Protecting Location Information in Collaborative Sensing of Cognitive Radio Networks

Yunlong Mao
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing 210023, China
njucsmyl@163.com

Tingting Chen
California State Polytechnic University
Pomona, CA 91768
tingtingchen@cpp.edu

Yuan Zhang
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing 210023, China
zhangyuan@nju.edu.cn

Tiancong Wang
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing 210023, China
go.tcwang@gmail.com

Sheng Zhong
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing 210023, China
zhongsheng@nju.edu.cn

ABSTRACT

Collaborative sensing has become increasingly popular in cognitive radio networks to enable unlicensed secondary users to coexist with the licensed primary users and share spectrum without interference. Despite its promise in performance enhancement, collaborative sensing is still facing a lot of security challenges. The problem of revealing secondary users' location information through sensing reports has been reported recently. Unlike any existing work, in this paper we not only address the location privacy issues in the collaborative sensing process against semi-honest adversaries, but also take the malicious adversaries into consideration. We propose efficient schemes to protect secondary users' report from being revealed in the report aggregation process at the fusion center. We rigorously prove that our privacy-preserving collaborative sensing schemes are secure against the fusion center and the secondary users in semi-honest model. We also evaluate our scheme extensively and verify its efficiency.

Categories and Subject Descriptors

C.2.m [**Computer-Communication Networks**]: Miscellaneous

Keywords

Location Privacy; Privacy Preserving; Collaborative Sensing; Cognitive Radio

1. INTRODUCTION

With the development of wireless communication and the proliferation of mobile devices in recent years, dynamic spectrum allocation is considered an effective way to remedy the problem of spectrum shortage. Cognitive radio networks in particular have been proposed to enable dynamic spectrum allocation and increase the efficiency of resource utilization. In cognitive radio networks, unlicensed (secondary) users can sense the spectrum and tune their transmitters to the available channel, under the prerequisite that their communication does not introduce interference to the users with licenses (primary users) [10]. For the reason that the primary user has no obligation to help secondary users allocate the channels, secondary users need to cognitively sense the spectrum to avoid interference with existing primary users.

In order to effectively avoid interference in cognitive radio networks, collaborative sensing has been leveraged to detect the existing communication of primary users [18]. In particular, each unlicensed user measures the received signal strength (RSS). Then it either forwards the RSS to a centralized fusion center as a report, or sends its local decision on whether the licensed communication exists to the fusion center after analyzing the RSS. The fusion center collects all the reports from participating secondary users and draws a joint conclusion. If the spectrum is idle, the fusion center coordinates the secondary users to access the available channels. In this way, the white space not being used by the primary users can be fully utilized.

While collaborative sensing has become increasingly popular, some security concerns in this process have been raised. For example, if the reports sent by secondary users are caught and altered by an attacker, it may lead to a wrong sensing result at the fusion center and thus an interference. Even more seriously, collaborative sensing is facing the challenge that secondary users can be malicious and deliberately submit fake or invalid sensing reports. To address these issues, many research works have been proposed [5,7–9,24,25]. Recently, a new privacy issue, i.e., location privacy for secondary users in collaborative radio networks, has attracted people's attention. Related work (e.g., [11,16]) has shown

*This work was supported in part by NSFC-61321491, NSFC-61425024, NSFC-61300235, and NSFC-61402223.

MSWiM'15, November 2–6, 2015, Cancun, Mexico.
© 2015 ACM. ISBN 978-1-4503-3762-5/15/11 ...$15.00.
DOI: http://dx.doi.org/10.1145/2811587.2811594.

Table 1: guarantee and assumption of attackers in different schemes

scheme	Zhaoyu's	Shuai's	Ours
can be malicious?	No	Yes	Yes
can collude with FC?	No	Yes	Yes
can FC be malicious?	No	No	Yes

that in the sensing process, the secondary user's location information is highly correlated to the reported signal strength after the propagation from the primary user to the secondary user. Hence the attackers can utilize the reports to explore the location information of the secondary users. As the first remedy of the location privacy issue, [16] proposes a cryptographic scheme to enable the secondary user to conceal its sensing reports in the aggregation process at the fusion center. After that, a very similar privacy issue has been studied by [12, 13]. In their work, secondary users query a central database to obtain spectrum availability information for places around his location, then attackers can infer user's location by finding the overlapping area of spectrum the user has used.

However, the existing solutions for protecting location privacy in collaborative sensing have only considered limited attack scenarios and models. For example, in [16] it is assumed that the fusion center cannot be more than curious, i.e., it must faithfully perform sensing report aggregation although it may try to reveal secondary users' privacy. And according to [13] the solution should be performed in normalized cognitive radio networks with trusted central databases. The difference between our scheme and these solutions is shown in the Table.1. As shown in the table, Shuai's scheme is more relevant to ours. But our scheme is much more efficient. We will discuss the comparing in Section 5.

In this paper, we aim to provide complete privacy protection against the semi-honest adversaries, and then extend it against malicious adversaries (assuming that secondary users and the fusion center can deviate from the sensing protocol). In particular, in our scheme, we leverage an efficient and novel cryptographic scheme as a building block, and carefully design the scheme for each step of the collaborative sensing. Our scheme secures the report information against the attacks by the fusion center or by other secondary users. Compared with other existing works based on public-key schemes, one advantage of our work is that it is more efficient and more flexible. In particular, the scheme enables us to use randomly generated public key to encrypt sensing reports in each round, instead of using and managing the same key pair. To summarize, the contributions of this paper are as follows.

- We study the location privacy issues in collaborative sensing process both in the semi-honest model and in the malicious model. We propose efficient schemes to protect secondary users' report from being revealed in the report aggregation process at the fusion center.

- We show that our privacy-preserving collaborative sensing schemes are secure against the fusion center and the secondary users, in the semi-honest model and in the malicious attack model.

- We extensively evaluate the performance of our schemes and verify their efficiency.

