IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 24, 2020, accepted August 29, 2020, date of publication September 7, 2020, date of current version September 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3021583

An Efficient Location Privacy-Preserving Authentication Scheme for Cooperative Spectrum Sensing

HUIBIN LAI, LI XU, (Member, IEEE), AND YALI ZENG
Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350007, China

Corresponding author: Li Xu (xuli@fjnu.edu.cn)

This work was supported in part by the Nation Natural Science Foundation of China under Grant 61771140 and Grant U1905211, in part by the Fujian Province University Industry Cooperation of Major Science and Technology Project under Grant 2017H6005, and in part by the Enterprise Cooperation Project (IUI) under Grant DH-1307, DH-1412.

ABSTRACT In cognitive radio networks, cooperative spectrum sensing can improve the performance of spectrum utilization and accuracy of spectrum result. However, it suffers from security and privacy threats. Firstly, secondary users' sensing reports that have to be sent to the fusion center are heavily correlated to their locations, thereby leading to the leakage of locations of secondary users in the process of reports transmission and aggregation. Moreover, malicious secondary users are likely to submit fake sensing reports or alter sensing reports of other secondary users, which finally result in a wrong aggregated result. To address these questions, we propose an efficient location privacy-preserving authentication scheme for cooperative spectrum sensing. To be specific, our scheme incorporates a reputation mechanism and enables reliable secondary users to participate in cooperative spectrum sensing. Selected users with pseudo IDs instead of real identities send encrypted sensing reports to the fusion center. This can eliminate the correlation between sensing reports and secondary users and prevent the fusion center from associating sensing reports with secondary users' real identities while decrypting and aggregating reports, thereby protecting the location privacy of secondary users. Besides, to ensure a true aggregated result, we utilize elliptic curve cryptography technique to verify the legitimacy of sensing reports when the fusion center receives them. Theoretical analyses show that the proposed scheme protects the location privacy of secondary users. Numerical results demonstrate that the proposed scheme brings less overhead than previous schemes.

INDEX TERMS Authentication, cooperative spectrum sensing, elliptic curve cryptography, location privacy-preserving, reputation mechanism.

I. INTRODUCTION

Radio spectrum is a very precious communication resource [1]. On one hand, with the application of new technologies such as 5th-Generation, Internet of Things (IoT), virtual reality, the number of wireless devices has tremendously increased, thus leading to a rapid expansion of demand for spectrum [2]–[4]. According to the report, 50 billion devices will be connected to the development of IoT by 2030 [5]. On the other hand, static spectrum allocation policies have led to lower spectrum resource utilization. A survey by the Federal Communications Commission (FCC) finds that the average utilization in the licensed spectrum band is currently around 30% [6]. Consequently, in the case of limited spectrum resources, how to improve the performance of spectrum utilization to meet people's spectrum needs has become the research goal of many scholars.

In 1999, Mitola and Maguire propose cognitive radio technology [7]. The characteristics of cognitive radio technology are that it can sense the wireless communication environment, and then obtain the unused spectrum information of authorized users through active learning, reasoning and decision-making within a period of time, and finally realize "secondary utilization of spectrum" without disturbing the authorized users. Cognitive Radio Networks (CRNs) is a network built on cognitive radio technology. In CRNs, there are two types of users: Primary Users (PUs) and Secondary Users (SUs). PUs are authorized users, and can

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

access their spectra at any time. SUs are unlicensed users. When a PU is off-line, a SU is allowed to access the PU's spectrum. On the arrival of PU, the SU needs to vacate the PU's spectrum immediately without disturbing the PU's transmission [8].

In CRNs, multiple SUs collaboratively explore spectrum availability information, called cooperative spectrum sensing [9]. Specifically, each SU senses the signal of a PU through energy detection [10], generates a sensing report (known as Received Signal Strength, RSS), and then sends it to the Fusion Center (FC). The FC aggregates these sensing reports, and then compares the aggregated result with the energy threshold value. If the result is larger than the threshold value, the spectrum is occupied by the PU, otherwise, the spectrum is in idle. It has been shown in [11] that sensing reports which are generally signal strength measurements of the TV spectrum are closely related to SUs' physical locations. If SUs directly submit sensing reports in the form of plaintext, it is likely to comprise their locations during transmission and aggregation. The experiment result in [11] shows that through the sensing report, the adversary can locate the victim's location with a probability of more than 90%. The fine-grained location information can be inferred a series of individual privacy including beliefs, preferences and behavior [12]. Noting such privacy threat, SUs are reluctant to participate in cooperative spectrum sensing, thereby discouraging CRNs.

In addition, malicious SUs may submit fake sensing reports and even alter sensing reports of other SUs, which results in a wrong aggregated result and cause interference to the PU.

To sum up, in cooperative spectrum sensing, we ought to consider three requirements: How to select reliable SUs to participate in spectrum sensing? How to protect the location privacy of selected SUs? How to verify the legitimacy of sensing reports? Consequently, we propose an efficient location privacy-preserving authentication scheme for cooperative spectrum sensing. The contributions of this paper are summarized as follows:

- In the proposed scheme, SUs with specified reputation score are allowed to participate in spectrum sensing. This can select reliable SUs for spectrum sensing in a way and therefore ensure the authenticity of sensing report at the source. Reputation scores of SUs is calculated according to the performance of SUs in previous spectrum sensing.
- In the proposed scheme, SUs with pseudo IDs instead of real identities send encrypted sensing reports to the FC, which eliminates the correlation between sensing reports and SUs and prevents the FC from correlating decrypted sensing reports with real identities of SUs, thereby protecting the location privacy of SUs. In addition, other adversaries can not know SUs' physical locations from encrypted sensing reports and thus protecting the location privacy of SUs.
- Besides, utilizing elliptic curve cryptography technique, the proposed scheme verifies the legitimacy of sensing reports. In this way, the FC receives legitimate reports and aggregates them to obtain true result.
- The proposed scheme has advantages over existing alternatives in communication cost and storage cost. And compared with other schemes, our scheme brings less computation cost on the FC side.

The rest of this paper is organized as follows. Section II overviews the related work about location privacy-preserving in cooperative spectrum sensing. In section III and section IV, we describe our scheme which consists of system model, threat models, design objectives and solution. In section V and section VI, we analyze our scheme from the aspects of safety and performance, and compare with other schemes. Finally, we conclude this paper in section VII.

II. RELATED WORK

In this section, we introduce existing solutions for SUs' location privacy-preserving in cooperative spectrum sensing.

In the context of cooperative spectrum sensing, Li *et al.* first discover the location privacy leakage of SUs [11]. They find that SUs' locations can be inferred with a high probability from SUs' sensing reports (i.e., observed RSS values) and call this the Single Report Location Privacy (SRLP) attack. Later, they also discover another attack and call it the Differential Location Privacy (DLP) attack, where the adversary can deduce the leaving or joining user's sensing report from the differences in the final aggregated results of sensing reports before and after a SU quits or joins cooperative spectrum sensing. To address these attacks, Li *et al.* propose a privacy-preserving spectrum sensing protocol. In this protocol, authors utilize secret share and privacy preserving aggregation [13] process to cope with the SRLP attack and dummy report injections to cope with the DLP attack. However, the protocol does not support fault tolerance [14], that is the FC can not perform fusion analysis if a single SU does not submit a sensing report. In addition, since any two SU need to share a set of key pairs, it will bring extra communication cost.

