SECURITY AND PRIVACY OF COLLABORATIVE SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS

ZHAOYU GAO, HAOJIN ZHU, SHUAI LI, AND SUGUO DU,
SHANGHAI JIAO TONG UNIVERSITY
XU LI, INRIA LILLE

ABSTRACT

Collaborative spectrum sensing is regarded as a promising approach to significantly improve the performance of spectrum sensing in cognitive radio networks. 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 aspect of security and privacy. In this article, we first identify the potential security threats toward 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 location. 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 a success rate of more than 90 percent. We also show that the proposed privacy preserving framework could significantly improve the location privacy of secondary users with a minimal effect on the performance of collaborative sensing.

INTRODUCTION

The proliferation of smart phones and mobile Internet-based applications require 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 idle spectrum as long as it does not introduce interference to primary users. As an important regulatory step, the Federal Communications Commission (FCC) 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 resource.

One major technical challenge in designing a dynamic spectrum access system is to detect the presence of primary users and to further determine the availability of a certain channel. It was recently discovered that collaboration among multiple secondary users can significantly improve the performance of spectrum sensing by exploiting their spatial diversity. As a consequence, 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, such as 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. Furthermore, a selfish node may try to enjoy free wireless access service without contributing to the spectrum sensing result. Last but not least, an untrusted collaborative spectrum fusion center may try to compromise the

1536-1284/12/$25.00 © 2012 IEEE

location privacy of a specific user by geo-locating it from its collaborative spectrum sensing report.

In the sequel, we summarize existing security threats toward collaborative spectrum sensing in CRNs, and review existing solutions to thwart 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 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 engaged, the attacker can compromise a secondary user's location privacy at a success rate of more than 90 percent. 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.

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 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 to 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 generally be classified as centralized or distributed sensing, as illustrated in Fig. 1. In centralized sensing, a central node called a 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 the FC via the control channel. Finally, the 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 other in a peer-to-peer manner and iteratively converge to a unified decision on the presence or absence of PUs. 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 1 ms for a channel). In this article, we adopt energy detection to detect signals. However, the proposed scheme could be readily extended to other signal detection techniques.

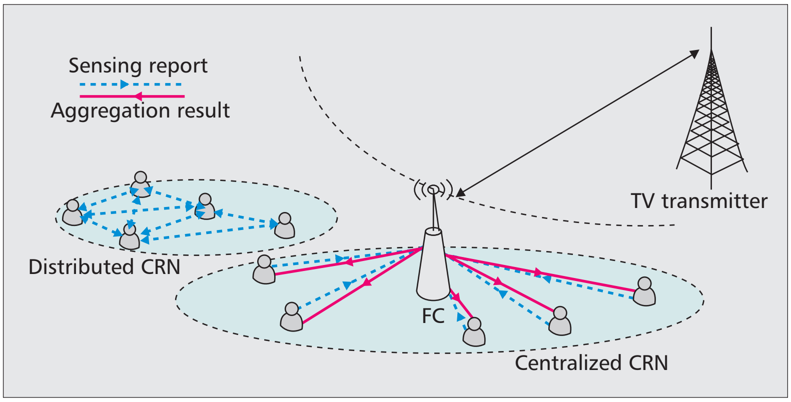


Figure 1. *Distributed CRN and centralized CRN.*

Security Challenges in Collaborative Sensing

In collaborative spectrum sensing of CRNs, there are several main emerging security challenges, 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 a primary user's signal (e.g., use the same pilot or synchronization word) to bypass the PU detection methods. Consequently, secondary users may incorrectly identify the attacker's signal as a PU's signal and will not use the relevant channels. Such attacks are called primary user emulation (PUE) attacks [1, 2]. To thwart this attack, secondary users should authenticate the identity of the received signal when sensing the targeted channel.
- Secondary user authentication: When an 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 the secondary users' identities can be authenticated during the sensing report aggregation process, it is possible that some secondary users are malicious and report unauthentic sensing results as an internal attack. This attack is called a spectrum sensing data falsification (SSDF) attack [3, 4]. Hence, the sensing reports of each secondary user should be authenticated as well.

Location privacy threats represent a unique security challenge in CRNs. This is mainly because a secondary user's sensing reports on the signal propagation of the primary users are highly correlated to its physical location.

