Output**: the winner and corresponding spectrum W.
3: **Initialization**: set $R = \{1, ..., k\}$ and $W = \emptyset$.
4: **while** $T \neq \emptyset$ **do**
5: randomly select r from R in uniform probability and find the maximum value $T_{bx,r}$ in rth column.
6: add $[bx, r]$ to W
7: delete $T_{o,r}, \forall o \in N(bx)$ and the bxth row of T.
8: **if** $R \neq \emptyset$ **then**
9: delete r from R.
10: **else**
11: $R = \{1, ..., k\}$
12: **end if**
13: **end while**

After executing the bid submission protocol, the auctioneer actually obtains a table of users' bids. The row of the table is one bidder's bid price for all spectrum while the column contains different users' bid for the same channel. At first, the auctioneer randomly selects a channel and finds out the maximum bid utilizing the approach elaborated in the previous section. Then after the winner has been determined, the auctioneer deletes the winner's row and his neighbor nodes' bid item for the same channel (here the neighbor nodes has conflict relationship with the winner). Next, we randomly choose another spectrum to iteratively execute the procedure above until all the channels have been selected once. The auctioneer then goes back to randomly choose one channel to repeat this operation until all the items are removed from the table. The detailed algorithm is shown in Algorithm 3. For the simplicity of presentation, we denote the bid table as T and $T_{i,j}$ as the element of ith row and jth column which represents the bid price of user SU_i on channel j, $N(i)$ as the index set of bidders interfering with SU_i.

B. Charging Algorithm

To securely charge the winners, we need a trusted third party (TTP) to decrypt the winners' bids and send them back to the auctioneer. After executing the spectrum allocation algorithm, the auctioneer delivers the masked winning bid b_{gc} encrypted by the TTP's key gc and the corresponding prefix set to the TTP. Then the TTP decrypts b_{gc} and obtains the plaintext b. Note that the bid price has already been mapped to a range (We would explain the reason in the next paragraph). We divide it by cr and acquire the original bid price $\lfloor \frac{b}{cr} \rfloor$. Here, $\lfloor x \rfloor$ refers to the largest integer not greater than x. Next, if the bid price is zero (belonging to the range $[0, rd]$), the TTP would send a notification to inform the auctioneer that this winning price is invalid. Otherwise, TTP will verify the bid price and its corresponding prefix to confirm that the bidder do not manipulate the price, as the price is sealed to the auctioneer.



(a) Number of possible cells (b) Successful rate (c) Results in 4 areas

Fig. 4. (a) Number of possible cells and (b) successful rate of BCM and BPM attack in Area 4. (c) Results of BCM and BPM in 4 areas

The operation of multiplying the bids by cr is due to the reason as follows. After obtaining the charging price, the auctioneer may have some plaintext-ciphertext pairs of bids. By searching the price with the same ciphertext, the auctioneer could deduce the corresponding plaintext of the bid. To thwart this information leakage, we map each bid value to a range and thus encrypt the same price into several different ciphertexts indistinguishable to the auctioneer.

C. Further Discussion

1) Truthful Auction: We choose our charging algorithm as the first-price payment where the winner pays the exact amount of his bid. Note that although this auction may not be truthful (strategy-proof), we focus our research on location privacy compromising issue and leave the truthfulness of the auction to future work.

2) Reducing the Online Time of TTP: To preserve the privacy of the bid price, our auction needs a TTP to help the auctioneer decrypt the winner charges, which would definitely increase the workload of TTP. To reduce the online time of TTP, we would once send the results of several auctions to TTP for batch process. The number of auction results delivered once could be determined by both the real-time requirement of the system and the longest online time of TTP.

3) Participating in Auction Several Times: If a user participates the auction several times without ID changed, the auctioneer could collect much information about this SU even with our protocol. What's worse, if one user wins the auction a few times, the attacker may utilize the winning spectrum to launch the BCM attack with a high accuracy. To thwart this issue, we can mix the buyers' IDs once the auction finished or use the different ID pools in each auction.

VI. Experiment Results

In this section, we first demonstrate the efficacy of our attack algorithm and then evaluate our PPBA and PSD protocol from aspects of users' location privacy leakage and impact on auction performance.

A. Experiments Setup

We set up our experiment utilizing the spectrum available information of Los Angeles released by FCC on TVFool [17]. There are totally 129 channels in LA and Fig 1. (b) shows the coverage area of one. To conduct our experiment, we select four places with the area $75km \times 75km$ and divide them into 100×100 cells, where the SUs are distributed randomly. Each SU_i determines its bid on channel j using the formula $b_j^i = q_j\beta_i + \eta$. Here, q_j is the spectrum quality, quantified by the intensity of PU signal. β_i is the user's transmission emergency value, which indicates the urgency degree of SU's communication. Due to the fact that SUs may sometimes determine their bid price based on other factors besides channel quality, we add a noise $|\eta| \leq 20\%q_j\beta_i$. Although according to the FCC rules a channel is regarded as unoccupied if the corresponding transmission power is less than or equal to -114dBm, we set this threshold to -81dBm considering the practical limitation [16].