To protect the location privacy of SUs in CRNs, Mao *et al.* propose two schemes one after another. The first scheme [15], Cooperative Spectrum Sensing with Derivative ElGamal introduces a modified derivative ElGamal algorithm and a helper to prevent the FC from matching the affiliation of each sensing report while decrypting sensing reports. However, Mao *et al.* point out that this scheme is vulnerable to SU's malfunction as the helper is selected from internal SUs. Then they propose the second scheme [16], Cooperative Spectrum Sensing with Threshold Cryptosystem, to be more robust when facing single-point failure. This scheme utilizes a noninteractive threshold cryptosystem [17] to select t out of n SUs to decrypt the ciphertexts. However, for selected SUs, it is costly in communication cost and computation cost.

Mohamed *et al.* also propose two schemes to protect the location privacy of SUs in CRNs. The first scheme [18] combines order preserving encryption [19] and Yao's Millionaires protocol [20], where SUs encrypt their sensing reports using order preserving encryption, then send them to the FC. The FC runs Yao's Millionaires protocol to count the number of SUs' sensing reports above or below the threshold but can not learn each report. However, in the first scheme, the FC can still learn the order of encrypted RSS values of SUs. So in the second scheme [21], Mohamed *et al.* introduce a gateway to solve the deficiencies.

In addition to utilizing cryptography tools, researchers also use differential privacy to realize the location privacy-preserving of SUs in CRNs. Wang and Zhang [22] propose a privacy-preservation framework with multiple service providers in cooperative sensing. In this framework, each sensing report is transformed into a single value. Transformed values from a group of SUs are merged in a cloak. Each cloak will be perturbed by adding random noise to the number of SUs in the cloak. At last, the cloaks with noisy counts aggregated from all SPs can be taken as the input of general cooperative sensing schemes. However, when there are more FCs or fewer SUs, the privacy-preserving level will decline.

In our previous work, a scheme with fault tolerance is proposed to protect the location privacy of SUs [23]. We assign n secret keys for each sensing task, which the sum of n secret keys is 0, and then randomly assign one secret key out of n secret keys to each SU. SUs encrypt sensing reports by assigned secret keys. Finally, the FC aggregates encrypted sensing reports directly and obtains aggregated result without learning sensing report of each SU, therefore protecting the location privacy of SUs. Moreover, to verify the legitimacy of sensing reports, we provide an authentication mechanism for SUs' sensing reports, which do not be taken into account in other schemes.

Inspired by our previous work, we propose another location privacy-preserving scheme for cooperative spectrum sensing. Specifically, we protect the location privacy of SUs by eliminating the correlation between sensing reports and SUs. Besides, we utilize the authentication mechanism in [23] for SUs' sensing reports. What's more, the proposed scheme enables reliable SUs to participate in spectrum sensing by incorporating a reputation mechanism.

III. PRELIMINARIES

A. SYSTEM MODEL

Our system model is based on centralized cooperative spectrum sensing which is showed in FIGURE 1. In this model, there are three entities, the FC, the third party (TP), and SUs. The responsibility of each entity in the system is as follows.

- **FC**: The responsibilities of FC are to receive SUs' sensing reports, and then to analyze them to obtain the spectrum status of a PU.
- **TP**: The TP has strong computing power and sufficient storage and is authorized by the FCC [24]. In our system, the TP is responsible for generating system parameters and registering SUs. Additionally, the TP stores SUs' reputation scores and updates them after a spectrum sensing.

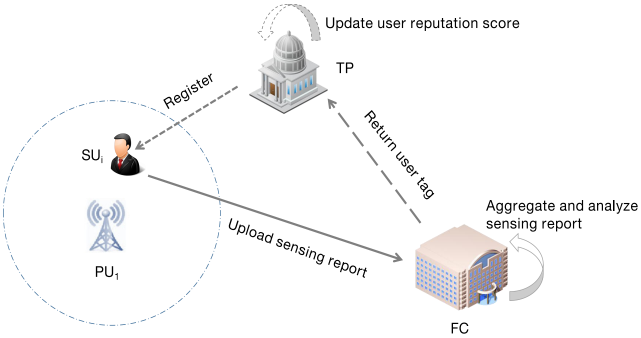
Update user reputation score
TP
Register
Return user tag
SU$_i$
Upload sensing report
PU$_1$
Aggregate and analyze sensing report
FC

FIGURE 1. System model.

- **SUs**: SUs provide the system with spectrum status of PUs. SUs usually carry smart devices that support spectrum sensing. The rewards that SUs receive through spectrum sensing are out of the scope of this paper.

The general process of our scheme is described as follows.

(1) The FC issues a sensing task in the system;

(2) If SUs intend to participate in the sensing task, they need to complete the registration process first with the help of the TP;

(3) When SUs register successfully, they start to perform spectrum sensing individually, and then generate sensing reports. According to [25], if SUs adopt the method of energy detection, generated sensing reports follow the distribution:

$$m_i = \begin{cases} \mathcal{N}\left(n_0, \dfrac{n_0^2}{M}\right), & \boldsymbol{H}_0 \\ \mathcal{N}\left(s_i + n_0, \dfrac{(s_i + n_0)^2}{M}\right), & \boldsymbol{H}_1 \end{cases} \tag{1}$$

where n_0 is the noise power, s_i is the SU_i's received signal power of a PU, and M is the number of signal samples. $\boldsymbol{H}_0$ represents the PU is off-line, whereas $\boldsymbol{H}_1$ represents the PU is on-line;

(4) SUs send sensing reports to the FC;

(5) The FC receives sensing reports and aggregates them as follows:

$$r = \sum_{i=1}^{n} w_i m_i, \tag{2}$$

in which w_i is the weight of m_i, r is the aggregated result. Without loss of generality, we adopt equal gain combination and set w_i to 1 [25].

(6) The FC compares r with the energy threshold δ, if $r \geq \delta$, it represents the channel is occupied by the PU, if $r < \delta$, it represents the channel is not occupied by the PU. Finally, the FC stores the PU's spectrum status in the database.

B. THREAT MODELS

In the context of cooperative spectrum sensing, we consider three types of adversary: the semi-honest FC, the semi-honest

TP, and malicious SUs. The behavior of each adversary is as follows.

