International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Location Privacy Preservation in Database-DrivenWireless Cognitive Networks

Masku Naveen Kumar & Golla Saidulu
[1]Assistant Professor, Dept of CSE, SCIENT Institute of Technology
[2]Assistant Professor, Dept of CSE, CMR College of Engineering And Technology

ABSTRACT:*In this paper, we recommend new vicinity privatenesskeeping schemes for database-driven cognitive radio networks(CRNs) that guard secondary customers' (SUs) region privatenesseven as allowing them to study spectrum availability of theirlocation. Our schemes harness probabilistic set membership recordsstructures to make the most the based nature of spectrum databases(DBs) and SUs' queries. This allows us to create a compactillustration of DB that might be queried by SUs withouthaving to proportion their area with DB, consequently guaranteeing theirlocation privateness. Our suggested schemes provide extraordinary value overall performance characteristics. Our first scheme is based on a simplebut powerful two-party protocol that achieves unconditionalsecurity with a practicable communication overhead with the aid of makingDB send a compacted version of its content material to SU which needshandiest to query this facts structure to analyze spectrum availability.*

KEYWORDS-

I. INTRODUCTION

Mobile context awareness can be defined as a mobile device's ability to identify and infervarious information which can be related to location, time, social status, physiological condition of the user etc. Context awareness can be leveraged by a mobile device in orderto enhance some underlying computational function. For example, while scheduling a taxipickup, a mobile device can leverage its GPS positioning system and provide the underlying application with its exact location coordinates. A mobile recommendation system canleverage location, as well as social status information, in order to recommend more relevantproducts to close friends and family. Mobile health and fitness applications can leverage auser's location, mobility speed and heart rate in order to map running routes, compute fatburning and other physiological functions which can reported as daily health charts.

While context awareness has played a catalytic role towards the rise in popularity ofmobile computing, it has done so at the expense of user privacy. Out of various potentialprivacy threats, the threat towards location privacy is probably the biggest one that canarise as a result of abusive treatment and mis-management of a mobile device's contextawareness. Location privacy is the fundamental block against the fast growing erosion ofprivacy and anonymity in a digital world. Movement patterns not only could be used toidentify us as individuals, but they can be used to leak sensitive information about us suchas health conditions, lifestyle, political/religious affiliations, etc.

The allocation of radio spectrum for mobile wireless networking is governed by federal agencies via a fixed (static) spectrum sharing strategy. However, with the ever growing need formobile wireless services and applications, the static sharing method has led to the depletion of the available spectrum. Furthermore, the actual usage of pre-assigned spectrumbands has been measured to have a very low average utilization. For example, in the US,the Federal Communications Commission (FCC) has reported that many spectrum bandsallocated via static assignment policies have been used only in bounded geographical areasand over very limited periods of time. Such utilization has been measured to be between15% and 85% [9].

Currently, there is wide consensus that the static method of spectrum allocation hasmajor drawbacks. As a result, the need for opportunistic and dynamic spectrum accesstechnologies has risen sharply. A flexible and dynamic spectrum access strategy is necessary,in order to eliminate the underutilization and spectrum depletion effects of the current staticallocation scheme. The FCC has stated that no other technology “holds greater potentialfor literally transforming the use of spectrum in the years to come than the development ofsoftware-defined and cognitive/smart radios”.

To this end, DSA allows users to access licensed spectrum bands when not in use bytheir respective owners. DSA is built on top of Cognitive Radio (CR), an intelligent wirelesscommunications system that is aware of its spectral environment. A CR node must beable to dynamically adapt to the environmental spectral changes in order to abide by thespectral etiquette set forth by the FCC. One of the most important functions that a CR nodemust perform is the identification of unoccupied spectrum opportunities (SOPs). SOPs arespace, time, and frequency dependent blocks, during which the license-exempt can utilizethe registered owner’s spectrum in a DSA manner.

In this paper, we suggest two location privacy-preservingschemes for database-driven CRN s with different performance and architectural benefits. The first scheme, locationprivacy in database-driven CRNs (LPDB), provides optimallocation privacy to SU s within DB’s coverage area by leveraging set membership data structures (used to test whetheran element is a member of a set) to construct a compactversion of DB. The second scheme, LPDB with two servers(LPDBQS), minimizes the overhead at SU ’s side at the costof deploying an additional entity in the network.

