Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks

Zhaoyu Gao[†], Haojin Zhu[†], Shuai Li[†], Suguo Du[†] and Xu Li[‡]

[†]Shanghai Jiao Tong University, Shanghai 200240, P. R. China

{gaozy1987}@gmail.com, {zhu-hj, shuailee, sgdu}@sjtu.edu.cn

[‡]INRIA Lille - Nord Europe, France

xu.li@inria.fr

Abstract

Collaborative spectrum sensing is regarded as a promising approach to significantly improve the performance of spectrum sensing in Cognitive Radio Networks (CRNs). However, due to the open nature of wireless communications and the increasingly available software-defined radio platforms, collaborative spectrum sensing also poses many new research challenges, especially in the aspects of security and privacy. In this article, we firstly identify the potential security threats towards the collaborative spectrum sensing in CRNs. Then we review the existing proposals related to secure collaborative spectrum sensing. Furthermore, we identify several new location privacy related attacks in collaborative sensing, which are expected to compromise secondary users' location privacy by correlating their sensing reports and their physical locations. To thwart these attacks, we propose a novel privacy preserving framework in collaborative spectrum sensing to prevent location privacy leaking. We design and implement a real-world testbed to evaluate the system performance. The attack experiment results show that, if there is no any security guarantee, the attackers could successfully compromise a secondary user's location privacy at the success rate larger than 90%. We also show that the proposed privacy preserving framework can significantly improve the location privacy of secondary users with a minimal effect on the performance of the collaborative sensing.

Keywords **Security, Location Privacy, Privacy Preserving, Collaborative Sensing**

I. INTRODUCTION

The proliferation of smart phones and mobile Internet based applications require a better utilization of radio channels. To address the ever increasing demand for wireless bandwidth,

cognitive radio networks (CRNs) have been proposed to improve the efficiency of channel utilization under the current static channel allocation policy. Unlike conventional spectrum regulation paradigms in which the majority of the spectrum is allocated to fixed licensed users (or primary users) for exclusive use, a CRN system permits unlicensed users (or secondary users) to utilize the idle spectrum as long as it does not introduce interference to the primary users. As an important regulatory step, the FCC (Federal Communications Commission) has recently adopted rules to allow unlicensed radio operation in the unused portions of the TV spectrum, commonly referred as white space, which is expected to provide additional spectrum.

One major technical challenge in designing dynamic spectrum access systems is to detect the presence of primary users and to further determine the availability of a certain channel. It is recently discovered that collaboration among multiple secondary users can significantly improve the performance of spectrum sensing by exploiting their spatial diversity. Therefore, collaborative spectrum sensing has been widely adopted in all existing standards or proposals, i.e., IEEE 802.22 WRAN, CogNeA, IEEE 802.11af and WhiteFi.

Collaborative spectrum sensing is regarded as a promising approach to significantly improve the performance of spectrum sensing in CRNs. However, due to the open nature of wireless communications and the increasingly available software defined radio platforms, e.g., Universal Software Radio Peripherals (USRPs), it also poses many new research challenges, especially in the aspects of security and privacy. A malicious node may seek to exploit a channel in a region by falsely reporting a present primary signal, or dually, seek to vandalize the network by reporting that a present primary is not detected thereby encouraging interference from secondary users. Further, a selfish node may try to enjoy a free wireless access service without contributing to the spectrum sensing result. Least but not last, untrusted collaborative spectrum fusion center may try to compromise the location privacy of a specific user by geo-locating it from its collaborative spectrum sensing reports.

In this article, we summarize the existing security threats towards collaborative spectrum sensing in CRNs, and review existing solutions to them. We then identify several new security attacks in collaborative spectrum sensing, which aim to compromise secondary users' location privacy by correlating their sensing reports and their physical locations. To thwart these attacks and preserve location privacy, we propose a novel privacy preserving framework for collaborative spectrum sensing. We design and implement a real-world testbed to evaluate its performance.

The attack experiment results indicate that, when there is no security technique employed, the attacker can compromise a secondary user's location privacy at a success rate larger than 90%. We further show that the proposed privacy preserving framework can significantly improve the location privacy of secondary users without jeopardizing the collaborative spectrum sensing performance.