- **Semi-Honest FC**: The semi-honest FC will obey his/her responsibilities (e.g., receives and analyzes sensing reports of SUs) but meanwhile be curious about the location of some SU in the system.
- **Semi-Honest TP**: The semi-honest TP will obey his/her resonbilities (e.g., generates system parameters, registers SUs and updates reputation scores of SUs) but meanwhile be curious about the location of some SU in the system.
- **Malicious SUs**: Malicious SUs have the following behavior: (1) To affect the final aggregated result and disrupt cooperative spectrum sensing, malicious SUs may send fake sensing reports to the FC; (2) Like the semi-honest FC and TP, malicious SUs may covet the location of other SU in the system and intercept the sensing report of other SU; (3) After obtaining the sensing report of other SU, malicious SUs may launch replay attacks and modification attacks (i.e., alter the sensing report of other SU and resend to the FC).

In cooperative spectrum sensing, adversaries learn locations of SUs mainly by obtaining sensing reports of SUs. What's more, it is generally recognized that the location privacy of SUs is disclosed if and only if adversaries associate locations (namely sensing reports) of SUs with their real identities. In the next section, we will define location privacy. Besides, we assume that the FC does not collude with the TP in our system.

C. DESIGN OBJECTIVES

Based on the aforementioned system model and threat models, the design objectives of the proposed scheme are as follows.

- **Location Privacy-Preserving**: The proposed scheme should protect the location privacy of each SU in the system. This objective is the most fundamental goal of our scheme. Here, we give the definition of location privacy as follows:

$$LP_i = \{RID_i, LOC_i\}, \tag{3}$$

  in which RID_i denotes the real identity of SU_i and LOC_i denotes the physical location of SU_i. In the previous section, we talk about that only when adversaries obtain SU_i's RID_i and LOC_i at the same time and associate them, can SU_i's location privacy be disclosed. Intuitively, the exposure of any one piece of information does not result in the disclosure of SU_i's location privacy.
- **Reputation Mechanism**: The proposed scheme should enable reliable SUs to participate in spectrum sensing so as to guarantee the authenticity of sensing reports at the source. Specifically, the proposed scheme gives each SU a reputation score based on the performance of previous spectrum sensing, and SUs with specified reputation score are allowed to participate in spectrum sensing.
- **Authentication**: The proposed scheme should verify the legitimacy of sensing reports. Specifically, when the FC receives sensing reports, it is necessary to verify the validity (to avoid replay attacks) and integrity (to avoid modification attacks) of sensing reports to obtain true aggregated result.
- **Fault Tolerance**: The proposed scheme should achieve fault tolerance. To be specific, when a group of SUs in the system do not submit sensing reports due to network failure, the FC can make a decision about spectrum opportunities based on the received sensing reports.
- **Dynamism**: The proposed scheme should achieve dynamism. To be specific, when a SU joins or leaves the system, the proposed scheme should allow the system to keep running. What's more, it does not pose a location privacy threat to the joining/leaving user.

D. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is employed in our scheme [26]. We now show the definition of ECC. Let F_p denote a finite prime field where p is a large prime and $p > 3$. An elliptic curve E over a finite prime field F_p is defined as follows:

$$y^2 = x^3 + ax + b \mod p, \tag{4}$$

where $a, b \in F_p$ and $4\,a^3 + 27\,b^2 \neq 0 \bmod p$. A cyclic additive group G consists of all points (x, y) on the elliptic curve E/F_p and a point at infinity. That is:

$$G = \left\{(x, y)|x, y \in F_p\ ,\ y^2 = x^3 + ax + b \bmod p)\right\} \cup \{\mathbf{O}\}. \tag{5}$$

Let P be a generator of G. Elliptic curve discrete logarithm problem [27] is defined as follows: for a random variable $x \in Z_q^*$, Given P and $x \cdot P$, it is difficult to find x in polynomial time.

IV. THE PROPOSED SCHEME

We present the proposed scheme which includes six phases: initialization phase, sensing task release phase, user registration phase, sensing report-encryption phase, sensing report-decryption phase, and sensing report-analysis phase. The notations used in our scheme are defined in TABLE 1.

A. INITIALIZATION PHASE

The initialization phase will generate some system parameters for later use and be executed only once. The initialization process is specified as follows.

(1) Based on Section $III - D$, The TP selects a random large prime p and determines the tuple $\left\{F_p, E/F_p, G, P\right\}$.

(2) The TP randomly selects $sk_{TP} \in Z_q^*$ as his/her secret key and keeps it secret. Meanwhile, the TP computes the corresponding public key $PK_{TP} = sk_{TP} \cdot P$.

TABLE 1. Notations used in the scheme.

Notation	Description
p, q	Large prime
F_p	A finite prime field
E/F_p	An elliptic curve E over a finite prime field F_p
G	A group composed of all points on E/F_p and a special point
P	A generator of G
Z_q^*	A multiplicative group of invertible integers modulo q
m_i	The sensing report of SU_i
γ	The length of a sensing report
H_1, H_2	Hash function, $H_1 : \{0,1\}^* \to Z_q^*$, $H_2 : \{0,1\}^* \to \{0,1\}^\gamma$
sk_{TP}	The secret key of the TP
PK_{TP}	The public key of the TP
sk_{FC}	The secret key of the FC
PK_{FC}	The public key of the FC
sk_i	The secret key of SU_i
PK_i	The public key of SU_i
n	The number of SUs participating in cooperative spectrum sensing
l_{ecc}	The key size of ECC
δ	Energy threshold
ξ_{id}	The boundary RSS value for $Task_{id}$
RID_i	The real identity of SU_i
PID_{i1}	The first part of SU_i's pseudo ID
PID_{i2}	The second part of SU_i's pseudo ID
T_i	The expiration date of the pseudo ID
U_i	SU_i's public key used for authentication
u_i	SU_i's secret key used for authentication
$Task_{id}$	The serial number of the sensing task
$Task_c$	The specified sensing channel for $Task_{id}$
$Task_t$	The specified sensing period for $Task_{id}$
$Task_m$	The number of SUs required for spectrum sensing
$Task_r$	The rule for $Task_{id}$
R_{id}	The radius of sensing area for $Task_{id}$
W	Set of SUs applying for registration
S	Set of SUs through application, $\|S\| = n$
Q	Set of participating SUs that succeed to submit sensing reports
P	Number set of participation
R	Set of reputation score
T	Tag set

(3) The TP determines two secure hash functions:

$$H_1 : \{0,1\}^* \to Z_q^*, \quad H_2 : \{0,1\}^* \to \{0,1\}^\gamma . \tag{6}$$

(4) The TP publishes system parameters:

$$\left\{F_p, E/F_p, G, P, PK_{TA}, H_1, H_2\right\} . \tag{7}$$

Based on the published system parameters, the FC randomly selects $sk_{FC} \in Z_q^*$ as his/her secret key and keeps it secret. Meanwhile, the FC computes the corresponding public key $PK_{FC} = sk_{FC} \cdot P$ and publishes it.