Incentive mechanism: Most existing collaborative spectrum sensing schemes assume that all secondary users are ready to sense. This assumption might easily be violated in the presence of selfish users, who may not cooperate in order to save their precious wireless resources (e.g., energy or transmission time) while enjoying sensing results from others [5, 6]. Such selfish behaviors seriously degrade the performance of collaborative spectrum sensing.

Data confidentiality: This 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 easily be achieved by end-to-end encryption, which requires the presence of mutual authentication among sensing collaborators.

Privacy preservation: Compared to the above mentioned security problems, privacy issues, which regard primarily preserving the anonymity of a sensing node and/or the privacy of its location, have received little attention in literature [7]. Location privacy protection intends to prevent adversaries (e.g., another sensing node or an external observer) from linking a sensing node's sensing report to the node's physical location.

Existing Proposals for Securing Cognitive Radio Networks

In this section, we summarize the existing works related to the security problems in CRNs. All of these works mainly focus on the PUE, SSDF, and incentive problems, and none of them notice the privacy problems in CRNs.

Thwarting a PUE attack: The 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 a PU's signal and therefore mitigate a 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 PU based on prior knowledge of the PU's location. In [2], a link signature is adopted to authenticate the PU's signal. A helper node is proposed to inform a secondary user about the link signature of the PU at its location. Then, when the attacker launches PUE attack, the secondary user is able to detect it by comparing the link signature between the PU and the received signal.

Thwarting an SSDF attack: In [3], an abnormal misbehavior detection scheme is proposed. This scheme is based on the assumption that the spectrum usage pattern of the PU 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 of the spectrum usage pattern 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 [8], 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 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 cooperation, because scanning the spectrum and broadcasting the sensing results will cost them extra time and energy. There are quite a few previous proposals addressing selfish behaviors in CRNs. In [5], for a free rider, not to share sensing result is proved to be the dominating strategy in non-incentive CRNs. Besides, some classic incentive strategies (Tit-for-Tat, 2-player Trigger, etc.) are demonstrated to be improper for enhancing collaborative spectrum sensing, since punishing a specific node without affecting others will be a challenging problem. In order to thwart selfishness, an *N* player horizontal infinite game is adopted to analyze several incentive strategies, such as Grim Trigger and ; 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 the secondary user to have an evolutionary stable strategy based on their own payoff observations.

Notice that the privacy problem in CRNs has never been mentioned in these works, which are discussed in detail in the following section.

Privacy Threats in Collaborative Sensing

Location privacy threats represent a unique security challenge in CRNs. This is mainly because a secondary user's sensing reports on the signal propagation of the PUs 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 introduce a novel location privacy preserving framework to resist these attacks.

External CR report and 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 and location correlation attack: A malicious attacker (e.g., an FC) may participate in collaborative spectrum sensing as a legitimate node and receive sensing reports from other nodes as rewards. After obtaining the sensing reports, it compromises any other node's location privacy by correlating the node's CR reports and physical location.

Internal differential CR report and location correlation attack: Unlike the previous two attacks, which 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 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 as *CR report location correlation* attack (or RLC attack) and the last one as *differential CR report and location correlation* attack (or DLC attack), respectively. We also illustrate these two kinds of attacks in Fig. 2.

