International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 12th Nov 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-12

Title: DATA PRIVACY PRESERVATION AND LOCATION OF A ALTERNATE USER IN A WIRELESS COGNITIVE NETWORKS

Volume 07, Issue 12, Pages: 137–146.

Paper Authors

M.BHADRAJA, E.V.V.S.SIVAKUMAR , S.RAJESH

PB Siddhartha College of arts and science, vijayawada

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

DATA PRIVACY PRESERVATION AND LOCATION OF A ALTERNATE USER IN A WIRELESS COGNITIVE NETWORKS

[1]M.BHADRAJA, [2]E.V.V.S.SIVAKUMAR , [3]S.RAJESH

[1]Lecturer, Department of Computer Science, PB Siddhartha College of arts and science, Vijayawada.
[2]Lecturer, Department of Computer Science, PB Siddhartha College of arts and science, Vijayawada.
Lecturer, Department of Computer Science, PB Siddhartha College of arts and science, Vijayawada.

ABSTRACT: The extant system provides location privacy preserving schemes for cognitive radio networks (CRNs)that protect secondary users (SUs) location privacy while allowing them to preserve their own sensitive details. Itcontains harness probabilistic set membership data structures to exploit the structured nature of spectrum databases(DBs) and SUs queries. This enables us to create a compact representation of DB that could be queried by SUs withouthaving to share their location with DB, thus guaranteeing their location and data privacy. In our proposed work, thesystem allows user to register in the Network and allows them to upload any kind of sensitive detail through settingdown into it. The system provides security for the data of a secondary user (SU) in a cognitive network through AESencryption algorithm. If any of the intruder in network tries to steal user's details,they will use fake details for settingdown .In the mean time, server in the network is warned about cybercriminal entering and it tracks IP address, ISP andgeographical information of the Intruder and blocks Invader from entering within the network.

KEYWORDS: Privacy preservation, Wireless Cognitive Network, Advanced Encryption Standard(Algorithm),LPDBQS(Algorithm) ,Interloper attack

I.INTRODUCTION

A **wireless network** is a computer network that uses wireless data connections between network nodes. Wirelessnetworking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between variousequipment locations(Fig.1).

Wireless network classified as:

WirelessPAN(personal area network)
Wireless LAN(local area network)
Wireless ad hoc network
wireless MAN (metropolitan area networks)
Wireless WAN (wide area networks)
Cellular network
Global area
network Space
network

Fig.1.Wireless Network

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Wireless Cognitive Network(WCN):

Cognitive radio is an adaptive, intelligent radio and network technology that can automatically detectavailable nodes in a wireless spectrum and change transmission parameters enabling more communication to runconcurrently.Cognitive Radio Network (CRN) is regarded as a emerging technology to address the increasing demandfor node resources. It solves the node resource shortage problem by allowing a Secondary User (SU) to access thechannel of a Primary User (PU) when the channel is not occupied by the PU, in which an SU queries a database toobtain node availability information by submitting a location based query(Fig.2).

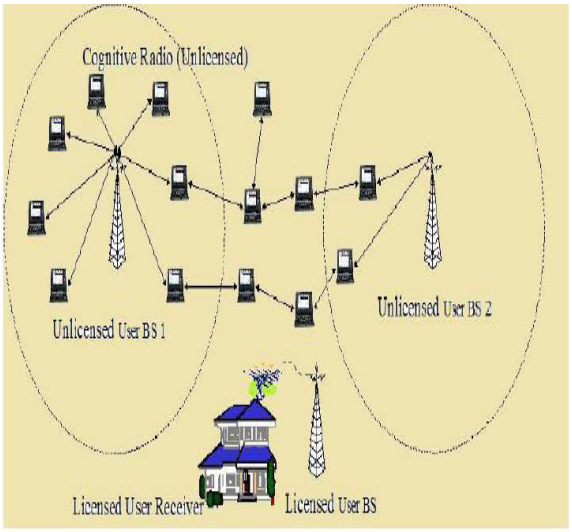


Fig.2.Wireless Cognition Network

Primary user(PU): They were the **licensed user** of the network and have the access for their account features.

