LPOS: Location Privacy for Optimal Sensing in Cognitive Radio Networks

Mohamed Grissa[*], Attila Yavuz[*], and Bechir Hamdaoui[*]

[*]Oregon State University, grissam,yavuza,hamdaoub@onid.oregonstate.edu

Abstract—**Cognitive Radio Networks (CRNs) enable opportunistic access to the licensed channel resources by allowing unlicensed users to exploit vacant channel opportunities. One effective technique through which unlicensed users, often referred to as Secondary Users (SUs), acquire whether a channel is vacant is cooperative spectrum sensing. Despite its effectiveness in enabling CRN access, cooperative sensing suffers from location privacy threats, merely because the sensing reports that need to be exchanged among the SUs to perform the sensing task are highly correlated to the SUs' locations. In this paper, we develop a new *Location Privacy for Optimal Sensing (LPOS)* scheme that preserves the location privacy of SUs while achieving optimal sensing performance through voting-based sensing. In addition, *LPOS* is the only alternative among existing CRN location privacy preserving schemes (to the best of our knowledge) that ensures high privacy, achieves fault tolerance, and is robust against the highly dynamic and wireless nature of CRNs.**

I. Introduction

Cognitive Radio Networks (CRNs) have emerged as a key technology for improving spectrum utilization through opportunistic spectrum access. They do so by allowing unlicensed spectrum users, often referred to as Secondary Users (SUs), to identify and exploit unused opportunities of licensed channels, so long as they do not cause any interference to licensed users, often referred to as Primary Users (PUs) [1].

Two main approaches can be used by SUs to acquire whether PUs are present in a licensed channel [2]. The first approach is based on geo-location databases and is very similar to what is used in LBSs (location-based services). The second approach, referred to as cooperative spectrum sensing, relies on the SUs themselves to visit and sense the licensed channels, on a regular basis, to collaboratively decide whether a channel is vacant or not. In this paper, we focus on the cooperative spectrum sensing approach whose general architecture is shown in Fig. 1. In this architecture, the Fusion Center (FC) is the entity responsible for orchestrating the SUs to perform the sensing task so as to collectively decide whether PUs are present or not. Through a control channel, FC queries SUs, each having sensing capability, to tune to specific channels/frequencies, measure the energy level (known as Received Signal Strength (RSS)) observed in each of these channels, and report the observed RSS values back to FC[1]. FC then first combines the RSS values collected from the different SUs and then compares the combined value against a detection threshold, τ, to decide whether a channel is available. Channel availability decisions are sent back to the SUs to rely on during their opportunistic spectrum access.

[1]Energy detection is the most popular method for signal detection due to its simplicity and small sensing time [3].
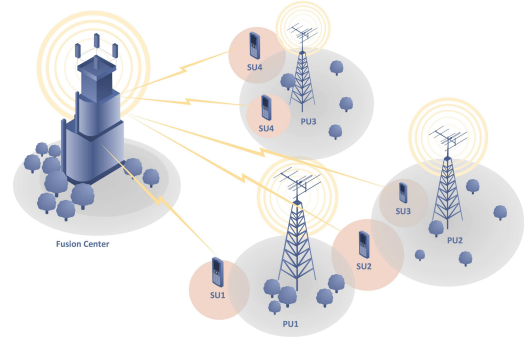

Fig. 1: Cooperative spectrum sensing architecture

Despite its effectiveness in improving sensing performance, cooperative sensing suffers from many security and privacy threats that make SUs shy away from participating in the cooperative sensing task. One of these threats is location disclosure. Cooperative spectrum sensing exploits spatial diversity for enhancing accuracy of sensing and this can jeopardize the location privacy of SUs. It has been shown in [4] that RSS values are heavily correlated to the SUs' physical locations, thus making it not too difficult to compromise the location privacy of SUs. Disclosing the location information is undesirable especially when FC is run by an untrusted service provider [5]. The fine-grained location data can be used to determine a lot of information about an individual's beliefs, preferences, and behavior [6]. In fact, by analyzing location traces of a user, an adversary can learn that he/she regularly goes to a hospital, and may then sell this information to pharmaceutical advertisers without the user's consent. In addition, malicious adversaries with criminal intent could use this information to pose a threat to an individual's security and privacy. Being aware of such potential privacy risks, SUs may not want to share their data with FC s or databases [6], making the need for preserving the location privacy of these users of a high importance.

This paper addresses the SUs' location disclosure threat, considered as one of the most important threats to CRN users' privacy, by designing a protocol that guarantees a high location privacy by concealing the RSS values from FC while enabling optimal sensing using the half-voting rule proposed in [7].