B. SENSING TASK RELEASE PHASE

The FC broadcasts sensing task $Task$ in the system. The sensing task can be described as $Task = \{Task_{id}, Task_c, Task_t, Task_m, Task_r, R_{id}\}$. Each notation's meaning is showed in TABLE 1. In order to improve the sensing accuracy and reduce the impact of collusion attacks, $Task_m$ should be large enough. Furthermore, we require that SU_i perform spectrum sensing in a circular area centered on the PU showed in FIGURE 2. Besides, this circual area should be large enough so as to prevent SU_i from directly exposing the location information while performing spectrum sensing. ξ_{id} is caluated by the FC and we will show its function later.

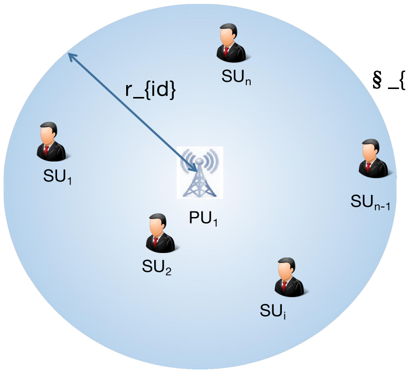

FIGURE 2. Sensing area.

Algorithm 1 Selection Algorithm

```
Input: $W, P, R$
Output: $S$
for each $W_i \in W$ and $P_i \in$ P do
    while $0 < P_i \leq 10$ do
        if $P_i \leq 5$ and $(R_i \geq 3 \vee R_i = P_i)$ then
            Application=True
            $P_i \leftarrow P_i + 1$
        else if $5 < P_i \leq 10$ and $R_i \geq 6$ then
            Application=True
            $P_i \leftarrow P_i + 1$
        end if
    end while
end for
if $SU_i \in W$ participates in task for the first time then
    Application=True
    $P_i \leftarrow 1$
end if
```

C. USER REGISTRATION PHASE

After receiving the system broadcast, if SU_i is interested in participating in sensing task $Task_{id}$, he or she first submits registration application to the TP. Based on the reputation score of SU_i, the TP decides whether to pass SU_i 's application. **Algorithm 1** shows the TP how to select reliable SUs.

On passing the application, SU_i starts to register with the assistance of the TP. The user registration phase mainly

TABLE 2. User information.

RID	PID	P	R
RID_1	$(PID_{11}^1, PID_{12}^1, T_1)$, ... ,$(PID_{11}^2, PID_{12}^2, T_1^2)$	2	1, 1
RID_2	$(PID_{21}, PID_{22}, T_2)$, ... ,$(PID_{21}^5, PID_{22}^5, T_2^5)$	5	1, 0, 1, 1, 1
...	...	...	...

includes two processes: generates pseudo ID for a SU and public/secret keys for subsequent authentication. SU's pseudo ID consists of two parts, one part is generated by SU himself and the other part is generated by the TP. We use *PID* to denote the pseudo ID. The concrete registration process is specified as follows.

(1) SU_i randomly selects $\alpha_i \in Z_q^*$ and computes the first part pseudo ID

$$PID_{i1} = \alpha_i \cdot P. \tag{8}$$

(2) SU_i sends $\{RID_i, PID_{i1}\}$ to the TP via a secure channel and stores α_i.

(3) On receiving the message $\{RID_i, PID_{i1}\}$ from SU_i, the TP utilizes $\{RID_i, PID_{i1}\}$ to construct the second part of the pseudo ID. the TP computes

$$PID_{i2} = RID_i \bigoplus H_1\left(PID_{i1}, sk_{TP} \cdot PID_{i1}, T_i\right). \tag{9}$$

In our scheme, $\{PID_{i1}, PID_{i2}\}$ can only be used once, in other words, once SU_i has applied for a pseudo ID from the TP, it can only be used for one sensing task.

(4) The TP generates public and secret keys for subsequent authentication for SU_i. The TP selects a random number $\beta_i \in Z_q^*$, then computes

$$U_i = \beta_i \cdot P \tag{10}$$

and

$$u_i = \beta_i + sk_{TP} \cdot H_1\left(PID_i, U_i\right). \tag{11}$$

(5) The TP sends $\{RID_i, PID_i, U_i, u_i\}$ to SU_i via a secure channel, where $PID_i = (PID_{i1}, PID_{i2}, T_i)$.

(6) The TP updates user information in TABLE 2.

So far, SU_i has registered successfully. SU_i can use (PID_i, U_i, u_i) to participate in the next process.

D. SENSING REPORT-ENCRYPTION PHASE

SU_i carring a device goes to the designated area and starts to execute task. After finishing sensing, SU_i obtains a sensing report m_i. Before sending it to the FC, SU_i performs the follwing actions.

(1) SU_i randomly selects $sk_i \in Z_q^*$ as his or her secret key and keeps it secret.

(2) SU_i computes the corresponding public key $PK_i = sk_i \cdot P$ and publishes it.

(3) SU_i computes

$$C_i = m_i \bigoplus H_2\left(sk_i \cdot PK_{FC}\right). \tag{12}$$

(4) SU_i computes

$$V_i = sk_i + u_i \cdot H_1\left(PID_i, U_i, PK_i, C_i, t_i\right), \tag{13}$$

in which t_i is the current timestamp.

(5) SU_i sends $\{PID_i, C_i, V_i, U_i, t_i\}$ to the FC via a public channel.

E. SENSING REPORT-DECRYPTION PHASE

Receiving the message $\{PID_i, C_i, V_i, U_i, t_i\}$ from SU_i, the FC performs the follwing actions.

(1) The FC judges

$$t_i' - t_i \leq \Delta t, \tag{14}$$

where Δt is the transmission delay and t_i' is the receiving time. This verification is to check the validity of the message. If the message is not sent within the specified receiving period Δt, then the FC discards this message and halts.

(2) The FC performs the second verification. The FC computes

$$W_i = U_i + PK_{TP} \cdot H_1\left(PID_i, U_i\right), \tag{15}$$

and then confirms whether the following equation holds or not:

$$V_i \cdot P = PK_i + W_i \cdot H_1\left(PID_i, C_i, U_i, PK_i, t_i\right). \tag{16}$$

This verification is to confirm the integrity of the message. If the equation does not hold, then the message has been modified and the FC discards this message and halts.

To reduce the computation cost, the FC can simultaneously verify the integrity of n messages as follows:

$$\begin{aligned}\sum_{i=1}^{n} V_i \cdot P &= \sum_{i=1}^{n} PK_i + \sum_{i=1}^{n} W_i \\ &\quad \cdot H_1(PID_i, C_i, U_i, PK_i, t_i) \\ &= \sum_{i=1}^{n} PK_i + \sum_{i=1}^{n} U_i \\ &\quad \cdot H_1(PID_i, C_i, U_i, PK_i, t_i) \\ &\quad + PK_{TP} \cdot \sum_{i=1}^{n} H_1(PID_i, U_i) \\ &\quad \cdot H_1(PID_i, C_i, U_i, PK_i, t_i)\end{aligned} \tag{17}$$

(3) The FC decrypts the message. The FC computes

$$m_i = C_i \bigoplus H_2\left(sk_{FC} \cdot PK_i\right). \tag{18}$$

and obtains sensing report of SU_i.