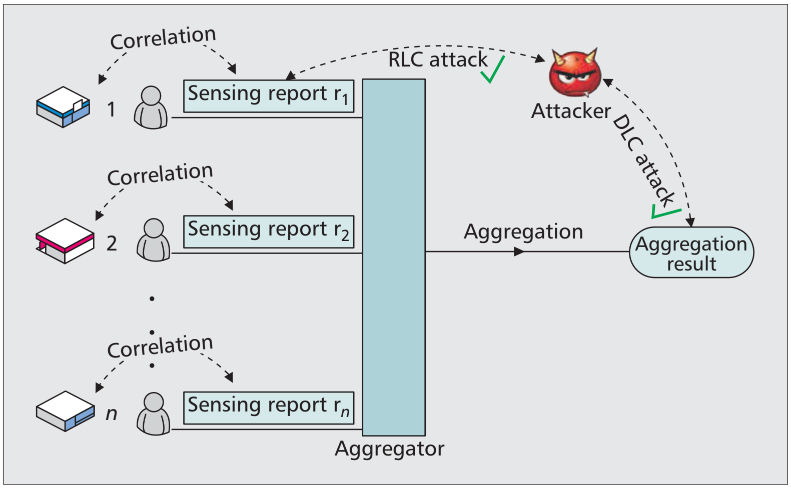


Figure 2. *RLC and DLC attacks in collaborative spectrum sensing of a CRN.*

To launch an RLC attack or a 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. That is, it eavesdrops all the sensing reports transmitted within the network and uses them to build a signal propagation model. By this means, 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 choose k-means classification method for the attack because this method works very well when number of clusters k (or number of collaborators) is known by the attacker. Furthermore, 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 the RLC attack, the attacker calculates the distance between the expectation of a user's sensing reports $E[r_i]$ and the centroid of each cluster. The expectation could 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 users can easily be violated. Note that a large ε may lead to 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.

The DLC attack can be performed as follows. After a sensing node joins or leaves the CRN, 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 as the RLC attack.

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 mainly composed of two parts: Privacy Preserving Sensing Report Aggregation (PPSRA) protocol and Distributed Dummy Report Injection (DDRI) protocol. Specifically, the PPSRA scheme utilizes applied cryptographic techniques to allow the FC to obtain the aggregation result from various secondary users without learning each individual's values, while the DDRI algorithm can provide differential location privacy for secondary users by introducing a novel sensing data randomization technique. Figure 3 shows the proposed framework described in detail as follows.

Privacy Preserving Sensing Report Aggregation against RLC Attack

The basic idea of PPSRA protocol is based on the concept of secret sharing in [10]. By sharing an FC's secret among n secondary users, each secondary user encrypts the sensing report with its secret; the FC cannot decrypt the secret unless it can collect and aggregate all of the encrypted sensing reports from all of the sensing nodes. In particular, PPSRA could 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 in CRNs and u_0 be the fusion center. A trusted third party generates a secret key sk_i for each user u_i, s.t. $\Sigma_{i=0}^{n} sk_i = 0$. We coin the scanned spectrum $\overline{C} = \{\overline{C}_1, \overline{C}_2, \ldots, \overline{C}_M\}$, which denotes user u_i's sensing report on spectrum $\overline{C}_k$ as r_i^k. Let $\mathbb{G}$ denote a cyclic group of prime order p for which decisional Diffie-Hellman is hard, and H: $\mathbb{Z} \rightarrow \mathbb{G}$ denotes a hash function modeled as a random oracle.

PPSRA could successfully address Internal RLC attacks since each sensing result is encrypted with the user's secret and FC can only obtain the overall aggregation result while FC has no idea about each individual value. However, though it can successfully thwart RLC attacks, PPSRA cannot thwart DLC attacks.