A. Related Work

Although lots of research efforts have already been made when it comes to addressing issues related protocol design [8], resource optimization [9]–[11], spectrum sensing [2], and performance modeling and analysis [12], [13], very little has been made in regards to location privacy issues [4], [14]. For instance, Shuai Li et al. [4] showed that location information of SUs could be inferred from the sensing reports, and called this attack Single

CR Report Location Privacy (SRLP) attack. Another attack in the same context occurs when a user joins or leaves the network. Any malicious entity can estimate the report of a user and hence its location from the variations in the final aggregated RSS measurements when the node joins and leaves the network. This is termed Differential Location Privacy attack. To cope with these attacks, the authors propose *PPSS*, a Privacy Preserving collaborative Spectrum Sensing protocol, that uses secret sharing and the Privacy Preserving Aggregation (PPA) process to hide the content of specific sensing reports. It also uses dummy report injections to cope with the Differential Location Privacy attack. However, *PPSS* has several limitations. First, it requires all the sensing reports in order to decode the aggregated result, which makes it quite impractical since the wireless channel may be unreliable, making some sensing reports not accessible by FC. Hence, FC will not be able to decrypt the aggregated sensing result. Moreover, it cannot cope with the dynamics resulting when multiple users join or leave the network simultaneously. In addition, the pairwise secret sharing process incurs extra communication overhead, which results in an additional delay especially when all the keys need to be updated when a user joins or leaves the network. Also, the encryption scheme used here is practical only when the plaintext space is small, since the decryption of the aggregated result requires solving the DLP problem, which is very costly as shown in Table II.

Despite the importance of this issue and the potential that CRNs present, little attention has been paid to this problem. This drove us to look outside the context of CRNs and try to find an approach that might be applied to our setup. We were particularly interested in the work proposed by Chen et al. [14] where they present a privacy-preserving data aggregation scheme with fault tolerance for smart grid communications, termed *PDAFT*. They considered a setting very similar to the one we study in this work, and tried to preserve users' privacy when smart meters installed within each house sense the consumption information and send it to the control center.

PDAFT combines Paillier cryptosystem with Shamir's secret sharing, where a set of smart meters sense the consumption of different households, encrypt their reports using Paillier, then send them to a gateway. The gateway multiplies these reports and forwards the result to the control center, which selects a number of servers (among all servers) to cooperate in order to decrypt the aggregated result. However, *PDAFT* requires a dedicated gateway to collect the encrypted data and a minimum number of working servers in the control center to be able to decrypt the aggregated result. In addition, *PDAFT*, like most of the aggregation-based methods, is prone to differential attacks that we mentioned earlier, and does not provide a mechanism that prevents this attack. Another drawback, which is common to simple aggregation-based methods, is that they usually do not provide optimal sensing performance and might be affected by the distribution of the RSS values. Throughout this paper, by optimal sensing we mean final decision accuracy regrading the channel availability.

B. Our Contribution

We developed *LPOS*, a new location privacy for optimal sensing scheme in CRNs. Its main idea lies in enabling privacy-preserving comparison of RSS values and FC's threshold in an efficient manner via a novel integration of Order Preserving Encryption (OPE) [15] and Yao's Millionaires' protocol [16]. We summarize the key features of our scheme below, compare it in Table I to other schemes, and give detailed performance analysis and comparison in Section V.

The key features of *LPOS* are:

1) Optimal Sensing: To the best of our knowledge, *LPOS* is the first scheme that enables location privacy in CRNs with an optimal spectrum sensing performance. It does so by privacy-preserving realization of the *half-voting* rule proposed in [7], which has been shown to be the optimal decision rule for spectrum sensing using energy detection. Unlike aggregation methods that may be vastly impacted by the distribution of RSS values (and misleading FC to make inaccurate decisions), this rule enjoys an optimal sensing performance.

2) High Location Privacy: Unlike some aggregation type protocols [4], [14], *LPOS* does not leak RSS information when users join/leave the network, nor does it require dummy report injection to prevent differential attacks as done in [4].

3) Fault Tolerance: In our scheme, if some users cannot sense the channels or fail to send their reports, FC only needs to update the voting threshold, λ, with the available users to make an accurate decision. However, some existing schemes cannot handle such failures. For example, *PPSS* [4] requires inputs from all (pre-determined) users to be able to decrypt the aggregated RSS and make a decision. *LPOS* does not have such a limitation, since it relies on a voting-based approach and FC evaluates each contribution of users towards the decision individually, which makes *LPOS* more fault-tolerant compared to *PPSS* [4].

4) Scalability and Computational Efficiency: *LPOS* offers the smallest communication overhead among its counterparts for large network sizes, and its computational complexity is logarithmic in the number of users, which makes it more practical and scalable (a detailed analysis is given in Section V).

5) Robust Against Network Dynamism: When a group of users join or leave the network, the system security and performance should be maintained. Unlike its counterparts (e.g., *PPSS* [4]), which can deal with the joining/leaving of only a single user at a time, *LPOS* can effectively handle multiple, simultaneous join/leave operations.

