International Journal of Multimedia and Ubiquitous Engineering
Vol. 10, No. 1 (2015), pp. 403-416
http://dx.doi.org/10.14257/ijmue.2015.10.1.37

Localization and Privacy Preservation in Cognitive Radio Networks

Xu Zhang[1], Xia Ying[1], Hongrui Mao[1]and Hae Young Bae[1,2]

[1]*Department of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China*
[2]*Department of Computer and Information Engineering, Inha University, Incheon, South Korea*
{zhangx, xiaying}@cqupt.edu.cn, maohongr@hotmail.com, hybae@inha.ac.kr

Abstract

Cognitive Radio Networks (CRNs) has been considered as a key technology for future wireless communications and mobile computing. Localization of primary user is crucial in enabling several key capabilities in CRNs. In this paper, we present a survey of representative methods dealing with user localization and location privacy preservation issues and propose a taxonomy that summarizes the state-of-the-art. The objective is to provide a comprehensive analysis and guide of existing efforts around localization and location privacy preservation in cognitive radio network. This survey is intended to help researchers in quickly understanding existing works and challenges, and possible improvements to bring.

Keywords: *Primary User Localization, Location Privacy, Cognitive Radio Networks*

1. Introduction

The rapid proliferation of wireless technology and explosion of wireless devices and mobile data creates an ever-increasing demand for more radio spectrum. The spectrum scarcity issue is expected to occur due to the limited spectrum resources. Recently, Cognitive Radio Networks(CRNs) has been considered as a key technology for future wireless communications and mobile computing, which is pretty much consistent of Haykin's definition of cognitive radio [1]:

Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit-power, carrier-frequency, and modulation strategy) in real-time, with two primary objectives in mind: highly reliable communication whenever and wherever needed; efficient utilization of the radio spectrum.

Cognitive radio networks that can sense their environment and dynamically adapt their transmission waveform, channel access method, spectrum use, and networking protocols as needed for good network and application performance. A major technical challenge in the CRNs is to acquire knowledge about spectrum occupancy properties through spectrum sensing [2,41]. In CRNs, the secondary users (SUs) can sense the spectrum and utilize the licensed bands when the spectrum is not being utilized by the primary user (PU), as it is shown in Figure 1.

ISSN: 1975-0080 IJMUE

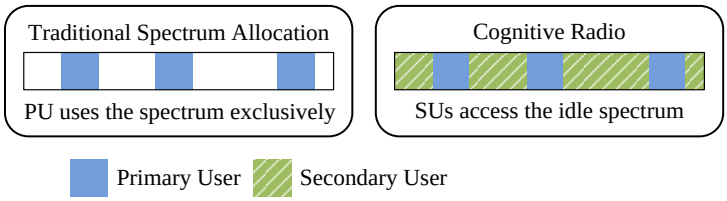


Figure 1. Cognitive Radio

Localization problem in CRNs is in general different from localization in other applications such as Wireless Sensor networks(WSN) and Global Positioning System(GPS), in which the target to be localized cooperates with the localization devices. In contrast, a PU does not communicate directly with the CRs during the localization process [3].

The SUs at different locations in the CRNs with a given interference ranges of the PUs, may perceive different profiles of spectrum holes due to different distances from the PUs. In order to reuse the unoccupied spectrum in an opportunistic fashion, it is important for the SUs to know the position information of the PUs. Localization is a methodology that can be adopted to obtain such kind of position information. Existing localization can be categorized into self-positioning, remote positioning and in terms of different localization objectives, where PU position estimation performed by the SUs belongs to remote positioning [4].

Privacy preservation has become a major issue across different applications, from information sharing to data publishing, from wireless communication to location-based services [2]. Location privacy was first introduced in mobile network, and then it arises with the open nature of wireless communication as well as software defined radio platforms in CRNs. Two types of location privacy issues in CRNs should be considered, namely, *collaborative spectrum sensing location privacy* and *database query privacy* [2].

The remainder of this paper is organized as follows. First, we give an introduction of Cognitive Radio Networks in Section 2, and review the existing techniques in localization and location privacy preservation in Section 3. Section 4 addresses the primary user localization in CRNs. And, the location privacy preservation issues in CRNs are discussed in Section 5 and draw a conclusion in Section 6.

2. Cognitive Radio Networks

The limitation of spectrum has motivated a paradigm shift from static spectrum allocation towards a more “liberalized” notion of dynamic spectrum management in which non-license holders can “borrow” idle spectrum from those who hold licensees [5]. Thus, the effective utilization of these spectrums becomes a necessary, which make the cognitive radio becomes the promising technology. The cognitive radio is termed as the software defined radio technology that avails the license to the unlicensed users without any inference.

2.1 Cognitive Radio Architecture

A typical cognitive radio consists of a sensor, a radio, a knowledge database, a learning engine, and a reasoning engine. As it is shown in Figure 2, the architecture of the cognitive radio consists of 4 components: physical layer, linke layer, network layer and transport layer [6]. Each layer performs different functions as follows.

