International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 41-52
http://dx.doi.org/10.14257/ijsia.2015.9.4.06

Location Positioning and Privacy Preservation Methods in Location-based Service

Xu Zhang[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@cqupt.edu.cn, hybae@inha.ac.kr

Abstract

Location-based services (LBS) become more feature-rich and versatile due to the explosion of mobile devices and the advances of positioning technologies. However, revealing personal private locations to potentially un-trusted LBS server and others may raise serious privacy concerns if these locations are not protected adequately. In this paper, we present a survey of existing methods dealing with outdoor and indoor localization techniques and location privacy protection techniques. We propose a taxonomy that summarizes the state-of-the-art. This survey is intended to help researchers in quickly understanding existing works and challenges, and possible improvements to bring.

Keywords: *Localization Technology, Location Privacy, Location-based Service, Privacy Preservation*

1. Introduction

Recently, various location-detection technologies have been implemented to record indoor and outdoor movement, e.g., Global Positioning System (GPS), cellular networks, Wi-Fi and radio frequency identification (RFID). Location-based services (LBS) become more feature-rich and versatile due to the explosion of mobile devices and the advances of positioning technologies that have been implemented to record indoor and outdoor movement. Explosion of mobile data with location information may reveal personal private locations to potentially un-trusted LBS server and others may raise serious privacy concerns if these locations are not protected adequately. There is a potential conflict of interest in LBS: the high quality of service and utility needs a precise description of location, while the users want to enjoy the LBS by not disclosing sensitive movements with anonymized location.

Although many people clearly consider their privacy a fundamental right, comparatively few can give a precise definition of the term and cannot distinguish it from security. Privacy is defined as the right of individuals to determine for themselves *when*, *how*, and *to what extent* information about them is communicated to others. Privacy indicates a specific form of data protection requiring flexible control over the disclosure of personal information. Location-based service facilitates human daily life, however, recorded location data enables intrusive inferences that may reveal personal habits, social customs, and religious that can be used for unauthorized advertisement.

ISSN: 1738-9976 IJSIA

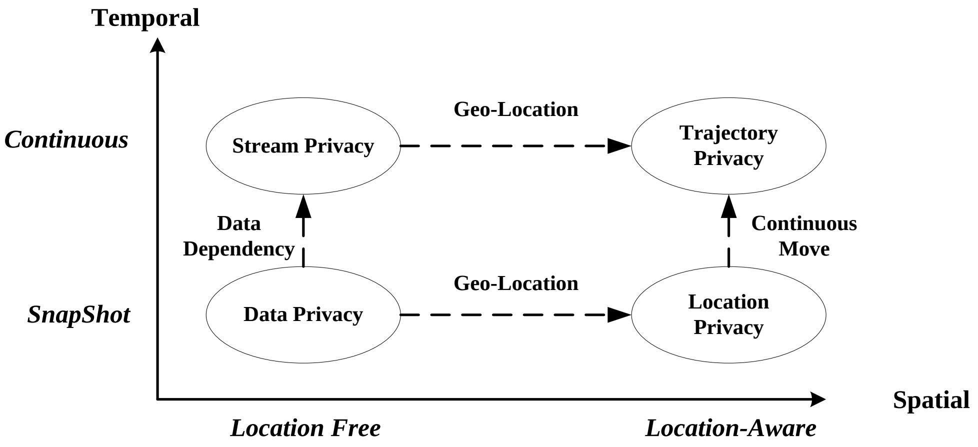


Figure 1. Category of Privacy Protection

As it is shown in Fig.1, we conclude privacy protection issue with the consideration of spatial and temporal information. Data privacy concerns about privacy preservation problem with independent data at the left bottom. When considering privacy preservation in spatial dimension, each data is attached with geographic location. Thus, how to prevent adversaries from obtaining geographic related activities is the main issue in location privacy. Then we consider temporal features between data from snapshot to continuous. Continuously processed data involved dependency from past to future, which make it possible to infer hidden information behind data. This is concerned as stream privacy. In location-based service, mobile users issue location-based queries to LBS service providers to obtain information based on their geographic location. This is a new challenge to traditional data privacy-preserving techniques due to both temporal and spatial information should be concerned. Furthermore, temporal and spatial information should not be considered separately. Spatio-temporal feature may indicate significant implicit information, which should be protected.

