Optimal Strategies for Defending Location Inference Attack in Database-driven CRNs

Long Zhang, Chenliaohui Fang, Yi Li, Haojin Zhu
School of Computer Science and Technology
Shanghai Jiaotong University, Shanghai, China
Email: {hckrzl,fclh1991,dakongyi,zhu-hj}@sjtu.edu.cn

Mianxiong Dong
Muroran Institute of Technology, Japan
Email: mx.dong@ieee.org

***Abstract*—Database-driven Cognitive Radio Network (CRN) has been proposed to replace the requirement of spectrum sensing of terminal devices so that the operation of users is simplified. However, location privacy issues introduce a big challenge for securing database-driven CRN due to spectrum availability information. The existing works consider either PU or SU's location privacy while not the both. In this study, we identify a unified attack framework in which a curious user could infer a target's location based on the spectrum availability/utilization information. Further, we propose a location privacy protection mechanism, which allows both SU and PU to protect their location privacy by adopting a series of countermeasures. The location privacy and spectrum utility are the trade-off. In the countermeasures of location privacy preserving spectrum query process, both SU and database aim to maximize the location privacy with constraints of spectrum utility. Thus, they can obtain higher location privacy level with sacrifice of spectrum utility as long as the spectrum utility meets the requirements. We evaluate the unified attack and defence approaches based on simulation and demonstrate the effectiveness of the proposed location privacy preserving approaches.**

I. Introduction

The ever increasing demand of spectrum for wireless applications has inspired the emerging concept of CRN, which is considered as a promising way to improve the utilization of the scarce radio spectrum. In CRN, primary users (PUs) own exclusive privilege to access the licensed spectrum while unlicensed or secondary users (SUs) are allowed to opportunistically access the spectrum bands as long as they do not cause any interference to PUs. Recently FCC has proposed another approach, Database-driven CRN [1], in which an SU can request Spectrum Availability Information (SAI) from an authorized database instead of spectrum sensing. The SU is required to submit its geo-location information and some device parameters to the database. FCC has designated several entities [2](e.g. Comsearch, Google Inc.) as TV bands database administrators. Recently, two TV Bands database systems designed by Koos Technical Services, Inc. and Telecordia Technologies, Inc. have been approved by FCC for operation. Database-driven CRN has a great advantage in enhancing the efficiency of spectrum utilization, improving the accuracy of available spectrum identification, and reducing the complexity of terminal devices. However, as a variant of Location Based Service (LBS), one of the major research challenges for database-driven CRN is the privacy issues, especially in the aspect of location privacy. The existing researches [3] [4] have pointed out that both channel utilization information and transmission power information can be exploited by the adversary to infer the locations of SU or PU, respectively. This will incur serious location privacy leaking for the SU or PU.

In recent years, location privacy is receiving an increasing attention in both of academia and industrial community. From SU's point of view, the existing studies have shown that location traces of users can leak information about the individuals' habits, interests, activities, and relationships [5]. What's more, loss of location privacy can expose users to unwanted advertisements and location-based spams/scams, cause social reputation or economic damage, and make them victims of blackmail or even physical violence. From PU's point of view, location privacy issue is also of high importance, especially considering the recent calls in the United States for spectrum sharing of federal government including military with non-government systems, in the 3.5 GHz band. Note that, 3.5 GHz is currently used by the U.S. Department of Defense (DoD) for certain radar installations. Therefore, protection of location privacy is highly desirable for both SU and PU.

There are several existing literatures [3] [4] [11] working on location privacy issues in database-driven CRN, which focus on privacy of either SU or PU. However, none of them considers both. In this study, we first introduce a unified location privacy attack framework in which an attacker can exploit the spectrum availability/utilization to launch a location inference attack towards a target SU or PU. We then introduce a location privacy protection framework based on K-anonymity technique [10], including approaches of spectrum query and spectrum response as well as privacy preserving channel selection.

The contributions of this work are summarized as follows:

- We propose a unified framework for location privacy inference attack on both SU and PU in database-driven CRN. To thwart the problem of location privacy leaking, we introduce a location privacy preserving framework for available spectrum query and retrieval.
- We quantify the location privacy level and spectrum utility in the context of unified location privacy preserving framework. Our analysis shows that the location privacy level and spectrum utility of SU are determined not only by its own actions but also the choices of the database, and vice versa.
- We formulate the optimal strategies of the SU and the database as optimization problems from the system perspective. We conduct extensive evaluations to

978-1-4673-6432-4/15/$31.00 ©2015 IEEE

demonstrate the efficiency of the proposed location privacy preserving scheme.