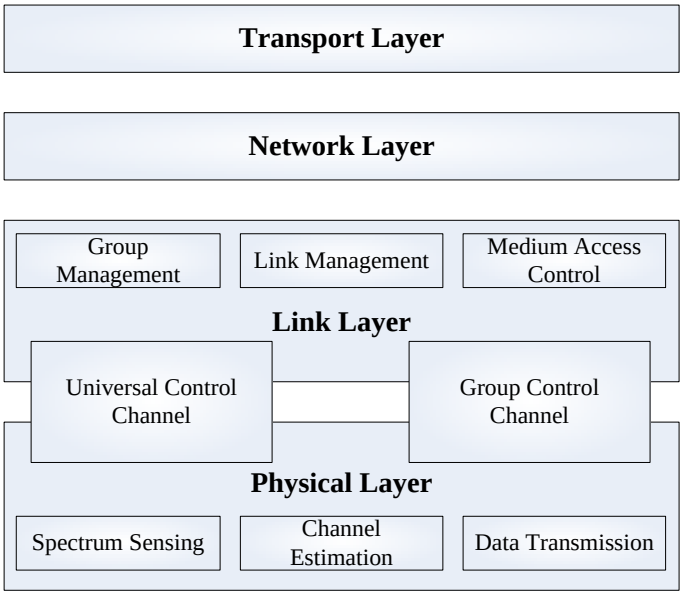


Figure 2. Architecture of Cognitive Radio

- Physical Layer
  - *Spectrum Sensing* means sense the available free medium for an effective transmission. And, it also can avoid the occurrence of any interference to potential primary users in their vicinity.
  - Before setting up the link, the quality of the sub channels is estimated based on their transmission parameters with *Channel Estimation.*
  - *Data Transmission* happens after the first two steps. It can operate at variable symbol rates, different channel coding schemes, power levels and capable of using multiple antennas to nullify the interference.
- Link Layer
  - In *Group Management*, the arriving user can join any of the existing groups or form a new one through a univesal control channel.
  - *Link Management* covers the set up on the link to enable the communication between any two secondary users. It also maintains the link until the duration of the communication.
  - If any of the sub channels is used by the particular secondary users, then the particular channel cannot be used by any other secondary user. This control is managed by *Medium Access Control*.

2.2. Cognitive Radio Capability and Type

Cognitive Radios are the devices that have the capability of sensing the spectrum and utilize its free sections in an opportunistic way. These free sections of the spectrum are cited as "*white spaces*" or "*spectrum holes*".

The characteristics over the cognitive radio are *Cognitive Capability*, *Reconfigurable Capability* and *Self-Organized Capability*. Cognitive capability consists of 5 components: Spectrum Sensing can detect "spectrum holes" which are those frequency bands not used by the licensed users or having limited interference with them. Spectrum Sharing provides a mechanism that enable sharing of spectrum under the terms of an agreement between a licensee and a third party. *Location Identification* is the ability to determine its location

and the location of other transmitters, and then select the appropriate operating parameters such as the power and frequency allowed at its location. *Service Discovery* usually accompanies with *Network/System Discovery* guarantees that the available networks and service around should be discovered.

Reconfigurable Capability also consists of 5 main components: *Frequency Agility* indicates the ability of a radio to change its operating frequency. *Dynamic Frequency Selection* is defined in the rules as a mechanism that dynamically detects signals from other radio frequency systems and avoids co-channel operation with those systems. *Adaptive Modulation/Coding* is used to modify transmission characteristics and waveforms the provide opportunities for improved spectrum access and more intensive use of spectrum. *Transmit Power Control* allows transmission at the allowable limits when necessary, but reduces transmitter power to a lower level to allow greater sharing of spectrum when higher power operation is not necessary. *Dynamic System/Network Access* guarantees CRNs to be compatible with other communication systems/networks.

Self-Organized Capability consists of 3 important features: *Spectrum/Radio Resource Management* provides an efficiently management scheme and organize spectrum holes information among cognitive radios. *Mobility* and *Connection Management* ensures a better routing and networking for neighborhood discovering, detecting available internet access and supporting vertical handoffs in a complex CRN. *Trust/Security Management* guarantees the CRNs is safety.

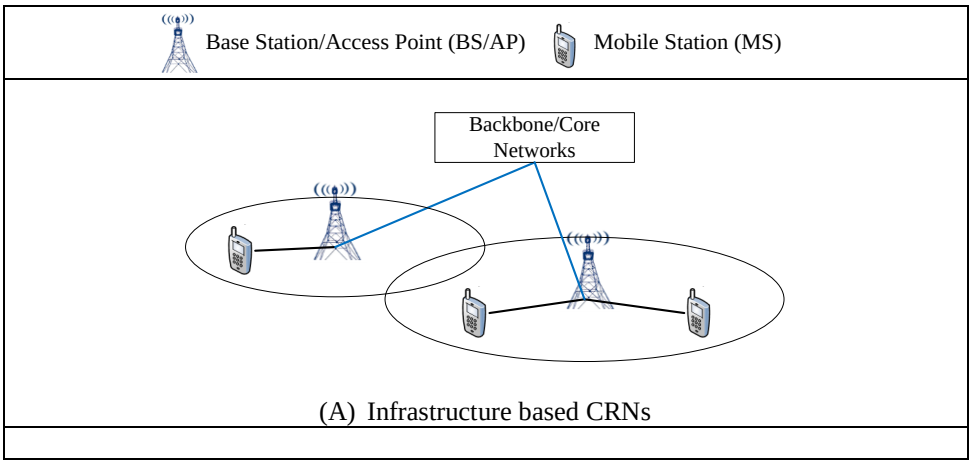
As it is shown in Table 1, there are three types of cognitive radios [5,7,8].

Table 1. Types of Cognitive Radio

Types	Description
Policy Radios	Governed by a set of rules called the radio's policy. Do not posses learning or reasoning engine.
Procedural Cognitive Radios	Operational adaptation is based on observations by utilizing hard-coded algorithms. Do not have learning capabilities and thus vulnerable to short-term attacks.
Ontological Cognitive Radios	Flexible and intelligent with reasoning and learning engine.