After this introduction, the rest of this paper is structured as follows. In Section 2, we provide a general introduction of all system models and cryptography tools we use. In Section 3 we propose our scheme and provide both security analysis and complexity analysis. In Section 4 we propose an approach in an entirely malicious model as the extension of our scheme. In Section 5 we describe the two-part simulation experiment we performed to verify our scheme's feasibility and efficiency. We conclude the paper in Section 6.

2. PRELIMINARY

In this section, we will have a brief review of the collaborative sensing model. Aiming at existing privacy problems, we use a classical and essential collaborative sensing model, and then based on this model, our secure models consisting of a semi-honest model and a restricted malicious model. The attack scenarios under each model will be introduced. The last subsection is an introduction of a novel cryptographic technique that we use in our scheme.

2.1 Collaborative Sensing

We use a centralized cognitive radio model [19], which has a central control unit, known as Fusion Center (FC), to coordinate the work of each secondary user (SU) in the network and holds the right to make the decision of each affair. Generally, the FC launches one round of sensing, to determine SUs' numbers and coordinate all of them. The whole working process can be considered consisting of two parts, collaborative sensing and spectrum allocation. Our works just focus on the first part, so we put the details of spectrum allocation aside.

Here is the cognitive radio network (CRN) that we consider. Each node (including the FC and SUs) in CRN has a set of fully functional radio equipment and every two nodes can establish direct communication. No node has motility. In this CRN, SU set U_s consists of n users $U_s = \{s_1, s_2, \ldots, s_n\}$. There is only one primary user (PU) U_p concerned, and the channels set $C = \{c_1, c_2, \ldots, c_m\}$ consists of all channels that U_p occupies. The FC is denoted by F. SU s_i's local sensing result in U_p's channel $c_j, j \in [1, m]$ is denoted by r_i^j, and if we just look at a certain channel every time, we can just use r_i instead. Finally, we use R to denote global sensing result the FC gives in the end of collaborative sensing.

Now we define a round of collaborative sensing (which will be omitted to round in the rest). The FC confirms participating SUs and assigns the target channel c_j. Once a new round begins, all participants sense the channel c_j, and send their sensing report r_i^j containing the received signal strength (RSS) of the PU to the FC. When the sensing process completes, the FC must give a final global sensing result R^j based on SUs' reports aggregation. Various methods are available to detect the PU's signal [2]. Generally, we choose the method based on RSS, which follows the distribution below [17]:

$$r_i^j \sim \begin{cases} N(n_0, \frac{n_0^2}{M}), & H_0 \\ N(p_i^j + n_0, \frac{(p_i^j + n_0)^2}{M}), & H_1 \end{cases} \tag{1}$$

In the formula above, we denote SU s_i's sensing report by r_i^j and n_0 is the additive white Gaussian noise (AWGN). p_i

stands for the s_i's received signal power from the primary transmitter on channel c_j. M is the signal sample number. Let H_0 be channel's idle state, and H_1 be channel's busy state. Final result that the FC gives can be described as:

$$R^j = \sum_{i=1}^{n} \omega_i r_i^j, \tag{2}$$

In the formula above, ω_i is the weight of SU s_i's sensing result. We just use equal gain combination (EGC), setting all weights as 1 [17]. And R^j is the statistical result of the channel c_j.

2.2 Attack Model

Firstly we design our scheme to be effective in both a semi-honest model and a restricted malicious model. Then in section 4, we will extend our scheme to a malicious model. All the parties in the semi-honest model must follow the protocol of collaborative sensing and our scheme, but they can keep their own intermediate results, and in this model, honest users are the majority [15]. In other words, SUs and the FC must honestly do coin flipping and send their result whether they are semi-honest or not. In the restricted malicious model, loosely speaking, only SUs can be malicious, who can behave beyond prescribed protocol and nobody can predict their next move. And malicious users may submit arbitrary reports to disturb collaborative sensing result. Our goal is that our scheme is still secure with the number of malicious users which is smaller than that of half of the SUs. The FC is probably operated and maintained by an untrusted organization.

Because the main difference between the semi-honest model and the restricted malicious model is that SUs can be malicious, to be succinct, we use the semi-honest model as the default setting if no additional statement is attached. And we will have a separate discussion for the restricted malicious model.

Our attention focuses on user's location privacy. The *attacker* we called is the one who wants to acquire SU's location information. Any party in the network including SUs and the FC can be an attacker. We allow attackers to collude in our scheme. That means a semi-honest SU can collude with other semi-honest SU or semi-honest FC. The only assumption of our scheme is that if the FC is an attacker, it cannot collude with the Helper (which is to be introduced at the beginning of section 3), and neither of them could be malicious in the semi-honest model and the restricted malicious model. And this assumption can be removed in the extension of our scheme.

We consider attackers to use the same method as in [16] to get user's location information that we briefly describe here. Generally, we consider one attacker s_a in the set of U_s, who casts covetous eyes on location information of $s_d (\in U_s)$. First of all, s_a collects as much as possible sample locations' information. Then, s_a classifies the RSS sample data of each region into m classes using the input from two channels, and obtains each cluster's central value. Finally, s_a eavesdrop on s_d's sensing reports in the two channels, and calculates their distance with each cluster's central value. If s_a finds that s_d's distance with cluster k is the minimum distance, s_a can regard s_d's location the same as cluster k's.

2.3 Problem Formulation

Now we take care in defining proper notions of security for our problem. Our security is defined in the semi-honest model firstly, and then we will discuss the security in malicious model in Section 4. Intuitively, we want SUs to know nothing from our protocol, and the FC to know only a random permutation of all SUs' sensing results. We formalize the above idea using standard cryptographic terms as follows. Let $I = \{1, \ldots, n\}$ be the index set of the SUs and $\mathbf{r} = (r_1, \ldots, r_n)$ denotes the sensing results from all SUs. Let $\rho(\mathbf{r})$ be a uniformly random permutation of $\mathbf{r}$.