(4) The FC aggregates decrypted sensing reports as defined in Section III-A and stores the result of spectrum availability in the database.

F. SENSING REPORT-ANALYSIS PHASE

Apart from aggregating sensing reports, the FC analyzes each sensing report. That is by analyzing the authenticity of each sensing report, the FC evalutes each SU. Specifically, if $m_i \geq \xi_{id}$, it shows that SU_i offers legal sensing report, then the FC attaches a tag of $\{+1\}$ to SU_i; if $m_i < \xi_{id}$, it shows that SU_i offers fake sensing report, then the FC attaches a tag of $\{-1\}$ to SU_i. SUs use advanced smart devices, so the probability of erroneous results due to the malfunction of the devices is very small, and we will not consider them. The calcuation of ξ_{id} can refer to [28], [29]. Finally, the FC sends $\{PID_i, TAG_i\}$ to the TP via a secure channel.

According to **Algorithm 2**, the TP computes the reputation score of SU_i and updates TABLE 2. Besides, the records in the table are cleared every 10 times. If the TP does not receive the tag of SU_i from the FC, it means SU_i fails to participate in the sensing task, then the TP removes the registration record of SU_i at this time.

Algorithm 2 Reputation Assessment Algorithm

```
Input: $S, P, T$
Output: $R$
for each $SU_i \in S$ do
    if $P_i = 1$ then
        initialize $R_i \leftarrow 0$
        $R_i \leftarrow R_i + T_i$
    else if $1<P_i \leq 10$ then
        $R_i \leftarrow R_i + T_i$
    else if $P_i>10$ then
        $R_i \leftarrow T_i$
    end if
end for
```

V. SECURITY ANALYSIS

In this section, we analyze the security of the proposed scheme. Moreover, we compare our scheme with other schemes from five aspects which showed in TABLE 3.

- **Location Privacy-Preserving**: The location privacy-preserving of SUs is the most fundamental goal of our scheme. In Section III-B, we have described three adversaries who covet SUs' locations. Now we introduce in detail how the proposed scheme avoids three adversaries.
    - SU_i with a pseudo ID submits encrypted sensing report to the FC. The FC can obtain the sensing report of SU_i for aggregating through decryption. To some extent, the FC knows the physical location LOC_i of SU_i. However, the FC just knows the pseudo ID of SU_i but can not know the real identity RID_i of SU_i. The reasons are as follows. The pseudo ID of SU_i is generated by SU_i and the TP together, which consists of RID_i of SU_i. In order to learn the RID_i of SU_i, the FC needs to obtain sk_{TP}, PID_{i1} and T_i, then solves the formula $PID_{i2} = RID_i \bigoplus H_1(PID_{i1}, sk_{TP} \cdot PID_{i1}, T_i)$. As sk_{TP} is kept secret in the TP, it is impossible for the FC to obtain sk_{TP}. What's more, T_i and PID_{i1} are only known to SU_i and the TP. As the FC and the TP does not collude, the FC can not know T_i and PID_{i1}. According to the definition of location privacy defined in Section III-C, the FC just obtains SU_i's LOC_i but no RID_i, That is, SU_i's location privacy is protected.
    - The TP owns the real identity RID_i of SU_i. To get the physical location LOC_i of SU_i, the TP needs to know the sk_i of SU_i first, and then solves the formula $C_i = m_i \bigoplus H_2(sk_i \cdot PK_{FC})$. As sk_i is kept secret in SU_i, it is impossible for the TP to learn sk_i. Thus, the location privacy of SU_i is protected.
    - Other SU can not learn the location of SU_i through the pseudo ID of SU_i and encrypted sensing reports.
- **Reputation Mechanism**: The FC analyzes the authenticity of each sensing report and sends a tag (e.g., "+1" represents SU_i offers legal sensing report, "−1" represents SU_i offers fake sensing report) to the TP. Then the TP updates reputation scores of SUs based on the tag of each SU. According to reputation scores of SUs, the proposed scheme selects reliable SUs.
- **Authentication**: After receiving $\{PID_i, C_i, V_i, U_i, t_i\}$, the FC verifies the legitimacy of message twice. The first verification is to resist replay attacks, and the second verification is to resist modification attacks. Two verifications are to ensure that the sensing report is completely sent by the SU without any blocking.
    - **Prevention of Replay Attacks**: In order to resist replay attacks, we require that SUs add a timestamp to the message before sending it to the FC. The timestamp can help the FC to judge whether the message was replayed and determine whether to discard the message. Specifically, when receiving $\{PID_i, C_i, V_i, U_i, t_i\}$ from SU_i, the FC verifies $t_i' - t_i \leq \Delta t$. Once the message is sent outside the period Δt, then the FC discards it.
    - **Prevention of Modification Attacks**: In order to resist modification attacks, we require that SUs calculate $V_i = sk_i + u_i \cdot H_1(PID_i, U_i, PK_i, C_i, t_i)$ while encrypting sensing reports and send V_i to the FC. After receiving the message $\{PID_i, C_i, V_i, U_i, t_i\}$, the FC calculates $W_i = U_i + PK_{TP} \cdot H_1(PID_i, U_i)$ and then verifies the equation $V_i \cdot P = PK_i + W_i \cdot H_1(PID_i, C_i, U_i, PK_i, t_i)$. Through this equation, we know that no matter which value in the message is modified by the adversary, the equation does not hold, so the FC discards this message. Conversely, if the equation holds, the FC judges that the message is complete and receives this message.

TABLE 3. Comparison with other schemes.

Scheme	Location Privacy	Fault Tolerance	Dynamism	Authentication	Reputation Mechanism
Li et al. [11]	✓	×	×	×	×
Mao et al. [15]	×	✓	✓	×	×
Mao et al. [16]	✓	✓	×	×	×
Zeng et al. [23]	✓	✓*	✓	✓	✓*
Ours	✓	✓	✓	✓	✓

* In Section V, we will analyze advantages of the proposed scheme in fault tolerance and reputation mechanism.

- **Fault Tolerance**: Based on the definition of fault tolerance defined in Section III-C, the proposed scheme achieves fault tolerance. On receiving encrypted sensing report C_i, the FC computes as follows: $m_i = C_i \bigoplus H_2 (sk_{FC} \cdot PK_i)$. It means that the FC decrypts C_i using sk_{FC} and PK_i, that is, when a group of SUs do not submit sensing reports, the FC can still decrypt the received sensing reports and aggregate them. All in all, unsubmitted sensing reports do not affect the final aggregated process.
- **Dynamism**: When a SU joins/leaves cooperative spectrum sensing, the adversary can deduce the joining/leaving user's sensing report from the differences in the final aggregated results. However, since the SU participates in spectrum sensing under a pseudo ID and the pseudo ID can only be used once, the adversary can not associate the sensing report with the real identity of SU, then the location privacy of the joining/leaving user is protected.
- **Comparison with Other Schemes**: From five aspects, we compare the proposed scheme with previous schemes. As we can see in TABLE 3, we know that our scheme has five functions and is superior to the schemes proposed in [11], [15], [16]. Besides, our scheme has the exact same function as Zeng *et al*'s [23]. However, our scheme gets its advantages in fault tolerance and reputation mechanism. When a group of SUs fail to submit sensing reports, Zeng *et al*'s brings more computation cost than ours on the FC side. In terms of reputation mechanism, Zeng *et al.* evaluate the reputation scores of SUs based on the completion of the task. Specifically, if a SU completes the sensing task, his/her reputation score increases by 1, otherwise the reputation score decreases by 1. But in our scheme, we use the authenticity of sensing reports to evaluate the reputation values of SUs.