2.3. Cognitive Radio Networks Architecture

The CRNs can be classified into three broad categories: Infrastructure based [9], Ad-hoc based [10] [11] and Mesh based architectures [12].



(A) Infrastructure based CRNs

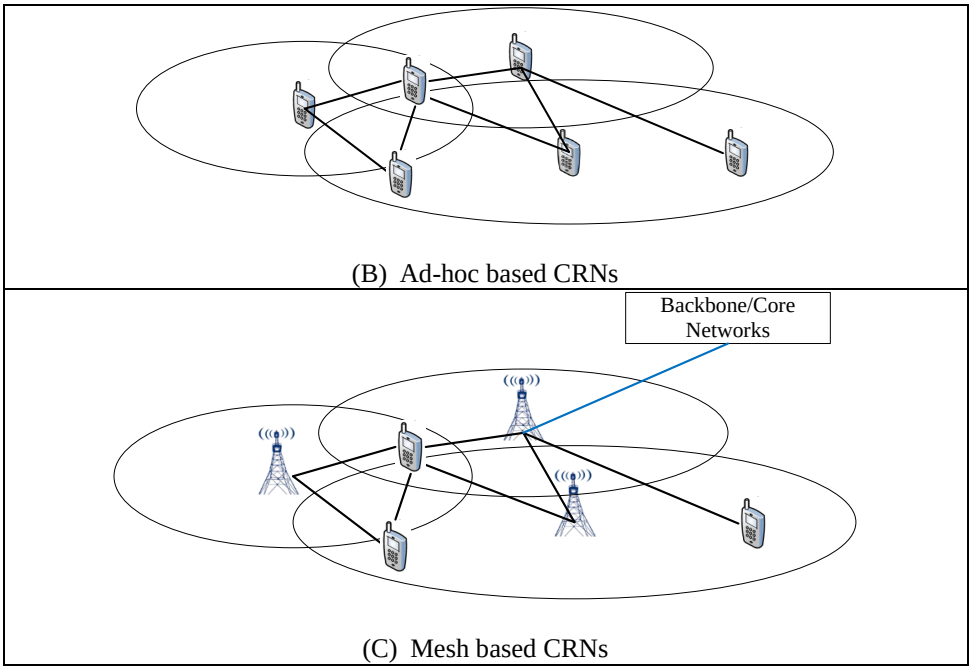


Figure 3. Architecture of Cognitive Radio Networks

As it is shown in Figure 3, the *infrastructure based architecture* indicates that the MS can only access a BS/AP in the one-hop manner. Communication between different cells are routed through backbone/core networks. The MSs can communicate under the transmission range of their BS/AP. In *ad-hoc based architecture*, MS can recognize other MS nearby and set up a link to form an ad-hoc network. The *mesh based architecture* is a combination of the other two architectures. MSs can either access the BS/AP directly or use other MS as multi-hop relay nodes.

3. Localization and Location Privacy Preservation Techniques

3.1. Localization Techniques

Localization of an object has long been the subject of research within the signal processing community and industry area like outdoor/indoor location-based services. Classic localization is based on the *cooperative* or *non-cooperative* use of RF emissions by the object to be located or RF emissions made by a set of anchor nodes and processed by the radio to be located.

As it is shown in Table 2, there are several metrics to classify existing works.

Table 2. Classification of Localization Algorithms

Metric	Class
Distance/Angle	Range-based(TOA, TDOA, AOA, RSS) [13] [14]
	Semi Range-based [15] [4]
	Range-free [16]
Topology of Networks	Centralized
	Distributed
	Cooperative
	Non-Cooperative