The remainder of this paper is organized as follows. In section II, we present the background and the system model. In section III, we introduce the unified attack scheme. In section IV, we give the location privacy preserving scheme and analyse the maximum location privacy which can be obtained by the users. In section V, we evaluate the attacks and corresponding solutions. Finally we conclude our work in section VI.

II. Background and System Model

A. Overview of Database-driven CRN

Database-driven CRN provides opportunistic spectrum access service based on the location of SU. It mainly consists of four categories of components: Database, Base Station (BS), PU and SU. SAI is calculated and stored in the database based on the knowledge of PUs and environmental parameters. BS is a radio infrastructure that provides wireless interfaces and connects the SU and the database. PU registers on the database for exclusive privilege of spectrum utilization and doesn't necessarily interact with the SU. However, when PU changes status, i.e., from on-line to off-line or from off-line to on-line, it should inform the database to re-calculate the spectrum availability. For the SU, prior to accessing the spectrum, it has to communicate with the database to obtain SAI via internet connection [6]. This process is known as spectrum availability retrieval. Based on the SAI retrieved from the database, SU can select an available channel and optionally send notification to the database. The detailed operations of the database will be described later in this section.

B. System Model

1) Basic Assumptions: In this article, we assume a region R which is regulated by a database is divided into $n \times n$ square cells, in which the spectrum availability is relatively stable. The cells are represented by c_{ij}, where i is the row index and j is the column index. We assume that there are totally C channels and C PUs, i.e., there is at most one PU operating on a channel. The spectrum availability provided by the database is denoted as $((ch_1, P_1, t_1), (ch_2, P_2, t_2), ..., (ch_k, P_k, t_k))$, where ch_i denotes the channel, P_i is the maximum allowable transmission power of ch_i, and t_i is the allowable operation duration on ch_i. The maximum allowable transmission power is calculated by a function $P = h(\cdot)$, where $\cdot$ represents the information used to calculate the spectrum availability including relative distance between SU and PU [4]. The Maximum Transmission Power (MTP) calculated by the database is divided into several levels. Specifically, when the distance between SU and PU is less than d_0 which is the protection radius, SU is not allowed to transmit on the PU's channel. If the distance turns larger, the SU is allowed to transmit at an increasing power level based on the increasing distance till the largest transmission power P_{max} is achieved. Here, P_{max} is the maximum allowed transmission power in database-driven CRN regulated by FCC.

2) Database Query Process: According to the latest IETF standard [6], a typical spectrum query process can be depicted in detail as follows:

- **Spectrum Query**: SU_i gets its geo-location via the built-in positioning module and sends the query message $Que = (ID_i, loc_i)$ to database. Here ID_i is the unique identifier of SU_i and loc_i represents the located cell of SU_i. Note that, SU could query spectrum availability for multi-cells in the vicinity.
- **Spectrum Response**: The database searches the channels which can be used at loc_i and then returns the available channel set and corresponding MTP to SU_i in response message. We assume that the available channel set contains all the available channels. One unit of spectrum availability in the response message is denoted as $Res = (c_{ij}, ch_k, P_k, t_k)$.
- **Spectrum Notification**: SU_i selects a channel and then sends a notification message to the database. Note that, the notification message is not required. However, spectrum notification information is beneficial to the database to manage the spectrum database more efficiently. The notification message is denoted as $Not = (ID_i, ch_k, P_k)$.

C. Attack Model

We assume that there might be some curious SUs in the network and both the database and the SUs may be potential attackers who are curious of each other's location privacy. The attacker's goal is to infer the location of a target SU or PU whose position is relatively fixed in a certain time duration. The attacker is assumed to know the complete communication contents between the SUs and the white space database.

We consider a general curious-but-honest model, which means both of the SU and the database will never falsify the data or query results maliciously. What's more, the SU knows how the database calculates SAI. We also assume the attacker has sufficient computational resources such that it can perform real-time analysis and run necessary algorithms to geo-locate the target.