II. Collaborative Sensing in Cognitive Radio Networks

In CRNs, a fundamental task of each CR user is to detect the presence of primary users (PUs) if they exist or to identify the available spectrum if PUs are absent. Although the FCC's recent ruling eliminates spectrum sensing as a requirement for devices that have geo-location capabilities and can access a new TV band (geo-location) database, it is expected that spectrum sensing and its variants will still play an important role in improving the performance of CRNs for the following reasons. First, collaborative spectrum sensing can be used to support the operation of sensing-only devices that cannot access the database. Second, compared with the database built from propagation models, collaborative spectrum sensing can provide a more accurate view of spectrum availability since the database may be conservative and declare many channels (at locations away from the TV transmitters) as occupied even if they are idle. Third, the details of spectrum sensing results assist in selecting higher quality channels for operation when multiple channels are available. Finally, utilizing the geo-location database for spectrum availability information is similar to traditional location based services; it will inevitably leak users' location information, and may not be desirable for location-privacy-sensitive secondary users.

Collaborative spectrum sensing methods can be generally classified as centralized or distributed sensing, as illustrated in Fig. 1. In centralized sensing, a central node called Fusion Center (FC) controls a three-step cooperative sensing process. First, the FC selects a control channel and instructs all cooperating CR users to individually perform local sensing. Second, all cooperating CR users report their sensing results to FC via the control channel. Finally, FC combines the received local sensing reports to determine the presence of PUs, and diffuses the decision back to cooperating CR users. On the contrary, distributed sensing does not need any centralized FC to make the cooperative decision; CR users communicate with each others in a peer-to-peer manner and iteratively converge to a unified decision on the presence or absence of PUs.

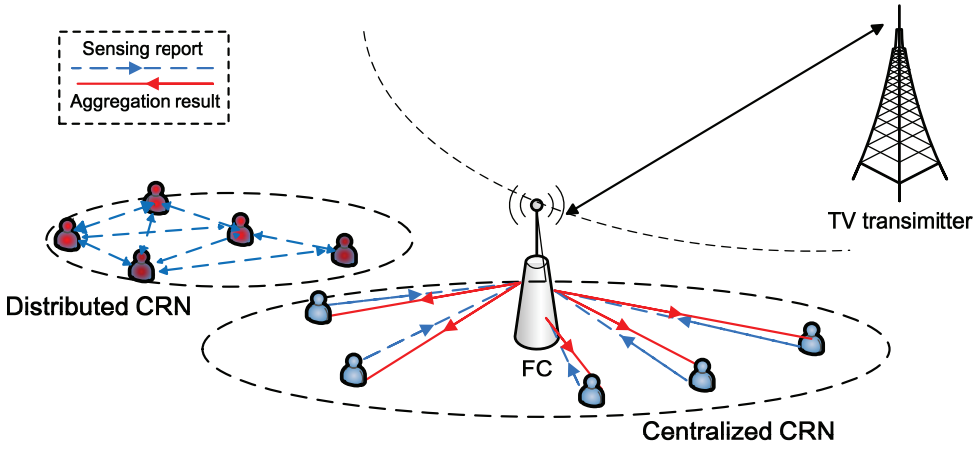


Fig. 1. Distributed CRN and Centralized CRN

Common signal detection techniques include matched filter, energy detection, cyclostationary detection and wavelet detection, among which energy detection is the most popular approach due to its simplicity and short sensing time (less than 1ms for a channel). In this article, we adopts energy detection to detect signal. However, the proposed scheme could be readily extended to other signal detection techniques.

III. Security Challenges in Collaborative Sensing

In collaborative spectrum sensing of CRNs, there are several main emerging security challenges as introduced below.

- **Authentication**: Several aspects of authentication issues should be considered when securing collaborative spectrum sensing.
  - *Primary User Authentication*: In CRNs, an attacker may transmit its signal with high power or mimic specific features of the primary user's signal (e.g., use the same pilot or synchronization word) to bypass the primary user detection method used. Consequently, secondary users may incorrectly identify the attacker's signal as the primary user's and will not use the relevant channel. Such attack is called Primary User Emulation (PUE) attack [1], [2]. To thwart this attack, secondary users should authenticate the identity of received signal when sensing the targeted channel.

