A Framework for Securing User's Location in CRN’s by developing LPDB and LPDBQS

Neha Nazmeen
M. Tech, CNIS
G. Narayanamma Institute of Technology
and Science, Hyderabad.

M. Sridevi
Assistant Professor
G. Narayanamma Institute of Technology
and Science, Hyderabad.

ABSTRACT— Cognitive radio networks (CRNs) Become a promising answer for overcoming the lack along with ineffective make use of bandwidth sources by means of permitting secondary user (SUs) to get right of entry to the primary users' (PUs) channels so long as they do now not intervene with them. Despite its significance, the location privateness trouble in CRN s simplest recently won interest from the research network. Some works centered on addressing this difficulty in the context of collaborative spectrum sensing while others targeted on addressing it inside the context of dynamic spectrum auction. However, those works did no longer focused on the place privacy of the customers. within term paper, we suggest location privateness-preserving schemes for database-pushed CRNs. The first scheme, location privateness in database-driven CRNs (LPDB), provides finest place privateness to SUs within DB’s coverage place by means of leveraging set club statistics structures (used to test whether or not an detail is a member of a hard and fast) to construct a compact version of DB. The second scheme, LPDB with servers (LPDBQS), minimizes the overhead at SU’s side at the fee of deploying an extra the network.

s— Networking, Cognitive Radio Networks, Database, Data Structure

1. INTRODUCTION

Over the last decade, the ever growing spectrum demand for emerging wireless programs has inspired the concept of cognitive radio (CR) that is anticipated to improve the usage of the precious natural resource, radio spectrum. Different from the traditional spectrum control paradigms in which maximum of the spectrum is allocated to number one customers (PU) for distinctive use, a CR system lets in secondary customers (SU) or decrease-priority customers to make the most the unoccupied spectrum opportunistically. By reusing the waste spectrum of a few number one spectrum holders, CR might partially deal with the spectrum scarcity difficulty. A promising and incentive approach to re-distribute spectrum assets among PUs and SUs in CR network is dynamic spectrum public sale. Through auction, SUs could gain spectrum admittance within a cost-powerful manner even as PUs would receive compensation from SUs as the praise of contributing their spectrum sources to others. Unlike different traditional auction schemes, dynamic spectrum public sale lets in the nicely-separated bidders to utilize the same channel simultaneously, denoted as spectrum reusability.

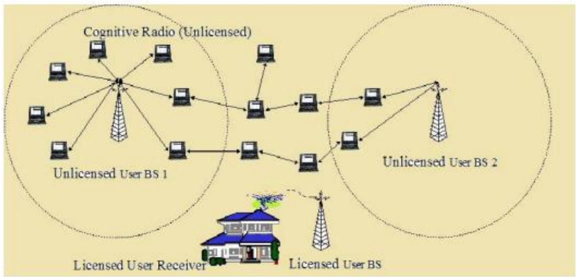


Fig1. Example Cognitive Radio Network

Within a distinctive cognitive radio operation, SU's expense on the way to PU depends on SU's complete procedure details, such as at what time as well as how extensive the certified scale have be utilize. PU desires this practice in order to compute otherwise validate the expense, other than comprehensive procedure in sequence be responsive toward SU as well as the discovery of this data might concession SU's confidentiality. So, defending PU's benefit in addition to preserve SU's confidentiality at the same time become extremely demanding. in the direction of the finest of our awareness, not any of the existing effort have address this difficulty into cognitive radio communication. Within this term paper, we suggest a novel privacy-preserving mechanism designed for cognitive radio transactions. This mechanism not no more than preserves SU's privacy however as well protect PU's interests. Within this method, PU simply know a small section of SU's responsive data during a bill phase by means of the consequence that SU's privacy be preserved. On the identical time, PU know the whole expense intended for a billing period along with is certain that the expense be properly planned as well as PU's wellbeing be confined. This system employ assurance scheme along with zero-knowledge verification. by the conclusion of a billing period, SU commit all comprehensive procedure data in addition to the compensation intended for every consumption instance, as well as provide a zero-knowledge verification meant for every consumption occurrence that the payment be properly considered. These commitment along with proof, all along by means of the entirety charge, be send toward PU.