III. A Unified Location Inference Attack in Database-driven CRN

The database-driven CRN faces serious location privacy issues due to the nature of LBS. On one hand, an SU must submit accurate location to the database to obtain spectrum availability. In the latest IETF standard, location of the SU will be directly sent to the database. Once the database is curious about the location privacy of the SU or it mishandles the received location data, the SU will face serious security threats. Even when the location blinding scheme [3] is adopted, based on the spectrum notification messages which contain selected channel and corresponding transmission power, location privacy of the SU still leaks since the transmission power can be translated to a spatial coverage. On the other hand, the spectrum availability provided by the database can also be translated to a spatial coverage of PU. A curious SU can collect the SAI continuously to gradually reveal the actual location of a specific PU. Existing works either focus on geo-locating SU or geo-locating PU. However, none of them considers the location privacy issues from both PU and SU's sides. In this section, we show two cases which incur location privacy leaking in the spectrum query process and introduce a unified

location privacy attack which can potentially be exploited by an attacker.

A. Two Identified Attacks of Location Privacy

Based on the MTP function, the allowable transmission power is strongly correlated with the relative distance between a specific SU and a specific PU. Specifically, each spectrum unit (ch_k, P_k) reveals some distance information, i.e., the power can be translated into a spatial coverage based on the MTP function. We identify two cases which incur location privacy leaking. In this article, duration of operation is not taken into consideration.

1) ***Attack Based on Power Limitation****:* We know that the MTP is discretely leveled so that the database could provide spectrum utility more efficiently. In an ideal situation, we assume the coverage of a limited transmission power can be mapped into an annular area. Whenever a spectrum unit is received by the SU or reported to the database, the SU or PU's location privacy leaks. Fig. 1(a) is an illustration of location inference attack based on power limitation.

In Fig. 1(a), if an attacker receives an spectrum unit (ch_k, P_k) in which $P_k < P_{max}$, it is derived that the target is located with high probability in an annular area which takes the attacker itself as the center and d_1, d_2 as the internal radius and external radius respectively. Both the database and an SU can be the attacker.

2) ***Attack Based on Channel Switch****:* Another case which incurs location privacy leaking is when an SU is in the protection region of a specific PU. Here the protection region is the area in which no SU is allowed to transmit. If the PU is off-line and the SU selects to use the PU's channel and then the PU turns on-line, the SU has to switch to another channel. Suppose that the protection region is a circle with radius d_0. Thus, the attacker knows that the target is in a circular area which takes the attacker's location as the center and d_0 as the radius with high probability. Fig. 1(b) illustrates the case.

In Fig. 1(b), when the PU turns from off-line to on-line, the SU has to switch to another channel so that the target must be located in a circular area C_1/C_2 with high probability.

B. The Unified Location Inference Attack Algorithm

The Unified Location Inference Attack is designed to infer a specific target's location based on the information in the spectrum query process. When the attacker is an SU, we suppose that the target is a specific PU. When the SU is curious about other PUs, it can similarly launch the attack scheme against them. Without loss of the generality, we generally denote the spectrum unit sequence which will be exploited in the attack as $S = ((loc_1, ch_1, P_1), (loc_2, ch_2, P_2), \ldots, (loc_n, ch_n, P_n))$. Note that, when the attacker is an SU, ch_i should be the channel on which the target PU operates. If the database is the attacker, there is no location information due to the location blinding technique. Based on the spectrum availability and spectrum usage information in the history, an attacker can gradually reduce the possible distribution area of the target. Suppose the covered area based on the center loc_i and the transmission power P_i is denoted as $Cov(loc_i, P_i)$ which can be readily calculated, the detailed attack process can be illustrated in Algorithm 1. In the attack implementation, we set a $n \times n$ probability matrix for cells in R and update the matrix following the Bayes Rule proposed in [4]. Once the probability of a specific cell exceeds a pre-defined threshold δ, we consider that the cell might be a candidate location of the target.