Definition 1. ***(Security against secondary users)*** *We say a collaborative sensing scheme (CSS) is* secure against all SUs *in the sense that it reveals* ***nothing other than the total number of SUs*** *to all SUs if, given any R and a security parameter t, for each $i \in \{1, \ldots, n\}$, there exists a probabilistic polynomial-time simulator S_i such that for every probability*

$$\{S_i(r_i, n, t)\} \overset{c}{\equiv} \{CSS\_View_{s_i}(R, t)\},$$

where $CSS\_View_{s_i}(R, t)$ denotes the view *of SU i while it runs the sensing scheme with R being all SUs' sensing results.*

Here, a user's view consists of its own coin flips and all messages from other participants that it sees in the scheme. The notation $\overset{c}{\equiv}$ denotes *computational indistinguishability* (please refer to [14] for a precise definition) of two *probability ensembles* [14]. Intuitively, this definition states that what a SU sees from the scheme can be efficiently simulated by a simulator given this user's private input, the total number of SUs and a public security parameter as the only inputs. Therefore, we can conclude that the CSS reveals nothing to all SUs.

Similarly, we can define the security against the FC as follows.

Definition 2. ***(Security against the fusion center)*** *We say a collaborative sensing scheme is* secure against all SUs *in the sense that it reveals only* ***a random permutation of all SUs' sensing results*** *if, given any R and a security parameter t, there exists a probabilistic polynomial-time simulator S_{FC} such that for every probability*

$$\{S_{FC}(\rho(R), t)\} \overset{c}{\equiv} \{CSS\_View_{FC}(R, t)\},$$

where $CSS\_View_{FC}(R, t)$ denotes the view *of the FC in the scheme.*

2.4 Derivative ElGamal encryption

ElGamal encryption algorithm is a classic asymmetric key encryption algorithm. Its encryption result is determined by not only plain text and public key, but also a random integer from encoder. In our scheme, we use a derivative algorithm of ElGamal encryption [27]. In addition, we modify it to apply to multiple parties. Choose a big prime with form of $p = 2q+1$, where q is another big prime. Denote a quadratic residues generator in Z_p^* by g, $g \neq 1$. In this scheme, considering that every node in the network including the FC may be untrusted, we separate receiver party's private key into two parts x_1 and x_2. Both of them are chosen from Z_q randomly, and kept by the receiver. Combine x_1, x_2 to get keys by calculating $x \equiv x_1 + x_2 \ mod \ q$ and $y = g^x \ mod \ p$.

Now, we have (p, g, y) as the public key, and (p, g, x) as the private key. Anyone who wants to send a message m with encryption can randomly choose an integer k from Z_q, encrypt plain text m into (g^k, my^k), then send it to the receiver. The receiver firstly decrypts the cipher text with one part of private key x_1 by calculating $my^k g^{-kx_1}$, and then it can get the original message from calculating $my^k g^{-kx_1} g^{-kx_2}$ in another part.

3. PROPOSED SCHEME

The goal of our scheme is to ensure that SUs will not expose their location privacy during the process of collaborative sensing in CRNs. SUs' sensing reports are original input data, and we want to get the final collaborative sensing result as output with location privacy preserved. But, considering the FC may be an attacker, a preprocessing is needed to protect original data before the FC's aggregation. SUs should anonymize their reports, so that the FC cannot match each report's source. SUs could do this by self-organizing or a trusted third-party.

In order to be more efficient and avoid involving a trusted third-party as much as possible, a SU will be selected to be an assistance Helper to prevent the attack from the FC. The Helper, a new role in our scheme, can be played by any SU. In other words, the Helper is a special SU who assists the FC with the perception of the PU's signal. Except that, the Helper has the same equipment with any SU. We can use many existing methods to select a SU as the Helper [6] [2], such as a voting algorithm. Besides, a novel encryption tool is used to protect sensing report. Since a SU will cost more energy to do computation as the Helper, this role can be played in turn. Many incentive schemes developed for CRNs [1, 21] can be easily applied to compensate for the energy cost, which is out of our concern.

As for the location attacks based on physical layer, it is beyond our discussion. Since this type of attack can be widely found in various kinds of networks instead of just aimed at cognitive radio's location privacy, it deserves separate research, and there are many effective methods to defeat it, such as [23].

3.1 Procedure Of Our Scheme

Our scheme consists of four steps, initializing, reports encrypting, the Helper's decrypting and the FC's decrypting. Generally, we randomly choose a SU as the Helper for one round before the sensing starts. Since the Helper can also be untrusted, to avoid the situations where the Helper is watched or is adversary itself, we re-randomize permuting the combination of users' sensing reports. However, this will not cause any effect on the final aggregating result. This involves our scheme's correctness, and we will prove it later in the end of this subsection.

We use the encryption tool in the following way. The receiver's two parts in derivative algorithm are the FC and the Helper, both of which hold part of the private key respectively. All SUs who want to submit sensing report in a sensing round need to encrypt his report with the public key. Then reports are sent to the Helper who will decrypt reports with his part of the private key and re-randomize permuting the match of reports and sources. The FC will get anonymous sensing data by decrypting report with his part of the private key. Our algorithm's specific flow is shown in Alg.1.