  - *Secondary User Authentication*: When the FC (or a secondary user) collects sensing reports from other users, it should authenticate the identities of the secondary users. Otherwise, a potential attacker may forge the identity of a secondary user to send false sensing reports.
  - *Sensing Report Authentication*: Although secondary users' identities can be authenticated during the sensing report aggregation process, it is possible that some legitimate but malicious secondary users report unauthentic sensing results in an internal attack. This attack is coined as Spectrum Sensing Data Falsification (SSDF) attack [3], [4]. Hence, the sensing reports of each secondary user should be authenticated as well.
- **Incentive Mechanisms**: Most of existing collaborative spectrum sensing schemes assume that all secondary users are ready to sense. This assumption might be easily violated in the presence of selfish users, who may not cooperate in order to save their own wireless resources (e.g., energy or transmission time) while enjoying the sensing results from others [5], [6]. Such selfish behaviors seriously degrade the performance of collaborative spectrum sensing. Incentive mechanisms are necessary to stimulate collaboration.
- **Data Confidentiality**: It implies that a sensing report is well protected and not revealed to unauthorized external users who may monitor the communication channels by eavesdropping. Data Confidentiality can be easily achieved by end-to-end encryption, which requires the presence of mutual authentication among sensing collaborators.
- **Privacy Preservation**: Compared with the above mentioned security problems, privacy issues have received little attention in CRNs so far. Privacy is primarily regarded as preserving the anonymity of a sensing node and/or the privacy of its location. Location privacy protection intends to prevent adversaries (e.g., other sensing nodes or external observers) from linking a sensing node's sensing report to the node's physical location.

IV. Existing Proposals for Securing Cognitive Radio Networks

In this section, we summarize the existing works related to the security issues in CRNs. All of these works mainly focus on the PUE, SSDF and incentive problems, while few of them consider the privacy issues in CRNs.

- **Thwarting Primary User Emulation (PUE) Attack**: PUE attack is introduced for the first time in [1]. In the same article, a location distinction approach is suggested to distinguish

an attacker's signal from the primary user's signal and therefore mitigate PUE attack. This approach uses received signal strength (RSS) to estimate the source location of a signal, and decides whether the signal is from the primary user based on the prior knowledge of the primary user's location. In [2], link signature is adopted to authenticate the primary user's signal. A helper node is proposed to inform a secondary user about the link signature of the primary user at its location. Then, when the attacker launches PUE attack, the secondary user is able to detect it by comparing the link signature of the primary user and that of the received signal.

- **Thwarting Spectrum Sensing Data Falsification (SSDF) Attack**: In [3], an abnormal misbehavior detection scheme is proposed. In this scheme, it is unrealistically assumed that the spectrum usage pattern of the primary user, which usually is an ON-OFF ratio of the primary user's signal, is known. A secondary user whose sensing reports conflict with this pattern is regarded as malicious. The effectiveness of this scheme decreases when the ON-OFF ratio approximates to 1. A machine learning based scheme is proposed in [4], which does not rely on any specific signal propagation model. In this scheme, a trusted initial set of signal propagation data in a region is taken as input to build a Support Vector Machine (SVM) classifier. The classifier is then used to detect integrity violations. In [7], the proposed User-centric Misbehavior Detection Scheme (UMDS) is based on the fact that a secondary user tends to trust its own sensing reports rather than others'. A user chooses its own sensing reports over multiple target channels as the trust base and evaluates other users' trust levels. It regards the users with fairly different sensing reports as malicious. The advantage of UMDS is that it also performs well in attacker-dominant situations.
- **Stimulating Selfish Behaviors in Collaborative Sensing**: Selfish users in collaborative sensing may not be willing to contribute to the cooperation, because scanning the spectrum and broadcasting the sensing results will cost their extra time and energy. There are a few previous proposals addressing selfish behaviors in CRNs. In [5], for a free-rider, not to share sensing results is proved to be the dominating strategy in non-incentive CRNs. Besides, some classic incentive strategies (Tit-for-Tat and 2-player Trigger, etc.) are demonstrated to be improper for enhancing collaborative spectrum sensing, since punishing a specific node without affecting others is an easy task. In order to thwart selfishness, an N player horizontal infinite game is adopted to analyze several incentive strategies, such as Grim

Trigger and Carrot-and-Stick, furthermore some improved strategies under random errors are proposed to achieve better system performance. In [6], an evolutionary game is adopted to study how to collaborate for a secondary user when there are selfish users. Evolution Dynamics is used to analyze whether the secondary user should choose to be a free-rider at the risk of no contributor in the network, or to contribute at some cost. Learning algorithms are also proposed to enable secondary users to have the evolutionary stable strategy based on their own payoff observations.

From the above discussions, it can be concluded that most of the current works mainly focus on the security aspects of CRNs while privacy issue has not been investigated before. In the following section, we will identify several new privacy threats in CRNs.

