A STUDY ON PRIVACY-PRESERVING LOCATION PROOF FOR SECURING LARGE-SCALE DATABASE –DRIVEN COGNITIVE RADIO NETWORKS

C.Theebendra[1], Dr.T.Ramaprabha[2]

Research Scholar, PG & Research Department of Computer Science and Applications[1]

Vivekanandha College of Arts and Sciences for women (Autonomous), Namakkal, Tamilnadu, India

Professor, PG & Research Department of Computer Science and Applications[2]

Vivekanandha College of Arts and Sciences for women (Autonomous), Namakkal, Tamilnadu, India

theebendra@gmail.com[1], ramaradha1971@gmail.com[2]

***Abstract*—The latest FCC ruling has enforced database-driven cognitive radio networks (CRNs), in which all secondary users (SUs) can query a database to obtain Spectrum Availability Information (SAI). Database-driven CRNs are regarded as a promising approach for dynamic and highly efficient spectrum management paradigm for large-scale Internet of the Things (IoTs). However, as a typical location-based service (LBS), before providing services to the user, there is no verification of the queried location, which is very vulnerable to Location Spoofing Attack. A malicious user can report a fake location to the database and access the channels that may not be available for its location. This will introduce serious interference to the PUs. In this study, we identify a new kind of attack coined as location cheating attack, which allows an attacker to spoof other users to another location and make them query the database with wrong location, or allows a malicious user to forge location arbitrarily and query the database for services. To thwart this attack, we propose a novel infrastructure-based approach that relies on the existing Wi-Fi or Cellular network Access Points (or AP) to provide privacy-preserving location proof. With the proposed solution, the database can verify the locations without knowing the user's accurate location. We perform comprehensive experiments to evaluate the performance of the proposed approach. Experimental results show that our approach, besides providing location proofs effectively, can significantly improve the user's location privacy.**

***Keywords*—Location cheating attack, location proof verification, database-driven CRNs.**

I. INTRODUCTION

The rapid advancement of the emerging wireless technology and the ubiquitous computing applications has significantly increased the demand for the communication media resource, wireless spectrum. According to the conventional static spectrum allocation paradigm, most of the spectrum resources have been assigned to the existing primary users (e.g. such as Military communications and broadcast TV). To address the ever increasing demand for spectrum resources and allow more and more Internet-of-things applications, cognitive radio networks (CRNs) have been proposed to improve the efficiency of spectrum utilization. In CRNs, primary users (PUs) are licensed users who have exclusive privilege to access the licensed channels that have been pre-assigned whenever they need. Secondary users (SUs) are unlicensed users who are only allowed to opportunistically access the channels when
the channels are not occupied by the PU.

Database-driven CRNs are regarded as a promising ap- proach to allow the dynamic spectrum sharing in many large- scale IoT applications. In database-driven CRNs, all SUs can query a database to obtain Spectrum Availability Information (SAI). Instead of spectrum sensing, SUs are required to submit a request containing its current location information to the database. Until now, FCC has designed several entities as TV band database administrator. Though database-driven CRNs are considered as a promising approach to improve the efficiency of spectrum utilization, they face serious security challenges. Most of the existing research focus on the location privacy issue. But as a variant of location-based service (LBS), we focus on another security challenge that the user may cheat about its location when querying the database for services. Since there is no location verification for database-driven CRNs, the user can report a fake location information to the database and access the channels that are not available for its location, which can cause serious interference to the PUs. For instance, the United States has announced the spectrum sharing between federal government including military and non-government systems in 3.5GHz band, which is used by the U.S. Department of Defense (DoD) for critical radar systems. Therefore, location spoofing attack will lead to the unauthorized spectrum access of SUs and thus introduce serious interferences to the PUs, which are not acceptable for CRNs. Therefore, location verification in database-driven CRNs is highly desirable.

On the other hand, privacy issue is another important issue in CRNs. As pointed out by the existing researches, the attacker can geo-localize the SUs by tracking the users' spectrum query or spectrum utilization history. The existing researches pointed

out that, in an anonym zed trace data set, four spatiotemporal points are sufficient to uniquely identify the individuals and little outside or social network information is needed to re-identify a targeted individual or even discover real identities of users. Further, loss of location privacy can expose users to unwanted advertisement and location-based spam's, cause social reputation or economic damage, and make them victims of blackmail or even physical violence.