Algorithm 1: procedure of our scheme

```
$F$, $H$:
randomly pick $p,\ q,\ p = 2q + 1$, $p$ is $l$-bit length;
choose one generator of $Z_p^*$ as $g$ ;
$H$ randomly chooses $x_1$ in $Z_q$, $F$ randomly chooses $x_2$ in $Z_q$;
$x \equiv x_1 + x_2\ (mod\ q)$;
$y = g^x\ mod\ p$, $y_1 = g^{x_1}\ mod\ p$, $y_2 = g^{x_2}\ mod\ p$;

$s_i$:
foreach $i \in U_s$ do
    randomly chooses $k_i$ in $Z_q$;
    $\bar{r_i} \leftarrow (g^{k_i}\ mod\ p, r_i y^{k_i}\ mod\ p)$;
    $s_i$ sends $\bar{r_i}$ to $H$;
end

$H$:
re-randomized permuting $(\bar{r_1}, \bar{r_2}, \ldots, \bar{r_n}) \rightarrow (\hat{r_1}, \hat{r_2}, \ldots, \hat{r_n})$;
foreach $\hat{r_i} = (r_{\hat{i},1},\ r_{\hat{i},2})$ do
    $r_{\tilde{i},2} \leftarrow \frac{r_{\hat{i},2}}{(r_{\hat{i},1})^{x_1}}\ mod\ p$;
end
$H$ sends $((r_{\hat{1},1}, r_{\tilde{1},2}), (r_{\hat{2},1}, r_{\tilde{2},2}), \ldots, (r_{\hat{n},1}, r_{\tilde{n},2}))$ to $F$;

$F$:
foreach $i \in [1, n]$ do
    $r'_i \leftarrow \frac{r_{\tilde{i},2}}{(r_{\hat{i},1})^{x_2}}\ mod\ p$;
end
$F$ aggregates all of the $r'_i$ to get the final sensing result $R$.
```

Here are some explanations of the procedure. First of all, a secure length parameter l should be determined, and it can be set with firmware. Then a pair of primes p, q are generated, and the length of q is l-bit while $p = 2q + 1$. A generator g of Z_p^* is randomly chosen. The Helper and FC respectively generate random integer $x_1,\ x_2 \in Z_q$, x_1 and x_2 can not be exposed to others. Then let the Helper and FC work together to get $x,\ x \equiv x_1 + x_2\ (mod\ q)$ [1] and $y,\ y_1,\ y_2,\ y = g^x\ mod\ p,\ y_1 = g^{x_1}\ mod\ p,\ y_2 = g^{x_2}\ mod\ p$, the public key can be sent to all SUs through broadcasting. Once a SU s_i finishes local sensing, s_i encrypts the sensing report with the public key (p, g, y), and sends the encrypted report to the Helper instead of directly to the FC. The Helper re-randomizes permuting sensing reports received, decrypts reports with its part of the private key x_1 and sends result to the FC. The FC decrypts reports from the Helper with another part private key x_2 to get the original sensing report, do the final aggregation work and announce global collaborative sensing result R.

In the semi-honest model, an SU attacker can obtain nothing about other SU's location even if he colludes with the FC or the Helper. Similarly, if the FC or the Helper is attacker, he cannot obtain anything about any SU's location except those he colluded with. To keep our statement coherent, we put all these proofs in Theorem.5-7. As for the restricted malicious model, the information malicious SUs can obtain is no more than when they are semi-honest, and the security can be guaranteed by Theorem.5.

[1] we recommend to obtain x by introducing a trusted third party. However if the trusted third party is not available, we can still obtain x with cryptographic protocols easily.

THEOREM 3. *Our scheme keeps the correctness of sensing result in both semi-honest model and restricted malicious model.*

PROOF. Recall that the FC receives SUs' reports and give aggregation by $F(\mathbf{r})$. Let $A(\mathbf{r})$ denote our scheme algorithm execution. If we can prove that $F(\mathbf{r}) = F(A(\mathbf{r}))$, we can ensure the correctness. We use the same symbols in our scheme's procedure. The Helper has $\bar{r_i} = (g^{k_i} \mod p$, $r_i y^{k_i}$ *mod* $p)$, $\forall r_i \in \mathbf{r}$, then after randomly permuting, we assume that $\hat{r_j} = \bar{r_i} = (r_{\bar{i},1},\ r_{\bar{i},2})$. Then the Helper partially decrypts $\hat{r_j}$ by $r_{\tilde{j},2} = \frac{r_{\bar{i},2}}{(r_{\bar{i},1})^{x_1}}$ *mod* p. Now we have $(r_{\bar{i},1},\ r_{\tilde{j},2})$ as input for the FC. Finally, the FC calculates $r_i{}' = \frac{r_{\tilde{j},2}}{(r_{\bar{i},1})^{x_2}}\ (mod\, p) = \frac{r_{\bar{i},2}}{(r_{\bar{i},1})^{x_1+x_2}}\ (mod\, p)$, where $x_1+x_2 = x\ (mod\, q)$, and $r_{i,1} = g^{k_i}\ (mod\, p), r_{i,2} = r_i y^{k_i}\ (mod\, p)$, then $r_{i,1}^x = y^{k_i}\ (mod\ p)$, $r_i{}' = \frac{r_i y^{k_i}}{y^{k_i}}\ (mod\ p) = r_i$. $\mathbf{r}'$, the set of $r_i{}'$ is exactly the same set as $\mathbf{r}$. And the FC can give the same result because the aggregation is unrelated to the permutation of reports [20].

Unlike semi-honest SU, a malicious SU may falsify his sensing report r_m in uncertain ways. But no matter what content is in r_m, the FC can still give the same result as long as the number of malicious SU's false reports is below the aggregation's threshold which is usually set as half the number of SUs [20]. Therefore, if less than half SUs are malicious, our scheme's correctness can be kept. □

3.2 Security Analysis

Here we formally prove the security of our scheme. After the Helper is introduced, we should take a new attack scenario into consideration, a SU attacker colluding with the Helper. First of all, we define the security requirement for the Helper similarly to the security requirements for SUs and the FC in Section 2.3.