Algorithm 1: Unified Location Inference Attack

Input: spectrum availability/notification sequence S.
possible prior knowledge of the target's locations R'.
$R' = R$ if no prior knowledge.
Output: the target's possible location set L.
Initialization: $L = \phi$, δ, $n \times n$ probability matrix PR with all elements $\frac{1}{2}$
for (power limitation or channel switch) **do**
  M = number of cells in $Cov(loc_i, P_i) \cap R'$
  for all c_{ij} in $Cov(loc_i, P_i) \cap R'$ **do**
    $pr_{ij} = \frac{pr_{ij}}{1 - \frac{1}{M}(1 - pr_{ij})}$
  end for
  if $pr_{ij} \geq \delta$ **then**
    $L = L \cup c_{ij}$
  end if
end for
return: L

Based on Algorithm 1, the possible located region of the target can be significantly reduced to a relatively small area, which is demonstrated in section V.

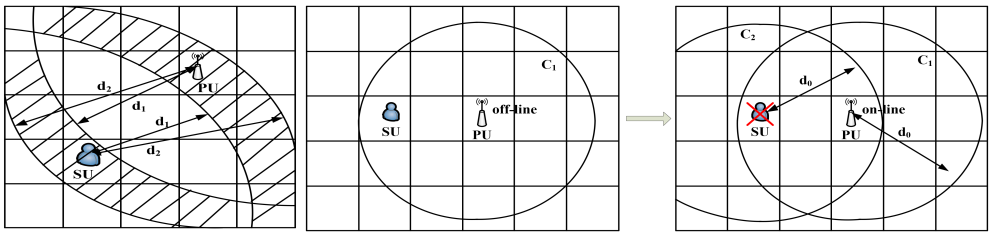
IV. Location Privacy Preservation in Spectrum Query Process

In database-driven CRN, an SU aims to enjoy efficient spectrum utilization and the database also aims to provide spectrum resource sharing among SUs and PUs. However, sharing of spectrum resources may lead to breaches of location privacy. In this section, we propose to exploit the K-Anonymity technique to enhance the location privacy of both PUs and SUs.

A. Basic Solution

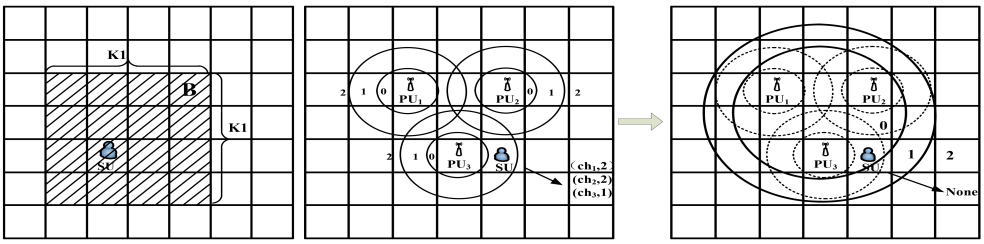
1) ***K-Spectrum Query****:* An SU is able to simultaneously query for multi-cells around it. We propose that an SU who is sensitive in location privacy queries SAI in a square cloak region B with size $K_1 \times K_1$ cells shown in Fig. 2(a), including SU's actual location. On one hand, the SU might be a relay node and need to provide spectrum availability information for other SUs who do not own the capacity of directly communicating with the database [7]. On the other hand, the actual location of the SU can be confused without any location blinding technique. K_1 and the position of B can be determined in a user centric manner. Note that, $R' = B$ is considered as the prior knowledge of the attacker so that the SU will always set a relatively large K_1 based on its own security requirement. The SU will query SAI for the same cloak B to avoid further location privacy leaking.

2) ***K-Anonymity Response****:* The database will honestly provide SAI in all cells in B queried by the SU. Intuitively, a PU's location will be readily inferred based on the attack scheme. Thus, we introduce K-anonymity technique to group K_2 PUs together as a virtual PU so as to enlarge the protection



(a) Attack with Limited Power (b) Attack with Channel Switch

Fig. 1: Location Inference Attacks



(a) K-Spectrum Query (b) K-Anonymity Response

Fig. 2: Location Privacy Preservation in Spectrum Retrieval

region of the PUs. Then the spectrum availability should be re-calculated based on these virtual PUs.

To perform K-anonymity for PUs, we first group all the PUs into $\lceil \frac{C}{K_2} \rceil$ groups, in which there are K_2 PUs. Grouping can be achieved by selecting the nearest $K_2 - 1$ neighbours.