The remainder of this paper is organized as follows. First, we give an introduction of general positioning technologies in location-based service in Section 2, and discuss privacy categories and system architecture of LBS in Section 3. Section 4 addresses the privacy preservation algorithms. And, the some specialized area like indoor environment, wireless sensor network and cognitive radio network are discussed in Section 5 and draw a conclusion in Section 6.

2. 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 1, there are several metrics to classify existing works.

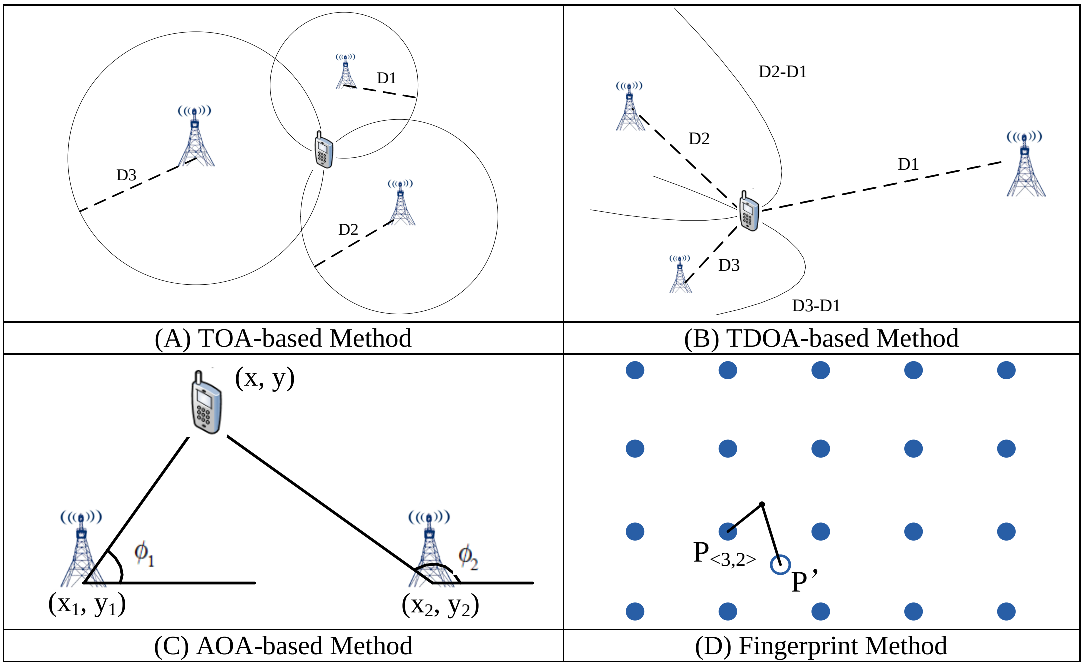
Table 1.Classification of Localization Algorithms

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

Networks	Distributed
	Cooperative
	Non-Cooperative

A. Distance 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 Figure4, 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 different devices. In AOA-based (Angle Of Arrival) method, the combined angle information to compute an intersection point of the target device. 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.



(A) TOA-based Method

(B) TDOA-based Method

(C) AOA-based Method

(D) Fingerprint Method

Figure 2. Range-based Localization

B. Centralized VS Distributed Localization

As it is shown in Fig. 3, 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.