Secondary user(SU): They were the **unlicensed user** of the network .Also known as Mobile users(on travel).

In CRNS, the SUs are allocated with primary user's node for accessing when they are at rest from network.In this case, the data of the SU were visible to PU. For this issue many researches were undertaken and found solutionsby introducing two party protocols ,filters such as cuckoo and bloom. Though the security is provided for SUs the intruder's in the network tries to hack the network and steals the data of the users. Security is a major factor thatreduces the performance in Wireless Cognitive Network(WCN).However, one concern about database-driven CRNs is that the queries sent by SUs will inevitably leak the location information. Instead of directly learning the SUs' locations from their queries, our discovered attacks can inferan SU's location through his used nodes. The location privacy preservation schemes for database driven cognitive radionetworks provides a optimal location privacy to secondary users within database coverage network by leveraging setmembership data structure to construct a compact version of database. Even though the location is preserved fromIntruder ,they tries to hack the sensitive details of SUs such as Business information, Personal information,Financial information etc,..This system allows the SUs to store the sensitive details and keep track from hackers.If any hacker tries tohack the network where the SUs work ,the server in the network tracks the Intruder and finds their IP addressISP,Gateway and geological information of the SUs like latitude and longitude value.Finally blocks the Hackers.

Disadvantages of extant system:

- The location privacy issue in database-driven CRNs.
- It introduces some noise to SU's location which may cause erroneous spectrum availability information.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

II.LITERATURE REVIEW

The authors Mohamed Grissa et al. ,in 2017 introduced a system that allows to preserve the location privacy ofSUs while performing reliable and efficient spectrum sensing using Cryptographic mechanisms[4].The researchers S.Selvakanmani et al., in 2017 presented a system that achieves a balance by minimizinginterference to licensed users and maximizing the entire system performance providing opportunistic access to numberof secondary users such as opportunistic spectrumsensing and adaptive channel assignment through mathematical analysis and MC-OSACA technique [9]..The expertsH. Zhu et al., in 2016 invented Jammer Inference based Jamming Defense (jDefender)Framework. The main idea of jDefender is inferring the likelihood of a user being a jammer based on the observed

jamming events and then utilizing the inferred attack likelihood to enhance the effectiveness of a series of proposedanti-jamming strategies[2].The researchers Mohamed Grissa ,et al., in 2015 proposed a system that provides an efficient scheme for databasedrivenCRNs that preserves the location privacy of SU through Cuckoo filter [1].The experts XuZhang,et al., in 2014 provided a comprehensive analysis and guide of existing efforts aroundlocalization and location privacy preservation in cognitive radio network.The cognoscenti Z. Gao,et al., in 2013 designed Private Spectrum Availability Information Retrieval scheme thatutilizes a blind factor to hide the location of the SU and proposed a novel prediction based Private Channel Utilization protocol that reduces the possibilities of location privacy leaking by choosing the most stable channels[11].Despite its importance, the location privacy issue in CRNs only recently gained interest from the researchcommunity[4]. Some works focused on addressing this issue in the context of collaborative spectrum sensing [5]–[8],[14]-[15]. Protecting SU s' location privacy in database-driven CRNs is a very challenging task, since SU s arerequired to provide their physical locations to DB in order for them to be able to learn about spectrum opportunities intheir vicinities[1].However, direct adaptation of such concepts yield either insecure or extremely costly results. Forinstance, k-anonymity guarantees that SU 's location is indistinguishable among a set of k points, which could beachieved through the use of dummy locations by generating k properly selected dummy points, and performing k

location privacy and maximizing some utility, which makes it suffer from the fact that achieving a high locationprivacy level results in a decrease in spectrum utility. PIR, on the other hand, allows a client to obtain information froma database while preventing the database from learning which data is being retrieved. Several approaches have used thisapproach[11] proposed a PIR-based approach.