A. Distance based Localization

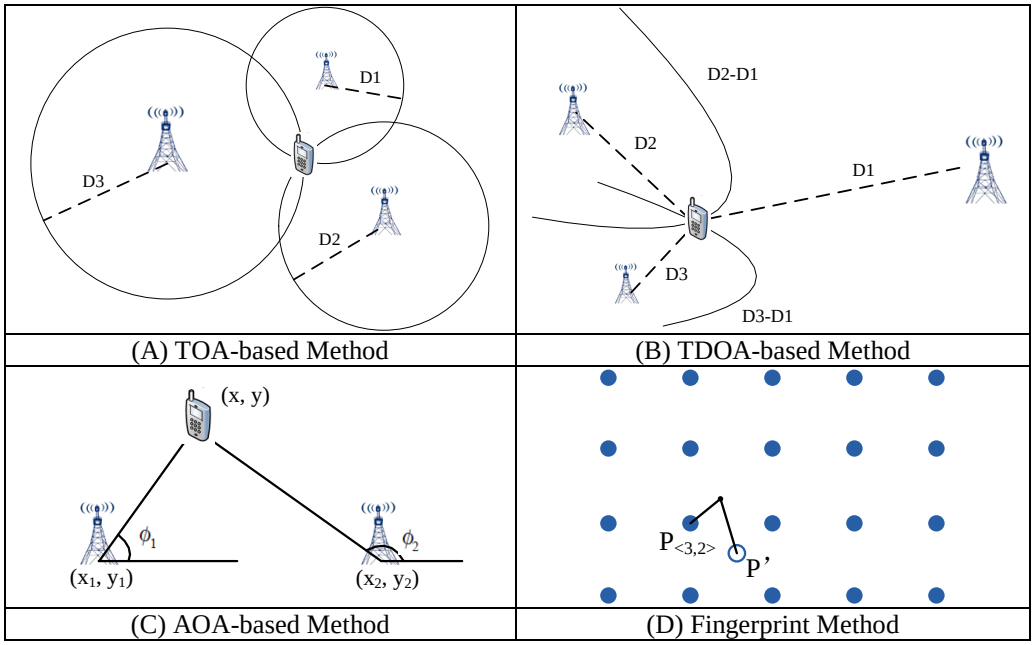


Figure 4. Range-based Localization

In range-based algorithms, necessary information to estimate the distance can be obtained by some estimation techniques, such as Time Of Arrival (TOA), Time Difference Of Arrival (TDOA), Angle Of Arrival (AOA) and Received Signal Strength (RSS). As it is shown in Figure 4, basic theory and computation method of range-based localization is illustrated in detail. In TOA-based (Time Of Arrival) trilateration, range measurements to at least three base stations make up a set of nonlinear equations that can be solved to estimate the position of a unit. The PU time-tag the transmitted signal and the SUs measure the exact TOA of that signal. In TDOA-based (Time Difference Of Arrival) method, the time difference of arrival approach requires the ability to measure the time difference between the receptions of on PU signal at different SUs. In AOA-based (Angle Of Arrival) method, an antenna array is required at the SU. Then, multiple SUs estimate the AOA of a signal, and combine the angle information to compute an intersection point of the PU. On the other hand, there is not enough information can be exploited to estimate the exact distance in the range-free algorithms. The semi range-based localization algorithm is a compromise between range-based and range-free method.

B. Centralized VS Distributed Localization

As it is shown in Figure 5, in centralized localization, there is one central base station for computation. Thus, it suffers from overhead and cost increases. In distributed localization, computation is done by distributed server or nodes communication between each other to get their position in the network.

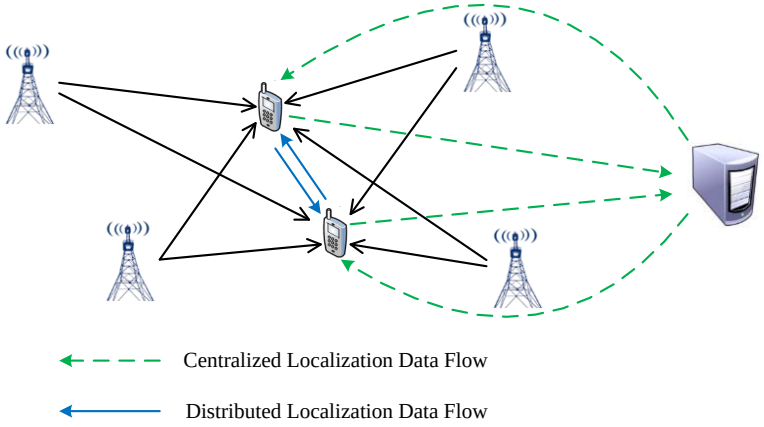


Figure 5. Centralized/Distributed Localization

C. Cooperative VS Non-Cooperative Localization

Cooperative localization was first proposed in Japan to acquire real-time positioning information on mobile robots [17]. When mobile unit cannot independently determine its own position based on distance estimates with respect to the anchors (base stations), they can cooperatively find their positions. Generally, cooperative localization can dramatically increase localization performance in terms of both accuracy and coverage [18]. As it is shown in Figure 6, base station (anchor) is needed for cooperative localization.

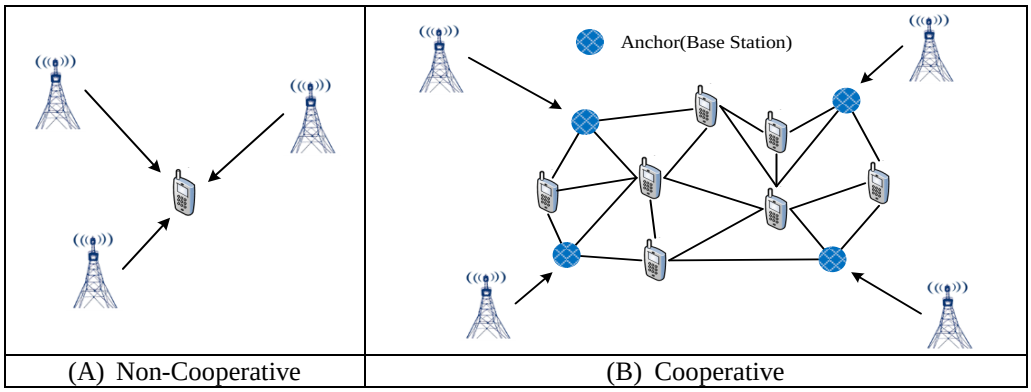


Figure 6. Non-Cooperative & Cooperative Localization

3.2. Location Privacy Preservation Techniques

In this section, we introduce some basic concepts and fundamental knowledge of privacy preservation techniques that can be used in CRNs. The state-of-the-art privacy techniques can be categorized into four classes: *anonymization* [19] [20] [21], *perturbation* [22], *differential privacy* [23], and *cryptographic* [24] techniques. In location privacy protection, anonymization can be further divided into *privacy policies*, *false locations*, *space transformation* and *spatial cloaking* method [25].

The k-anonymity [20] is the first and the most fundamental anonymization privacy model. The goal of k-anonymity is to ensure that each individual's location is indistinguishable from at least k-1 other individuals' location. Based on the notion of k-anonymity, many other anonymization models have been proposed including l-diversity [19], (α, k)-anonymity [21]. A large number of spatial cloaking algorithms have been proposed for protecting the location privacy of mobile users. Spatial cloaking techniques rely on k-anonymity concept and cloaking granularity, which blurs a user's location into a

cloaked spatial area that satisfies the user's specified privacy requirements. Existing works on spatial cloaking follow the same idea to blur a user's location into a cloaking region.