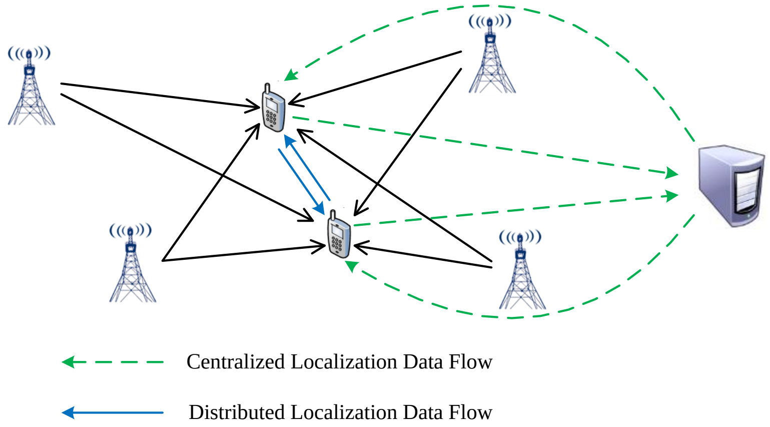
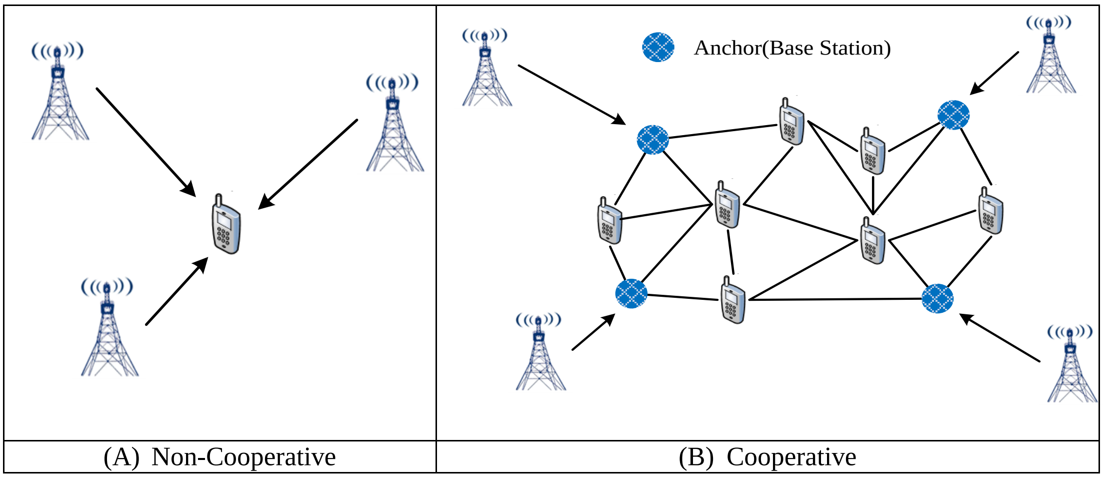

Centralized Localization Data Flow
Distributed Localization Data Flow

Figure 3. 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 Fig. 4, base station (anchor) is needed for cooperative localization.



(A) Non-Cooperative

(B) Cooperative

Figure 4. Non-Cooperative & Cooperative Localization

3. Privacy Issue and Architecture in LBS

Location privacy and trajectory privacy stand for two aspects in location-based service. As it is shown in Table 2, location privacy generally considers independent locations, while trajectory privacy concerns more about continuous query and dependent locations.

Table 2. Privacy Issue in Location-based Service

	Location Privacy	Trajectory Privacy
Purpose	Keep privacy of currently received independent location data	Keep privacy of dependent location data
Query	Explicit/Implicit query	Explicit/Implicit query
	Snapshot query	Continuous query

Existing privacy preservation issues considered in LBS can be separated in three categories from the architecture perspective: *Client-Server*, *Third Trusted Party* and *Peer-to-Peer Cooperative*.

- Client-Server Architecture

As it is shown in Fig. 5, all the users request for location-based service directly communicated with a single server to query information and perform an anonymization. It is easy to be implemented and integrated with existing technologies, however, the quality of service is low. Privacy issues concerned in this area mainly try to cheat the server with either fake locations or fake spaces. Featured privacy protection algorithms including CAP [42], PIR [43] and Dummy-Q [44].