II. PRELIMINARIES

CRN System and Sensing Model. We consider a centralized CRN that consists of a FC and n SUs, as shown in Fig. 1. We assume that each SU is capable of assessing RSS values of channels through energy detection methods [3], and communicating them to FC, which it then combines them to make decisions regarding whether channels are available. FC then broadcasts the final decisions back to SUs.

Half-voting rule. Two reasons motivated our choice of a voting-based rule over an aggregation-based fusion rule: (i) it has a better sensing performance than aggregation-based rules [17], and (ii) it does not expose users to the privacy issues, we mentioned earlier, that would otherwise be exposed to when aggregation-based rules are used. The authors in [7] derived a voting threshold, λ, for optimal spectrum sensing in voting-based CRNs, which is termed half-voting rule. With this, when

TABLE I: Privacy, dynamism handling, fault tolerance and sensing performance of our scheme and previous schemes

Evaluation		Location Privacy	Dynamism	Fault Tolerance	Sensing Performance
Our Scheme: LPOS		High	Multiple	yes	optimal [7]
Generic	ECC El Gamal	Low	Multiple	yes	not optimal
	PDAFT [14]	Low	Multiple	yes	not optimal
PPSS [4]		Medium	Single	No	not optimal

Privacy: If *FC* can learn the aggregated result we evaluate the privacy to be low since an estimation of sensing reports of some users is possible when there are users leaving/joining the network. *Medium* privacy if there is a mechanism to cope with the mentioned problem but still using aggregation. We qualify our scheme to have *High* privacy since it does not have this vulnerability. **Dynamism:** *Multiple* when the scheme can handle multiple users leaving/joining the network simultaneously and *Single* when only one SU joining/leaving the network is supported. **Fault Tolerance:** whether or not the system still works normally when one of the SUs fails to send its report. **Sensing Performance:** a scheme is optimal if its sensing performance is proven to be optimal otherwise it is not optimal

the number of users whose RSS values are greater than τ is higher than λ, then FC can conclude that the channel is busy. **Notation.** Operators $||$ and $|x|$ denote the concatenation and the bit length of variable x, respectively. $x \overset{\$}{\leftarrow} S$ denotes that x is randomly and uniformly selected from the set S. Large primes q and $p > q$ such that $q|(p-1)$, and a generator α of the subgroup G of order q in $\mathbb{Z}_p^*$ are selected such that Discrete Logarithm Problem (DLP) [18] is intractable. (sk, PK) denotes a private/public key pair of ElGamal Encryption [19], generated under (G, p, q, α). $c \leftarrow OPE.E_K(M)$ denotes order preserving encryption (as defined in Definition 1) of a message $M \in \{0,1\}^d$ under private key K, where integer d is the block size of OPE. **Cryptographic Building Blocks.** Our scheme utilizes various cryptographic building blocks, which are described below:

• *Order Preserving Encryption (OPE) [15]:*

Definition 1. *An OPE is a deterministic symmetric encryption scheme whose encryption operation preserves the numerical ordering of the plaintexts, i.e. for any two messages m_1 and m_2 s.t. $m_1 \leq m_2$, we have $c_1 \leftarrow OPE.E_K(m_1) \leq c_2 \leftarrow OPE.E_K(m_2)$.*

The OPE concept was first formalized by Boldyreva et. al [15]. Note that our scheme can use *any secure OPE* scheme (e.g., [20]) as a building block, and receive the benefits of the security enhancement (e.g., [20]). However, we chose the publicly available implementation of Boldyreva's scheme [15] so as to evaluate our scheme in terms of execution time. In [15], an ideal security notion, called *indistinguishability under ordered chosen-plaintext attack (IND-OCPA)*, was introduced, which implies that OPE has no leakage, except the order of ciphertexts. However, Boldyreva et. al [21] showed that the ideal OPE security is unachievable, since it requires a ciphertext size that is at least exponential in the size of the plaintext, leading to the introduction and adoption of a weaker security notion of *Random Order-Preserving Functions (ROPF)*, as defined below.

Definition 2. *An OPE based on ROPF leaks the order of plaintexts and also at least half of the high-order bits of the plaintext [21].*

• *Secure Comparison Protocol:* The Yao's Millionaires' (YM) protocol [16] enables two parties to execute "the greater-than" function, $GT(x,y) = [x > y]$, without disclosing any other information apart from the outcome of the comparison. We use an efficient YM scheme [22], referred to as $YM.ElGamal$, which ensures that only the initiator learns the outcome.