In this study, we study the problem of location proof in Database driven CRNs without leaking the users' accurate lo- cation information. A straightforward solution against location spoofing attack is to enforce the users to provide location proof while querying for services. A location proof is a piece of electronic data that certifies someone's presence at a certain location for some duration.

As Wi-Fi APs become increasingly prevalent, using Wi-Fi AP for location proof will be fairly effective, especially in urban areas. Different from the previous researches, we propose a novel hybrid infrastructure-based approach that relies on the existing Wi-Fi AP networks or the cellular networks to provide secure and privacy-preserving location proof. In the case of presence of Wi-Fi APs, the users can prove their locations under the help of Wi-Fi APs. However, in the case of unavailable Wi-Fi APs nearby, the users can turn to the cellular tower to request location proof, since the latter can provide a much larger coverage. To protect their location, we adopt the private proximity testing technology to allow the users to query the database for service without leaking their accurate location. Further, we discuss how to achieve the tradeoff of the user privacy and localization accuracy via various system settings.

The contributions of this paper are summarized as below:

- We identify a new kind of attack coined as location cheating attack in database-driven CRNs, which allows an attacker to mislead a user with a fake location and make them query the database with fake locations, or allows malicious user to claim a location arbitrarily and query the database for service.
- We propose a novel infrastructure-based approach that re- lies on the existing Wi-Fi AP network or cellular network to provide guarantees for location cheating prevention and location privacy for the users. The users can choose the location privacy level as he needs, and, enable the user to prove his location without leaking his accurate location. We also discuss how to find the user's optimal choice to maximize the location privacy while ensuring the service quality.

  We perform the comprehensive experiments to evaluate the performance of the proposed approach. Our experi- mental results show that our approach, besides providing location proofs effectively, can significantly improve the user's location privacy and also demonstrate the effec- tiveness of the optimal strategy.

II. BACKGROUND AND ATTACK MODEL

A. Overview of Database-Driven CRNs Service

The Database-driven CRNs are normally comprised of three components: a set of primary users (PUs), s set of secondary users (SUs), and the database. The Spectrum Availability In- formation (SAI) is calculated and stored in the database based on the knowledge of status of PUs and terrain parameters. In order to obtain the SAI before starting to access the channels, the SUs should query the database. The database queryprocess has three phases:

- **Query Phase**: An SU sends a query that contains his current location obtained from his built-in GPS location readings to the database for services. Note that, an SUcan query the database for SAI of multiple locations around, i.e., in the vicinity of his current location.
- **Response Phase**: The database calculates the SAI that contains available channels and corresponding maximum transmission power (MTP) for the SU's locations and sends it back to the SU.
- **Notify Phase**: After receiving the SAI from the database, the SU chooses an available channel from the SAI and registers the chosen channel in database. Note that, the notification message is optional. However, the notification phase is important based on the fact that the database can leverage the notification message to manage the system more efficiently.

B. Location Cheating Attacks in Database-driven CRN

As mentioned above, an SU receives the SAI from the database by sending a query containing its current location. Since this happens completely on the SU side, it is relatively easy to launch the attack. In what follows, we define the attack in two cases as summarized below and present more details about the possible damage.

1) ***Active Location Cheating Attack****:* A malicious SU can simply launch an active location cheating attack by reporting a fake location to the database accordance with his own wish. His goal is to obtain the SAI for the reported fake location to gain more advantages.

From the system implementation point of view, there are several ways for a malicious SU to forge a location and make the device believe that it is really in the fake location. In a Location Faker is developed as a system device to conduct a fake location arbitrarily which can be accepted as a real location by Android device. Figure 1 shows the concept of such location cheating. Thus, a malicious SU can implement this kind of component to forge a location as they wish, and then report it to the database to obtain the SAI for the fake location.

In database-driven CRNs, a mobile SU prefers to choosing a channel with better quality and stable available time to achieve larger communication throughput when it is moving.