The basic of random perturbation is to replace the original data values with some synthetic data values so that the statistical information remains relatively the same while the original values never get disclosed. It has been adopted in many privacy preservation applications such as data mining [26], collaborative sensing [27] and collaborative spectrum sensing [28]. Differential privacy uses priori and posterior beliefs to guarantee the data privacy. For the location privacy, location data and sensing data from a user should be considered as a tuple in histogram data or contingency data table, and then it can be processed with differential privacy model. There is seldom cryptographic based study on location privacy due to the computation overhead.

4. User Localization in CRNs

The location information of primary user can be helpful for communication between cognitive radios. Also, it is important for the SUs to identify their spectrum-access opportunities while avoiding harmful interference to the PUs. A lot of localization algorithms have been proposed in the literature for estimating the location of the PUs in CRNs.

In CRNs, knowledge of the position of the PUs is important as it can be used to avoid harmful interference to the primary network while at the same time be exploited to improve the spectrum utilization.

Range-free localization algorithms never try to estimate the absolute distance, but exploit the protocol-oriented metric (*e.g.*, hop count, number of listened beacons). However, these approaches are problematic when the user to be estimated is out of the convex hull of anchor.

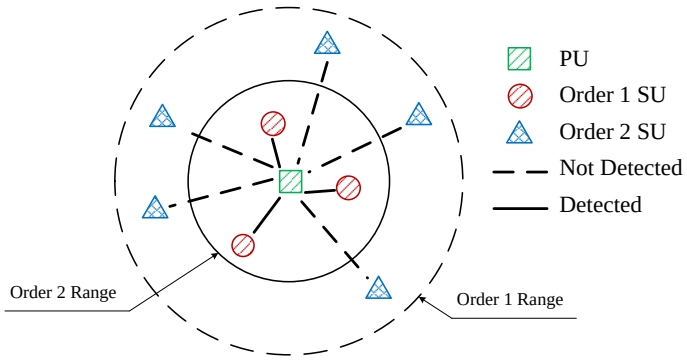


Figure 7. Range-free Localization

Compared with traditional networks, the key difference in CRNs is that the SUs should be transparent to the PUs, which implies that there is no cooperation between them during the localization process [4]. As it is shown in Figure 7, an order-based geometric range free localization is proposed with two steps: 1st order geometric location and high order geometric localization [16].

To overcome the weakness of pure range-free algorithms in estimation accuracy while avoiding the tough requirement of the conventional range-based algorithms on the physical layer equipment, semi range-based localization algorithm is proposed as a compromise. The "semi range-based" terms highlights the two key features. First, it follows the same idea with range-free algorithm that only binary sensing results from the SUs are required. Second, the detection probabilities of each SU, which can be obtained from their binary detection results, respectively, are exploited to estimate the distances

from each SU to the target PUs. In [4], a semi range-based localization algorithm is proposed for the SUs in CRNs to estimate the positions of the PUs. The basic idea is to take advantage of the estimated detection probabilities, which can be obtained from the binary detection indicators of the SUs, to estimate the distances between themselves and the PUs. First, each Su estimates the average detection probability using their binary sensing results, which is then collected by a common receiver. Second, the common receiver estimates the position of the PU utilizing the collected sensing results, taking advantage of the relationship between the distance and the detection probability. A weighted least-squares method and an iterative procedure are proposed to further improve the accuracy of localization. The basic idea of this method is illustrated in Figure 8. There are three SUs locating the position of a certain PU. Three circles indicate the estimated distances between the SUs and PU respectively. The l_{ij} represents the line passing through the two intersects of the two circles of user i and user j. The expected position of the PU is the intersection of these three circles. In [15], a practical semi range-based localization algorithm is proposed. The combined estimation of PU transmitter's position and transmitting power is performed so that no prior knowledge of the PU transmitter is required, making the algorithm practical. Furthermore, they proposed to take advantage of cooperative spectrum sensing technique to make estimations of the PU occupancy status with pinpoint accuracy. This improved the accuracy of estimated possibility of detection of the sensing nodes.

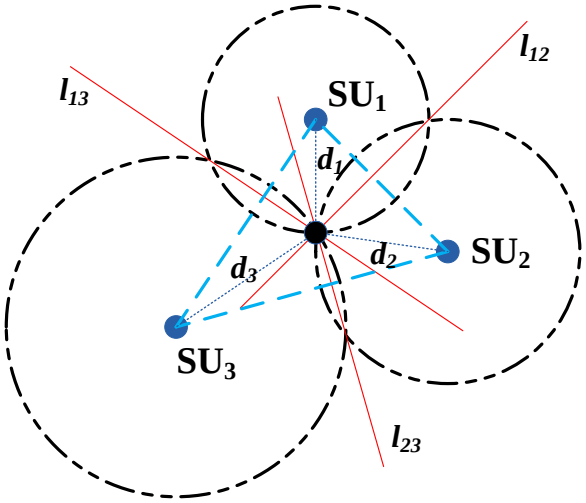


Figure 8. Semi Range-based Localization Algorithm

Range-based localization algorithms use distance metric to measure how far between the PU and SU. In [29], a range-based algorithm is proposed in which the RSS information is exploited to obtain the distance information directly. However, the requirement of precise measurement of the physical layer limits the application of the algorithms in practice. In [30], a method for determining the near future location of a SU in a CR network is proposed. This method incorporates a TOA location estimation algorithm with a Hidden Markov Model (HMM) based channel occupancy prediction model. Employing multiple bandwidths, based on HMM prediction, it was observed that an overall relative improvement of 27% was obtained from the location estimation process of SUs operating. In [31], multi-dimensional infinite impulse response space-time beam filters with a combination of DOA estimation in localization is investigated.