VI. PERFORMANCE EVALUATION

In this section, we analyze the computation cost, communication cost, and storage cost of the proposed scheme. In addition, we also compare the performance of our scheme with the schemes proposed in [11], [15], [16] and [23].

A. COMPUTATION COST

We use symbols to denote different cryptographic operations. According to [23], the running time of each cryptographic operation is showed in TABLE 4. Besides, owing to the running time of one xor operation is very short, the proposed scheme does not consider the computation cost. The computation cost of each phase is as follows.

TABLE 4. Running time of different calculation operations.

Notation	Description	Running Time (ms)
C_{em}	Elliptic curve point multiplication	1.567
C_{ea}	Elliptic curve point addition	0.041
C_m	Modular multiplication	0.014
C_a	Modular addition	0.004
C_{exp}	Modular exponentiation	2.892
C_{inv}	Modular inverse	0.366
C_h	Hash function	0.001
C_{bp}	Bilinear pairing	4.916

(1) In the user registration phase, each SU performs one elliptic curve point multiplication operation, and the TP performs one elliptic curve point multiplication operation, one hash operation, and one modular addition operation. Therefore, the computation cost of one SU is C_{em}. For n SUs, the computation cost of the TP is $2 \cdot n \cdot C_{em} + 2 \cdot n \cdot C_h + C_m \cdot n + C_a \cdot n$.

(2) In the sensing report-encryption phase, only SUs are involved. Each SU performs two elliptic curve point multiplication operations, two hash operations, and one modular addition operation. Therefore, the computation cost of one SU is $C_{em} + 2 \cdot C_h + C_m + C_a$.

(3) In the sensing report-decryption phase, only the FC participates in the decryption process. To decrypt a sensing report, the FC performs three hash operations, one elliptic curve point multiplication operation, and one modular addition operation. If the FC simultaneously verifies the integrity of n messages, to obtain the final aggregated result, the total computation cost of the FC is $(2n+1)C_{em}+(3n-1)C_{ea}+n\cdot C_m+(2n-2)C_a+3n\cdot C_h$.

Now we compare the computation cost of the proposed scheme with other schemes in terms of the FC and one SU in TABLE 5, FIGURE 3, FIGURE 4, and FIGURE 5.

FIGURE 3 shows the comparison of computation cost on SU side. From FIGURE 3, we can see that the computation cost of the proposed scheme is lower than the schemes pro-

TABLE 5. Computation cost in different schemes.

Scheme	Computation Cost	
	SU	FC
Li et al. [11]	$2C_{exp} + C_m + C_h$	$2^{\gamma-1} \cdot n \cdot C_{exp} + (n+1)\, C_m + C_h$
Mao et al. [15]	$2C_{exp} + C_m$	$n\,(C_{exp} + C_{inv})C_m)$
Mao et al. [16]	$4C_{exp} + C_m + C_h$	$(2n+2t)\, C_{bp} + n \cdot C_{exp} + (n + t^* - 1)\, C_m + C_h$
Zeng et al. [23]	$C_{em} + C_m + 3C_a + 2C_h$	$(3n+1)\, C_{em} + (3n-1)\, C_{ea} + n \cdot C_m + (3n-2)\, C_a + 4n \cdot C_h$
Ours	$2C_{em} + C_m + C_a + 2C_h$	$(2n+1)C_{em} + (3n-1)C_{ea} + n \cdot C_m + (2n-2)C_a + 3n \cdot C_h$

* t is the threshold in Mao et al. [16].

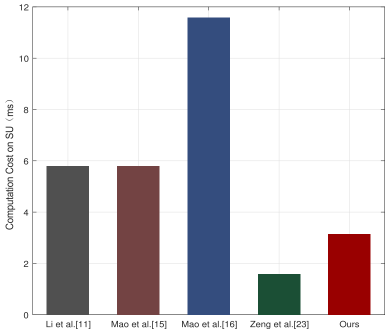

FIGURE 3. Comparison of computation cost on SU side.

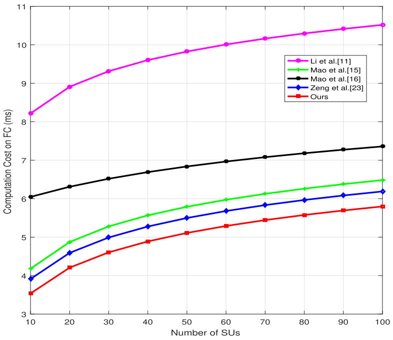

FIGURE 4. Comparison of computation cost on FC side of five schemes.

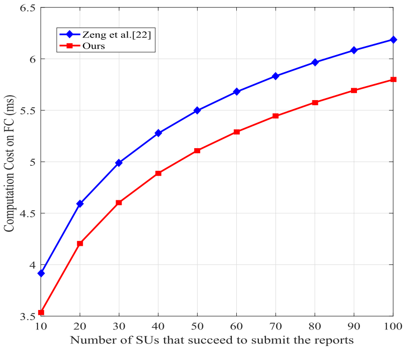

FIGURE 5. Comparison of computation cost on FC side of two schemes.

posed in [11], [15] and [16]. That is because Li *et al.* [11], Mao *et al.* [15], and Mao *et al.* [16] need to execute at least two modular exponentiation operations, and our scheme requires two elliptic curve point multiplication operations. As shown in TABLE 4, one modular exponentiation operation costs more than one elliptic curve point multiplication operation. In addition, our scheme's computation cost on SU side is slightly higher than Zeng *et al.*'s [23]. This is due to the fact that SUs need to execute extra one elliptic curve point multiplication operation to generate the first part of pseudo ID in the proposed scheme, however, in Zeng *et al.*'s [23], SU's pseudo ID is completely generated by the TP. From a security perspective, it is safer that the pseudo ID is generated by SU and the TP together. In case the TP disguises as the SU_i and sends fake sensing report to the FC, then the FC can remove the TP's delivery by comparing the part of the pseudo ID generated by SU_i.

FIGURE 4 shows the comparison of computation cost on FC side, where we set $\gamma = 8$, $t = 30$. From FIGURE 4, we know that our scheme brings less computation cost compared with Li *et al.*'s [11], Mao *et al.*'s [15], Mao *et al.*'s [16], and Zeng *et al.*'s [23].