V. Privacy Threats in Collaborative Sensing

Location privacy threats represent a unique security challenge in CRNs. This is mainly because that a secondary user's sensing reports on the signal propagation of primary users are highly correlated to its physical location. Therefore, similar to geo-locating individuals via WiFi or Bluetooth signals, a malicious attacker may exploit the correlation to geo-locate the secondary user and thus compromise the user's location privacy. Below, we identify a few new location privacy attacks in CRNs. In the next section, we will introduce a novel location privacy preserving framework to resist these attacks.

- **External CR Report** & **Location Correlation Attack:** Due to the open nature of wireless communications, an external attacker may easily obtain the CR reports of a specific sensing node by eavesdropping and compromise its location privacy by correlating the CR reports and the node's physical location.
- **Internal CR Report** & **Location Correlation Attack:** A malicious attacker, e.g., the FC, may participate in the collaborative spectrum sensing as a legitimate node and receives sensing reports from other nodes as rewards. After obtaining the sensing reports, it compromises any of these nodes' location privacy by correlating the node's CR reports and physical location.
- **Internal Differential CR Report** & **Location Correlation Attack:** Unlike previous two attacks that are based on individual sensing reports, this attack analyzes the aggregation result of the sensing reports. The adversary appears as an internal node. It estimates a specific

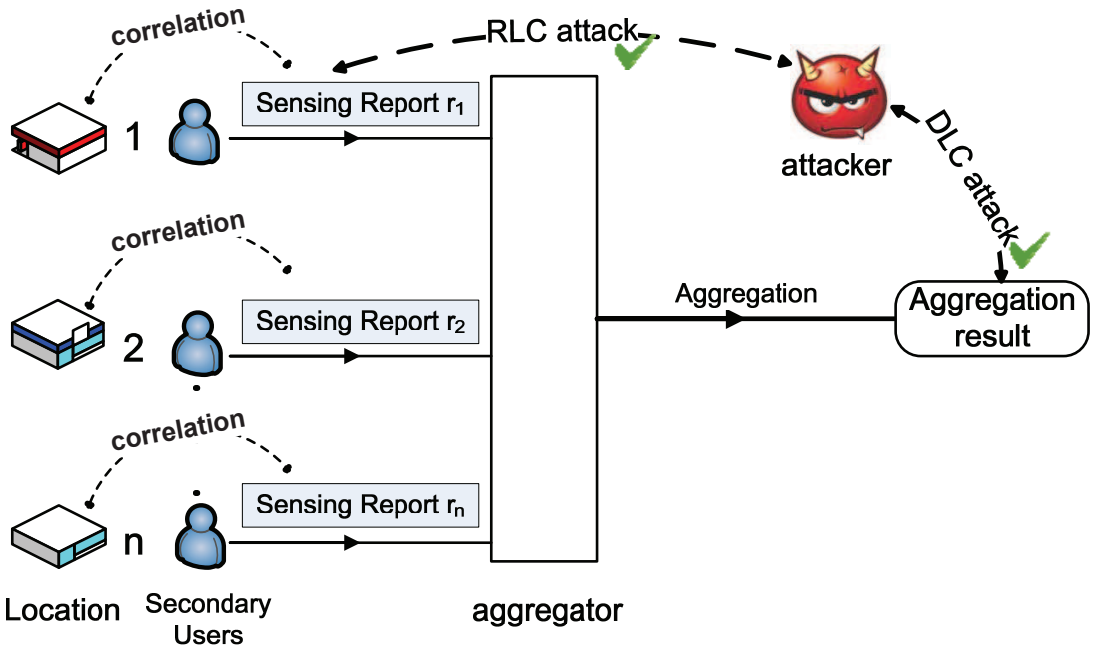


Fig. 2. RLC and DLC attacks in collaborative spectrum sensing of CRN. These two attacks may correlate users' sensing reports with their physical locations.

node's sensing report and infers its location information by comparing the aggregation result before and after the node joins/leaves the network.

For ease of presentation, we refer to the first two attacks collectively as *CR Report & Location Correlation* Attack (or RLC attack) and term the last one as *Differential CR Report & Location Correlation Attack* (or DLC attack), which are shown in Fig.2.