II. RELATED WORK

Despite its importance, the location privacy issue in CRN sonly recently gained interest from the research community [12]. Some works focused on addressing this issue inhe context of collaborative spectrum sensing [13]–[17] whileothers focused on addressing it in the context of dynamicspectrum auction [18]. However, these works are not withinthe scope of this paper as we focus on the location privacyissue in database-driven CRN s.Protecting SU s’ location privacy in database-driven CRN sis a very challenging task, since SU s are required to providetheir physical locations to DB in order for them to be

able to learn about spectrum opportunities in their vicinities.Recently developed techniques mostly adopt either the kanonymity [19], Private Information Retrieval (PIR) [20], ordifferential privacy [21] concepts. However, direct adaptationof such concepts yield either insecure or extremely costly results. For instance, k-anonymity guarantees that SU ’s locationis indistinguishable among a set of k points, which could beachieved through the use of dummy locations by generatingk−1 properly selected dummy points, and performing kqueries to DB using both the real and dummy locations. Forexample, Zhang et al. [22] rely on this concept to make eachSU query DB by sending a square cloak region that includesits actual location. Their approach makes a tradeoff betweenproviding high location privacy and maximizing some utility,which makes it suffer from the fact that achieving a highlocation privacy level results in a decrease in spectrum utility.PIR, on the other hand, allows a client to obtain information from a database while preventing the database fromlearning which data is being retrieved. Several approacheshave used this approach.

III. PROPOSED WORK

A. Database-driven CRN Model

We first consider a CRN that consists of a set of SU s and a geo-location database (DB). SU s are assumed to beenabled with GPS and spectrum sensing capabilities, and tohave access to DB to obtain spectrum availability informationwithin its operation area. To learn about spectrum availability,a SU queries DB by including its location and its devicecharacteristics. DB responds with a list of available channelsat the specified location and a set of parameters for transmission over those channels. SU then selects and uses one ofthe returned channels. While using the channel, SU needs torecheck its availability on a daily basis or whenever it changesits location by 100 meters as mandated by PAWS [10].We then investigate incorporating a third entity to thenetwork along with DB and SU s. This entity, referred toas query server (QS), has a dedicated high throughput linkwith DB. QS is used to guarantee computational locationprivacy while reducing the computational and communicationoverhead especially on SU s' side.

B. Security Model and Assumptions

DB and QS are assumed to be honest but curious. Thatis, DB and QS follow the protocol honestly but may try toinfer information on the input of other parties beyond whatthe output of the protocol reveals. Specifically, our objectiveis to prevent these two entities from learning SU s' location.Therefore, our security assumptions are as follows:

Security Assumption 1. DB and QS do not modify theintegrity of their input. That is, (i) DB does not maliciouslychange SU 's query's content; (ii) QS does not modify theinput that it receives from DB or SU .

Security Assumption 2. DB and QS do not collude witheach other to infer the location of SU s from their queries.

In this section, we describe our proposed schemes. The firstscheme, LPDB, is simple as it involves only two parties,SU s and DB, and provides unconditional location privacy toSU s within the coverage area of DB. The second scheme,LPDBQS, offers computational privacy with a significantlyreduced overhead on SU s' side compared to LPDB, but atthe cost of introducing an extra architectural entity.Since we are unable to access the actual spectrum database, we relied on two sources to have an estimate of this structure:

First, we have relied on the recommendation of the PAWSstandard [10], which defines the interaction between SU s andDB and what information they should exchange. Second, weused graphical web interfaces provided to the public by whitespace database operators like Google, Microsoft ,iconectiv etc. These web interfaces comply with PAWSrecommendation and allow an interested user to specify alocation of interest and learn spectrum availability in thatlocation to emulate the interaction between a SU and DB inreal world. While the purpose of these interfaces was initiallyto provide a working platform as a showcase for FCC toacquire approval for operating spectrum database, we believe it has enough information to enable us to estimate the structureof the database and SU s' queries.