When a group of SUs fail to send sensing reports to the FC, to obtain the aggregated result, the computation cost of FC in Zeng *et al.*'s [23] is $(3\,|Q| + 1)C_{em} + (3\,|Q| - 1)C_{ea} + |Q| \cdot C_m + (3\,|Q| - 1)C_a + 4\,|Q| \cdot C_h$, and the computation cost of the FC in our scheme is $(2\,|Q| + 1)C_{em} + (3\,|Q| - 1)C_{ea} + |Q| \cdot C_m + (2\,|Q| - 2)C_a + 3\,|Q| \cdot C_h$. We show the comparison result in FIGURE 5. From FIGURE 5, we know that our scheme brings less computation cost when a group of SUs fail to submit sensing reports.

B. COMMUNICATION COST

We assume that RID_i, T_i, t_i are 32 bits, respectively. q is 160 bits. The communication cost of each phase is as follows.

(1) In the user registration phase, SU_i sends $\{RID_i, PID_{i1}\}$ to the TP, resulting in a communication cost of $32 + 2 \cdot l_{ecc}$. Therefore, the total communication cost of n SU is $32 \cdot n + 2 \cdot n \cdot l_{ecc}$. The TP sends $\{RID_i, PID_i, U_i, u_i\}$ to SU_i, so for n SUs, the total communication cost of the TP is $32 \cdot n + 2 \cdot n \cdot l_{ecc} + 160 \cdot n + 32 \cdot n + 2 \cdot n \cdot \text{ł}_{ecc} + 160 \cdot n$.

(2) In the sensing report-encryption phase, SU_i sends $\{PID_i, C_i, U_i, t_i\}$ to the FC, so the total communication cost generated by n SU is $2 \cdot n \cdot l_{ecc} + 160 \cdot n + 32 \cdot n + n \cdot \gamma + 2 \cdot n \cdot l_{ecc} + 32 \cdot n$.

TABLE 6. Communication cost in different schemes.

Scheme	Communication Cost (bits)
Li et al. [11]	$n \cdot \lvert\widetilde{p}\rvert^*$
Mao et al. [15]	$4 \cdot n \cdot \lvert\widetilde{p}\rvert$
Mao et al. [16]	$(5 \cdot n + 2 \cdot) \cdot \lvert\widetilde{p}\rvert$
Zeng et al. [23]	$n \cdot (544 + 4 \cdot l_{ecc}) + 160 \cdot n$
Ours	$648 \cdot n + 10 \cdot n \cdot \gamma$

[*] $\widetilde{p}$ denotes security parameter.

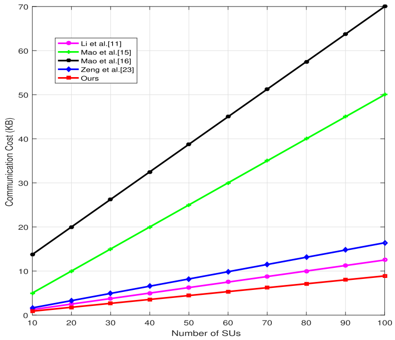

FIGURE 6. Comparison of total communication cost.

FIGURE 6 shows the comparison of total communication cost in different schemes, where we set $\gamma = 8$ *bits*, $|\widetilde{p}| = 1024$ *bits*. As we can see from FIGURE 6, our scheme is the most efficient one of these schemes in computation cost. In contrast, Mao *et al.* [16] brings the highest communication cost as selected t SUs are required to receive all sensing reports from each SU.

C. STORAGE COST

The physical storage performance of the FC and the TP is strong, and the devices carried by SUs generally do not support large-capacity storage. Therefore, in this paper, we only analyze the storage cost of SUs. In our scheme, each SU stores $\{P, PID_{i2}, T_i, U_i, u_i, PK_{FC}\}$, so the storage cost of one SU is $2 \cdot l_{ecc} + 160 + 32 + 2 \cdot l_{ecc} + 160 + 2 \cdot l_{ecc}$.

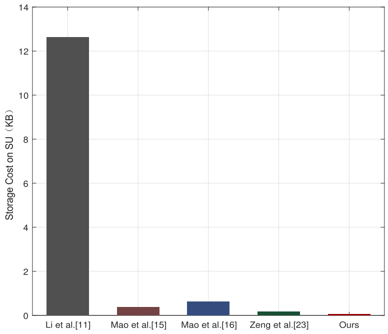

FIGURE 7. Comparison of storage cost on SU side of five schemes.

TABLE 7. Storage cost of a SU in different schemes.

Scheme	Storage Cost (bits)
Li et al. [11]	$(n+1)\,\lvert\widetilde{p}\rvert$
Mao et al. [15]	$3 \cdot \lvert\widetilde{p}\rvert$
Mao et al. [16]	$5 \cdot \lvert\widetilde{p}\rvert$
Zeng et al. [23]	$480 + 6 \cdot l_{ecc}$
Ours	$8\gamma + 352$

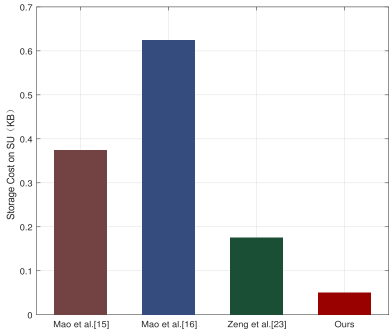

FIGURE 8. Comparison of storage cost on SU side of four schemes.

FIGURE 7 shows the comparison of storage cost on SU side among five schemes. Moreover, we use FIGURE 8 to show more clearly between Mao *et al.* [15], Mao *et al.* [16] Zeng *et al.* [23], and our scheme. From two figures, we can see that the storage cost of our scheme is the lowest in terms of SU side. In Li *et al.*'s [11], each SU needs to storage $n - 1$ pairwise secret keys, so it requires the largest storage space among five schemes.

All in all, our scheme has advantages over existing schemes in terms of communication and storage cost. For the computation cost, the pseudo ID of a SU is generated by the SU in cooperation with the TP in our scheme, so our scheme is not optimal.

VII. CONCLUSION

To protect the location privacy of SUs in cooperative spectrum sensing, we propose a scheme where it adopts a pseudonym method and thus eliminates the correlation between sensing reports and SUs. In addition, to guarantee a true aggregated result, the proposed scheme enables reliable SUs to participate in spectrum sensing by incorporating a reputation mechanism and utilizes elliptic curve cryptography technique to verify the legitimacy of reports. Security analyse show that our scheme not only protects the location privacy of SUs, but also resists various attacks. Performance analyse shows that the feasibility of our scheme in various metrics.

In future work, we will study distributed cooperative spectrum sensing model and consider how to use blockchain technology to achieve our research goals.

REFERENCES

[1] R. B. Chaurasiya and R. Shrestha, "Fast sensing-time and hardware-efficient eigenvalue-based blind spectrum sensors for cognitive radio network," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 4, pp. 1296–1308, Apr. 2020.