DEFINITION 4. ***(Security against the Helper)*** *We say a collaborative sensing scheme is* secure against the Helper *in the sense that it reveals* ***nothing other than the total number of SUs*** *to the Helper if, given any R and a security parameter t, there exists a probabilistic polynomial-time simulator S_H such that for every probability*

$$\{S_H(n,t)\} \overset{c}{\equiv} \{CSS\_View_H(R,t)\},$$

where $CSS\_View_H(R,t)$ denotes the view *of the Helper in the scheme.*

THEOREM 5. *Our scheme is secure against secondary users.*

PROOF. Recall that our security definition against SUs states what a SU sees from the scheme can be efficiently simulated by a simulator given only the total number of SUs and its own sensing result as the inputs. According to our scheme, a SU s_i's view consists of three parts: s_i's internal coin flips cfs, the encrypted sensing results $(\bar{r_j})_{j\in I\setminus\{i\}}$ sent from other users to the Helper (user i could know these by eavesdropping the communication between other users and the Helper), and the half-decryption results $((r_{\hat{j},1}, r_{\tilde{j},2}))_{j\in I}$ sent from the Helper to the FC (s_i could know these by eavesdropping the communication between the Helper and the FC). Now we construct a simulator S_i as follows.

Given inputs n, t, S_i runs our scheme alone and uses the coin flips cfs^* to simulate cfs. Also, S_i computes $\bar{r_j}^*$ ($j \in I\setminus\{i\}$) by running the key generation algorithm of Elgamal with security parameter t to generate a random encryption key and uses it to encrypt 1. In addition, S_i uses $(\bar{r_j}^*)_{j\in I\setminus\{i\}}$ to simulate $(\bar{r_j})_{j\in I\setminus\{i\}}$. Similarly, S_i computes n random encryptions of 1 (denoted by $((r_{\hat{j},1}{}^*, r_{\tilde{j},2}{}^*))_{j\in I}$) and uses them to simulate $((r_{\hat{j},1}, r_{\tilde{j},2}))_{j\in I}$.

Clearly, distributions of cfs^* and cfs are the same. Also, due to the multi-messages indistinguishability [14] of Elgamal encryption, $(\bar{r_j})_{j\in I\setminus\{i\}}$ and $(\bar{r_j}^*)_{j\in I\setminus\{i\}}$ are computationally indistinguishable. In addition, it is easy to verify that $((r_{\hat{j},1}, r_{\tilde{j},2}))_{j\in I}$ are n Elgamal encryptions using encryption key y_2, thus $((r_{\hat{j},1}{}^*, r_{\tilde{j},2}{}^*))_{j\in I}$ and $((r_{\hat{j},1}, r_{\tilde{j},2}))_{j\in I}$ are computationally indistinguishable according to the multi-messages indistinguishability of Elgamal encryption.

It is easy to see: 1)cfs is independent from $(\bar{r_j})_{j\in I\setminus\{i\}}$ and $((r_{\hat{j},1}, r_{\tilde{j},2}))_{j\in I}$. 2)$cfs^*$, $(\bar{r_j}^*)_{j\in I\setminus\{i\}}$ and $((r_{\hat{j},1}{}^*, r_{\tilde{j},2}{}^*))_{j\in I}$ are pairwise independent. Due to the uniformly random permutation and re-randomization on the ciphertexts performed by the Helper, it can be proved that $((r_{\hat{j},1}, r_{\tilde{j},2}))_{j\in I}$ are random encryptions of a random permutation of all users' sensing results and are independent of $(\bar{r_j})_{j\in I\setminus\{i\}}$. Therefore, we know cfs, $(\bar{r_j})_{j\in I\setminus\{i\}}$ and $((r_{\hat{j},1}, r_{\tilde{j},2}))_{j\in I}$ are pairwise independent, and the two ensemble distributions of $(cfs,\ (\bar{r_j})_{j\in I\setminus\{i\}},\ ((r_{\hat{j},1},\ r_{\tilde{j},2}))_{j\in I})$ and $(cfs^*,\ (\bar{r_j}^*)_{j\in I\setminus\{i\}},\ ((r_{\hat{j},1}{}^*,\ r_{\tilde{j},2}{}^*))_{j\in I})$ are computationally indistinguishable. □

THEOREM 6. *Our scheme is secure against the Helper.*

PROOF. Recall our security definition against the Helper requires that the Helper knows nothing other than the total number of SUs. We prove this by constructing a simulator S_H as follows.

According to our scheme, the Helper's view consists of two parts: its internal coin flips cfs and the encrypted sensing results $(\bar{r_j})_{j\in I}$. Given inputs n, t, S_H runs our scheme alone and uses the internal coin flips cfs^* to simulate cfs. It is easy to see that the two distribution ensembles are the same. Also, S_H simulates each $\bar{r_j}$ with a random encryption of 1 generated by running the key generation algorithm of Elgamal with security parameter t to generate a random encryption key and using it to encrypt 1. Due to the multi-messages indistinguishability of Elgamal, the joint distribution of n random encryptions of 1 is indistinguishable with $(\bar{r_j})_{j\in I}$. In addition, it is easy to see that the distribution of coin flips and distribution of the encryption results are independent. Therefore, we can conclude that the ensemble of the coin flips and encryptions generated by S_H are computationally indistinguishable to the Helper's view. □

THEOREM 7. *Our scheme is secure against the fusion center.*

PROOF. Recall our security definition against the FC requires that the FC knows nothing other a random permutation of all users' sensing results. We prove this by constructing a simulator S_{FC} as follows.

According to our scheme, the FC's view consists of two parts: the encrypted sensing results $(\bar{r_j})_{j\in I}$ sent from other users to the Helper (the FC can know these by eavesdropping the communication between SUs and the Helper), and the half-decryption results $((r_{\hat{j},1}, r_{\tilde{j},2}))_{j\in I}$ sent from the Helper to the FC. Now we construct a simulator S_{FC} as follows.