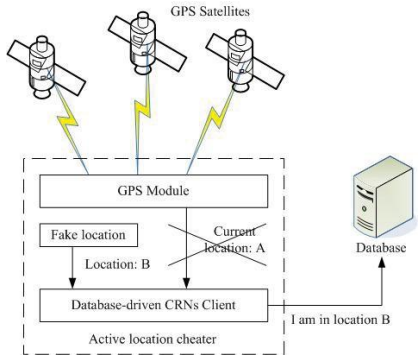


Fig. 1. Illustration of active location cheating. Location Faker generates location B and makes the device believe it is really in location B.

According to FCC ruling, the system allows an SU to load SAI for multiple locations around, i.e., in the vicinity of its current location and use such information to obtain one or multiple available channels within that area]. If the location is a little far away from his current location and also on its moving route, malicious SU can obviously launch an active location cheating attack to occupy the channels with better quality in advance and gain more benefits. For example, he obtains the SAI for location *B* while actually is located at location *A* (see **Fig.1**). Then, he chooses a channel with better quality and sends a notification message to the database, thus making the database believe that he is accessing this channel while he is actually not. If the attacker chooses several channels, this introduces Denial of service (DoS) to other SUs in location *B*, and also causes loss of the quality of service.

1) Passive Location Cheating Attack: The attacker is another malicious attacker that is located in the same cell with the victim who is launching a query towards the database for SAI. The attacker's goal is to mislead the victim that he is located in a wrong location and obtain the wrong SAI, which will introduce the interference to the PU.

As pointed out in [12], an attacker can use GPS spoofing device (like a GPS signal simulator) to generate and broadcast fake GPS signals synchronized with the real GPS signals to the target receiver. Then, the fake GPS signals gradually overpower the real GPS signals and replace it. Finally, the target receive locks on the fake GPS signals. After replacing the real GPS, the attacker can fool the target receivers to an arbitrary location. If all victims receive the fake signals from the same attacker, they are all spoofed to the same location L' as shown in **Fig.2**. Thus, a malicious SU can launch such an attack to spoof SUs that are located in the same cell and make them query the database for services by reporting the spoofed location.

Then, the attacker can occupy the available channel with better quality for location *L* as his exclusive channel to achieve better transmission throughput. The SUs who query the database for services with spoofed location L' may also cause interference to the primary users, since they access the channels that may not be available for location *L*.

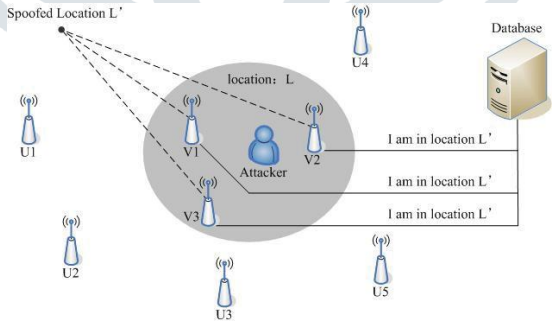


Fig. 2. Illustration of passive location cheating. All victims in location L that query the database for services are spoofed to location L'.

III. SYSTEM ARCHITECTURE

To prevent SUs from cheating their reported locations, we propose a novel infrastructure-based approach which is based on an infrastructure of Wi-Fi APs or cellular towers to provide secure and privacy location proofs, such that the database can verify the reported location before providing spectrum services. In this section, we describe the different entities involved in our system: SUs, a Wi-Fi AP network operator or a cellular network, and the database that contains SAI provider database, location

proof server, and certificate authority (CA). Figure 3 depicts the overview of the system we consider.

A. The Users

We assume that some users are going to obtain the Spectrum Availability Information (SAI) from the database when they are moving. According to the latest ITEF paws-protocol, a user is allowed to query the database for the SAI by submitting a region that contains his location [1]. To protect the location privacy, we assume that the location submitted to the database by the users specifies a region. These users are equipped with GPS, Wi-Fi, and Cellular-enabled devices, and are capable of connecting to the Internet through WiFi or Cellular networks . We also assume a unit-disc model for Wi-Fi APs and cellular towers, that means a user can communicate with a Wi-Fi AP or a cellular tower only if the distance between them is lower than a given radius *R*, which is equal for all users, Wi-Fi APs and cellular towers. Before querying the database for services, the user should obtain the location proof from a Wi-Fi AP or a cellular tower firstly.