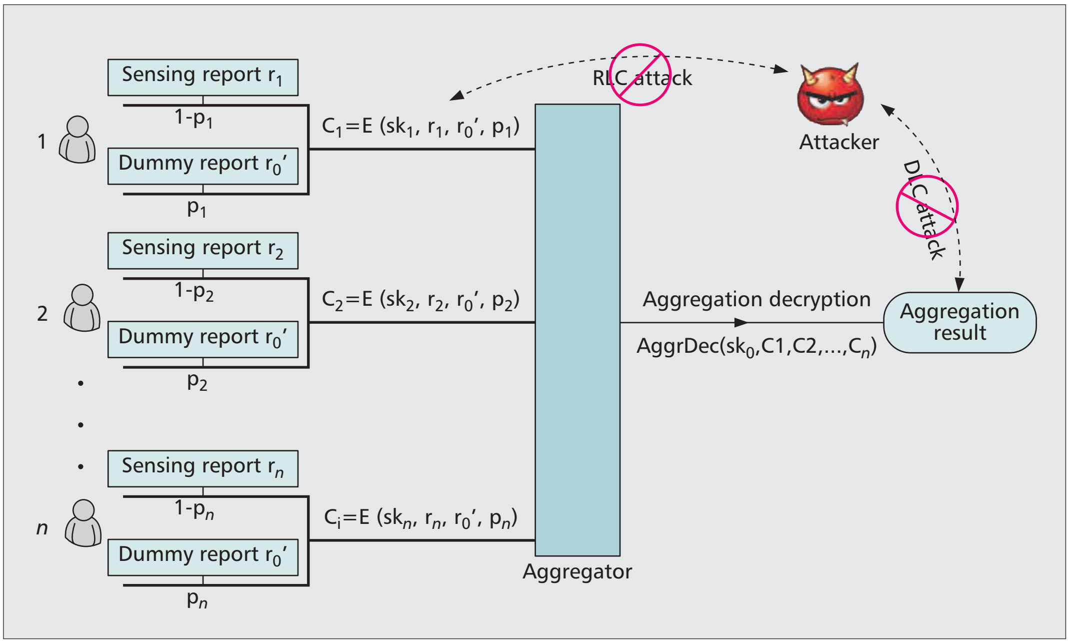


Figure 3. *A privacy preserving collaborative spectrum sensing framework.*

Sensing report encrypting: Each secondary user $u_i \in \mathcal{U}$ performs its spectrum sensing on the spectrum C_k at time slot t, and then encrypts its 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 fusion center.

Aggregation phase: After receiving the spectrum sensing reports from all the participants, the fusion center could obtain the final aggregated sensing results by computing

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

Since $\Sigma_{i=1}^n sk_i = 0$, it is obvious that $V_k = g\Sigma_{i=1}^n R_i^k$. Therefore, to obtain the aggregated sensing result for time slot t, the fusion center needs to compute the discrete log of V_k base g and then obtain $\Sigma_{i=1}^n R_i^k$. Note that the RSS value in a collaborative sensing report is 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 [10], when the plaintext space is small, decryption can be accomplished via a brute force search. To further speed up the decryption speed, Pollard's lambda method is suggested for fast decryption, which requires decryption time roughly square root in the plaintext space.

PPSRA could successfully address internal RLC attacks since each sensing result is encrypted with the user's secret, and the FC can only obtain the overall aggregation result, having no idea about each individual value. However, as we pointed out earlier, although it can successfully thwart RLC attacks, PPSRA cannot thwart DLC attacks. In the following, we show how to protect the differential location privacy of secondary users by injecting some "special noises."

Distributed Dummy Report Injection against DLC Attack

In traditional differential privacy literature, the standard procedure for ensuring differential privacy is for the FC to add an appropriate magnitude of noise or for each participant to add the noise in a distributed way before publishing the desired statistic [9]. However, adding noise to the 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 DDRI to protect the location privacy of secondary users.

The basic idea of DDRI is that during the user leaving/joining phase, other users can use a dummy sensing report $r^k{}_0$, which could be provided by the FC's own sensing (or any voluntary secondary user) to replace their real sensing report at a predefined probability p. Different from the traditional noise-based differential privacy protection technique, 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 reduces 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 $r^k{}_0$, DDRI could pose a minimized effect on the performance of collaborative spectrum sensing, which is presented in the next section.

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 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.

System Setup

Our experiment environment is set up at the building of the Electronic Information and Electrical Engineering School at Shanghai Jiao Tong University, Minghang Campus. We use USRP-with a TVRX daughterboard (5–860 MHz receiver) and a wideband antenna (70–1000 MHz) to detect the TV radio signal in the building. Then we scan the spectrum from 600 to 860 MHz at 13 places with each spectrum scanned for 10 s total while every 8 MHz of spectrum is scanned for 33 ms. To evaluate the privacy leaking risks of various attacks, we emulate an attacker's behavior to geo-locate a secondary user as presented earlier.

Experiment Results

To demonstrate the effectiveness of the identified RLC and DLC attacks, we consider two performance metrics, attack successful rate (ASR) and location privacy entropy (LPE). In both RLC and DLC attacks, if the attacker can correctly geo-locate a secondary user by correlating its sensing report to its physical locations out of a total of 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. Instead, 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 certain location information of secondary users. Therefore, by adopting the definition of entropy, we could have a similar definition of location privacy, which is used to describe the uncertainty of the attackers to correlate a sensing report (or a secondary user) to a specific location. The experiment result of RLC and DLC without any privacy preserving method is shown in Table 1, where ε is the bound of distance between centroid and sample point.