Definition 3. *Let $(\mathcal{X}, \mathcal{Y})$ and $(x, y) \in \{0,1\}^l$ be two parties and l-bit integers to be compared, respectively. Let $\pi = (l, q, p, \alpha, \{sk, PK\})$ be $YM.ElGamal$ parameters generated by the protocol initiator $\mathcal{X}$. $YM.ElGamal$ returns a bit $b \leftarrow YM.ElGamal (x, y, \pi)$, where $b = 0$ if $x < y$ and $b = 1$ otherwise. Only $\mathcal{X}$ learns b but $(\mathcal{X}, \mathcal{Y})$ learn nothing else. $YM.ElGamal$ is secure in the semi-honest setting if ElGamal encryption scheme [19] is secure.*

• *Group Key Establishment and Management:* We use a dynamic and contributory group key establishment and management protocol for secure group communication purposes.

Definition 4. Tree-based Group Elliptic Curve Diffie-Hellman (TG ECDH) *[23] permits n distinct users to collaboratively establish and update a common group key K by extending 2-party ECDH key exchange protocol to n-party.* TGECDH *is secure if Elliptic Curve Discrete Logarithm Problem (ECDLP) is intractable [23].*

III. THE PROPOSED SCHEME

Voting-based spectrum sensing offers several advantages over its aggregation-based counterparts as discussed in Section II. However, this approach requires comparing FC's threshold τ and the RSS value r_i of each user U_i, thereby forcing at least one of the parties to expose its information to the other. One solution is to use a secure comparison protocol, such as $YM.ElGamal$, between FC and each user $U_1, \ldots, U_n$ in the network, which permits FC to learn the total number of users above/below threshold τ (as discussed in Section I-A) but nothing else. However, secure comparison protocols involve several costly public key crypto operations (e.g., modular exponentiation), and therefore $\mathcal{O}(n)$ invocations of such a protocol per sensing period incur prohibitive computational and communication overhead.

The key observation that led us to overcome this challenge is the following: If we enable FC to learn the relative order of RSS values but nothing else, then the number of $YM.ElGamal$ invocations can be reduced drastically. That is, *the knowledge of relative order permits FC to execute $YM.ElGamal$ protocol at worst-case $\mathcal{O}(log(n))$ by utilizing a binary-search type approach*, as opposed to running $YM.ElGamal$ with each user in total $\mathcal{O}(n)$ overhead.

This simple yet powerful observation enables us to develop *LPOS*, which achieves the above objective via an innovative integration of OPE scheme, *TGECDH* and $YM.ElGamal$ protocols. *The crux of the idea is to make users OPE encrypt their*

Algorithm 1 *LPOS* Algorithm (the proposed scheme)

Initialization: Executed only once at the beginning.

1: FC sets its energy sensing and optimal voting thresholds τ and λ, respectively as in [7]. Bit-length $\gamma = |\tau| = |r_i|$ for $i = 1, \ldots, n$, where r_i denotes RSS value of user U_i.

2: FC generates $YM.ElGamal$ parameters π (as defined in Definition 3) and pre-computes ElGamal encryption values in π based on τ to accelerate $YM.ElGamal$ protocol. FC also generates a random padding $D \xleftarrow{\$} \{0,1\}^{d-\gamma-1}$, where d is the block size of OPE. D is known to all users.

3: There are n users $\{U_i\}_{i=1}^n$ in the system, whose RSS values are denoted as r_i for $i = 1, \ldots, n$, respectively.

4: $\mathcal{G} = \{U_i\}_{i=1}^n$ collaboratively establish a group key K via *TGECDH* (Definition 4).

5: FC establishes an authenticated secure channel chn_i with each user U_i for $i = 1, \ldots, n$.   ▷ (e.g., via SSL/TLS) .

Private Sensing: Executed every sensing period t_w

6: U_i computes $c_i \leftarrow OPE.E_K(D||r_i)$ for $i = 1, \ldots, n$.

7: U_i sends c_i to FC over chn_i for $i = 1, \ldots, n$.

8: FC sorts encrypted RSS values as $c_{min} \leq \ldots \leq c_{max}$ (by Definition 1).

9: FC initiates $YM.ElGamal$ as $b \leftarrow YM.ElGamal$ $(\tau, r_{id_{max}}, \pi)$ with user id_{max} having the maximum c_{max}.

10: **if** $b = 1$ **then**

11:     $decision \leftarrow$ Channel is free.

12: **else**

13:     FC initiates $YM.ElGamal$ as $b \leftarrow YM.ElGamal(\tau, r_{id_{min}}, \pi)$ with user id_{min} having the minimum c_{min}.

14:     **if** $b = 0$ **then**

15:         $decision \leftarrow$ Channel is busy.

16:     **else**

17:         FC initiates $YM.ElGamal$ with a subset of users based on a binary search of τ on the remaining encrypted RSS values as described below. Let index I be the index of user c_I, where $YM.ElGamal$ with binary search process is finalized (i.e., $r_{I-1} \leq \tau \leq r_I$).