To protect the user's privacy, the users will register to the *Certification Authority* (CA) with some randomly generated pseudonyms and they can use such pseudonyms to protect their privacy while gaining location proof. A pseudonym contains a public/private key pair (K_{pri}, K_{pub}), generated with a public- key encryption scheme. The public key K_{pub} serves as the pseudonym of the user, while the private key K_{pri} enables the user to digitally sign the message. We assume that users do not give their pseudonyms to other users, and the pseudonyms also should not be easily spoofed and cloned. While registering, we also assume that the CA can generate some other public/private key pairs ($P\ K_{pri}$, $P\ K_{pub}$), in which $P\ K_{pub}$ is given to the user and $P\ K_{pri}$ is kept by the CA.

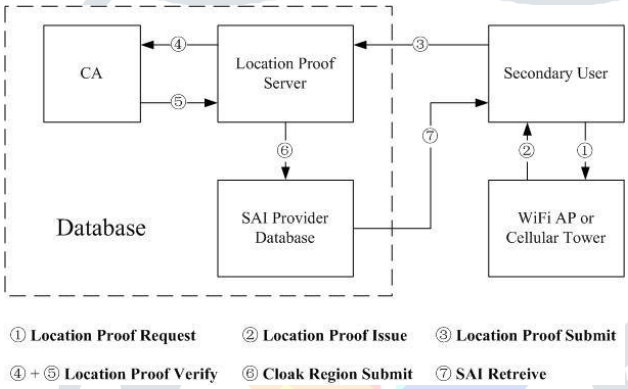


Fig. 3. Overview of the system. First, the user obtains location proof from the nearby WiFi AP or cellular tower, then submits it to the location proof server. Second, CA verifies whether the location proof is legitimate. Only if the verification is pass, then SAI provider database provides the SAI to the user.

A. Wi-Fi AP network and Cellular network

We assume that there are one or multiple Wi-Fi AP networks or cellular networks and each network contains a set of fixed Wi-Fi APs or cellular towers deployed in the area. Each Wi-Fi AP or cellular tower knows its geographic position and its transmission range and can embed its location information into the location proof. All Wi-Fi APs or cellular towers have synchronized clocks within a few hundreds of milliseconds (this can be achieved by using the NTP [3]). Each Wi-Fi AP or cellular tower from the same network shares a public-key group key pairs (ttK_{pub}, ttK_{pri}), in which ttK_{pub} is known to the users and the database, whereas ttK_{pri} is only known to the Wi-Fi APs or the cellular towers.

We assume that the Wi-Fi AP network and cellular network are honest but curious, which means that they will obey the rules that we proposed and also may be interest in tracking the users' locations based on the collected information. We also assume that the Wi-Fi AP network and cellular network do not collude with the database.

B. Database

To prevent users from cheating about their location, we need to add the location verification functionality in the database's side, thus in our system we make a little change to the database and divide it into three parts: *Location Proof Server*, *Certification Authority (CA)* and *SAI Provider Database*.

1) Location Proof Server: Location proof Server directly communicate with the users who submit their location proofs. The goal of the *Location proof Server* is to collect location proofs. As the identities of the location proofs are stored as pseudonyms, even though the *Location proof Server* is compromised by the attacker, it is impossible for the attacker to know the real identity of the location proof.

2) *CA:* As commonly assumed in many networks, we con- sider an online CA run by a trusted party. CA is the only party who knows the mapping between real identity and pseudonym. CA also knows the secret key $P\ K_{pri}$ corresponding to the user, since the location proof is encrypted with $P\ K_{pub}$, thus it can use $P\ K_{pri}$ to verify the location proof. We assume the CA is trusted and does not collude with the WiFi AP network.