Then we have to find the minimum covering circle of each group. Assume the center of the minimum covering circle is X and the radius is R_X, we can derive X and R_X by solving the following problem:

$$\min_{X} \max_{loc_i} d(loc_i, X) \tag{1}$$

By following the MTP function introduced in [4], we can get the updated MTP function after performing K-anonymity as 2:

$$P = \begin{cases} 0 & when\ d(X) < R_X + d_0 \\ P_1 & when\ R_X + d_0 < d(X) \leq R_X + d_1 \\ ... & \\ P_{max} & when\ d(X) > R_X + d_n \end{cases} \tag{2}$$

Here, $d(X)$ represents the relative distance between a location and X.

K-anonymity based location obfuscation can certainly improves the location privacy since it ensures the enlargement of the protecting region of each PU. Fig. 2(b) is an example of performing K-anonymity.

Each time the database receives a message querying for multi-cells, it checks the PU's location privacy leaking based on the spectrum availability in the queried region. It determines whether to perform K-anonymity and the value of K_2 according to the estimation of location privacy leaking based on the attack algorithm.

*3) **Improved Channel Selection**:* The crucial step for an SU to protect location privacy is selecting which channel to use. The available channels received by an SU can be divided into three cases which is analysed as below.

- (ch_k, P_{max}) in all the cells: The PU operating on ch_k might probably be off-line. SU will not select the channel.
- (ch_k, P_{max}) in some but not all cells: The SU knows that the PU operating on ch_k is on-line but far away. This channel is preferred to be used.
- $(ch_k, P(< \ P_{max}))$: If there is no channel as in the last case, SU selects a channel with the largest transmission power as far as possible due to the largest coverage of the power level.

B. Optimal Parameters

Based on the proposed location privacy preserving scheme, we can stand on the point of system designer who knows the global knowledge to optimize the parameters, based on which the location privacy can be maximized while ensuring the spectrum utility. We first define the metrics of spectrum utility and location privacy and then devise parameter determination programs to find out the optimal choices for both users.

1) Metrics of Spectrum Utility and Location Privacy:

- **Spectrum Utility:** Intuitively, the spectrum utility can be represented by channel capacity. For simplicity, assuming the capacity is constant as the frequency varies in a channel band and the channel capacity is constant in a specific cell, the capacity of ch_k can be represented by Equation 3 [9].

$$Cap_k = W_k log_2(1 + SINR_k) \tag{3}$$

Here, W_k is the bandwidth of ch_k and $SINR_k$ is the Signal to Interference and Noise Ratio (SINR) on ch_k. $SINR_k$ is mainly determined by the transmission power on ch_k, as well as path loss etc [9].
We define the spectrum utility of an SU as average capacity of the used channels. Let CH and $|CH|$ denote the sequence and the number of the used channels, the utility of the SU can be written as Equation 4.

$$Uti_{SU} = \frac{1}{|CH|} \sum_{ch_k \in CH} Cap_k \tag{4}$$

When an SU queries spectrum availability information for a cloak region B, spectrum utility of database can be viewed as the cell-averaged channel capacity provided. We denote the available channels as CH_A. Thus, the utility of database can be written as Equation 5.

$$Uti_{DB} = \frac{1}{K_1^2} \sum_{c \in B} \sum_{ch_k \in CH_A} Cap_k \tag{5}$$

Note that, an SU is mainly concerned about the utility of used channels. However, the database, as a service provider, focuses on the total provided available spectrum in the region.

- **Location Privacy:** According to the proposed attack scheme, the target will be inferred to be in region L. We follow the definition in [8] and quantify the user's location privacy as the expected error distance in the attack. We assume the target is uniformly distributed in L. Thus, the target is located in $c \in L$ with the probability $\frac{1}{|L|}$ and 0 in other cells, where $|L|$ is the number of cells in L. We can describe the attack result as a probability density function $A(loc'|\cdot)$, where $\cdot$ is the information in spectrum query process and loc' is the inferred location by the attacker. Thus, We can compute the location privacy with Equation 6.

$$Pri = \sum_{loc' \in L} A(loc'|\cdot) d(loc, loc') \tag{6}$$

Here, loc and loc' are the actual location and inferred location of the target respectively. $d(loc, loc')$ is the Euclidean distance between loc and loc'. When the attacker is an SU, the attack result will be strongly affected by the K_1 and K_2. Thus, we define the privacy of database as Equation 7.

$$\begin{aligned} &Pri_{PU}(loc, SAI(K_1, K_2)) \\ &= \sum_{loc' \in L} A(loc'|SAI(K_1, K_2)) d(loc, loc') \end{aligned} \tag{7}$$

When the attacker is the database, the attack result mainly depends on the selected channel and corresponding transmission power. The location privacy of SU is shown in Equation 8.

$$\begin{aligned} &Pri_{SU}(loc, S) \\ &= \sum_{loc' \in L} A(loc'|S)) d(loc, loc') \end{aligned} \tag{8}$$

S is the sequence of channels which have been used by the SU.