Algorithms for PU localization based on the received signal strength (RSS) have been well studied in the literature [32, 33]. The weakness is that many secondary sensors need to collaborate in order to obtain accurate results since the RSS is heavily influenced by the channel. Furthermore, the localization works only for a single PU in the observation area

because the distinction between multiple PUs is impossible in the RSS domain. In [34], instead of attempting localization of individual transmitters, they adopt a model-based approach, attempting to infer either a model or selected key statistics describing how transmitters are distributed over the region of interest. The study shows that such estimates can be made with much smaller number of measurements and with higher degree of accuracy than would be required for solving the full localization problem.

5. Location Privacy Preservation in CRNs

Author names and affiliations are to be centered beneath the title and printed in Times New Roman 12-point, non-boldface type. Multiple authors may be shown in a two or three-column format, with their affiliations below their respective names. Affiliations are centered below each author name, italicized, not bold. Include e-mail addresses if possible. Follow the author information by two blank lines before main text.

The open nature of wireless communication as well as software defined radio platforms makes CRNs face many new challenges in the aspects of location privacy. Nowadays, the growing privacy threats of sharing location information in wireless sensor networks and cognitive radio networks have been widely concerned. The fine-grained location data may indicates user's beliefs, regular activity and behavior. It may raise serious privacy concerns if these locations are not protected adequately. Being aware of such potential privacy risks, SUs may not want to share its data with fusion center or database. This safety consideration of SU may disable itself enjoying the benefit from collaborative spectrum sensing and database-driven CRNs if their privacy is not guaranteed. Therefore, it is essential to enable SUs to enjoy services provided by CRNs with privacy preserving approaches.

Location privacy issues in collaborative spectrum sensing are divided into two contexts: *single-service-provider context* and *multi-service-provider context* [2].

As it is shown in Figure 9, six SUs are served by one FC, and sense three channels. Each SU sends sensing reports containing RSS values to FC, and FC combines the sensing reports to learn the spectrum. Since the sensing results are highly correlated to user's physical location, which can be exploited by adversaries to launch location privacy attacks including:

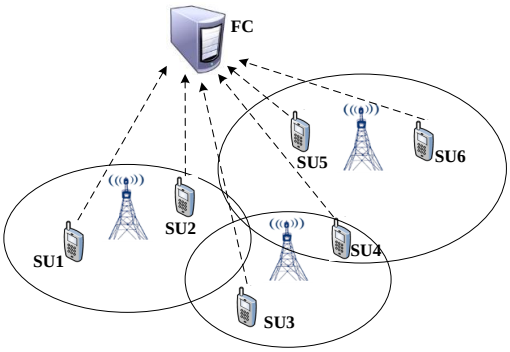


Figure 9. Spectrum Sensing with One FC(Fusion Center)

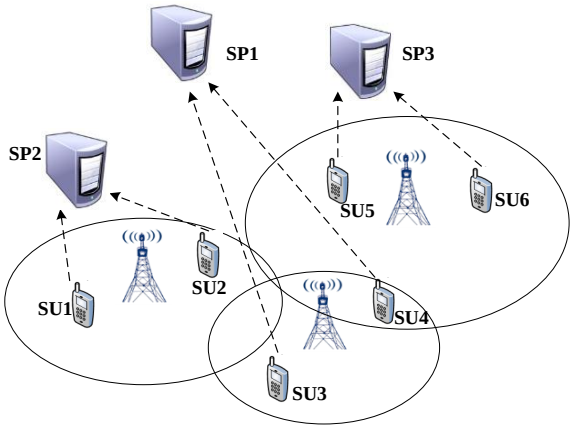


Figure 10. Spectrum Sensing with Multi-SPs

As it is shown in Figure 10, SU1~SU6 are served by three SPs, and sense three channels. Each SU sends sensing reports containing RSS values to its own SP. The three SPs exchange information with each other to collaboratively learn the spectrum.

In [28], a framework with two protocols to cope with privacy threats in the single-SP collaborative spectrum sensing was proposed. To prevent RLC attacks, it adopts secret sharing technique to enable to the FC to obtain the aggregated results without knowing each individual sensing report. Privacy preservation is also studied in distributed settings, in which the aggregated results are derived from multiple partitions of data held by different entities. This is privacy preserving spectrum sensing in multi-SP scenario. The distribution setting are classified into *vertical partitioning* [35] [36] and *horizontal partitioning* [37]. However, all these methods fall short under the collusion attacks in multi-SP context. Thus, more strict privacy preservation schemes that are specially designed for multi-SP collaborative spectrum sensing are required, which currently is still an open issue.

Besides spectrum sensing, geo-location database query approach is another typical approach to obtain spectrum availabilities at SU's location. The database query approach is enforced by the latest FCC's rule released in May 2012 [38, 2]. In [39], it discusses the impersonation attacks towards master device, database and man-in-the-middle-attack between SUs and DB. The database is assumed to be semi-honest or an easy-to-be-attacked, that is, the database exactly follows the protocol but tries to infer SU's locations. Potential privacy threats can come both from database and secondary users. In [40], the knowledge of database is assumed to include the complete communication content between SU and the database, and the spectrum utilization information of SUs. Instead of directly learning the SUs' locations from their queries, some attacks can infer an SU's location through his used channels. They show a new kind of location privacy attack, Spectrum Utilization based Location Inferring (SULI) attack. They propose a novel Private Spectrum Availability Information Retrieval (PSAIR) scheme that utilizes a blind factor to hide the location of the SU. To defend against the discovered attack, a novel prediction based Private Channel Utilization (PCU) protocol is proposed, which reduces the possibilities of location privacy leaking by choosing the most stable channels.