As required by PAWS, SU s must be registered with DB tobe able to query it for spectrum availability. RegisteredSU starts by sending an initialization query to DB whichreplies by informing the SU of specific parameterized-rulevalues. These parameters include time periods beyond whichthe SU must update its available-spectrum data, and maximum location change before needing to query DB again.Afterwards, SU queries DB with an available spectrum querywhich contains its geolocation, device identifier, capabilities(to limit DB's response to only compatible channels) andantenna characteristics (e.g. antenna height and type). DB thenreplies with the set of available channels in the SU 's locationalong with permissible power levels for each channel.

A. LPDB: In this section, we describe our basic scheme, which isreferred to as location privacy in database-driven CRN s(LPDB). The novelty of LPDB lies in the use of set membership data structures to construct a compact (space efficient)representation of DB that can be sent to querying SU s toinform them about spectrum availability.

Algorithm 1 *LPDB* Algorithm

SU queries DB with $query \leftarrow f(char, ts)$;
DB retrieves *resp* containing r entries satisfying *query*;
DB constructs CF;
for $j = 1, \ldots, r$ **do**
  if $avl_j = 1$ **then**
    $x_j \leftarrow (locX_j \| locY_j \| chn \| ts \| \ldots)$;
    DB inserts x_j into CF: $CF.Insert(x_j)$;
DB sends CF to SU;
SU initializes $decision \leftarrow$ Channel is busy
for `all possible combinations of` ***par*** **do**
  SU computes $y \leftarrow (locX \| locY \| chn_i \| ts \| \ldots \| par^n)$;
  if $CF.Lookup(y)$ **then**
    SU senses chn;
    if $Sensing(chn) \leftarrow$ available **then**
      $decision \leftarrow chn$ is available; **break**;
return $decision$

B. LPDBQS: In this section, we propose a new scheme, LPDBQS, whichoffers better performance at SU s' side than that of LPDB.This comes at the cost of deploying an additional entity,referred to as query server (QS), and having a computationalsecurity as opposed to unconditional. QS is introduced tohandle SU s' queries instead of DB itself, which preventsDB from learning information related to SU s' location

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

information. QS learns nothing but secure messages sent bySU s to check the availability of a specific channel.

Algorithm 2 *LPDBQS* Algorithm

SU queries DB with $query \leftarrow f(k, char, ts)$;
DB retrieves $resp$ containing r entries satisfying $char$;
DB constructs CF_k;
for $j = 1, \ldots, r$ **do**
  if $avl_j = 1$ **then**
    $x_j \leftarrow (locX_j \| locY_j \| ts \| \ldots \| row_j(c))$;
    $CF_k.Insert_{HMAC_k}(x_j)$;
DB sends CF_k to QS over a high throughput link;
SU initializes $decision \leftarrow$ Channel is busy
for `all possible combinations of` par **do**
  SU computes $y \leftarrow (locX \| locY \| chn \| ts \| \ldots \| par^n)$;
  SU computes $y_k \leftarrow HMAC_k(y)$ and sends it to QS;
  QS looks up for y_k in CF_k using $Lookup$;
  if $CF_k.Lookup(y_k)$ **then**
    SU senses chn;
    if $Sensing(chn) \leftarrow$ available **then**
      $decision \leftarrow chn$ is available; **break**;
return $decision$

IV. CONCLUSION

In this paper, we have proposed two location privacypreserving schemes, called LPDB and LPDBQS, that aimto preserve the location privacy of SU s in database-drivenCRN s. They both use set membership data structures totransmit a compact representation of the geo-location databaseto either SU or QS, so that SU can query it to check whethera specific channel is available in its vicinity.

REFERENCES

[1] M. Grissa, A. A. Yavuz, and B. Hamdaoui, “Cuckoo filter-basedlocation-privacy preservation in database-driven cognitive radio networks,” in WSCNIS. IEEE, 2015, pp. 1–7.

[2] “Spectrum policy task force report,” Federal Communications Commission, Tech. Rep. ET Docket No.02-135, 2002.

[3] B. Khalfi, M. B. Ghorbel, B. Hamdaoui, and M. Guizani, “Optimalpower allocation for smart-grid powered point-to-point cognitive radiosystem,” in ComComAp, 2014 IEEE, pp. 316–320.