2) Parameter Determination: The obtained spectrum utility and location privacy mainly lies on K_2 and the selected channels, based on the locations of PUs and SUs are obfuscated. According to the proposed attack algorithm, we can naturally devise two parameter determination problems for an SU and the database to work out the optimal strategy, based on which the SU and the database can obtain maximum location privacy while ensuring spectrum utility.

- Determine K_2: The database sets a threshold of minimum accepted spectrum utility σ_{DB} and then do the following maximization problem to determine the optimal K_2 based on the pre-determined K_1 to obtain the maximal location privacy while ensuring the spectrum utility:

$$\max_{K_2} Pri_{PU}(l, SAI(K_1, K_2)) \tag{9}$$

subject to

$$Uti_{DB} \geq \sigma_{DB} \tag{10}$$

- Determine ch_k: The SU sets a minimum accepted threshold of spectrum utility σ_{SU} and then do the following maximization problem to determine the optimal ch_k while ensuring the spectrum utility:

$$\max_{ch_k} Pri_{SU}(l, S \cup ch_k) \tag{11}$$

subject to

$$Uti_{SU} \geq \sigma_{SU} \tag{12}$$

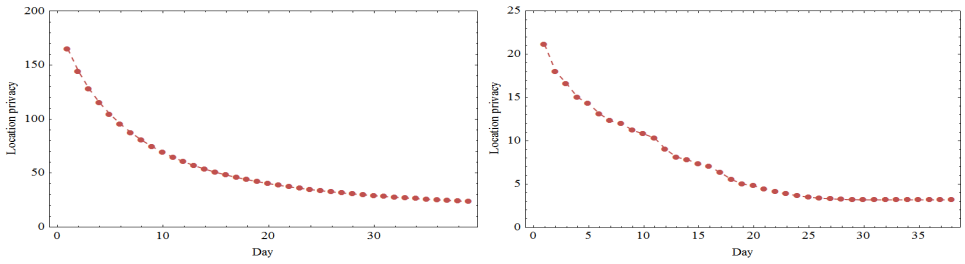
Due to the small search space, we can launch exhaustive searches to work out the optimal solution.

V. Experimental Analysis

We conduct experiments on an implementation platform with Intel I5 CPU of 2.8GHz and 4GB memory. We evaluate the effectiveness of the proposed location privacy preserving scheme under random parameter settings. Specificaly, e consider a regulated region of 400×400 cells. There are 50 PUs/channels as well as 500 SUs randomly distributed in the region. MTP is divided into 5 levels from 0 to 4(P_{max}). In the regulated region, PUs switch the status between on-line and off-line randomly but not frequently. For simplicity, we use the side length of a cell as the length unit for measuring the location privacy while not the actual Euclidean distance.

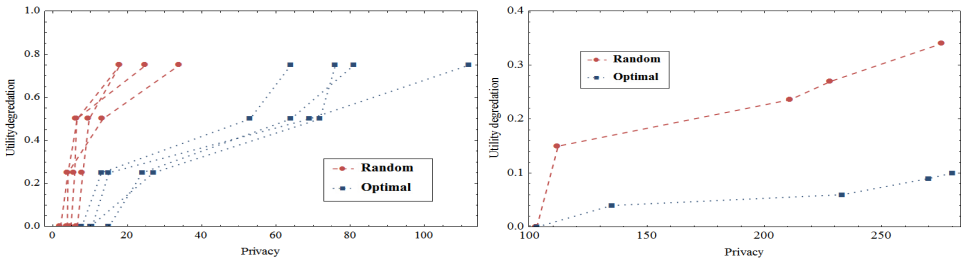
We first conduct experiments of the unified attack against the SUs and the PUs. The results of the attack is illustrated in Fig. 3.