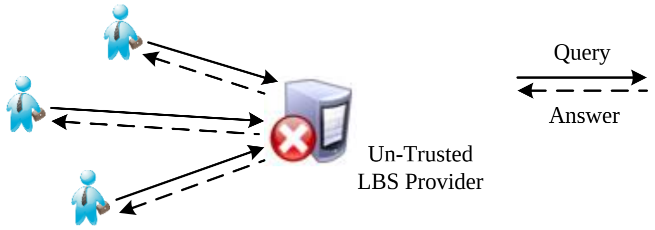


Figure 5. Client-Server Privacy Protection LBS Architecture

- Third Trusted Party Architecture

A trusted party server is deployed between users and service provider that take the response for gathering information, positioning and providing required privacy. As it is shown in Fig. 6, the trusted anonymizer receives exact locations from users, blurs locations and sends the blurred locations to service provider. This architecture can provide powerful privacy guarantees with high quality of services. However, it suffers same system bottleneck problems as client-server architecture, and it need sophisticated implementations. The common purpose of proposed methods with this architecture is to minimum anonymized queries and thus answer set to reduce both computation and communication overhead. Featured algorithms including Casper[45], DGCC [46], L2P2 [47] and IClique [48].

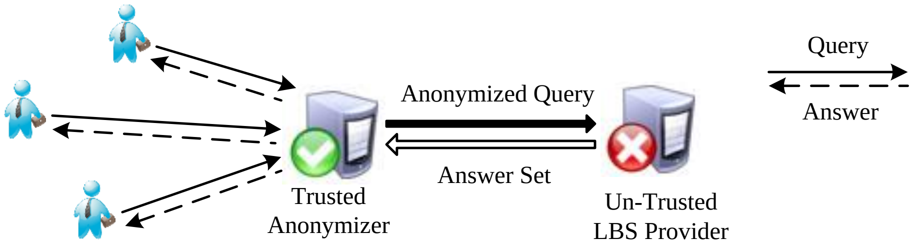


Figure 6. Third Trusted Party Privacy Protection LBS Architecture

- Peer-to-Peer Cooperative Architecture

In a peer-to-peer environment, users can collaborate with each other without the interleaving of a centralized server to reduce communication cost. As it is shown in Fig. 7, a trusted anonymizer is not necessary. However, a certificate could be applied to approve trustworthy users. There are two assumption scenarios: (1) both the peer users and service providers are malicious adversaries, (2) only service providers are malicious adversaries. Featured algorithm is P2P-IS-HL-CA[49].

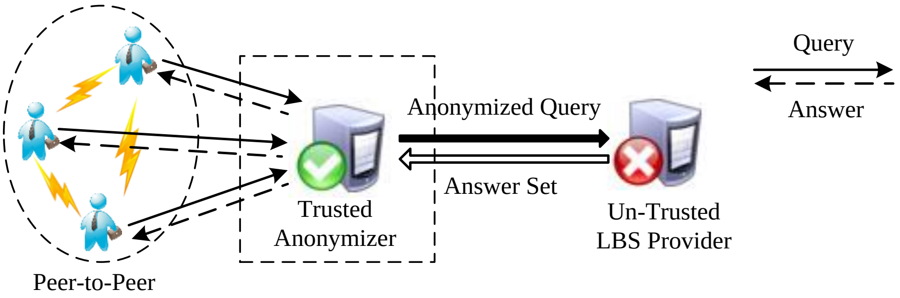


Figure 7. Peer-to-peer Cooperative Privacy Protection LBS Architecture

4. Privacy Preservation Algorithms

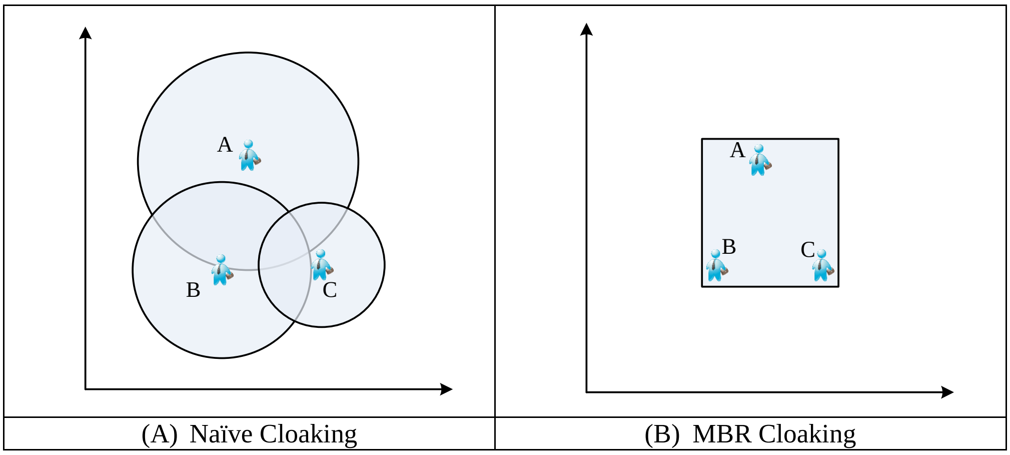
Recently, various privacy protection techniques in LBS have been widely studied based on several concepts: *privacy policies*, *false locations*, *space transformation* and *spatial cloaking*.