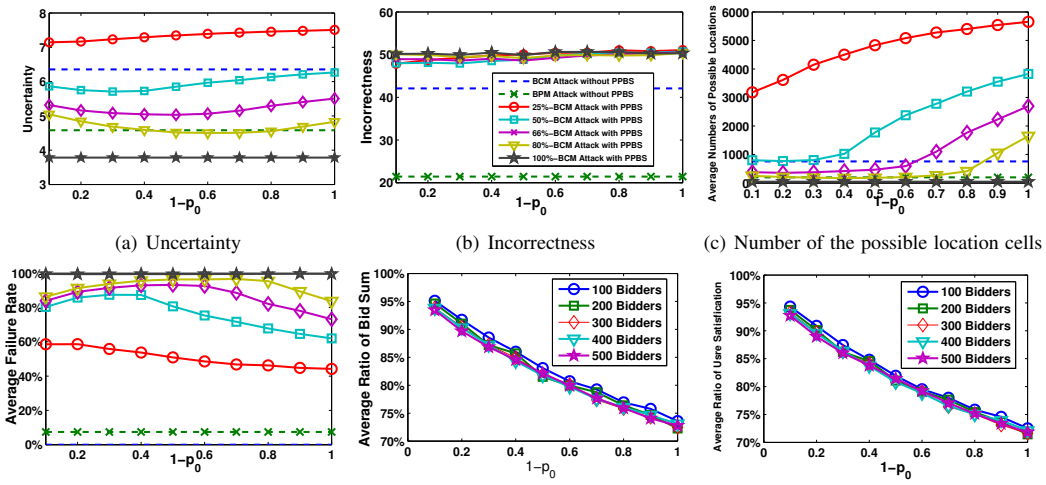
To evaluate the effectiveness of our attack scheme, we first launch the BCM attack to obtain the possible range of SU's locations and then execute the BPM attack to further geo-locate the SU with a higher accuracy. Note that, for BPM attack, we choose different percentages of the total possible location cells (obtained by the BCM attack) with the least dq values as the final results.

To assess the efficacy of our LPPA protocol, we analyze the location privacy leakage of users under BCM and BPM attack with and without LPPA through the metric of uncertainty, incorrectness, failure rate and the number of possible position cells. From [13], we define *uncertainty* as $\sum_{x\in P_i} Pr_x \log \frac{1}{Pr_x}$, where P_i is the possible region of SU_i from the attack result and Pr_x is the probability of SU_i in cell x. *Incorrectness* is represented as $\sum_{x\in P_i} Pr_x \|l_x - l_0\|$, where $\|l_x - l_0\|$ is the distance from cell x to the true location l_0 of SU_i. We further regard the attack failure as that SU_i's position does not belong to the range obtained by the attacker. It should be mentioned that the larger the values of uncertainty, incorrectness, failure rate and numbers of possible locations are, the better SUs preserve their location privacy.

At last, we evaluate the impact of our security protocol on auction performance in two aspects: sum of winning bids and user satisfaction. *sum of winning bids* represents the gross of all the winners' charges and *user satisfaction* indicates the proportion of the bidders possessing the spectrum. We compare the results through the auctions with and without LLPA.

B. Evaluation of BCM and BPM Attacks

We set up the experiment evaluating the effectiveness of BCM and BPM attack in four areas and the results are shown in Fig.4. Fig.4 (a) (b) demonstrates the amount of possible



(a) Uncertainty (b) Incorrectness (c) Number of the possible location cells

(d) Failure rate (e) Sum of winning bids (f) User satisfaction

Fig. 5. (a) Uncertainty, (b) incorrectness ,(c) number of the possible location cells and (d) failure rate of BCM and BPM attack, respectively, with and without LPPA. (e) Reduction of winning bids sum and (f) user satisfaction with LPPA

location cells and the average successful rates of our attack set up in Area 4 with different numbers of auction channels and percentages chosen by BPM attack ($\frac{1}{2}, \frac{1}{3}, ...$). As we can see, the BCM attack algorithm could decrease the possible area of users from 10000 cells into almost less than 1800 cells. Meanwhile, for BPM attack, with the percentage of total cells declining, the size of locations decreases dramatically while error rate rising. Note that the rightmost node of each curve is the one-hundred percent of probable cells, which indicates the output of BCM scheme. To better improve the BPM attack performance, we set a threshold to limit the largest number of cells chosen by the algorithm. For instance, we define this threshold as 250 for the 80 channels auction and 50 percent attack. That is to say, if half of the total cells are larger than 250 (i.e. threshold), we only select the 250 least value cells as the result, causing the average size less than $\frac{800}{2} = 400$. Fig.4 (c) shows the results of all the four areas under 129-channel auction. Note that we only draw a part of the curve for Area 2 because the BCM attack output is quite large. We can observe the effectiveness of our attack is usually better in rural distinct than urban ones due to the influence of terrain factor.