Due toward the defeat possessions of the planned method, the commitment achieve but not expose several facts concerning the exhaustive procedure in order. Suitable in the direction of the required possessions of the assurance system, SU cannot refuse the value that is use to make the commitment. Furthermore, by verify the zero-knowledge proof provide by SU, PU is able to verify that the payment for each operation occurrence be accurate. To avoid SU as of commit scheme, such as choose not to suggest all consumption instance or else submit fake consumption instance, we establish a random-checking monitor that can provide some ground-truth information on the spectrum utilization status. PU can opportunistically query the monitor to ask for a few pieces of ground-truth information, and use this information to challenge SU. Once SU is challenged, it has to provide proof to match the random-checking in sequence.

2. RELATED WORK

The region dataleakage trouble within the CRN context has lately began to advantage attention from the research network because of its significance, and numerous studies efforts had been made to address it. However, to the satisfactory of our data, none of those works have tried to perceive the vulnerabilities which are behind this trouble or discuss the techniques that could be deployed to save you it. M. Grissa, B. Hamdaoui, and A. A. Yavuz tried to fill this hole via presenting a comprehensive survey that investigates the various area privacy dangers and threats which could rise up from the unique components of this CRN technology, and explores the distinct privateness assaults and countermeasure solutions that have been proposed inside the literature to cope with this region privacy trouble. They additionally discuss a few open studies troubles, associated with this trouble, that need to be triumph over by using the studies network to take gain of the advantages of this key CRN generation without having to sacrifice the customers' privateness.

B. Khalfi, M. B. Ghorbel, B. Hamdaoui, and M. Guizani proposed a useful resource allocation scheme for a smart grid-enabled cognitive radio consumer. The clever grid allows the consumer to achieve actual time power pricing policy. This data is exploited by means of the user to decrease its power intake fee thru wise strength allocation. Analytic expressions of the allocated strength are advanced for exceptional value functions and low-fee algorithms are offered for the strength allocation. Simulation effects showed the gain that the cognitive device finished by way of cashing in on the dynamic electricity pricing thru the proposed strength allocation scheme.

M. Grissa, A. A. Yavuz, and B. Hamdaoui designed a region privacy maintaining scheme for CRNs that achieves high sensing accuracy. Their scheme has several key features, making it greater practical, at ease, and reliable for big-scale CRNs. When compared to current procedures, LPOS executed superior sensing performances with excessive region privateness while being sturdy against network dynamism.

3. FRAMEWORK

A. Overview of Proposed Framework

We keep in mind a normal cognitive radio network, which consists of a number primary user (PU) and a couple of secondary users (SUs). The PU has a few non-utilized spectrums to sell to SUs. In a cognitive radio transaction, PU publicizes the pricing policy for the non-utilized spectrum, normally a price feature depending on frequency, bandwidth, time, and many others. SU utilizes a few spectrum sources and pays PU consistent with the pricing coverage at the give up of a billing duration, which includes a day or a month.

In this paper, we recommend locationprivateness-preserving schemes for database-driven CRN s with exceptional overall performance and architectural blessings. The first scheme, location privacy in database-driven CRNs (LPDB), provides most suitable vicinity privateness to SU s inside DB's coverage region by way of leveraging set membership statistics systems (used to check whether an element is a member of a fixed) to construct a compact version of DB. The second scheme, LPDB with servers (LPDBQS), minimizes the overhead at SU's facet on the price of deploying an extra entity inside the community. The price overall performance tradeoff offers extra alternatives to gadget designers to decide which topology and which method is greater appropriate to their specific necessities. Both processes exploit two critical facts: (i) Spectrum databases are enormously dependent; and (ii) SU s queries comprise continually the identical device-specific traits.