Several methods have been proposed to relax trusted anonymization server and guarantee privacy in LBS. Private information retrieval (PIR) [43] can prevents any type of location-based attack, however, it incurs significant computational overhead on the server side and imposes stringent requirements on LBS server deployment. Dummy-Q method [44] is proposed to generate dummy queries with different attributes from same location, however, generated dummy queries maybe irrational and thus easily to be identified by adversaries.

To relax the trusted third party assumption and lower the communication costs, Mokbel et al. in [45,49] proposed a new scheme that leverages the peer-to-peer concept. However, peers are assumed to be trusted, which made the management of trust relationships among autonomous peers in LBS remains an open issue.

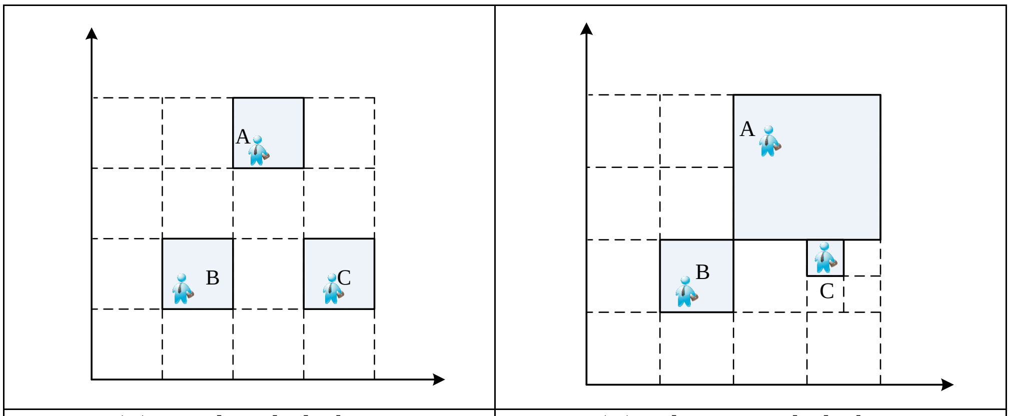
A lot of research work has focused on anonymity and obfuscation-based techniques for privacy preservation. The *k*-anonymity and *l*-diversity are generally used. The *k*-anonymity based location privacy protection methods[50][51] propose to extend a cloaking region until *k-1* other users are included, while *l*-diversity based location privacy protection methods take *l-1* different locations into consideration.

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].



(A) Naïve Cloaking

(B) MBR Cloaking



(C) Fixed Grid Cloaking

(D) Adaptive Grid Cloaking

Figure 8. Basic Spatial Cloaking Methods

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.

5. Specialized Area

5.1 Indoor Environment

As we know, GPS is not available in indoor environment, most localization methods rely on signal strength, which have driven much more attention in research and development during the last decade. For the localization issue in indoor environment, angle and distance methods can be used to some extent. However, due to the complex environment, localization accuracy is easy to be influenced. For example, human movement, arbitrary walls and settings may influence the signal strength and thus output worse location estimation. WiFi fingerprint-based localization is regarded as one of the most promising techniques for indoor localization [52]. Other methods proposed to use RFID or extra sensor nodes to improve localization accuracy. However, this is expensive and need pre-deployment.