III.PROPOSED SYSTEM

A.System model:

The Cognitive radio network that consists of a set of Secondary users stores geo-location information onthe database(DB). SUs are assumed to be enabled with GPS and node sensing capabilities, and to have access to DB toobtain node availability information

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

within its operation locale.The main issue faced by the SUs in CRNs is the state ofbeing free and cybercriminal attacks.The proposed system solves this issues by storing the details of along withlocation in the database using Encryption algorithms. When the Intruder tries use the SUs details, the presented systemimmediately notices the IP address,ISP of the Intruder,Gateway and geological informations such as latitude andlongitude values.When the server in the CRN knews about the attack as soon as he blocks them.So that the Intruderwon't be able to get into that network through that system.

B.System Design:

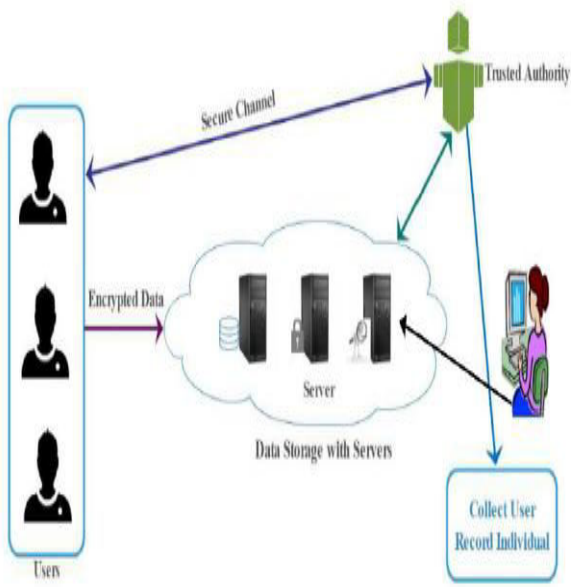


Fig:3 .Overview of extant system

This fig:1. Describes how the authority member provides channels for the SUs and they were usingthe network by querying the network.The authority member stores the information of the user in a separate databasethat is visually hidden from the user but abstracted.And also it shows how the Intruder tries to hack the network details.

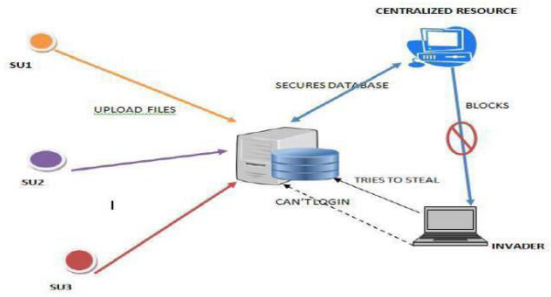


Fig.4: Proposed System

C.Detailed Description:

· Network ID Creation and Uploading data.·

· Examine the Intruder and their IP,ISP and Geographical information.·

· Blocking of User·

Network ID creation and Uploading Data

In this , the users in the network registers their own details like user name and password for Network IDregistration .This registration will track up location of the secondary user and automatically acquires geo-graphicalinformations such as latitude and longitude values and send those back to the Centralized resource.The server of the network allows users to upload file and stores their details in a database. While uploading dataof the user in network , the system generates a key for file using Encryption algorithms. If user wants those details fortheir use, they will be allowed to download files from web at anytime using the key .

Examine the intruder and their ip,isp and geographical information

If hacker tries to access the network illegally, then they will uses fake user name

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

and password to getin thenetwork.It will show incorrect user name details. In the mean time, the server is warned about maliciousentering inside the network.Then they check details of the interloper.Once they get the details of invader, thecentralized person tracks details of invader such as Internet Protocol address,Internet serviceprovider's,Gateway and Geo-graphical information such as latitude and longitude. By referring geographicalinformations, the server gets their location and also able to view the invader's Location through maps.