[4] H. Zhu, C. Fang, Y. Liu, C. Chen, M. Li, and X. S. Shen, “You canjam but you cannot hide: Defending against jamming attacks for geolocation database driven spectrum sharing,” IEEE Journal on SelectedAreas in Communications, vol. 34, no. 10, pp. 2723–2737, 2016.

[5] M. Guizani, B. Khalfi, M. B. Ghorbel, and B. Hamdaoui, “Largescale cognitive cellular systems: resource management overview,” IEEECommunications Magazine, vol. 53, no. 5, pp. 44–51, 2015.

[6] N. Adem and B. Hamdaoui, “The impact of stochastic resource availability on cognitive network performance: modeling and analysis,” WirelessCommunications and Mobile Computing, 2015.

[7] B. Khalfi, M. B. Ghorbel, B. Hamdaoui, and M. Guizani, “Distributedfair spectrum assignment for large-scale wireless dsa networks,” in International Conference on Cognitive Radio Oriented Wireless Networks.Springer, 2015, pp. 631–642.

[8] N. Adem and B. Hamdaoui, “Delay performance modeling and analysisin clustered cognitive radio networks,” in Global CommunicationsConference (GLOBECOM), 2014 IEEE. IEEE, 2014, pp. 193–198.

[9] W. Wang and Q. Zhang, Location Privacy Preservation in CognitiveRadio Networks. Springer, 2014.

[10] L. Zhu, V. Chen, J. Malyar, S. Das, and P. McCann, “Protocol to accesswhite-space (paws) databases,” 2015.

[11] S. B. Wicker, “The loss of location privacy in the cellular age,”Communications of the ACM, vol. 55, no. 8, pp. 60–68, 2012.

[12] M. Grissa, B. Hamdaoui, and A. A. Yavuz, “Location privacy incognitive radio networks: A survey,” IEEE Communications Surveys &Tutorials, 2017.

[13] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen, "Locationprivacy preservation in collaborative spectrum sensing," in INFOCOM,2012 Proceedings IEEE. IEEE, 2012, pp. 729–737.

[14] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Lpos: Location privacy foroptimal sensing in cognitive radio networks," in Global CommunicationsConference (GLOBECOM), 2015 IEEE. IEEE, 2015.

[15] W. Wang and Q. Zhang, "Privacy-preserving collaborative spectrumsensing with multipleservice providers," Wireless Communications,IEEE Transactions on, 2015.

[16] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "An efficient techniquefor protecting location privacy of cooperative spectrum sensing users,"in Computer Communications Workshops (INFOCOM WKSHPS), 2016IEEE Conference on.IEEE, 2016, to be published.

[17] "Preserving the location privacy of secondary users in cooperativespectrum sensing," IEEE Transactions on Information Forensics andSecurity, vol. 12, no. 2, pp. 418–431, 2017.

[18] S. Liu, H. Zhu, R. Du, C. Chen, and X. Guan, "Location privacypreserving dynamic spectrum auction in cognitive radio network," inDistributed Computing Systems (ICDCS), 2013 IEEE 33rd InternationalConference on. IEEE, 2013, pp. 256–265.

[19] M. Gruteser and D. Grunwald, "Anonymous usage of location-basedservices through spatial and temporal cloaking," in Proceedings of the 1stinternational conference on Mobile systems, applications and services.ACM, 2003, pp. 31–42.

[20] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," JACM, vol. 45, no. 6, 1998.

[21] C. Dwork, "Differential privacy: A survey of results," in InternationalConference on Theory and Applications of Models of Computation.Springer, 2008, pp. 1–19.

[22] L. Zhang, C. Fang, Y. Li, H. Zhu, and M. Dong, "Optimal strategiesfor defending location inference attack in database-driven crns," inCommunications (ICC), 2015 IEEE International Conference.

BIODATA

Masku Naveen Kumar working as Assistant Professor, Dept of CSE, in SCIENT Institute of Technology with Experience of 2 years.

Golla Saidulu working as Assistant Professor, Dept of CSE, in CMR College of Engineering And Technology with Experience of 3.6 years.