5.2 Wireless Sensor Network

In WSN, localization is one of the most active areas of research in recent years because the location information is typically useful for coverage, deployment, routing, location service, target tracking, and rescue. For a large number of sensor nodes, straightforward solution of adding GPS to all nodes in the network is not feasible. There are several challenges for locating sensor nodes needed to be solved. The first challenge is the energy consumption and localization accuracy problem. The second challenge is the NLOS ranging error problem. The third challenge is localization in low beacon density. Besides general adopted methods discussed in previous sections, there are some existing techniques which use two localization techniques such as multidimensional scaling (MDS) and proximity based map (PDM) [53] or MDS and Ad-hoc Positioning System (APS) [54].

5.3 Cognitive Radio Network

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[3,41]. Localization of primary user is crucial in enabling several key capabilities in Cognitive Radio Networks. There are various security concerns specific to CRNs, one of the most dominant threats among these is the Primary User Location Attack.

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 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 Fig. 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:

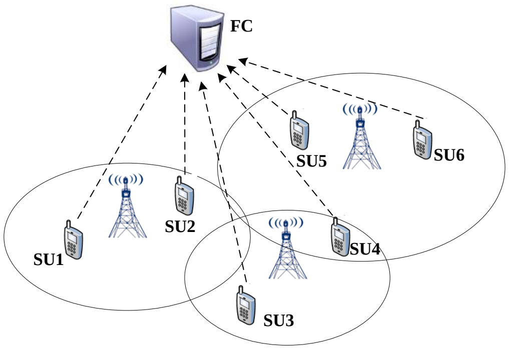


Figure 9. Spectrum Sensing with one FC(Fusion Center)

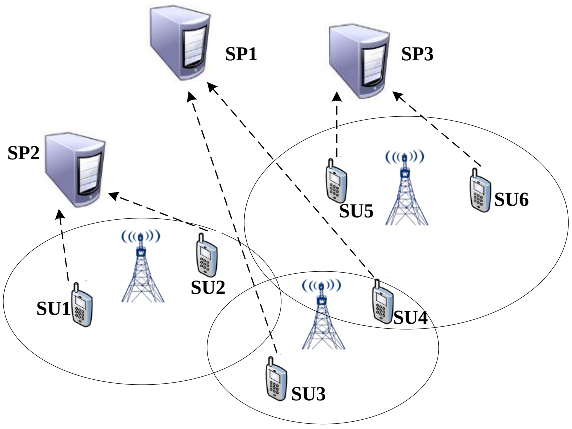


Figure 10. Spectrum Sensing with Multi-SPs

As it is shown in Fig. 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 privacy preservation mainly in location-based service, and also discussed in specialized areas such as indoor environment, wireless sensor network and cognitive radio network. The objective is to provide a comprehensive analysis and guide of existing efforts. 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).

This paper is a revised and expanded version of a paper entitled “Privacy-preserving Localization in Cognitive Radio Networks” presented at FGCN, Hainan, China on 22th DEC.

References

[1] S. Haykin, “Cognitive radio: brain-empowered wireless communications”, Selected Areas in Communications, IEEE Journal, 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)**; 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 SDR Forum Technical Conference, **(2005)**; Anaheim, USA.

[9] I. F. Akyildiz, W. Y. Lee, M. C. Vuran and S. Mohanty, “NextGeneration/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, IEEE, **(2009)**; Honolulu, HI, USA.

[11] J. Minho, H. Longzhe, K. Dohoon and H. P. In, “SelfishAttacks and Detection in Cognitive Radio Ad-Hoc Networks”, Network, IEEE, vol. 27, **(2013)**, pp. 46-50.

[12] C. Qian, M. Motani, W. W. 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, “GeolocationTechniques: Principles and Applications: Springer”, **(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 on, **(2012)**; 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, **(2010)**; 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)**; Beijing, China.

[17] R. Kurazume, S. Nagata and S. Hirose, “Cooperative Positioning with Multiple Robots in Robotics and Automation”, Proceedings of IEEE International Conference, **(1994)**; 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, Proceedings of the 22nd International Conference, **(2006)**; 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)**; 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”, InhaUniversity, **(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, **(2003)**; 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)**; Toronto, Canada.