3) SAI Provider Database: The *SAI Provider Database* is more similar to the traditional database described in the previous database-driven CRNs system. After the verification of location proof is pass, the *Location Proof Server* will submit the region in spectrum request to the *SAI Provider Database*. Then, the *SAI Provider Database* will calculate the SAI for the region and send it back to the user.

IV. THE PROPOSED PRIVACY PRESERVING LOCATION VERIFICATION SCHEME

In this section, we present our approach for privacy- preserving location verification (PPLV) scheme. First, we give an overview of the proposed approach and define the main processes it involves. Subsequently, we present the detailed work flow. Finally, we analysis the security and privacy. **Fig.3** shows an overview of the approach and main processes involved.

A. Overview of PPLV

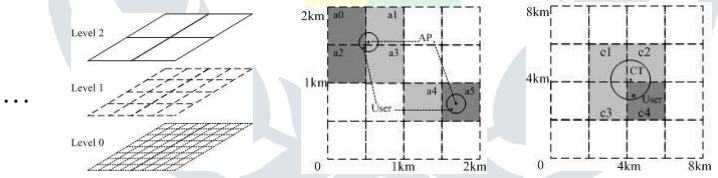
As Wi-Fi APs become increasingly prevalent and can provide more accurate location proof, in our scheme, the users prefer to requesting location proof with Wi-Fi AP; while there are no Wi-Fi APs nearby, then the users choose the nearby cellular tower to request for location proof. To protect the location privacy, we adopt a grid reference system with different levels to represent locations, and users can choose appropriate level to query for location proof.

In the case of cellular tower, since the cellular tower can provide a larger coverage, the user does not need to specify the region. He specifies a granularity of level to protect his location privacy, and requests location proof with the cellular tower. Then the cellular tower embeds its coverage to the location proof and sends back to the user. Then the user can query the database for services by submitting the location proof containing the cellular tower's coverage. Finally, the database calculates the SAI for the coverage and sends back to the user.

In the case of Wi-Fi AP, since the Wi-Fi AP's coverage is much smaller than the cell size, the user not only specifies the granularity of level, but also specifies the region. To further protect the location privacy (i.e. enable the user to prove his location without leaking the accurate cell to the database), we adopt private equality testing to determine if two cells match without revealing the exact cell number. The basic idea is that if the user is located at cell a and Wi-Fi AP is located at cell b, CA learns if $a = b$ and nothing else.

B. System Initialization

Global setup: The location of a user can be defined with different granularities. The user may want to define their location in appropriate granularity under different situations. For example, the user may be willing to use fine-grained location information in urban area while using coarse-gained location information in countryside. As show in Figure 4(a), the system adopts a grid reference [9] to represent locations, where grid indices represent areas covered by grid cells. All users, all Wi-Fi APs, all cellular towers and the *SAI provider Database* share a list of coordinate-axis aligned grid system denoted by $\Gamma(l)(l = 0, 1, 2,)$ of different levels. For each level l, the grid cell size, i.e. width and height, is fixed and equal. The grid cell size at level 0 is equal to $250m$, and the size at level $l - 1$ is always lower than that at level l. Every grid cell $c \in \Gamma(l)$ is identifiable by an index $id(c) \in$ N and is fully contained by several grid cells $c \in \Gamma(l - 1)$.



(a) Grid system (b) WiFi AP (c) Cellular Tower

Fig. 4. Grid reference system. We assume the grid cell with side length of 250 meters for level 0, the unit-disc communication model with a radius of 25 meters for WiFi APs and of 2 kilometers for cellular towers.

Here, P_{user} denotes the user's pseudonym; n denotes the beacon's sequence number or preamble's random number; l denotes the granularity of level. t denotes the request time. R_{user} is a set of cell ids that denote the region that the user queries for. $C_{loc}user$ encrypted with the public key $P K_{pub}$ contains the user's location information.