Given a random permutation $\rho(R)$, S_{FC} generates $(\bar{r_j}^*)_{j\in I}$, $|\rho(R)|$ random encryptions of 1, to simulate $(\bar{r_j})_{j\in I}$ similarly as S_i simulates $(\bar{r_j})_{j\in I\setminus i}$. Again, the computationally indistinguishability follows from the multi-message indistinguishability of Elgamal encryption. To simulate $((r\hat{_{j,1}}, r\tilde{_{j,2}}))_{j\in I}$, S_{FC} computes $((r\hat{_{j,1}}^*, r\tilde{_{j,2}}^*))_{j\in I}$ by encrypting $\rho(R)$ using encryption key y_2. The computationally indistinguishability between $((r\hat{_{j,1}}, r\tilde{_{j,2}}))_{j\in I}$ and $((r\hat{_{j,1}}^*, r\tilde{_{j,2}}^*))_{j\in I}$ follows from the uniformly randomness of the permutation performed by the Helper.

Clearly $(\bar{r_j}^*)_{j\in I}$ and $((r\hat{_{j,1}}^*,r\tilde{_{j,2}}^*))_{j\in I}$ are independent. Same as what we have showed in the proof of the security against users, $(\bar{r_j})_{j\in I}$ and $((r\hat{_{j,1}},r\tilde{_{j,2}}))_{j\in I}$ are indpendent. Therefore, $\{(\bar{r_j}^*)_{j\in I}$, $((r\hat{_{j,1}}^*,\ r\tilde{_{j,2}}^*))_{j\in I}\}$ and $\{(\bar{r_j})_{j\in I}$, $((r\hat{_{j,1}},\ r\tilde{_{j,2}}))_{j\in I}\}$ are computationally indistinguishable. □

3.3 Complexity Analysis

In CRNs, in order to guarantee that SU's dynamic access will not have any influence on the transmission of PU, the shorter the time collaborative sensing cost is, the better. If the sensing process spends more time than the limitation, it may cause the sensing result to be invalid. So it is necessary to analyse the time complexity of our algorithm. In the first part of algorithm, where the Helper and the FC generate the encrypting model cooperatively, the process can be finished in an invariable time $O(k_1)$. As for SUs' encryption process, every user can do the encryption individually. Besides, some fast algorithms of exponent arithmetic can ensure that user's process finishes in another invariable time $O(k_2)$. In the Helper's part, the total time of re-randomize permuting process and partly decrypting can be equivalent to $O(n)$. Similarly, in the FC's part, decrypting time and aggregating time can be equivalent to $O(n)$. It is evident that our algorithm's overhead depends on the amount of network users. Normally, a cognitive radio network can not contain so many SUs to result in an unacceptable overhead. With our proposed scheme, the Helper can assist the FC to coordinate SUs' sensing process, users can send reports to the Helper without worrying about exposing location information, and the FC can give the same aggregated result with the past. Also, our scheme's overhead is acceptable.

4. THE EXTENSION OF OUR SCHEME

In our work described above, we consider a semi-honest model and a restricted malicious model. The malicious user's effect can be wiped off by voting or statistics. Under the condition where the Helper and the FC keep the rule of the whole scheme, though attackers try to peek at other user's privacy, their attempts will be in vain for SUs without both x_1 and x_2, the Helper without x_2, and the FC without re-permutation clues.

However, if we take a look at an entirely malicious model, where anyone, including the Helper and the FC, can turn into a malicious attacker, our scheme will probably be disrupted. For example, a malicious Helper simply drops all reports from SUs and sends a mess to the FC, then the sensing process cannot finish as expected. Moreover, if a malicious Helper broadcasts part-decrypted reports with re-permutation clues, the FC can easily obtain user's privacy.

In the aim of the hope of extending our scheme to be more general and robust, we want to find an effective way to solve the problems emerged in the situation with malicious Helper. In fact, here we are faced with two questions: how can the FC verify the Helper's identity, and how can the FC trust that the reports the Helper sends are faithfully recorded instead of arbitrarily records. But after all, we should remember that the FC may be untrusted, so we cannot reveal any information of the Helper in the communication. Thus, we should let the FC obtain no knowledge about both the Helper's and SU's privacy except the part already included in encrypted and re-permuted reports.

In another view, we think about a special situation where a vicious user (denoted by V) may fake other users' message, including the Helper's message. V does not care about his own interest. The only purpose he holds is to obstruct sensing process by falsifying other user's report with mess bits. In the cognitive radio network with the protection of our scheme, all of the sensing reports have been transmitted twice, from SU to the Helper, and from the Helper to the FC. When V falsifies a SU's report, this report will be dropped off and cannot affect the final result on the FC, because the aggregation rule will ignore this noise. So, if V wants to exert some serious effects, his best and only choice is to fake or falsify the Helper's message to the FC.

In order to solve the two questions we proposed above, we need to introduce Fiat-Shamir heuristic [4], a paradigm of non-interactive zero-knowledge proof, into our scheme. The core idea is letting the Helper prove that he has private key x_1 and the reports he sends are not arbitrary to the FC, using non-interactive zero-knowledge proof. The proof flow can be illustrated as in Fig.1.

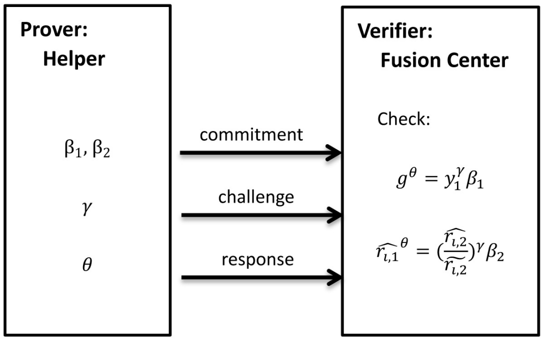

Prover:
Helper
β₁, β₂
γ
θ
commitment
challenge
response
Verifier:
Fusion Center
Check:
$g^\theta = y_1^\gamma \beta_1$
$\widehat{r_{i,1}}^\theta = (\frac{\widehat{r_{i,2}}}{\widetilde{r_{i,2}}})^\gamma \beta_2$