B. System Model

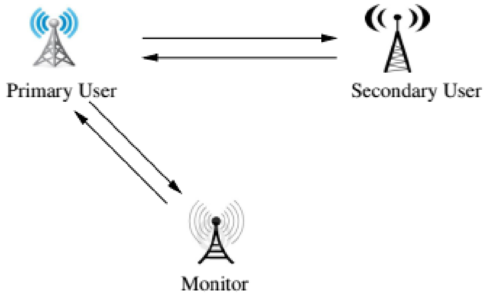


Fig2. Structure of the proposed system

The system model comprises 3 components, Primary User (PU), Secondary User (SU), and Monitor (M), as proven within the fig2. PU pronounces pricing coverage to SU that is within the shape of segments, with each phase representing the unit fee for a positive channel in a period of time. SU calculates a subfee for every utilization instance based on the pricing coverage if he utilizes a positive channel for a time frame. At the end of a billing period, SU sums up all of the subfees to reap a total rate and ship it to PU, collectively with the commitments of values in every usage instance. PU simplest obtains the data of the overall fee from SU, however it does no longer recognize while and the way lengthy SU has now not utilized a channel, nor does it recognize which channel SU has applied. In this manner, SU's privateness is preserved. To take a look at whether or not SU commits fraud, PU can ask for a few observations from the monitor M, and require SU to expose the corresponding commitments. If the observations and commitments are matched, then SU is considered sincere; in any other case, an excessive penalty could be imposed.

The first scheme, LPDB, is simple as it involves most effective two events, SU s and DB, and offers unconditional area privateness to SU s inside the insurance location of DB. The 2d scheme, LPDBQS, gives computational privateness with a extensively reduced overhead on SU s' aspect as compared to LPDB, however on the cost of introducing an additional architectural entity. Since we're not able to get right of entry to the actual spectrum database, we trusted two sources to have an estimate of this structure: First, we've relied on the advice of the PAWS (Protocol to Access WhiteSpace) fashionable, which defines the interaction among SU s and DB and what information they should trade. Second, we used graphical web interfaces supplied to the general public with the aid of white space database operators. These web interfaces comply with PAWS advice and permit an interested person to specify a region of interest and learn spectrum availability in that vicinity to emulate the interaction among a SU and DB in global.

C. Database-Driven CRN Model

We first take into account a CRN that consists of a set of SUs and a geo-location database (DB). SUs are assumed to be enabled with GPS and spectrum sensing talents, and to have get admission to DB to reap spectrum availability information inside its operation place. To study spectrum availability, a SU queries DB through consisting of its area and its device characteristics. DB responds with a listing of to be had channels at the specified place and a fixed of parameters for transmission over the ones channels. SU then selects and uses one of the returned channels. While the usage of the channel, SU wishes to recheck its availability on every day basis or whenever it modifications its region by using one hundred meters as mandated. We then look into incorporating a 3rd entity to the community along with DB and SUs. This entity, known as query server (QS), has a devoted high throughput hyperlink with DB. Query Server used to assure computational location privateness at the same time as reducing the computational and conversation overhead specifically on SUs' side.

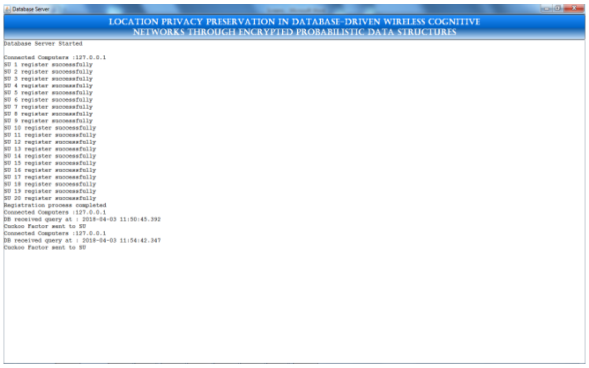
Finally, Making sure that the user location privacy information of SU s is protected has incredible advantages. First and most significantly, it promotes dynamic and opportunistic sharing of spectrum assets, thereby increasing spectrum usage performance. Knowing that their vicinity privacy is covered so that they do not must fear approximately their whereabouts being tracked and their privateness being compromised, SU s can be encouraged to participate in the cooperative spectrum sensing method, and to query spectrum databases for spectrum availability. Ensuring location privateness protection also can be beneficial to PU s. For instance, being involved that their region privacy records may be leaked to spectrum databases, SU s may attempt to use PU channels without registering and querying spectrum databases for spectrum availability, thereby inflicting dangerous interference to PU s.

4. EXPERIMENTAL RESULTS

In this experiment, we took DB server, Query server and two types of users such as PU and SU. Here, the secondary users (SU) must register into the DB server. The DB server can store registered details securely.

