This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2019.2938491, IEEE Transactions on Industrial Electronics

Privacy-Preserving Database Assisted Spectrum Access for Industrial Internet of Things: A Distributed Learning Approach

Mengyuan Zhang, Jiming Chen, *Fellow, IEEE*, Shibo He, *Member, IEEE*, Lei Yang, *Member, IEEE*, Xiaowen Gong, and Junshan Zhang, *Fellow, IEEE*

***Abstract*—Industrial Internet of Things (IIoT) has been shown to be of great value to the deployment of smart industrial environment. With the immense growth of IoT devices, dynamic spectrum sharing is introduced, envisaged as a promising solution to the spectrum shortage in IIoT. Meanwhile, cyber-physical safety issue remains to be a great concern for the reliable operation of IIoT system. In this paper, we consider the dynamic spectrum access in IIoT under a Received Signal Strength (RSS) based adversarial localization attack. We employ a practical and effective power perturbation approach to mitigate the localization threat on the IoT devices and cast the privacy-preserving spectrum sharing problem as a stochastic channel selection game. To address the randomness induced by the power perturbation approach, we develop a two-timescale distributed learning algorithm that converges almost surely to the set of correlated equilibria of the game. The numerical results show the convergence of the algorithm and corroborate that the design of two-timescale learning process effectively alleviates the network throughput degradation brought by the power perturbation procedure.**

***Index Terms*—Spectrum access, ICPS security, distributed algorithm, game theory.**

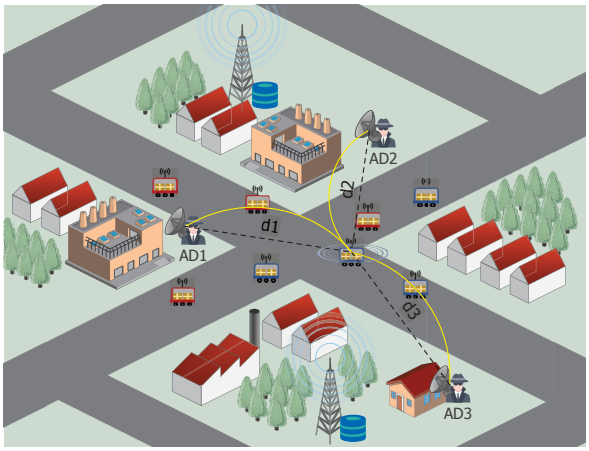


Fig. 1: An illustration of RSS based adversarial localization attack on an unmanned ground delivery system consisting of robotic vehicles belonging to two companies (differentiated by the colors). d_1, d_2, d_3 are distance estimations extracted from RSS measurements at three different positions, and are utilized to localize the target via trilateration technique.

I. Introduction

RECENT years have witnessed the innovation of modern industrial environment driven by the technology advancement of wireless communication, industrial control, artificial intelligence, and big data, etc. Under the support of the next-generation cyber-physical system (CPS) [2], Industrial Internet of Things (IIoT) has become one of the key building blocks of smart industrial applications including smart grid, smart factory, smart logistic management, and intelligent transportation system [3]. In these applications, the interconnected IoT devices continuously send the real-time industrial data to the IoT gateways that forward the data to the cloud/fog server for further processing and analysis [4].

With the expanding scale of IoT devices, the tremendous industrial data generated has put an increasing demand on bandwidth resources, which poses a significant challenge on the industrial spectrum management. To address the spectrum shortage, database-assisted spectrum access has been introduced where IoT are informed with the dynamic spectrum availability by a geo-location database, and access vacant licensed channels opportunistically [5], [6]. The key challenge of dynamic spectrum access remains as how to coordinate the spectrum sharing in a distributed way, so that the mutual interference between devices having access to the same vacant channel can be effectively mitigated [6]. To this end, game theoretic models have been adopted for solving dynamic spectrum access problem, where devices are interpreted as selfish players making channel access decisions strategically to maximize their payoffs [7].

Manuscript received October 23, 2018; revised June 5, 2019; accepted August 7, 2019. This work was supported in part by the NSFC under Grant 61629302, U.S. NSF under Grant IIS-1838024. *(Corresponding author: Jiming Chen)*.

A preliminary version of this paper was presented in 2015 GLOBECOM conference with the title of "Privacy-Preserving Database Assisted Spectrum Access: A Socially-Aware Distributed Learning Approach" [1].