To launch RLC attack or DLC attack, an attacker normally needs to generate the signal propagation patterns by collecting the average RSS value of each channel at every position. However, to avoid measuring RSS exhaustively, the attacker may adopt a simplified approach. Specifically, it eavesdrops all the sensing reports transmitted within the network and uses them to build a signal propagation model. By this approach, even without the corresponding location information, it can still turn to some classification method to partition the RSS data into multiple sets corresponding to various locations. In our experiments, we chooses k-means classification method for the attack because this method works very well in the case that the number of clusters k (or number of collaborators) is known to the attacker. Further, as a typical machine learning algorithm, it supports utilizing Euclidean distance as a metric or a variance as the measurement

of cluster scatters. After performing the classification, the attacker obtains the centroid of each cluster, which corresponds to a physical location.

When launching RLC attack, the attacker calculates the distance between the expectation of user's sensing reports $E[r_i]$ and the centroid of each cluster. The expectation can be calculated as the average value of the user's several sensing reports. If the distance between the expectation and the centroid of a specific cluster is less than a predetermined value ϵ, the sensing report is regarded as belonging to this cluster with a high correct probability, which means that this sensing collaborator is expected to be at this position. Thus the location privacy of the users can be easily violated. Note that, a large ϵ may lead to a poor localization accuracy (or multiple potential positions), while a small ϵ may make the attacker fail to link a sensing report to any cluster. The attacker needs to choose an appropriate ϵ empirically in order to have the best attacking performance.

DLC attack can be performed as follows. After a sensing node joins or leaves the network, the adversary estimates the node's submitted sensing report by comparing the changes of the aggregation result induced by the node's arrival/departure. After obtaining the estimated sensing report, it infers the location information of the node by determining whether the report belongs to a particular cluster in a similar way to RLC attack.

VI. Location Privacy Preserving Framework for Collaborative Sensing

In this section, we propose a novel location privacy preserving framework for collaborative spectrum sensing to thwart various attacks mentioned above and provide location privacy guarantee for secondary users. The proposed framework is composed of two parts: Privacy Preserving Sensing Report Aggregation protocol (PPSRA) and Distributed Dummy Report Injection Protocol (DDRI). Specifically, PPSRA utilizes applied cryptographic techniques to allow the FC to obtain the aggregation result from various secondary users without learning each individual's values while DDRI can provide differential location privacy for secondary users by introducing a novel sensing data randomization technique. Fig. 3 shows the proposed framework, which is to be described in detail below.

A. Privacy Preserving Sensing Report Aggregation against RLC Attack

PPSRA protocol is grounded on the concept of secret sharing in [9]. By sharing the FC's secret among n secondary users, each secondary user encrypts the sensing report with its secret and the FC cannot decrypt the secret unless it collects and aggregates the encrypted sensing reports from all the sensing nodes. In particular, PPSRA can be described as follows:

- *System Setup:* Let $\mathcal{U} = \{u_1, u_2, \ldots, u_{n-1}, u_n\}$ be the set of secondary users and u_0 be the FC. A trusted third party generates a secret key sk_i for each secondary user u_i, s.t. $\sum_{i=0}^{n} sk_i = 0$. We coin the scanned spectrums as $\widetilde{C} = \{\widetilde{C}_1, \widetilde{C}_2, \cdots, \widetilde{C}_M\}$ and denotes user u_i's sensing report on spectrum $\widetilde{C}_k$ by r_i^k. Let $\mathbb{G}$ denote a cyclic group of prime order p for which Decisional Diffie-Hellman is hard and $H : \mathbb{Z} \to \mathbb{G}$ denotes a hash function modeled as a random oracle.
- *Sensing Report Encrypting:* Each secondary user $u_i \in \mathcal{U}$ performs its spectrum sensing on spectrum $\widetilde{C}_k$ at time slot t, and then encrypts the sensing report r_i^k with its secret key as follows:

$$c_i^k = g^{r_i^k} \cdot H(t)^{sk_i}. \tag{1}$$

  Then u_i sends the encrypted sensing report c_i^k to the FC.
- *Aggregation Phase*: After receiving the spectrum sensing reports from all the participants, the FC obtains the final aggregate sensing result by computing:

$$V_k = H(t)^{sk_0} \prod_{i \in \mathcal{U}} c_i^k \tag{2}$$

Since $\sum_{i=1}^{n} sk_i = 0$, it is obvious that $V_k = g^{\sum_{i=1}^{n} r_i^k}$. Therefore, to obtain the aggregated sensing result for time slot t, the FC needs to compute the discrete log of V_k base g and then obtain $\sum_{i=1}^{n} r_i^k$. Note that, the RSS values in collaborative sensing reports are typically not large. In our experiment, RSS value varies in the range of $[-30, 0]$, which makes the plaintext space quite small. As pointed out by [9], when the plaintext space is small, decryption can be accomplished via a brute-force search. If utilizing the Pollards lambda method, this computation time could be finished in 6.93ms. Such a computational overhead can satisfy the real-time requirements of collaborative sensing, in which the time interval for two regular CR sensing is 2s.