6. Conclusion

In this paper, we study the fundamental techniques for user localization and location privacy preservation in cognitive radio networks. The objective is to provide a comprehensive analysis and guide of existing efforts around localization and location privacy preservation in cognitive radio network. This survey is intended to help

researchers in quickly understanding existing works and challenges, and possible improvements to bring.

Acknowledgement

This work was financially supported by the Natural Science Foundation of China (41201378), Natural Science Foundation Project of Chongqing CSTC (cstc2012jjA40014), Young Scientist Foundation of Chongqing University of Posts and Telecommunications (A2013-36), Talent Foundation of Chongqing University of Posts and Telecommunications (A2014-06), and Creative Foundation of WenFeng (A2014-12)

References

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communications", Selected Areas in Communications, IEEE Journal on, vol. 23, **(2005)**, pp. 201-220.
[2] W. Wang and Q. Zhang, "Location Privacy Preservation in Cognitive Radio Networks", Springer International Publishing, **(2014)**.
[3] J. Wang, P. Urriza, Y. Han and D. Cabric, "Weighted Centroid Localization Algorithm: Theoretical Analysis and Distributed Implementation", Wireless Communications, IEEE Transactions, vol.10, no.10, **(2011)**, pp. 3403-3413.
[4] Z. Ma, W. Chen, K. B. Letaief and Z. Cao, "A Semi Range-Based Iterative Localization Algorithm for Cognitive Radio Networks", Vehicular Technology, IEEE Transactions, vol.59, no.2, **(2010)**, pp. 704-717.
[5] S. Bhattacharjee, S. Sengupta and M. Chatterjee, "Vulnerabilities in cognitive radio networks: A survey. Computer Communications", vol. 36, **(2013)**, pp. 1387-1398.
[6] S. B. Nanthini, M. Hemalatha, D. Manivannan and L. Devasena, "Attacks in Cognitive Radio Networks (CRN)-a Survey",Indian Journal of Science and Technology, vol. 7, **(2014)**, pp. 530-536.
[7] L. Berlemann, S. Mangold and B. H. Walke, "Policy-based reasoning for Spectrum Sharing in Radio Networks",New Frontiers in Dynamic Spectrum Access Networks, the First IEEE International Symposium, **(2005)** November 8-11; Baltimore, MD, USA.
[8] K. Baclawski, D. Brady and M. Kokar, "Achieving Dynamic Interoperability of Communication at the Data Link Layer through Ontology based Reasoning", Proc. of 2005 SDR Forum Technical Conference, **(2005)** November 14-18; Anaheim, USA.
[9] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran and S. Mohanty, "Next Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey. Computer Networks", vol. 50, **(2006)**, pp. 2127-2159.
[10] M. Yao and K. Dong, "Centralized and Distributed Optimization of Ad-Hoc Cognitive Radio Network", Global Telecommunications Conference, **(2009)** November 30-December 4; Honolulu, HI, USA.
[11] J. Minho, H. Longzhe, K. Dohoon and H. P., "Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks. Network", IEEE, vol. 27, **(2013)**, pp. 46-50.
[12] C. Qian, M. Motani, W. Wai-Choong and A. Nallanathan, "Cooperative Spectrum Sensing Strategies for Cognitive Radio Mesh Networks", Selected Topics in Signal Processing, IEEE Journal of, vol. 5, **(2011)**, pp. 56-67.
[13] C. Gentile, N. Alsindi, R. Raulefs and C. Teolis, "Geolocation Techniques: Principles and Applications", Springer, New York, **(2013)**.
[14] H. Wang, Z. Gao, Y. Guo and Y. Huang, "A Survey of Range-based Localization Algorithms for Cognitive Radio Networks", Consumer Electronics, Communications and Networks (CECNet), the 2nd International Conference, **(2012)** April 21-23; Yichang, China
[15] W. Zaili, F. Zhiyong, S. Jingqun, H. Yang and Z. Ping, "A Practical Semi Range-Based Localization Algorithm for Cognitive Radio", Vehicular Technology Conference, IEEE, pp. 1-5, **(2010)** May 16-19; Taipei, Taiwan.
[16] D. Gong, Z. Ma, Y. Li, W. Chen and Z. Cao, "High Order Geometric Range Free Localization in Opportunistic Cognitive Sensor Networks", Communications Workshops, IEEE International Conference, **(2008)** May 19-23; Beijing, China.
[17] R. Kurazume, S. Nagata and S. Hirose, "Cooperative Positioning with Multiple Robots in Robotics and Automation", Proceedings of IEEE International Conference on, **(1994)** May 8-13; San Diego, CA, USA.
[18] H. Wymeersch, J. Lien and M.Z. Win, "Cooperative Localization in Wireless Networks", Proceedings of the IEEE, **(2009)**.
[19] A. Machanavajjhala, J. Gehrke, D. Kifer and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity", Data Engineering, ICDE '06, Proceedings of the 22nd International Conference, **(2006)** April 3-8; Atlanta, USA.