C. Evaluation of the Effectiveness of LPPA

Our simulation demonstrating the efficacy of our LPPA protocol is launched in Area 3. We use different zero-replace probability (i.e. $1 - p_0$) in our PPBS scheme. In Fig.5 (a) (b) (c) (d), we can observe that the numbers of possible locations, incorrectness and uncertainty of BPM attack decrease about 75%, 50% and 28% than BCM, respectively, paying an rise of failure rate at about approximately 7%. As elaborated above, by keeping bid price hidden to the auctioneer, our protocol could completely thwart the BPM attack and to some extent defend against the BCM attack. Meanwhile, our scheme obfuscates the bid price order by replacing zero with other large price, significantly increasing the failure rate of BCM attack. To assess the performance of our protocol in detail, we select 25%, 50%, 66%, 80% largest bids to set up the BCM attack. As illustrated in Fig.5, with the increasing of the percentage, uncertainty and location range decline while failure rate rising, due to the ascending number of 'available' spectrum recognized by the auctioneer. However, incorrectness varies according to the change of percentage and zero replacing probability.

The simulation results also show that, as the rising of the zero changing probability $1 - p_0$, the curves of four metrics vary significantly in different cases. The incorrectness remains nearly the same (at about 47%) even if the attacker uses different ratio of encrypted bids. However, as the probability increasing, the number of position firstly maintains the same and then bursts dramatically. This is because when the zero changing probability is relatively small, the largest price would not contain so many disguised zeros. But when the probability reaches a threshold, the forged available spectrum information decreases the performance of attack. It is quite interesting that the curves of failure rate do not monotonically change. We think the reason for this result is that the increase of forged information firstly decrease the effectiveness of attack, and then as the obtained zero bid rises, some truly available spectrum are selected by the attacker (because the bid of the available spectrum with low quality can be zero), leading to failure rate decreasing. Note that when the attacker use the 100% information of the bidding tables regardless of false messages, it has a failure at about 99.5%

D. Impact on Auction Performance

In this part, we focus on the evaluation of impact on auction performance. The tradeoff of our protocol between location privacy preservation and auction performance is shown in fig.5 (e) (f). As we can see, both of the sum of winning bids and user satisfaction decrease from about 95% to 73% when $1-p_0$ increase from 0.1 to 1. However, the ascending number of SUs does not have a strong influence on the performance, validating the scalability of our protocol. Moreover, we consider the sacrifice of our scheme is tolerable because the maximum of

cost is less than 30%. In order to maximize the performance of the whole auction system, the users should carefully select the zero replacing probability according to their location privacy preserving and spectrum utilization requirements.

VII. Related Works

A. Dynamic Spectrum Auction

The great potential and promise has motivated a lot of research works focusing on how to efficiently and truthfully execute a dynamic spectrum auction. Unlike other traditional auction schemes, dynamic spectrum auction permits the well-separated bidders to utilize the same channel simultaneously as long as the bidders subject to the conflict constraints. [2], [4], [9] have proposed several different auction mechanisms aiming at various objects (truthfulness and revenue maximization). However, these papers only consider a scenario where all channels have uniform characteristics and are available to all buyers, which is definitely insufficient for practical applications due to the spectrum spatial diversity. In [5], [7], [8], the authors introduce some auction approaches providing buyers capability and flexibility to express diverse channel preferences taking spectrum heterogeneity and spatial diversity into consideration.

B. Security Threats in Dynamic Spectrum Auction

While holding the promise in significantly improving spectrum utilization, dynamic spectrum auction is also facing a series of security vulnerabilities. Most of the existing literatures mainly concentrate on the truthfulness (strategy-proof) of the auction [2] [4], or purging back-room dealing [7]. In [6], aside from the bid rigging problem, the author proposes a novel attack in which selfish bidders can deliberately report forge arrival time to obtain unfair advantage in online spectrum auction. Nevertheless, none of the previous literatures consider the location privacy leakage in dynamic spectrum auctions. [7] introduces a cryptographic technique scheme based on paillier public key encryption to prevent the auctioneer from obtaining the real value of bids. However, it requires several auctioneers to share the secret and leads to a large number of communication costs, which does not fit for an efficient auction mechanism.