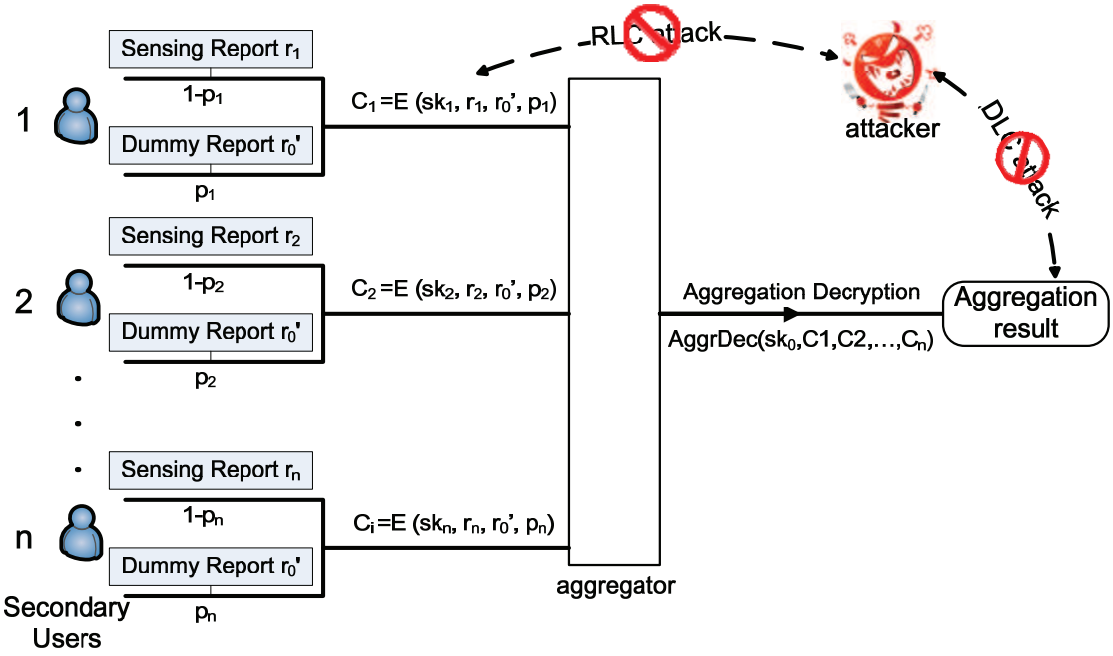


Fig. 3. A privacy preserving collaborative spectrum sensing framework

The security of PPSRA scheme is based on [9]. In PPSRA, the FC can only obtain the encrypted data c_i^k from u_i, and according to [9], the FC cannot deduce the sensing report r_i^k without the node's secret key sk_i. Therefore, PPSRA successfully resists Internal RLC attack since each sensing result is encrypted with the user's secret and the FC can only obtain the overall aggregation result with no clue about the individual values. However, as we pointed out in Section V, though it can successfully thwart RLC attack, PPSRA cannot thwart DLC attack. In the following, we will show how to protect the differential location privacy of secondary users by injecting some "*special noises*".

B. Distributed Dummy Report Injection against DLC Attack

In traditional differential privacy literature, the standard procedure for ensuring differential privacy is to let the FC add an appropriate magnitude of noise or to let each participant add the noise in a distributed way before publishing the desired statistic [8]. However, adding noise to sensing reports may seriously degrade the performance of collaborative sensing, which obviously deviates from the original goal of collaborative sensing. To address this problem, we introduce

a Distributed Dummy Report Injection protocol (DDRI) to protect the location privacy of the secondary users.

The basic idea of the DDRI is the following. During a user leaving/joining phase, other users uses a dummy sensing report r_0^k, which is provided by the FC's own sensing (or any voluntary secondary user's), to replace the real sensing report (of the leaving/joining user) at a predefined probability p. Unlike traditional noise based differential privacy protection techniques which may have a negative effect on collaborative sensing, such a dummy report based approach will not pollute the aggregation result. Instead, it only increases the weight of a real sensing report from the FC of the overall aggregation result and reduce the number of real participants involved in the collaborative sensing, which are two major metrics considered in the subsequent performance analysis. In our experiment, it is found that by choosing an appropriate probability r_0^k, DDRI can pose a minimal effect on the performance of collaborative spectrum sensing.