V. CONCLUSION

The proposed system identify a new kind of attack coined as location cheating attack in database-driven CRNs, in which users can cheat their locations to gain more advantages, and this can cause interference to PUs. To thwart this attack, we propose a novel infrastructure-based approach that relies on the existing Wi-Fi AP network or cellular network to provide secure and privacy location proof. On the one hand, we use a grid reference system with different granularities to represent locations, on the other hand, we adopt the private proximity testing technology to further improve the user's location privacy. We conduct the program to find the optimal strategy to maximum the user's location privacy. Simulations well demonstrate the effectiveness and efficiency of the pro- posed approach. Experiments by using the SAI of Atlanta in white space database release on TV Fool show the tradeoff between location privacy and service quality and demonstrate the effectiveness of the optimal strategy. Our future work includes other security issues in database-driven CRNs.

REFERENCES

[1] Chen V, Das S, Zhu L, et al. *Protocol to Access White-Space* (*PAWS*) *Databases*. draft-ietf-paws-protocol-10 (work in progress), 2014.

[2] Band, Broadcast. "FEDERAL COMMUNICATIONS COMMISSION 47 CFR Part 15."

[3] Mills D, Martin J, Burbank J, et al. *Network time protocol version 4*: *Protocol and algorithms specification*. IETF RFC5905, June, 2010.

[4] Narayanan, Arvind, et al. "Location Privacy via Private Proximity Test- ing." *NDSS*. 2011.

[5] Zhang L, Fang C, Li Y, et al. "Optimal Strategies for Defending Location Inference Attack in Database-driven CRNs," *International Conference on Communications(ICC), 2015 IEEE Conference on*. IEEE, 2015.

[6] Capkun, Srdjan, Levente Buttyan, and Jean-Pierre Hubaux. "SECTOR: secure tracking of node encounters in multi-hop wireless networks." *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*. ACM, 2003.

[7] "TV Fool," March, 2012. [Online]. Available: http://www.tvfool.com/

[8] Zhu, Zhichao, and Guohong Cao. "Applaus: A privacy-preserving location proof updating system for location-based services." *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011.

[9] Zheng, Yao, et al. "Sharp: Private proximity test and secure hand- shake with cheat-proof location tags." *Computer Security-ESORICS2012*. Springer Berlin Heidelberg, 2012. 361-378.

[10] Li, Muyuan, et al. "All your location are belong to us: Breaking mobile social networks for automated user location tracking." *ACM MobiHoc*. ACM, 2014.

[11] Gao, Zhaoyu, et al. "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures." *INFOCOM*, IEEE, 2013.

[12] Zeng, Kexiong, et al. "Location spoofing attack and its countermeasures in database-driven cognitive radio networks." *Communications and Net- work Security (CNS)*, IEEE, 2014.

[13] Shokri, Reza, et al. "Quantifying location privacy." *Security and Privacy (SP), 2011 IEEE Symposium on*. IEEE, 2011.

[14] Luo, Wanying, and Urs Hengartner. "Veriplace: a privacy-aware location proof architecture." *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems*. ACM, 2010.

[15] Saroiu, Stefan, and Alec Wolman. "Enabling new mobile applications with location proofs." *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*. ACM, 2009.

[16] Jiajia Liu, Shangwei Zhang, Nei Kato, et al. "Device-to-device commu- nications for enhancing quality of experience in software defined multi- tier LTE-A networks." *IEEE Network*, 2015, 29(4):46-52.

[17] Siksnys, Laurynas, et al. "Private and flexible proximity detection in mobile social networks." *Mobile Data Management (MDM), 2010 Eleventh International Conference on*. IEEE, 2010.

[18] He, Wenbo, Xue Liu, and Mai Ren. "Location cheating: A security chal- lenge to location-based social network services." *Distributed Computing Systems (ICDCS), 2011 31st International Conference on*. IEEE, 2011.

[19] Pham, Anh, et al. "Secure and private proofs for location-based activity summaries in urban areas." *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 2014.

[20] Jiajia Liu, Nei Kato, et al. "Throughput and Delay Tradeoffs for Mobile Ad Hoc Networks With Reference Point Group Mobility." *IEEE Transactions on Wireless Communications*, 2015, 14(3): 1266-1279.

[21] Gao Z, Zhu H, Liu Y, et al. "Location privacy leaking from spectrum utilization information in database-driven cognitive radio network." *ACM CCS*. ACM, 2012: 1025-10,2010.