[2] R. Struzak, "Cognitive radio, spectrum, and evolutionary heuristics," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 166–171, Jun. 2018.

[3] W. Yang, M. Wang, J. Zhang, J. Zou, M. Hua, T. Xia, and X. You, "Narrowband wireless access for low-power massive Internet of Things: A bandwidth perspective," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 138–145, Jun. 2017.

[4] X. Liu, M. Jia, X. Zhang, and W. Lu, "A novel multichannel Internet of Things based on dynamic spectrum sharing in 5G communication," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5962–5970, Aug. 2019.

[5] W. S. H. M. W. Ahmad, N. A. M. Radzi, F. S. Samidi, A. Ismail, F. Abdullah, M. Z. Jamaludin, and M. N. Zakaria, "5G technology: Towards dynamic spectrum sharing using cognitive radio networks," *IEEE Access*, vol. 8, pp. 14460–14488, 2020.

[6] A. Al-Saadi, R. Setchi, and Y. Hicks, "Semantic reasoning in cognitive networks for heterogeneous wireless mesh systems," *IEEE Trans. Cognit. Commun. Netw.*, vol. 3, no. 3, pp. 374–389, Sep. 2017.

[7] J. Mitola, III, and G. Q. Maguire, Jr., "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[8] B. Hamdaoui, "Adaptive spectrum assessment for opportunistic access in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 922–930, Feb. 2009.

[9] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Phys. Commun.*, vol. 4, no. 1, pp. 40–62, Mar. 2011.

[10] O. Fatemieh, A. Farhadi, R. Chandra, and C. A. Gunter, "Using classification to protect the integrity of spectrum measurements in white space networks," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, California, USA, 2011.

[11] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen, "Location privacy preservation in collaborative spectrum sensing," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 729–737.

[12] W. Wang and Q. Zhang, *Location Privacy Preservation in Cognitive Radio Networks* (Springer Briefs in Computer Science). Springer, 2014.

[13] E. Shi, T. H. Chan, E. G. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, 2011.

[14] T. H. Chan, E. Shi, and D. Song, "Privacy-preserving stream aggregation with fault tolerance," in *Proc. 16th Int. Conf. Financial Cryptogr. Data Secur. (FC)*, Kralendijk, Bonaire, 2012, pp. 200–214.

[15] Y. Mao, T. Chen, Y. Zhang, T. Wang, and S. Zhong, "Protecting location information in collaborative sensing of cognitive radio networks," in *Proc. 18th ACM Int. Conf. Model., Anal. Simulation Wireless Mobile Syst. (MSWiM)*, Cancun, Mexico, 2015, pp. 219–226.

[16] Y. Mao, T. Chen, Y. Zhang, T. Wang, and S. Zhong, "Towards privacy-preserving aggregation for collaborative spectrum sensing," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1483–1493, Jun. 2017.

[17] B. Libert and M. Yung, "Non-interactive CCA-secure threshold cryptosystems with adaptive security: New framework and constructions," in *Proc. 9th Theory Cryptogr. Conf. Theory Cryptogr. (TCC)*, Taormina, Sicily, Italy, 2012, pp. 75–93.

[18] M. Grissa, A. Yavuz, and B. Hamdaoui, "LPOS: Location privacy for optimal sensing in cognitive radio networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[19] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-preserving symmetric encryption," in *Proc. 28th Annu. Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT)*, A. Joux, Ed. Cologne, Germany, 2009, pp. 224–241.

[20] A. C. Yao, "Protocols for secure computations (extended abstract)," in *Proc. 23rd Annu. Symp. Found. Comput. Sci.*, Chicago, IL, USA, 1982, pp. 160–164.

[21] M. Grissa, A. Yavuz, and B. Hamdaoui, "An efficient technique for protecting location privacy of cooperative spectrum sensing users," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, San Francisco, CA, USA, Apr. 2016, pp. 915–920.

[22] W. Wang and Q. Zhang, "Privacy-preserving collaborative spectrum sensing with multiple service providers," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1011–1019, Feb. 2015.

[23] Y. Zeng, L. Xu, X. Yang, X. Yi, and I. Khalil, "Privacy-preserving aggregation for cooperative spectrum sensing," *J. Netw. Comput. Appl.*, vol. 140, pp. 54–64, Aug. 2019.

[24] R. Zhu, L. Xu, Y. Zeng, and X. Yi, "Lightweight privacy preservation for securing large-scale database-driven cognitive radio networks with location verification," *Secur. Commun. Netw.*, vol. 2019, pp. 9126376:1–9126376:12, Jan. 2019.

[25] A. W. Min, K. G. Shin, and X. Hu, "Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation," *IEEE Trans. Mobile Comput.*, vol. 10, no. 10, pp. 1434–1447, Oct. 2011.

[26] D. Hankerson and A. Menezes, "Elliptic curve cryptography," in *Encyclopedia of Cryptography and Security*, 2nd ed. Springer, 2011, p. 397.

[27] D. Hankerson and A. Menezes, "Elliptic curve discrete logarithm problem," in *Encyclopedia of Cryptography and Security*, 2nd ed. Springer, 2011, pp. 397–400.

[28] Z. Wei, Z. Feng, Q. Zhang, and W. Li, "Three regions for space–time spectrum sensing and access in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2448–2462, Jun. 2015.

[29] S. Chen, B. Shen, X. Wang, and S.-J. Yoo, "Geo-location information aided spectrum sensing in cellular cognitive radio networks," *Sensors*, vol. 20, no. 1, p. 213, Dec. 2019.

HUIBIN LAI received the B.S. degree from Fujian Normal University, China, in 2018, where she is currently pursuing the M.S. degree with the College of Mathematics and Informatics. Her main research interests include security and privacy in cognitive radio networks.

LI XU (Member, IEEE) received the B.S. and M.S. degrees in mathematics from Fujian Normal University, in 1992 and 2001, respectively, and the Ph.D. degree in information and communication engineering from the Nanjing University of Posts and Telecommunications, in 2004.

He is currently a Professor and a Ph.D. Supervisor with the College of Mathematics and Informatics, Fujian Normal University. He is also the Director of the Information Construction and Management Office and the Key Laboratory of Network Security and Cryptography in Fujian Province. He has authored or coauthored over 150 papers in refereed journals and conferences, including the IEEE TRANSACTIONS ON COMPUTER, *ACM Transactions on Sensor Network*, the IEEE TRANSACTIONS ON RELIABILITY, the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, *Information Science*, and *Computer Network*. His research interests include wireless networks and communication, network optimization and information security, complex networks and systems, and intelligent information in communication networks.

Dr. Xu is also a member of ACM, and a Senior Member of CCF and CIE in China. He has been invited to act as the PC Chair or a member in more than 30 international conferences.

YALI ZENG received the B.S., M.S., and Ph.D. degrees from Fujian Normal University, China, in 2013, 2016, and 2020, respectively. Her main research interests include security and privacy in cognitive radio networks.