VII. Experiment and Evaluation

In this section, we first demonstrate the practicality of the identified RLC and DLC attacks by using real-world experiments. Then, we show the effectiveness of the proposed PPSRA and DDRI protocols by comparing their privacy leaking with the traditional collaborative spectrum sensing. In our experiment, it is also shown that PPSRA and DDRI pose a limited negative effect on the performance of collaborative spectrum sensing.

A. System Setup

Our experiment environment is set up at Building of Electronic Information and Electrical Engineering School and located at Shanghai Jiao Tong University, Minghang Campus. We use Universal Software Radio Peripheral (USRP) with a TVRX daughterboard (50 MHz to 860 MHz Receiver) and a wide band antenna (70 MHz to 1000 MHz) to detect the TV radio signal in the building. Then we scan the spectrum from 600 MHz to 860 MHz at these 13 places with each spectrum scanned for 10 seconds totally while every 8 MHz spectrum scanned for 33ms. To evaluate the privacy leaking risks of various attacks, we emulate an attacker's behavior to geo-locate a secondary user as presented in Section V.

B. Experiment Results

To demonstrate the effectiveness of the identified RLC and DLC attacks, we consider two performance metrics, Attack Successful Rate (ASR) and the Location Privacy Entropy (LPE). In both of RLC and DLC attacks, if the attacker could correctly geo-locate a secondary user by correlating his sensing report to his physical locations out of total 13 locations, it is regarded as a successful attack. However, in some cases, the attacker may not accurately correlate a sensing report to a location. In stead, with a limited number of sensing reports, the attacker can still derive a potential location set, which includes the real location of the target secondary user. From the information theory point of view, with RLC and DLC attacks, the attacker can still obtain a certain location information of the secondary users. Therefore, by adopting the definition of entropy [10], we could have a similar definition on location privacy, which is used to describe the uncertainty of the attackers to correlate a sensing report (or the secondary user) to a specific location. The experiment result of RLC and DLC without any privacy preserving method is shown in TABLE. I, where ϵ is the bound of distance between centroid and sample point.

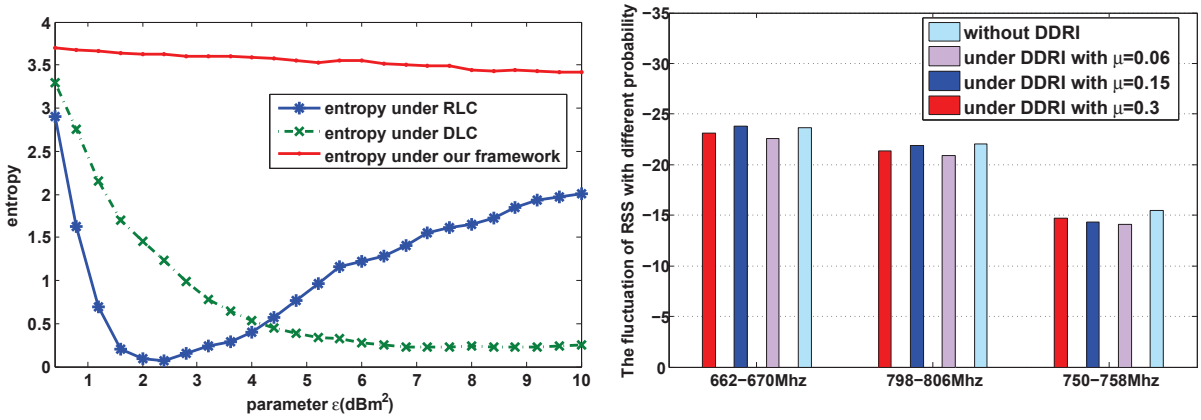
Attack Type	ϵ	Max ASR	Min ASR	Average ASR	Average LPE
RLC	1.44	100%	76.92%	91.31%	0.47
	2.25	100%	92.31	99.15%	0.06
	4.00	61.54%	46.15%	56.77%	0.47
DLC	2.25	92.31%	46.15%	71.08%	1.31
	4.00	92.31%	53.85%	79.31%	0.52
	6.25	100%	69.23%	84.38%	0.36

TABLE I

THE ATTACK SUCCESS RATE (ASR) AND THE LOCATION PRIVACY ENTROPY (LPE) UNDER DIFFERENT ϵ

It is observed that with a proper parameter ϵ, i.e. RLC with $\epsilon = 2.25$ and DLC with $\epsilon = 6.25$ in TABLE. I, in both attacks, ASR can reach about 90% , and the achieved entropy can be close to 0, while the maximum entropy is $\log_2 13 \approx 3.7$. So it indicates that, with a proper parameter ϵ, the attacker could launch both of the RLC and DLC effectively.