18:         FC counts the number of U_is s.t. $\tau \leq r_i : z \leftarrow n - I$

19:         **if** $z \geq \lambda$ **then**

20:             $decision \leftarrow$ Channel is busy

21:         **else**

22:             $decision \leftarrow$ Channel is free
        return $decision$

Group Membership Change Update:

23: If new user(s) join/leave $\mathcal{G}$ in t_w, the new set of users $\mathcal{G}'$ forms a new group key K' via *TGECDH*. FC may update its threshold and $YM.ElGamal$ parameters as λ' and π' when required.

24: Follow the private sensing steps with new (K', λ', π').

RSS values under a group key K, which is derived via TGECDH *at the beginning of the sensing period*. In this way, FC can learn the relative order of encrypted RSS values but nothing else (and users do not learn each others' RSS values, as they are sent to FC over a pairwise secure channel). FC then uses this knowledge to run $YM.ElGamal$ protocol by utilizing a binary-search strategy, which enables it to identify the total number of users above/below threshold τ (as defined by voting-based optimal sensing in [7]) with only $\mathcal{O}(log(n))$ complexity. This strategy makes *LPOS* the only alternative among its counterparts that can achieve CRN location privacy with an optimal spectrum sensing, fault-tolerance and network dynamism simultaneously (as discussed in Section I-B and Section V).

We give the detailed description of *LPOS* in Algorithm 1, and further outline the high-level description of *LPOS* as below:

● *Initialization:* FC sets up spectrum sensing and crypto parameters for cryptographic building blocks. Users establish a group key K via *TGECDH*, with which they will OPE encrypt their RSS values during the private sensing. FC also establishes a secure channel chn_i with each user U_i.

● *Private Sensing:* Each user U_i OPE encrypts its RSS value r_i with group key K and sends ciphertext c_i to FC over chn_i. This permits FC to sort ciphertexts as $c_{min} \leq \ldots \leq c_{max}$ without learning corresponding RSS values, and the secure channel chn_i protects the communication of U_i from other users (as each r_i is encrypted under the same K) as well as from outside attackers. FC then initiates $YM.ElGamal$ first with the user that has the highest RSS value r_{max}. If it is smaller than energy sensing threshold τ then the channel is free. Otherwise, FC initiates $YM.ElGamal$ with the user that has r_{min}. If it is bigger than τ then the channel is busy. Otherwise, to make the final decision based on the optimal sensing threshold λ, FC runs $YM.ElGamal$ according to the binary-search strategy as described in Steps 17-22, which guarantees the decision at the worst $\mathcal{O}(log(n))$ invocations.

● *Update Private Sensing after Group Membership Changes:* At the beginning of each sensing period t_w, according to the membership changes in the user group, a new group key may be formed via the update procedure of *TGECDH* efficiently. FC may optionally update sensing parameters. The private sensing for the new sensing period then begins with new parameters and group key K' and is executed as described above.

IV. SECURITY ANALYSIS

Threat Model: Our threat model focuses on the *location privacy (i.e., RSS values) of SUs*. We consider *honest but curious (semi-honest)* setting for FC and SUs forming group $\mathcal{G}$(no party, including FC, maliciously modifies the integrity of its input). This means that they execute the protocol honestly but will show interest in learning information about the other parties. That is, FC and other SUs in the group $\mathcal{G}$ may target the location information of a SU U_i. RSS value r_i of U_i reveals this location information and therefore should be protected. SUs also may target the threshold value τ of FC. However, we assume that FC does not collude with some SUs to localize the other SUs, nor do SUs collude with each others or expose the group key K to FC or external parties maliciously. Similarly, we assume that FC and SUs do not inject false τ or RSS values into

spectrum sensing. Finally, an external attacker $\mathcal{A}$ may launch passive attacks against the output of cryptographic operations and active attacks including packet interception/modification to FC and SUs. We rely on traditional authenticated secure channel to prevent such an external attacker $\mathcal{A}$.

Security Objectives and Analysis:

Definition 5. *Under our threat model described above,* LPOS *security objectives are: (i) RSS values r_i of each U_i remain confidential during all sensing periods. (ii) The sensing threshold τ of FC remains confidential for all sensing periods. (iii) A secure channel is maintained between each SU and FC. (iv) Objectives (i)-(iii) are maintained for every membership changes in $\mathcal{G}$.*

It is easy to show that *LPOS* is secure according to Definition 5, as long as its underlying cryptographic blocks are secure.