SU LPDB Query:

Here, the SU node will send a simple query to the server instead of its location, and then the server will sends all the spectrum locations in encrypted format by using cuckoo filters concept). Here it shows all the spectrum locations in cuckoos filter format and the nearest one will true and other are false.


Database Server
LOCATION PRIVACY PRESERVATION IN DATABASE-DRIVEN WIRELESS COGNITIVE
NETWORKS THROUGH ENCRYPTED PROBABILISTIC DATA STRUCTURES

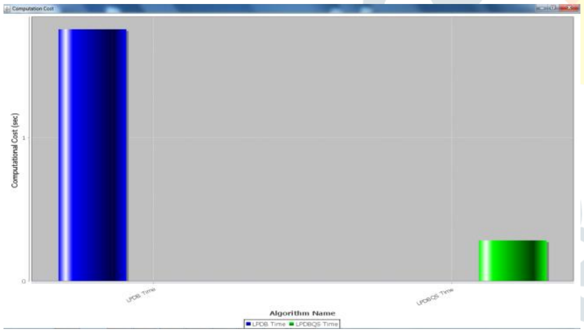
```
Database Server Started

Connected Computers :127.0.0.1
SU 1 register successfully
SU 2 register successfully
SU 3 register successfully
SU 4 register successfully
SU 5 register successfully
SU 6 register successfully
SU 7 register successfully
SU 8 register successfully
SU 9 register successfully
SU 10 register successfully
SU 11 register successfully
SU 12 register successfully
SU 13 register successfully
SU 14 register successfully
SU 15 register successfully
SU 16 register successfully
SU 17 register successfully
SU 18 register successfully
SU 19 register successfully
SU 20 register successfully
Registration process completed
Connected Computers :127.0.0.1
DB received query at : 2018-04-03 11:50:45.392
Cuckoo Factor sent to SU
Connected Computers :127.0.0.1
DB received query at : 2018-04-03 11:54:42.347
Cuckoo Factor sent to SU
```

SU LPDBQS:

Here it uses a query server to perform the required computations. With this the burden on to the SU will be removed.

Next we can observe the query server and DB server status.



Finally, we can view the cost computation graph for the proposed algorithms.

5. CONCLUSION

We conclude that in this paper we've proposed location privateness preserving schemes, known as LPDB and LPDBQS that goal to keep the region privacy of SU s in database-pushed CRN s. They each use set membership facts structures to transmit a compact representation of the geo-region database to both SU and QS, in order that SU can question it to check whether a selected channel is available in its location.

REFERENCES

[1] B. Khalfi, M. B. Ghorbel, B. Hamdaoui, and M. Guizani, "Optimal power allocation for smart-grid powered point-to-point cognitive radio system," in ComComAp, 2014 IEEE, pp. 316–320.

[2] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Lpos: Location privacy for optimal sensing in cognitive radio networks," in Global Communications Conference (GLOBECOM), 2015 IEEE.

[3] S. Liu, H. Zhu, R. Du, C. Chen, and X. Guan, "Location privacy preserving dynamic spectrum auction in cognitive radio network," in Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on. IEEE, 2013, pp. 256–265

[4] M. Grissa, B. Hamdaoui, and A. A. Yavuz, "Location privacy in cognitive radio networks: A survey," IEEE Communications Surveys & Tutorials, 2017.

[5] B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher, "Cuckoo filter: Practically better than bloom," in Proc. of the 10th ACM Int'l Conference on emerging Networking Experiments and Technologies, 2014, pp. 75–88

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

[7] W. Wang and Q. Zhang, Location Privacy Preservation in Cognitive Radio Networks. Springer, 2014.

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

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

[10] “Efficient location privacy for moving clients in database-driven dynamic spectrum access,” in 2015 24th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2015.

Biography:

Neha Nazmeen was born in telangana, India in the year 1996. She is pursuing her M.Tech in Computer Network and Infromation Technology from G.Narayanamma Institute of Technology and Science for women’s, Hyderabad, India. She had completed B.Tech Degree in 2017 in Laqshya Institute of Technology and Science, Khammam, India.

M.Sridevi currently working as Associate professor in Information Technology at G. Narayanamma Institute of Technology and Science. She has 10 Years of teaching experience. She has pursued B.Tech in MVSR College in 2006 and M.Tech from OSmania University in the Year of 2009.