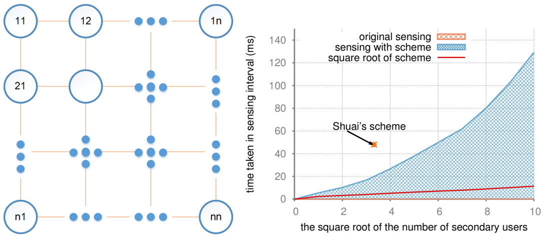
Figure 1: non-interactive zero-knowledge proof flow

As prover, the Helper should prove $\log_{r\hat{_{i,1}}} \frac{r\hat{_{i,2}}}{r\tilde{_{i,2}}} = \log_g y_1$ to the verifier, the FC. The Helper needs to pick α uniformly random from the quadratic residue in Z_p^*, then the Helper gets $\beta_1 = g^\alpha,\ \beta_2 = r\hat{_{r,1}}$ as the commitment in standard zero-knowledge proof (ZKP) [22]. A hash function H modeled as a random oracle is needed, and H is a cryptographic hash function whose range is Z_q. So that the Helper can get $\gamma = H(g,\ y_1,\ r\hat{_{i,1}},\ r\tilde{i},1,\ \beta_1,\ \beta_2)$, as challenge in ZKP. The last step is to get $\theta = \gamma x_1 + \alpha$ as response. Then the Helper sends $(\beta_1,\ \beta_2,\ \gamma,\ \theta)$ to the FC, who checks whether the following equations hold:

$$g^\theta = y_i^\gamma \beta_1 \tag{3}$$

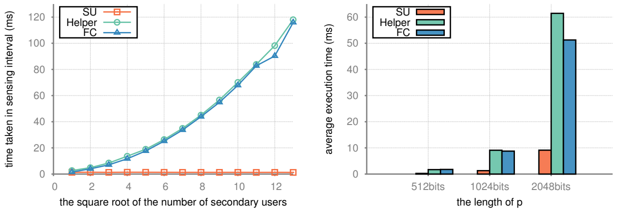
$$r\hat{_{i,1}}^\theta = (\frac{r\hat{_{i,2}}}{r\tilde{_{i,2}}})^\gamma \beta_2. \tag{4}$$

if these two equations hold, then the FC accepts the proof of the Helper.



(a) (b)

Figure 2: a) SUs' locations in CRN; b) sensing procedure time taken during the sensing interval.



(a) (b)

Figure 3: a) average execution time of each party; b) average execution time with different l.

5. EVALUATION

Since our scheme's security has been proved and the overhead of the sensing procedure is crucial [26], we perform a series of simulation experiments to evaluate our scheme's efficiency. We first evaluate the overhead carried by our scheme. Then we examine the overhead carried by each party of our scheme, so that we can analyze where the bottleneck is.

The environment we used for evaluation is an Ubuntu 14.10 64-bit distribution. The CPU is an intel i3-4130 clocked at 3.40GHz, and the installed RAM is 2GB. We implement our scheme with the help of CRE-NS3 [3], which is a cognitive radio extension of ns-3. CRE-NS3 has provided models including spectrum sensing, decision, mobility and sharing. Since our work focuses on location privacy during collaborative sensing process, we ignore other cognitive radio's models in the simulation except necessary components. We modify CRE-NS3, and add our scheme mainly to the spectrum sensing and decision models.

5.1 Setup

All SUs are deployed in grid in an open area. Each of the SUs has 802.11g standard wifi MAC with a rate of 54 Mbps. Every SU can establish direct communication with each other and is able to switch channels by himself. We assume that there are 11 channels that the PU and SUs and occupy. And according to the research of optimal sensing interval [26], we set the sensing interval to be 150ms. All of our simulating timer starts at the beginning of sensing and ends at the end of sensing decision.

Before an attacker seeks SU's location, necessary preparation is the collection of sample locations' information. Generally, we assume that every SU's location is sampled by the attacker. In order to be scalable for more SUs. We deploy SUs in grid and keep them equidistant. SUs' locations can be illustrated as in Fig.2(a).

Sample positions' location information is recorded and associated with signal strength. In each position, the attacker records the results of 20 rounds collaborative sensing on two channels of PU. Then the attacker binds the central values with positions' labels. The central values of sample positions in two dimensions on channels are recorded for further use.

5.2 Efficiency of Our Scheme

After the implementation of our scheme in CRE-NS3, we have measured execution time of collaborative sensing for different scales of SUs. Every time, we enlarge the SU set and add enough SUs on grid in a square area. We get every scale's average time to generate Fig.2(b) to compare with the time taken by original sensing process in CRE-NS3.

Since the abscissa is the square root of the number of SUs, time taken by our scheme is linearly increasing in fact. And its slope is about 1. Even when the number of SUs is around 100, our scheme can still work with feasible overhead, which is about 100ms, much less than 150ms interval.

Recall that there are three parties in our CRN, i.e. SU, the Helper, and the FC. Sometimes, just one party is to be concerned, so we measure average time on each party in our simulation. We record all SUs' execution time in a round, and calculate the average for each scale. As for the Helper and the FC, we record executing time of every round and get their average values for 100 rounds. From Fig.3(a), it is obvious that the Helper costs most time and has a great proportion on the total execution time. And it is reasonable that the Helper's and the FC's execution time grows linearly due to the increasing number of SUs, with abscissa being the square root of the number of SUs. In fact the slope of this increase is as small as about 1. The comparing result preliminary shows that when the scheme is applied to the network, a large portion of execution time depends on the Helper's efficiency. So if a high-performance node was selected to be the Helper, the total execution time it spends would decrease sensibly.

In the experiments above, we use 1024 bits as default set of the length of l, which is the security parameter of our scheme. To be comprehensive, we measure execution time of different lengths of l. In this situation, we set number of SUs as 10. As shown in Fig.3(b), our scheme is feasible for commonly used lengths of p.