Blocking Of User

In this part of the proposed system, When centralized person realized about malicious activity innetwork by invader, they identifies the geo-location and network providers of them. Immediately they will blockinvader system's IP address from network ,so that this people will not be able to setin to the network using theirsystem in anyway.

D.Algorithm Used:

1. LPDBQS(Location Privacy DataBase Query Server)

1:SU queries DB with query f(k; char; ts);
2: DB retrieves resp containing r entries satisfying char;

3: DB constructs CFk;
4: for j = 1; : : : ; r do
5: if avl j = 1 then
6: x j (locX jklocY jktsk : : : krowj(c));
7: CFk:InsertHMACk (x j);
8: DB sends CFk to QS over a high throughput link;
9: SU initializes decision Channel is busy
10: for all possible combinations of par do

11: SU computes y (locX klocY kchnktsk : : : kparn);
12: SU computes yk HMACk(y) and sends it to QS;
13: QS looks up for yk in CFk using Lookup;
14: if CFk:Lookup(yk) then
15: SU senses chn;
16: if Sensing(chn) available then

17: decision chn is available; break return decisionLPDBQS does not leak any information about SU s' location beyond HMAC secure values. LPDBQS, which offersbetter performance at SU s' side than that of existing system algorithm. Here the proposed offers better performance atSU s' side than that of LPDB in extant system.This comes at the cost of deploying an additional entity, referred to asquery server (QS), and having a computational security as opposed to unconditional. QS is introduced to handle SU s'queries instead of DB itself, which prevents DB from learning information related to SU s' location information. QS learns nothing but secure messages sent by SUs to check the availability of a specific channel.

STEPS IN LPDBQS:

STEP 1

SU queries the databse about the availability nodes. The database contents is retrieved as a collection ofCF(only the entries that have available channels) by sending a secret key k.

STEP 2

DB sends CFk to QS over a high throughput link

STEP 3

SU read about the channel engaging and tries to adapt the idle channel.

STEP 4

SU hashes y with the secret key k and sends the new value yk to QS to find out whether CFk of QS contains yk

STEP 5

It senses the channel that was included in the query. If the result of the sensing complies with the outcomeof the Lookup operation in CFk, then SU can conclude that this channel is available

STEP 6

DB can pre-compute several cuckoo filters for each possible combination of secret keys k .

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

STEP 7

For spectrum oppurtunities the DB shares a secret key k with SU and sends the corresponding CFk toQS,also gets Channel.

2. AES:

AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm wasdeveloped by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in bothhardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits

DESCRYPTION:

1. KeyExpansions· round keys are derived from the cipher key using Rijndael's key schedule. AES requires aseparate 128-bit round key block for each round plus one more.

2. InitialRound

a. AddRoundKey· each byte of the state is combined with a block of the round key using bitwisexor.

3. Rounds

a. SubBytes· a non-linear substitution step where each byte is replaced with anotheraccording to a lookup table.

b. ShiftRows· a transposition step where the last three rows of the state are shifted cyclically a certainnumber of steps.

c. MixColumns· a mixing operation which operates on the columns of the state, combining the fourbytes in each column.

d. AddRoundKey

4. Final Round (no MixColumns)

a. SubBytes

STEPS IN ADVANCED ENCRYPTION STANDARD:

STEP 1

Derive the set of round keys from the cipher key

STEP 2

Initialize the state array with the block data

STEP 3

Add the initial round key to the starting state array

STEP 4

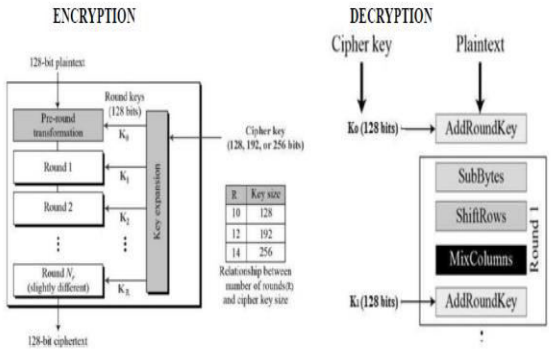
Perform nine rouinds of state manipulation