[28] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing and X. Shen, “Location Privacy Preservation in Collaborative Spectrum Sensing”, INFOCOM, Proceedings IEEE, **(2012)**; Orlando, FL, USA.

[29] S. Kim, H. Jeon and J. Ma, “Robust Localization with Unknown Transmission Power for Cognitive Radio”, Military Communications Conference, IEEE, **(2007)**; 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, **(2012)**; 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, IEEE, **(2013)**; 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”, Applied Sciences in Biomedical and Communication Technologies (ISABEL), the 3rd International Symposium, **(2010)**; 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)**; Stockholm, Sweden.

[34] P. Mahonen, 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)**; 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)**; 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, **(2003)**; Washington, DC, USA.

[37] H. Yu, X. Jiang and J. Vaidya, “Privacy-preserving SVM using Nonlinear Kernels on Horizontally Partitioned Data”, Proceedings of the ACM symposium on Applied computing, ACM, **(2006)**; 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, "LocationPrivacy in Database-driven Cognitive Radio Networks: Attacks and Countermeasures", INFOCOM, Proceedings IEEE, **(2013)**; 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)**.

[42] A. Pingley, W. Yu, N. Zhang, X. Fu and W. Zhao, "Cap: A context-aware privacy protection system for location-based services", Distributed Computing Systems, 29th IEEE International Conference, IEEE, **(2009)**.

[43] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi and K. L. Tan, "Private queries in location based services: anonymizers are not necessary", Proceedings of the ACM SIGMOD international conference on Management of data, ACM, **(2008)**.

[44] A. Pingley, N. Zhang, X. Fu, H. A. Choi, S. Subramaniam and W. Zhao, "Protection of query privacy for continuous location based services", INFOCOM, IEEE, **(2011)**.

[45] M. F. Mokbel, C. Y. Chow and W. G. Aref, "The new casper: query processing for location services without compromising privacy", Proceedings of the 32nd international conference on Very large data bases, VLDB Endowment, **(2006)**.

[46] H. I. Kim and J. W. Chang, "A grid-based cloaking scheme for continuous location-based services in distributed systems", Computer Science and its Applications, **(2012)**, pp. 69–78.

[47] Y. Wang, D. Xu, X. He, C. Zhang, F. Li and B. Xu, "L2p2: Location-aware location privacy protection for location-based services", INFOCOM, IEEE, **(2012)**, pp. 1996–2004.

[48] X. Pan, J. Xu and X. Meng, "Protecting location privacy against location-dependent attacks in mobile services", Knowledge and Data Engineering, IEEE Transactions, vol. 24, no. 8, **(2012)**, pp. 1506–1519.

[49] C. Y. Chow, M. F. Mokbel and X. Liu, "Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments", GeoInformatica, vol. 15, no. 2, **(2011)**, pp. 351–380.

[50] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location-based services", INFOCOM, The 27th Conference on Computer Communications, IEEE, **(2008)**.

[51] T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services", Proceedings of the 16th ACM conference on Computer and communications security, ACM, **(2009)**.

[52] H. Li, H. J. Zhu, X. Lu and X. Z. Cheng, "Achieving Privacy Preservation in WiFi Fingerprint-Based Localization", INFOCOM, IEEE, **(2014)**, pp.2337-2345.

[53] K. Y. Cheng, K. S. Lui and V. Tam, "Localization in Sensor Networks with Limited Number of Anchors and Clustered Placement", Proceedings of Wireless Communications and Networking Conference, **(2007)**.

[54] A. A. Ahmed, H. Shi and Y. Shang, "Sharp: A new approach to relative localization in wireless sensor networks", Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS), **(2005)**; Columbus, Ohio, USA.

Authors

Xu Zhang, he 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

HaeYoung Bae, he is a tenured full professor of Inha University of Korea, and he is an honorary professor of the Chongqing University of Posts andTelecommunications of China. His research area mainly includesdatabase and spatial information processing.

E-mail: hybae@inha.ac.kr