Theorem 1. LPOS *achieves security objectives in Definition 5, as long as OPE, YM.ElGamal and TGECDH are secure according to Definitions 2, 3 and 4, respectively.*

Proof. In sensing period t_w, objectives (i)-(iv) in Definition 5 are achieved as follows:

Initialization: In Step 1-2, FC sets up system and security parameters such that $YM.ElGamal$ and OPE are secure. Padding D and proper block size of OPE ensures the leftmost bit leakage from OPE as defined in Definition 2 does not leak RSS value during the private sensing. In Step 4, SUs establish a group K, which protects r_i values against FC via OPE encryption (as required by (i) in Definition 5). In Step 5, FC and each U_i establish a secure channel, which protects OPE encrypted r_i values c_i (under the same group key K) from other SUs and external attacker $\mathcal{A}$ (as required by (i) and (iii) in Definition 5).

Private Sensing: OPE encryptions in Step 6 ensure the confidentiality of r_i values against FC during the ciphertext sorting $(c_1,\ldots,c_n)$ in Step 8, as long as OPE is secure according to Definition 2 (with proper padding and OPE block size as set in the initialization phase). Step 7 ensures the confidentiality of r_i of U_i against other SUs as well as the protection of the communication against an external attacker $\mathcal{A}$ via the secure channel. Hence, objective (i) in Definition 5 is achieved during OPE phase of *LPOS*. Step 9 - Step 22 execute $YM.ElGamal$, which leaks no information on τ to SUs and r_i's to FC as required. Hence, objectives (i)-(iii) in Definition 5 are achieved during the whole private sensing steps.

Update Private Sensing after Group Membership Changes: Step 23 ensures that a new group key K' (based on Definition 4) and parameters (λ', π') are generated according to the membership status of the new group $\mathcal{G}'$. Step 24 ensures the private sensing steps are executed using new (K', λ', π') for each new sensing period. Thus, security objectives (i)-(iv) in Definition 5 are achieved for all sensing periods as required. □

V. ANALYSIS AND COMPARISON

Location Privacy, Sensing Accuracy and Reliability: As shown in Table I, *LPOS* achieves the highest level of privacy and decision accuracy among its counterparts. That is, *LPOS* is the only scheme that achieves high location privacy while enabling an optimal spectrum sensing. Moreover, *LPOS* provides

fault tolerance and support for dynamism of multiple SUs in the network, which makes it reliable. In addition, *LPOS* also achieves low communication, computation and storage overhead as discussed below.

Communication, Computation and Storage Overhead: Our analytical comparison is summarized in Table II, which also gives detailed explanations about variables, parameter sizes as well as overhead of building blocks and other schemes included in this comparison. The cost of *LPOS* is determined by $YM.ElGamal$, OPE, and TGECDH, whose costs are outlined in Table II. Notice that the overall cost of *LPOS* is dominated by $YM.ElGamal$ protocol, and yet $YM.ElGamal$ is invoked only $\mathcal{O}(log(n))$ at the worst case (as explained in Section III in detail). This permits high computational and communication efficiency.

As shown in Fig. 2(a)[2], *LPOS* offers the smallest communication overhead among all alternatives for large network sizes thanks to $\mathcal{O}(log(n))$ complexity for all public keys to be transmitted (the small constant ϵ_{OPE} per user has little impact on the overall communication overhead as seen in the Fig. 2(a)). It is followed by *ECEG*, who has small key sizes for small number of users due to compact ECC parameters. *PPSS* has a high communication overhead, while *PDAFT* incurs extremely large communication overhead due to heavy Pailler encryption.

As shown in Fig. 2(c)[3], all compared alternatives are significantly more computationally efficient than *PPSS*, while *LPOS* is comparable but little less efficient than *ECEG* and *PDAFT*.

Observe that while offering the smallest communication overhead (vital for scalability) and reasonable computation efficiency, *LPOS* is the only scheme that enables optimal spectrum sensing based on voting approach by also providing the highest level of location privacy, fault-tolerance and network dynamism.

VI. CONCLUSION

We design a location privacy preserving scheme for CRNs that achieves high sensing accuracy. Our scheme has several key features, making it more practical, secure, and reliable for large-scale CRNs. When compared to existing approaches, *LPOS* achieves optimal sensing performances with high location privacy while being robust against network dynamism.

REFERENCES

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

[2] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 4, pp. 40–62, 2011.

[3] O. Fatemieh, A. Farhadi, R. Chandra, and C. A. Gunter, "Using classification to protect the integrity of spectrum measurements in white space networks." in *NDSS*, 2011.

[4] 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*. IEEE, 2012, pp. 729–737.

[5] S. Bhattacharjee, S. Sengupta, and M. Chatterjee, "Vulnerabilities in cognitive radio networks: A survey," *Computer Communications*, vol. 36, no. 13, pp. 1387–1398, 2013.

---

[2]Communication overhead of each scheme is calculated by evaluating its corresponding analytical results in Table II with the parameter sizes given in item (ii)-Table II.

[3]The execution times were measured on a laptop running Ubuntu 14.10 with 8GB of RAM and a core M 1.3 GHz Intel processor, with cryptographic libraries MIRACL [27], Crypto++ [28] and *Louismullie*'s Ruby implementation of OPE [25].