STEP 5

Perform the tenth and final round of state manipulation

STEP 6

Copy the final state array out as the encrypted data



V.RESULTS

Performance Evaluation Results

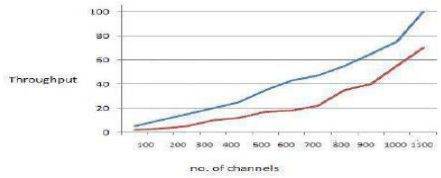


Fig.6.Briefs about performance

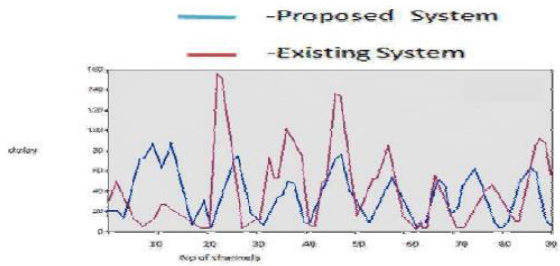


Fig.7.Delay graph

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

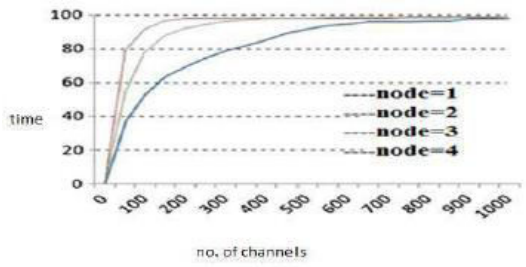


Fig.8. Node Utilisation

Fig.9. describes about registration for user in network using necessary details like name and password.

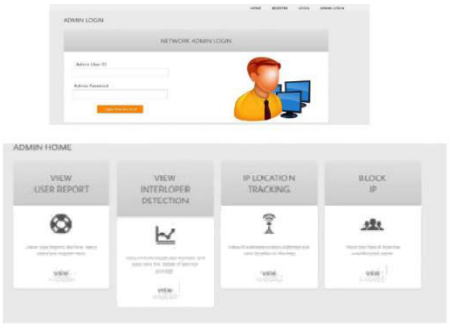


Fig.10. briefs how the server setin to network and tracks about user entering details and invader's fake details.

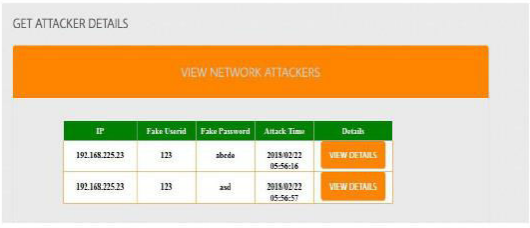


Fig.11. shows invader's fake details.

Fig.12. shows invader's network details.

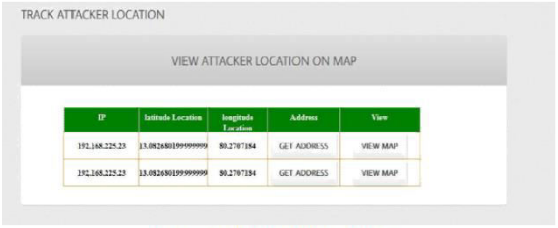


Fig.13. shows geographical info. of invader.