It is observed that with a proper parameter ε (i.e., RLC with ε = 2.25 and DLC with ε = 6.25 in Table 1 in both attacks), ASR can reach about 90 percent, and the achieved entropy can be close to 0, while the maximum entropy is $\log_2 13 \approx 3.7$. This indicates that with a proper parameter ε, the attacker could launch both 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 collaborative sensing. In our experiment, we derive the probability p from a normal distribution $N(\mu, \delta)$. It is obvious that without knowing the individual sensing report, both external and internal RLC may not be effective anymore. On the other hand, in terms of DLC, there are still some locations that can be inferred, but most of the correlation is not authentic. So ASR of DLC is also close to 0. In Fig. 4a, it is observed that under protection, the entropy level of secondary users' location privacy remains unchanged, which means the uncertainty of the attackers about a user's location remains unchanged. Thus, the user's location privacy could be well protected. Figure 4b shows that DDRI poses a limited effect on the performance of collaborative spectrum sensing.

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 1. *The attack success rate (ASR) and location privacy entropy (LPE) under different ε.*

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

Conclusion

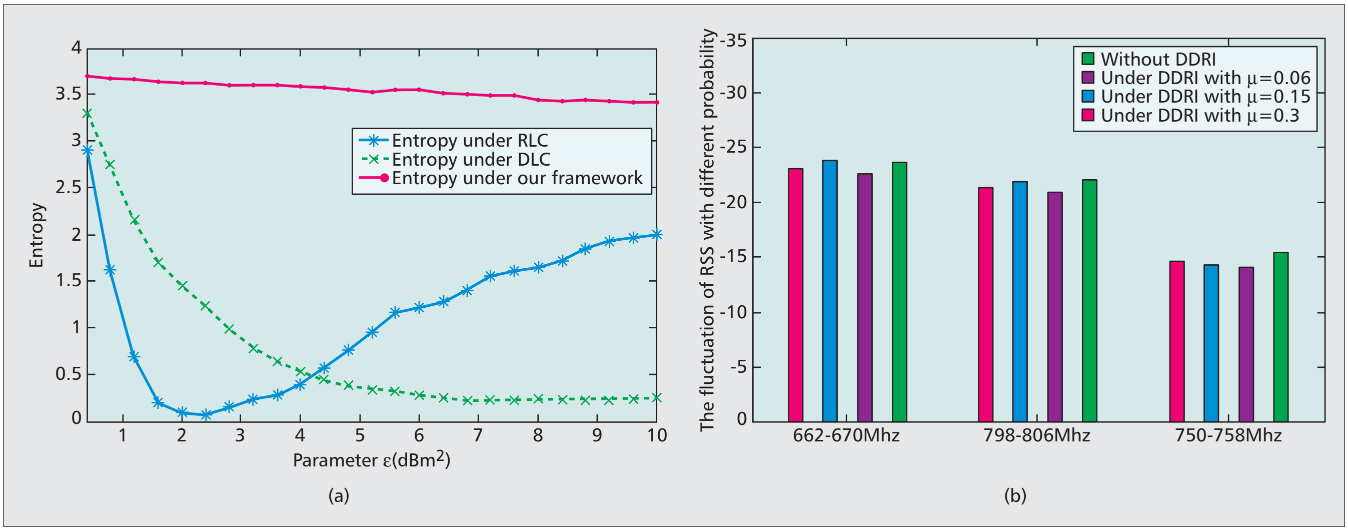
Collaborative spectrum sensing is regarded as a fundamental task for each secondary user in cognitive radio networks. In this article, we first identify the potential security threats in collaborative spectrum sensing. We then give a comprehensive survey on the existing works on secure collaborative spectrum sensing, which shows that location privacy has received little attention so far. With 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 protocol to thwart external/internal RLC attacks and a distributed dummy report injection protocol to prevent DLC attacks. 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 attacks with minimized overhead.

Acknowledgment

This research was supported by National Natural Science Foundation of China (Grant No. 61003218, 70971086, 61161140320, 61033014) and Doctoral Fund of Ministry of Education of China (Grant No.20100073120065).