In Shuai's work, when the security parameter has 1024 bits and the CRN has 10 SUs, the total computation time is roughly 48ms for one aggregation [16]. But with our scheme, the average computation time is about 20ms in the same setting. The comparing can be found in Fig.2(b). And it is obvious that our scheme can be more feasible in the massive users environment.

6. CONCLUSION

As the research of cognitive radio continues to improve, and with its outstanding dynamic spectrum accessing, it may well replace the traditional radio in the future. This paper studies the location privacy existed in collaborative sensing process of cognitive radio networks. We formalize privacy issue in both semi-honest model and malicious model. We take a series of simulating experiments to prove our scheme's validity and we discuss its feasibility by analysing the operating results. Our scheme gets robust when there may be malicious users behaving against the rules. Our scheme is proven to be feasible both in theory and simulation. In future work, we will consider the location privacy issue and malicious users who may cause false alarm problems to achieve a more complete protection scheme.

7. REFERENCES

[1] M. Abdelraheem, M. El-Nainay, and S. Midkiff. Spectrum occupancy analysis of cooperative relaying technique for cognitive radio networks. In *Computing, Networking and Communications (ICNC), 2015 International Conference on*, pages 237–241, Feb 2015.

[2] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Comput. Netw.*, 50(13):2127–2159, Sept. 2006.

[3] A. Al-Ali and K. Chowdhury. Simulating dynamic spectrum access using ns-3 for wireless networks in smart environments. In *Sensing, Communication, and Networking Workshops (SECON Workshops), 2014 Eleventh Annual IEEE International Conference on*, pages 28–33, June 2014.

[4] A. S. Amos Fiat. How to prove yourself: Practical solutions to identification and signature problems. *Advances in Cryptology âĂŤ CRYPTO âĂŹ86, Lecture Notes in Computer Science*, 263:186–194, 1986.

[5] K. Arshad. Malicious users detection in collaborative spectrum sensing using statistical tests. In *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on*, pages 109–113, 2012.

[6] D. Cabric, S. M. Mishra, D. Willkomm, R. Brodersen, and A. Wolisz. A cognitive radio approach for usage of virtual unlicensed spectrum. In *In Proc. of 14th IST Mobile Wireless Communications Summit 2005*, 2005.

[7] R. Chen and J.-M. Park. Ensuring trustworthy spectrum sensing in cognitive radio networks. In *Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on*, pages 110–119, 2006.

[8] R. Chen, J.-M. Park, and J. Reed. Defense against primary user emulation attacks in cognitive radio networks. *Selected Areas in Communications, IEEE Journal on*, 26(1):25–37, 2008.

[9] L. Duan, A. Min, J. Huang, and K. Shin. Attack prevention for collaborative spectrum sensing in cognitive radio networks. *Selected Areas in Communications, IEEE Journal on*, 30(9):1658–1665, 2012.

[10] FCC. Spectrum inventory table. http://www.fcc.gov/oet/info/database/ spectrum/. website.

[11] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li. Security and privacy of collaborative spectrum sensing in cognitive radio networks. *Wireless Communications, IEEE*, 19(6):106–112, 2012.

[12] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao. Location privacy leaking from spectrum utilization information in database-driven cognitive radio network. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 1025–1027. ACM, 2012.

[13] Z. Gao, H. Zhu, Y. Liu, M. Li, and C. Zhenfu. Location privacy in database-driven cognitive radio networks: Attacks and countermeasures. In *INFOCOM, 2013 Proceedings IEEE*, pages 2751–2759, April 2013.

[14] O. Goldreich. *The Foundations of Cryptography - Volume 2, Basic Applications*. Cambridge University Press, 2004.

[15] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, STOC '87, pages 218–229, New York, NY, USA, 1987. ACM.

[16] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen. Location privacy preservation in collaborative spectrum sensing. In *INFOCOM, 2012 Proceedings IEEE*, pages 729–737, 2012.

[17] A. Min, K. Shin, and X. Hu. Secure cooperative sensing in ieee 802.22 wrans using shadow fading correlation. *Mobile Computing, IEEE Transactions on*, 10(10):1434–1447, 2011.

[18] S. Mishra, A. Sahai, and R. Brodersen. Cooperative sensing among cognitive radios. In *Communications, 2006. ICC '06. IEEE International Conference on*, volume 4, pages 1658–1663, 2006.

[19] H. Rifa-Pous and J. Rifa. Spectrum sharing models in cognitive radio networks. In *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011 International Conference on*, pages 503–510, 2011.

[20] D. Teguig, B. Scheers, and V. Le Nir. Data fusion schemes for cooperative spectrum sensing in cognitive radio networks. pages 1–7, Oct 2012.

[21] N. Tran, D. Tran, L. B. Le, Z. Han, and C. S. Hong. Load balancing and pricing for spectrum access control in cognitive radio networks. In *Global Communications Conference (GLOBECOM), 2014 IEEE*, pages 1035–1040, Dec 2014.

[22] A. S. Uriel Feige, Amos Fiat. Zero-knowledge proofs of identity. *Journal of Cryptology*, 1:77–94, 1988.

[23] T. Wang and Y. Yang. Location privacy protection from rss localization system using antenna pattern synthesis. In *INFOCOM, 2011 Proceedings IEEE*, pages 2408–2416, 2011.

[24] W. Wang, H. Li, Y. Sun, and Z. Han. Attack-proof collaborative spectrum sensing in cognitive radio networks. In *Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on*, pages 130–134, 2009.

[25] W. Wang, H. Li, Y. Sun, and Z. Han. Catchit: Detect malicious nodes in collaborative spectrum sensing. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–6, 2009.

[26] X. Xing, T. Jing, H. Li, Y. Huo, X. Cheng, and T. Znati. Optimal spectrum sensing interval in cognitive radio networks. *IEEE Transactions on Parallel and Distributed Systems*, 25(9):2408–2417, 2014.

[27] S. Zhong. *Privacy, Integrity, and Incentive-Compatibility in Computations with Untrusted Parties*. PhD thesis, Yale University, 11 2004.