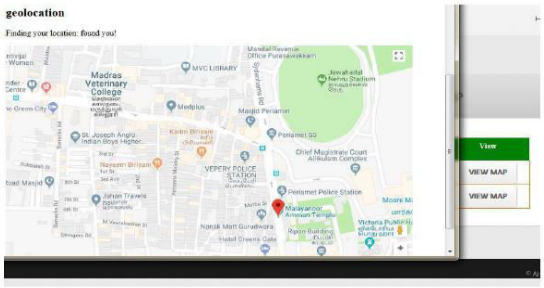


Fig.14. provides a view of exact location of invader.

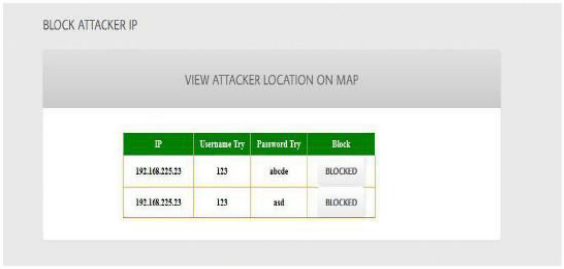


Fig.15. provides a status of invader blocking

TOOLS DESCRIPTION:

Front End	- HTML, J2EE
Server side Script	- Java Server Pages.
Database	- My sql

Database Connectivity - JDBC.

Java:

Java technology is both a programming language and a platform.

The Java Programming Language

The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple·
- Architecture neutral·
- Object oriented·
- Portable·
- Distributed·

- High performance
- Interpreted
- Multithreaded
- Robust
- Dynamic
- Secure

Java is developed by Sun Microsystems, later acquired by Oracle Corporation, that provides a system fordeveloping application software and deploying it in a cross-platform computing environment. Java is used in a widevariety of computing platforms from embedded devices and mobile phones to enterprise servers and supercomputers.While less common, Java applets run in secure, sand boxed environments to provide many features of nativeapplications and can be embedded in HTML pages.Writing in the Java programming language is the primary way to produce code that will be deployed as byte code in aJava Virtual Machine (JVM); byte code compilers are also available for other languages, including Ada, JavaScript,Python, and Ruby. In addition, several languages have been designed to run natively on the JVM, including Scala,Clojure and Groovy. Java syntax borrows heavily from C and C++, but object-oriented features are modeled after Smalltalk and Objective-C.[11] Java eschews certain low-level constructs such as pointers and has a very simplememory model where every object is allocated on the heap and all variables of object types are references. Memorymanagement is handled through integrated automatic garbage collection performed by the JVM.

Back End:

MySQL, the most popular Open Source SQL database management system, is developed, distributed, andsupported by Oracle Corporation.The MySQL Web site (http://www.mysql.com/) provides the latest information aboutMySQL software.

MySQL is a database management system:

A database is a structured collection of data. It may be anything from a simple shopping list to a picturegallery or the vast amounts of information in a corporate network. To add, access, and process data stored in acomputer database, we need a database management system such as MySQL Server. Since computers are very good athandling large amounts of data, database management systems play a central role in computing, as standalone utilities,or as parts of other applications.

MySQL databases are relational:

A relational database stores data in separate tables rather than putting all the data in one big storeroom. Thedatabase structures are organized into physical files optimized for speed. The logical model, with objects such as databases, tables, views, rows, and columns, offers a flexible programming environment.The SQL part of “MySQL” stands for “Structured Query Language”. SQL is the most common standardized language used to access databases. Depending on your programming environment, you might enter SQL directly (forexample, to generate reports), embed SQL statements into code written in another language, or use a language-specificAPI that hides the SQL syntax.SQL is defined by the ANSI/ISO SQL Standard. The SQL standard

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

has been evolving since 1986 and severalversions exist. "SQL-92" refers to the standard released in 1992, "SQL:1999" refers to the standard released in 1999,and "SQL:2003" refers to the current version of the standard. We use the phrase "the SQL standard" to mean thecurrent version of the SQL Standard at any time.