References

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



(a)

(b)

Figure 4. *The evaluation results about the RLC attack, DLC attack and DDRI and DDRI's impact on collaborative spectrum sensing: a) entropy under RLC, DLC and our framework and b) the fluctuation of RSS with different probability.*

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

[3] W. Wang *et al.*, "CatchIt: Detect Malicious Users in Collaborative Spectrum Sensing," *Proc. GLOBECOM'09*, 2009.

[4] O. Fatemieh *et al.*, "Using Classification to Protect the Integrity of Spectrum Measurements in White Space Networks," *Proc. 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, Apr. 2009.

[6] B. Wang, K. J. Liu, and T. C. Clancy, "Evolutionary Cooperative Spectrum Sensing Game: How to Collaborate?," *IEEE Trans. Commun.*, vol. 58, no. 3, Mar. 2010, pp. 890–900.

[7] S. Li *et al.*, "Location Privacy Preservation in Collaborative Spectrum Sensing," *Proc. INFOCOM'12*, 2012.

[8] S. Li *et al.*, "Believe Yourself: A User-centric Misbehavior Detection Scheme for Secure Collaborative Spectrum Sensing," *Proc. ICC'11*, 2011.

[9] C. Dwork "Differential Privacy," invited talk at ICALP, 2006.

[10] E. Shi *et al.*, "Privacy-Preserving Aggregation of Time-Series Data," *Proc. NDSS'11*, 2011.

Biographies

Zhaoyu Gao (gaozy1987@gmail.com) received his B.Sc. degree in applied mathematics (2009) from Wuhan University, China, and now he is an M.Sc. candidate with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His research interest includes cognitive radio networks, and security and privacy in wireless networks.

Haojin Zhu [M'09] (zhu-hj@sjtu.edu.cn) received his B.Sc. degree (2002) from Wuhan University, his M.Sc. (2005) degree from Shanghai Jiao Tong University, both in computer science, and a Ph.D. in electrical and computer engineering from the University of Waterloo, Canada, in 2009. He is currently an associate professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His current research interests include wireless network security and distributed system security. He received the SMC-Young Researcher Award (Rank B), Shanghai Jiao Tong University, in November 2011. He was a co-recipient of best paper awards of IEEE ICC 2007 — Computer and Communications Security Symposium and Chinacom 2008 — Wireless Communication Symposium. He serves on the editorial board of *KSII Transactions on Internet and Information Systems* and a guest editor of *IEEE Network*. He also serves on technical program committees for many international conferences such as INFOCOM, ICCCN, GLOBECOM, ICC, and WCNC.

Shuai Li (shuaileemail@gmail.com) received his B.Sc. degree (2009) from Nanjing University of Aeronautics and Astronautics, China, and his M.Sc. (2012) degree from Shanghai Jiao Tong University, both in electric automization. He will be a Ph.D. candidate at the University of Minnesota, Twin Cities. His current research focuses on security of wireless networks and implementation of cognitive radio networks.

Suguo Du (sgdu@sjtu.edu.cn) received her B.Sc. degree in applied mathematics from Ocean University of Qingdao, China, in 1993, her M.Sc. degree in mathematics from Nanyang Technological University, Singapore, in 1998, and her Ph.D. degree from the Control Theory and Applications Centre of Coventry University, United Kingdom, in 2002. She is currently an associate professor in the Management Science Department at Antai College of Economics and Management, Shanghai Jiao Tong University. Her current research interests include risk and reliability assessment, fault tree analysis using binary decision diagrams, fault detection for nonlinear systems, and wireless network security management.

Xu Li (xu.li@inria.fr) received a Ph.D. (2008) degree from Carleton University, Canada, an M.Sc. (2005) degree from the University of Ottawa, Canada and a B.Sc. (1998) degree from Jilin University, China, all in computer science. Prior to joining Inria, France as a research scientist, he held post-doctoral fellow positions at the University of Waterloo, Canada, Inria/CNRS, and the University of Ottawa. He is on the editorial boards of *Wiley Transactions on Emerging Telecommunications Technologies*, *Ad Hoc & Sensor Wireless Networks*, and *Parallel and Distributed Computing and Networks*. He is/was a guest editor of a few journal special issues. His current research focuses on machine-to-machine communications and mobile social networks, along with over 50 different works published in refereed journals, conference proceedings, and books.