TABLE II: Communication overhead, computation cost and storage needed of our scheme and previous schemes

Evaluation		Communication	Computation		Storage	
			FC	SU	FC	SU
Our Scheme: LPOS		$2\gamma \cdot |p| \cdot (2 + log\,n) + n \cdot \epsilon_{OPE} + |Q| \cdot log\,n$	$1/2 \cdot (2 + log\,n) \cdot \gamma \cdot |p| \cdot Mulp$	$(2\gamma \cdot |p| + 2\gamma) \cdot Mulp + OPE + 2\,log\,n \cdot PMulQ$	$4|p|$	$|p| + |K|$
Generic	ECEG	$4|Q| \cdot n$	$PMulQ + PAddQ + \sqrt{n \cdot \delta} \cdot Pollard$	$2PMulQ + (n-1) \cdot PAddQ$	$(1 + 2 \cdot O(log(n\delta))) \cdot |Q|$	$|Q|$
	PDAFT [14]	$2|N| \cdot (n+1)$	$2ExpN^2 + InvN^2 + y \cdot MulN^2$	$2ExpN^2 + MulN^2$	$2|N|$	$|N| + |N^2|$
PPSS [4]		$|p| \cdot n$	$H + (n+2) \cdot Mulp + (2^{\gamma-1} \cdot n + 2) \cdot Expp$	$H + 2Expp + Mulp$	$(n+1) \cdot |p|$	$(n+1) \cdot |p|$

(i) Variables: γ: size of the sensing reports, n: number of SUs, N: modulus in Paillier, p: modulus of El Gamal, H: cryptographic hash operation, K: group key used in OPE. $Expu$ and $Mulu$ denote a modular exponentiation and a modular multiplication over modulus u respectively, where $u \in \{N, N^2, p\}$. $InvN^2$: modular inversion over N^2, $PMulQ$: point multiplication of order Q, $PAddQ$: point addition of order Q. y: number of servers needed for decryption in *PDAFT*. **(ii) Parameter size:** For a security parameter $\kappa = 80$, suggested parameter sizes by *NIST 2012* are given by : $|N| = 1024$, $|p| = 1024$, $|Q| = 160$ as indicated in [24]. **(iii) OPE:** the computational complexity of the OPE is given by $OPE = (log\,|\mathcal{C}| + 1) \cdot T_{HGD} + (log\,|\mathcal{P}| + 3) \cdot (5log\,|\mathcal{C}| + \theta' + 1)/128 \cdot T_{AES}$, where $\mathcal{P}, \mathcal{C}$ are plaintext and ciphertext spaces respectively and θ' is a constant. ϵ_{OPE} is the maximum ciphertext size that could be obtained under the OPE encryption. This value was determined experimentally based on the OPE implementation in [25] and we noticed that it doesn't exceed the 128bits block size of the underlying AES block cipher $\Rightarrow \epsilon_{OPE} = 128\,bits$. **(iv) ECEG:** The SUs use the FC's *ECEG* public key to encrypt their RSSs and then one node is picked to collect the ciphertexts and multiply them together including its own encrypted RSS and then send the result to the FC. The decryption of the aggregated message in *ECEG* is done by solving the constrained ECDLP problem on small plaintext space similarly to [4] via Pollard's Lambda algorithm, which requires $O(\sqrt{n \cdot \delta}) \cdot Pollard$ computation and $O(log(n\delta))$ storage [18], where $\delta = a - b$ if $RSS \in [a, b]$ and $Pollard$ is the number of point operations in Pollard Lambda algorithm which varies depending on algorithm implementation used. **(v) YM.ElGamal:** The communication cost for one comparison is $4\gamma \cdot |p|$. The total computational cost of the scheme for one comparison is $5\gamma\,log\,p + 2n$. Since in our scenario the value of the energy threshold τ remains unchanged, we can encrypt it only once and offline so the encryption cost can be omitted and the new total computational cost would be $3\gamma \cdot |p| + 2\gamma$ for each comparison operation. **(vi) TGECDH:** It permits the alteration of group membership (i.e., join/leave), on average $\mathcal{O}(log(n))$ communication and computation (i.e., ECC scalar multiplication) [26].
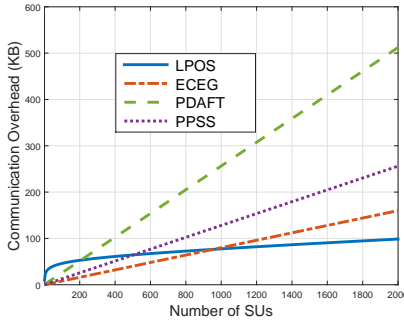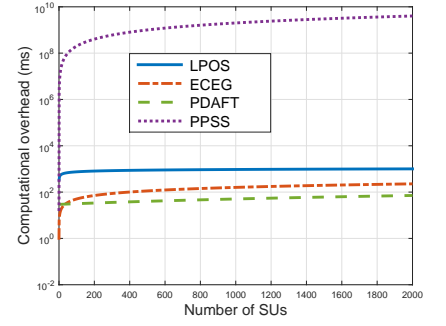

(a) Communication overhead

	Priv.	Dyn.	F. Tol.	Sen. Per.
LPOS	H	Mul.	✓	opt.
ECEG	L	Mul.	✓	not opt.
PDAFT	L	Mul.	✓	not opt.
PPSS	M	Single	✗	not opt.