C. Location Privacy in Cognitive Radio Network

Location privacy issue in cognitive radio network has received attentions recently. In [10], the authors propose a novel attack in collaborative spectrum sensing to geolocate the secondary users by exploiting their location-dependent sensing report. Meanwhile, [19] identifies a new kind of attack against location privacy of database-drive CRNs. Instead of directly learning the SUs' locations from their queries, the attacker can infer users' positions through their used channels.

VIII. Conclusion

In this paper, we identify the location privacy leakage problem in dynamic spectrum auction and propose two kinds of attack, BCM and BPM. To deal with such location privacy issues, we introduce LPPA protocol consisting of two components: PPBS and PSD. PPBS enables the user to privately submit their location and bid price while PSD allows the auctioneer to transparently launch the spectrum auction. Meanwhile, extensive experiment results based on the data released by FCC demonstrate the efficacy and efficiency of our scheme. Our further work will focus on the truthfulness of the location privacy preserving spectrum auction.

Acknowledgment

This work was partially supported by National Basic Research Program of China under the grant 2010CB731803, NSF of China under the grants 60934003, 61003218, 61272444, 61273181 and 61221003, and Research Fund for the Doctoral Program of Higher Education of China under the grant 20100073120065, 20110073130005.

References

[1] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "Next eneration/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks (Elsevier) Journal*, September 2006.

[2] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "Ebay in the sky: Strategy-proof wireless spectrum auctions," *Proc. of ACM MobiCom'08*, 2008.

[3] Spectrum Bridge, Inc.[online]. Available: http://www.spectrumbridge.com/.

[4] J. Jia, Q. Zhang, Q. Zhang, and M. Liu, "Revenue generation for truthful spectrum auction in dynamic spectrum access," *Proc. of ACM Mobihoc'09*, 2009.

[5] X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, "Tahes: a truthful double auction mechanism for heterogeneous spectrum," *Proc. of IEEE INFOCOM'12*, 2012.

[6] L. Deek, X. Zhou, K. Almeroth, and H. Zheng, "Preempt of not tackling bid and time based cheating in online spectrum auction," *Proc. of IEEE INFOCOM'11*, 2011.

[7] M. Pan, J. Sun, and Y. Fang, "Purging the back-room dealing secure spectrum auction leveraging paillier cryptosystem," *IEEE JSAC*, Vol. 29, No. 4, pp. 866-876, 2011.

[8] M. Parzy and H. Bogucka, "Non-identical objects auction for spectrum sharing in TV white spaces - the perspective of service providers as secondary users", *Proc. of IEEE DySPAN'11*, 2011.

[9] S. Gandhi, C. Buragohain, L. Cao, H. Zheng, S. and Suri, "A general framework for wireless spectrum auction," *Proc. of IEEE DySPAN'07*, 2007.

[10] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen, "Location privacy preservation in collaborative spectrum sensing," *Proc. of INFOCOM'12*, 2012.

[11] F. Chen, and A.X. Liu, "SafeQ: Secure and efficient query processing in sensor networks," *Proc. of IEEE INFOCOM'11*, 2011.

[12] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," *Proc. of ACM SIGMOD'04*, 2004.

[13] R. Shokri, G. Theodorakopoulos, J. Le Boudec, and J. Hubaux, "Quantifying location privacy," *Proc. of IEEE S&P'11*, 2011.

[14] Z. Gao, H. Zhu, Y. Liu, M. Li. and Z. Cao, "Location Privacy in Database-driven Cognitive Radio Networks: Attacks and Countermeasures," *Proc. of IEEE INFOCOM'13*, 2013.

[15] P. Gupta and N. McKeown, "Algorithm for packet classification,"*IEEE Network*, Vol. 15, No. 2, pp. 24-32, 2001.

[16] R. Murty, R. Chandra, T. Moscibroda and P. Bahl, "Senseless: A database-driven white spaces network," *IEEE TMC*, Vol. 11, No. 2, pp. 189-203, 2012.

[17] "TV Fool", March 2012.[Online]. Available: http://www.tvfool.com

[18] S. Li, H. Zhu, Z. Gao, X. Guan and K. Xing, "YouSense: Mitigating Entropy Selfishness in Distributed Collaborative Spectrum Sensing," *Proc. of IEEE INFOCOM'13*, 2013.

[19] S. Liu, H. Zhu, S. Li, X. Li, C. Chen, and X. Guan, "An Adaptive Deviation-tolerant Secure Scheme for Distributed Cooperative Spectrum Sensing," *Proc. of IEEE GLOBECOM'12*, 2012.