We further evaluate the effectiveness of the proposed PPSRA and DDRI protocols as well as the impact of DDRI on the performance of the collaborative sensing. In our experiment, we derive the probability p from a normal distribution $N(\mu, \delta)$. It is obvious that without knowing



(a) Entropy under RLC, DLC and our framework

(b) The fluctuation of RSS with different μ

Fig. 4. The evaluation results about the RLC attack, DLC attack and DDRI and DDRI's impact on collaborative sensing

the individual sensing report, both of the external or internal RLC may not be effective any more. On the other hand, in terms of DLC, there are still some locations can be inferred, but most of the correlation is not authentic. So ASR of DLC is also close to 0. In Fig. 4(a), it is observed that under the protection, the entropy level of secondary users' location privacy remains unchanged, which means the uncertainty of the attackers about user's location remains unchanged. Thus, the user's location privacy could be well protected. Fig. 4(b) shows that DDRI pose a limited effect on the performance of collaborative spectrum sensing.

In summary, the experiment results confirm the existence of RLC and DLC, and substantiate the effectiveness of the privacy preserving framework.

VIII. CONCLUSION

Collaborative spectrum sensing is regarded as a fundamental task for each secondary user in cognitive radio networks (CRNs). In this paper, we firstly identify the potential security threats in collaborative spectrum sensing. We then give a comprehensive survey on the existing works on secure collaborative spectrum sensing, which shows that location privacy issue has received little attention so far. With the real-world experiments, we point out three new location privacy related attacks in collaborative spectrum sensing. To thwart these new attacks, we propose a novel privacy preserving collaborative spectrum sensing framework including a privacy preserving sensing report aggregation (PPSRA) protocol to thwart external/internal RLC attack and distributed

dummy report injection (DDRI) protocol to prevent DLC attack. Our experiment results have demonstrated the practicality of the identified RLC and DLC attacks and the proposed PPSRA and DDRI protocols could effectively thwart these attack with a minimized overhead.

REFERENCES

[1] R. Chen, J. Park, and J.H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol.26, no.1, pp.25-37, Jan. 2008.

[2] Y. Liu, P. Ning, H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," in Proceedings of *IEEE Symposium on Security and Privacy* 2010, Oakland, CA, May 2010.

[3] W. Wang, H. Li, Y. Sun, Z. Han, "CatchIt: Detect Malicious Users in Collaborative Spectrum Sensing," in Proc. of *GLOBECOM'09*, 2009.

[4] O. Fatemieh, A. Farhadi, R. Chandra, and C. Gunter, "Using Classification to Protect the Integrity of Spectrum Measurements in White Space Networks," in Proc. of *NDSS'11*, 2011.

[5] C. Song and Q. Zhang, "Achieving cooperative spectrum sensing in wireless cognitive radio networks," *ACM MC2R, Special Issue on Cognitive Radio Technologies and Systems*, Vol. 13, Issue 2, April 2009

[6] B. Wang, K.J. Liu, and T.C. Clancy, "Evolutionary cooperative spectrum sensing game: how to collaborate?" *IEEE Trans. on Communications*, vol.58, no.3, pp.890-900, March 2010.

[7] S. Li, H. Zhu, B. Yang, C. Chen, X. Guan, "Believe Yourself: A User-centric Misbehavior Detection Scheme for Secure Collaborative Spectrum Sensing," in Proc. of *ICC'11*, 2011.

[8] C. Dwork "Differential privacy," Invited talk at ICALP, 2006.

[9] E. Shi, T. Chan, E. Rieffel, R. Chow, and D. Song,"Privacy-preserving aggregation of time-series data," in Proc. of *NDSS'11*, 2011.

[10] J. Freudiger, M.H. Manshaei, J.P. Hubaux, and D.C. Parkes,"On Non-Cooperative Location Privacy: a Game-Theoretic Analysis," in Proc. of *CCS'09*, 2009.