In Fig. 3(a), we illustrate the degradation of location privacy of SUs as time goes. Location privacy is considered as the averaged location privacy of all the SUs. We can see the location privacy of SUs degrades with time. Finally, the SUs can be geo-located in an small area with the average error of less than 25 after all possible cases which might cause location privacy leaking have occurred. Also, we show the degradation of location privacy of PUs which is averaged from all the PUs in Fig. 3(b). Due to the sufficient and fine-grained SAI, PUs



(a) SU (b) PU

Fig. 3: Location Privacy Leaking Based on Unified Location Inference Attack



(a) Samples of SU (b) Total of Database

Fig. 4: Location Privacy vs. Spectrum Utility

can be geo-located in an area with average error of less than 5.

We then demonstrate the efficiency of the optimal strategies, comparing with random selections. Fig. 4 illustrates the maximum achieved location privacy with certain constraints of spectrum utility. In Fig. 4(a), we compare the location privacy with and without optimal parameters. The samples of SUs are picked out randomly. It is obvious that the maximum location privacy is much higher with optimal parameters. Also, the average error can reach to more than 60, much better than without location privacy preserving scheme. In Fig. 4(b), we illustrate the comparison of location privacy of PUs with and without optimal strategy. We can see that the maximum achieved location privacy with optimal parameters is equal to that without optimal parameters. Also, the maximum location privacy of PUs is much higher since the attack error can reach to more than 200. This is due to the obfuscated protection regions of PUs. Further, the actions of the SUs and the database will affect each other. If the SU selects a larger K_1, it will obtain more spectrum availability which might be exploited to launch location inference attack on PUs. The database will set a larger K_2 to protect location privacy, which reduces the spectrum utility. Considering the same utility requirement, optimized parameters can result in a much higher location privacy level.

VI. Conclusion

In this article, we introduce a unified location privacy attack and corresponding countermeasures against the location privacy leaking in database-driven CRN. It is shown that the location privacy can be improved based on the proposed scheme. However, the improvement is limited due to the basic principle of database-driven CRN.

VII. Acknowledgement

This work is supported by National High-Tech R&D (863) Program (no. SS2015AA011309), NSFC (no. 61272444, U1401253, U1401253, U1401253), JSPS KAKENHI Grant Number 25880002, 26730056, JSPS A3 Foresight Program.

References

[1] Federal Communications Commission, "Second Memorandum Opinion and Order". http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-174A1.pdf, Sep. 2010.

[2] Federal Communications Commission, "White Space Database Administrators Guide". Available: http://www.fcc.gov/encyclopedia/white-space-database-administrators-guide

[3] Z. Gao, H. Zhu, Y. Liu, et al. "Location Privacy in Database-driven Cognitive Radio Networks: Attacks and Countermeasures" in Proc. of IEEE INFOCOM, 2013.

[4] B. Bahrak, S. Bhattarai, A. Ullah, et al. "Protecting the Primary Users' Operational Privacy in Spectrum Sharing" in Proc. of DySPAN14, 2014.

[5] M. Li, H. Zhu, Z. Gao, et al. "All Your Location are Belong to Us: Breaking Mobile Social Networks for Automated User Location Tracking" in Proc. of ACM MobiHoc, 2015.

[6] Internet Engineering Task Force (IETF), Internet-Draft, "Protocol to Access White-Space (PAWS) Databases", Sep. 2014. Available: http://tools.ietf.org/html/draft-ietf-paws-protocol-17

[7] Federal Communications Commission, "Third Memorandum Opinion and Order", May. 2012. Available: http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0405/FCC-12-36A1.pdf

[8] R. Shokri, G. Theodorakopoulos, J. Boudec, et al. "Quantifying Location Privacy" IEEE Symposium on Security and Privacy(SP), 2011. pp. 247-262.

[9] F. Hessar, S. Roy. "Capacity Considerations for Secondary Networks in TV White Space". arXiv preprint:1304.1785, 2013.

[10] L. Sweeney. "K-anonymity: A Model for Protecting Privacy". International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(05): 557-570.

[11] W. Wang, Q. Zhang. "Location Privacy Preservation in Cognitive Radio Networks", Springer briefs in Computer Science, 2014.