MySQL software is Open Source:

The MySQL software uses the GPL (GNU General Public License), http://www.fsf.org/licenses/, to definewhat you may and may not do with the software in different situations. If you feel uncomfortable with the GPL or needto embed MySQL code into a commercial application, you can buy a commercially licensed version from us. See theMySQL Licensing Overview for more information (http://www.mysql.com/company/legal/licensing/).

MySQL Server works in client/server or embedded systems:

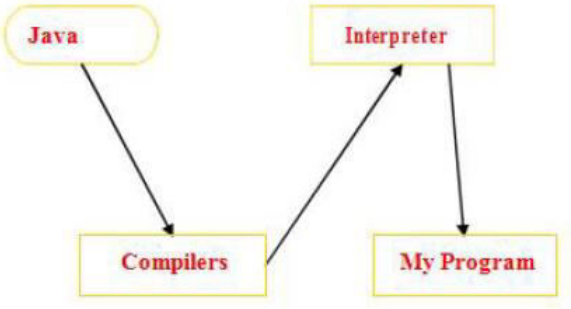
The MySQL Database Software is a client/server system that consists of a multi-threaded SQL server thatsupports different backends, several different client programs and libraries, administrative tools, and a wide range ofapplication programming interfaces (APIs).

A large amount of contributed MySQL software is available:

MySQL Server has a practical set of features developed in close cooperation with our users. It is very likelythat your favorite application or language supports the MySQL Database Server.

JDBC

In an effort to set an independent database standard API for Java; Sun Microsystems developed JavaDatabase Connectivity, or JDBC. JDBC offers a generic SQL database access mechanism that provides a consistent interface to a variety of RDBMSs. This consistent interface is achieved through the use of "plug-in" databaseconnectivity modules, or drivers. If a database vendor wishes to have JDBC support, he or she must provide the driverfor each platform that the database and Java run on.To gain a wider acceptance of JDBC, Sun based JDBC's framework on ODBC. As you discovered earlierin this chapter, ODBC has widespread support on a variety of platforms. Basing JDBC on ODBC will allow vendorsto bring JDBC drivers to market much faster than developing a completely new connectivity solution.JDBC was announced in March of 1996. It was released for a 90 day public review that ended June 8,1996. Because of user input, the final JDBC v1.0 specification was released soon after.The remainder of this section will cover enough information about JDBC for you to know what it is about and how touse it effectively. This is by no means a complete overview of JDBC. That would fill an entire book.



V. CONCLUSION

The system achieves the location and data privacy preservation of secondary user in wireless cognitivenetworks. It also stores the

data and geo-location of secondary user's information. Even if one of the coordinates isintentionally revealed by a SU, its location is still indistinguishable from remaining possible locations. This entity,referred to as query server (QS), has a dedicated high throughput link with DB. QS is used to guarantee computationallocation privacy while reducing the computational and communication overhead especially on SU s' side.

REFERENCES

[1]. M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Cuckoo filter-based location-privacy preservation in database-driven cognitive radio networks," inWSCNIS. IEEE, 2015, pp. 1–7.

[2]. H. Zhu, C. Fang, Y. Liu, C. Chen, M. Li, and X. S. Shen, "You can jam but you cannot hide: Defending against jamming attacks forgeolocation database driven spectrum sharing," IEEE Journal on Selected Areas in Communications, vol. 34, no. 10, pp. 2723–2737, 2016.

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

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

[5]. 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. IEEE, 2012, pp. 729–737.

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

[7]M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Preserving the location privacy of secondary users in cooperative spectrum sensing," IEEETransactions on Information Forensics and Security, vol. 12, no. 2, pp.418–431, 2017.

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

[9]. S Selvakanmani, M Sumathi ,"Multi-Channel Opportunistic Spectrum Analytics and Adaptive Channel Assignment in Cognitive RadioNetworks" 2017Asian Journal of Information Technology,vol.16,issue.2,pp.2348-363

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

[11] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks:Attacks and countermeasures," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2751–2759.

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