[20] L. Sweeney, "k-anonymity: A Model for Protecting Privacy", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, **(2002)**, pp. 557-570.
[21] R. C.-W. Wong, J. Li, A. W.-C. Fu and K. Wang, "(α, k)-anonymity: An Enhanced k-anonymity Model for Privacy Preserving Data Publishing", Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, **(2006)** August 20-23; Philadelphia, USA
[22] S. L. Warner, "Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias", Journal of the American Statistical Association, vol. 60, **(1965)**, pp. 63-69.
[23] R. Dewri, "Local Differential Perturbations: Location Privacy under Approximate Knowledge Attackers",Mobile Computing, IEEE Transactions, vol. 12, **(2013)**, pp. 2360-2372.
[24] S. Yekhanin, "Private Information Retrieval" Communications of the ACM, vol. 53, **(2010)**, pp. 68-73.
[25] X. Zhang, "Semantic Location-based Adaptive Spatial Cloaking Method for Privacy Protection in Location-based Service", Inha University, **(2013)**.
[26] W. Du and Z. Zhan, "Using Randomized Response Techniques for Privacy-preserving Data Mining", Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 505-510, **(2003)** August 24-27; Washington, DC, USA
[27] B. Liu, Y. Jiang, F. Sha and R. Govindan, "Cloud-enabled Privacy-preserving Collaborative Learning for Mobile Sensing", Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems, ACM **(2012)** November 6-9; Toronto, Canada.
[28] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing and X. Shen, Location Privacy Preservation in Collaborative Spectrum Sensing. In INFOCOM, 2012 Proceedings IEEE, pp.729-737, **(2012)** March 25-30; Orlando, FL, USA
[29] S. Kim, H. Jeon and J. Ma, Robust Localization with Unknown Transmission Power for Cognitive Radio. In Military Communications Conference, IEEE, pp.1-6, **(2007)** October 29-31; Orlando, FL, USA
[30] R.R. Thomas, S.D. Barnes and B.T. Maharaj, TOA Location Estimation based on Cognitive Radio Channel Occupancy Prediction. Wireless and Mobile Computing, Networking and Communications (WiMob), the IEEE 8th International Conference on, **(2012)** October 8-10; Barcelona, Spanish
[31] C. Wijenayake, A. Madanayake, L. T. Bruton and V. Devabhaktuni, DOA-estimation and Source-localization in CR-networks using Steerable 2-D IIR Beam Filters. Circuits and Systems (ISCAS), IEEE International Symposium on, IEEE, pp.65-68, **(2013)** May 19-23; Beijing, China
[32] K. A. Qaraqe, S. I. Hussain, H. Celebi, M. Abdallah and M. S. Alouini, An RSS based location estimation technique for cognitive relay networks. In Applied Sciences in Biomedical and Communication Technologies (ISABEL), the 3rd International Symposium on, pp.1-5, **(2010)** November 7-10; Rome, Italy
[33] V. Rakovic, M. Angjelicinoski, V. Atanasovski and L. Gavrilovska, "Location Estimation of Radio Transmitters based on Spatial Interpolation of RSS Values", Cognitive Radio Oriented Wireless Networks and Communications, the 7th International ICST Conference, **(2012)** June 18-20; Stockholm, Sweden.
[34] Mahonen, P, J. Riihijarvi and A. Kivrak, "Statistical Characterization of Transmitter Locations based on Signal Strength Measurements", Wireless Pervasive Computing (ISWPC), the 5th IEEE International Symposium, **(2010)** May 5-7; Modena, Italy.
[35] J. Vaidya and C. Clifton, "Privacy Preserving Association Rule Mining in Vertically Partitioned Data", Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining, ACM, **(2002)** July 23-26; Edmonton, Alberta, Canada
[36] J. Vaidya and C. Clifton, "Privacy-preserving k-means clustering over vertically partitioned data", Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 206-215, **(2003)** August 24-27; Washington, DC, USA
[37] H. Yu, X. Jiang and J. Vaidya, "Privacy-preserving SVM using Nonlinear Kernels on Horizontally Partitioned Data", Proceedings of the 2006 ACM symposium on Applied computing, ACM, pp.603-610, **(2006)** April 23 -27; Dijon, France.
[38] Federal Communications Commission, "Third Memorandum Opinion and Order", FCC 12, vol.36 **(2012)**.
[39] Y. Cui and Y. Wu, "Protocol to Access White Space Database", Security Considerations, **(2012)**.
[40] Z. Gao, H. Zhu, Y. Liu, M. Li and Z. Cao, "Location Privacy in Database-driven Cognitive Radio Networks: Attacks and Countermeasures', INFOCOM, Proceedings IEEE, pp.2751-2759, **(2013)** April 14-19; Turin Italy.
[41] X. Zhang, Y. Xia, H.R. Mao and H.Y. Bae, "Privacy-preserving Localization in Cognitive Radio Networks", The 8th International Conference on Future Generation Communication and Networking, Hainan, **(2014)**.

Authors

Xu Zhang is an assistant professor of Chongqing University of Posts and Telecommunications, received Ph.D degree from Inha University, South Korea. His research area mainly includes ubiquitous computing (sensor network, localization), large scale data processing, database, etc.

Email: zhangx@cqupt.edu.cn

Ying Xia is a professor of Chongqing University of Posts and Telecommunications. Her research area includes database, data mining, etc.

Email: xiaying@cqupt.edu.cn

Hongrui Mao is a master degree candidate of Chongqing University of Posts and Telecommunications. His research interests include database, data privacy, etc.

Email: maohongr@hotmail.com

HaeYoung Bae is tenured full professor of Inha University of Korea, and he is honorary professor of the Chongqing University of Posts and Telecommunications of China. His research area mainly includes database and spatial information processing.

E-mail: hybae@inha.ac. kr