Priv.: Privacy, **Dyn.**: Dynamism, **F. Tol.**: Fault Tolerance,
Sen. Per.: Sensing Performance, **H**: High, **L**: Low, **M**: Medium,
Mul.: Multiple, **opt.**: optimal,

(b) Properties of different schemes as in Table I

(c) Computational Overhead

Fig. 2: Performance Comparison

[6] W. Wang and Q. Zhang, *Location Privacy Preservation in Cognitive Radio Networks*. Springer, 2014.

[7] W. Zhang, R. K. Mallik, and K. Letaief, "Cooperative spectrum sensing optimization in cognitive radio networks," in *Communications, 2008. ICC'08. IEEE International Conference on*. IEEE, 2008, pp. 3411–3415.

[8] B. Hamdaoui and K. G. Shin, "OS-MAC: An efficient mac protocol for spectrum-agile wireless networks," *Mobile Computing, IEEE Transactions on*, vol. 7, no. 8, pp. 915–930, 2008.

[9] P. Venkatraman, B. Hamdaoui, and M. Guizani, "Opportunistic bandwidth sharing through reinforcement learning," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 6, pp. 3148–3153, 2010.

[10] M. Elmachkour, I. Daha, E. Sabir, A. Kobbane, and J. Ben-Othman, "Green opportunistic access for cognitive radio networks: A minority game approach," in *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 5372–5377.

[11] M. NoroozOliaee, B. Hamdaoui, and K. Tumer, "Efficient objective functions for coordinated learning in large-scale distributed osa systems," *Mobile Computing, IEEE Transactions on*, vol. 12, no. 5, 2013.

[12] M. Elmachkour, A. Kobbane, E. Sabir, J. Ben-othman *et al.*, "Data traffic-based analysis of delay and energy consumption in cognitive radio networks with and without resource reservation," *International Journal of Communication Systems*, vol. 28, no. 7, pp. 1316–1328, 2015.

[13] N. Adem and B. Hamdaoui, "Delay performance modeling and analysis in clustered cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2014 IEEE*. IEEE, 2014, pp. 193–198.

[14] L. Chen, R. Lu, and Z. Cao, "PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications," *Peer-to-Peer Networking and Applications*, pp. 1–11, 2014.

[15] A. Boldyreva, N. Chenette, Y. Lee, and A. O´ neill, "Order-preserving symmetric encryption," in *Advances in Cryptology-EUROCRYPT 2009*. Springer, 2009, pp. 224–241.

[16] A. C. Yao, "Protocols for secure computations," in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. IEEE, 1982.

[17] J. Shen, T. Jiang, S. Liu, and Z. Zhang, "Maximum channel throughput via cooperative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 10, 2009.

[18] A. Menezes, P. C. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996, ISBN: 0-8493-8523-7.

[19] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in Cryptology*. Springer-Verlag, 1985, pp. 10–18.

[20] F. Kerschbaum and A. Schroepfer, "Optimal average-complexity ideal-security order-preserving encryption," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 275–286.

[21] A. Boldyreva, N. Chenette, and A. ONeill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in *Advances in Cryptology–CRYPTO 2011*. Springer, 2011, pp. 578–595.

[22] H.-Y. Lin and W.-G. Tzeng, "An efficient solution to the millionaires' problem based on homomorphic encryption," in *Applied Cryptography and Network Security*. Springer, 2005, pp. 456–466.

[23] Y. Wang, B. Ramamurthy, and X. Zou, "The performance of elliptic curve based group diffie-hellman protocols for secure group communication over ad hoc networks," in *Communications, 2006. ICC'06. IEEE International Conference on*, vol. 5. IEEE, 2006, pp. 2243–2248.

[24] "Cryptographic key length recommendation," http://www.keylength.com/en/compare/#Biblio6.

[25] "Ruby ope implementation," https://github.com/louismullie/ope-rb.

[26] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-hellman key distribution extended to group communication," in *Proc. of the 3rd ACM Conf. on Computer and Comm. Security*. ACM, 1996, pp. 31–37.

[27] "Miracl library," http://www.certivox.com/miracl.

[28] "Crypto++ library," http://www.cryptopp.com/.