M. Zhang, J. Chen and S. He are with the State Key Laboratory of Industrial Control Technology and Alibaba-Zhejiang University Joint Institute of Frontier Technologies, Zhejiang University, Hangzhou 310027, China (e-mail: zhang418@zju.edu.cn; cjm@zju.edu.cn; s18he@zju.edu.cn).

L. Yang is with the Department of Computer Science and Engineering, University of Nevada, Reno, NV 89557 USA (e-mail: leiy@unr.edu).

X. Gong is with the Department of Electrical and Computer Engineering, Auburn University, AL 36849 USA (e-mail: xgong@auburn.edu).

J. Zhang is with the School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85287 USA (e-mail: Junshan.Zhang@asu.edu).

In addition to the spectrum scarcity, cyber-physical security remains to be another challenge for reliable operation of IIoT. As a main building block of industrial CPS, IIoT integrates the control, networking and computing components, providing fundamental supports for generation, collection and exchange of security-critical and privacy-sensitive data. The critical importance of IIoT makes itself an attractive and valuable target for cyber-physical attacks [8]. While extensive studies have been concerning the cyber-attacks and corresponding defenses, relatively less attention has been paid to the physical-layer attacks in IIoT. As a key vulnerability, the geo-location information of IoT devices, once being compromised, would put the device into great danger, which is extremely harmful for the reliability and safety of IIoT system.

In this study, we consider a practical RSS based adversarial localization attack that has been shown to be effective in pinpointing wireless IoT devices [9]. As illustrated in Fig. 1, given a few RSS measurements collected within the vicinity of the victim, the adversary can easily carry out the localization attack using existing triangulation technique [10]. Compared with localization approaches using other physical-layer informations (e.g., time of arrival (TOA), time difference of arrival (TDOA), angle of arrival (AOA) [11]), RSS based localization requires neither complex hardware nor active communication with the victim, which can be easily implemented by the adversary in practice.

Many efforts have been made on developing countermeasures to mitigate physical-layer localization attacks, such as deploying directional antenna to limit transmission coverage [12] and creating ghost locations to misguide adversaries via device-level cooperation [13]. However, these approaches might be costly and difficult for widely system deployment, given the fact that IoT devices are generally of small size with limited computation and energy resources. Therefore, we consider using the light-weight power perturbation approach to combat the RSS based localization attack [14]. The main idea behind is to add random noise to the transmission power level of IoT devices, with the aim to effectively lower the adversaries' localization accuracy [15].

Despite its practicability and effectiveness, the random power perturbation approach would result in inaccurate interference evaluation at IoT devices, which inevitably incurs performance degradation (e.g., throughput reduction) to the spectrum sharing system. Thus motivated, the goal of this study is to develop an effective spectrum sharing scheme in IIoT that can at the same time protect device's location privacy via transmission power perturbation.

Following [16], we formulate the privacy-preserving spectrum access problem as a stochastic game where IoT devices update their channel selection choices dynamically with the objective of maximizing their utilities, as will be defined in Section III-A. We analyze the dynamics of the game based on the characterization of the equilibrium criteria. Specifically, we consider the correlated equilibrium (CE), a generalization of Nash equilibrium, which allows for dependencies among players' strategies and is easily amenable to distributed implementation [17].

To solve for the CE of the channel selection game under the impact of random power perturbation, in this study we devise a two-timescale distributed learning algorithm. Specifically, at a slower timescale, each IoT device evolves her channel selection strategy according to a *modified regret-based rule* [18] using the locally maintained estimated utility. At a relatively faster timescale, the estimated utility keeps being updated via a learning process to address the randomness introduced by the power perturbation, which facilitates more effective strategy learning at the slower timescale. We show that under mild conditions on the learning timescales, the empirical frequency of users' joint actions converges to the set of CE. The simulation results show that, under the random power perturbation, our two-timescale learning algorithm outperforms the single timescale learning algorithm involving only the strategy adaptation of channel selection, which corroborates that the proposed two-timescale learning algorithm helps strike a balance between the system throughput and location privacy.

Summarizing, we have made the following contributions:

- We identify the issue of RSS based adversarial localization attacks against IoT devices in database-assisted spectrum access, and consider a light-weight power perturbation approach to reduce the localization accuracy.
- We jointly study the dynamic spectrum access and location privacy protection by formulating a privacy-preserving channel selection game where IoT devices use perturbed transmission power level and strategically make channel selection decisions to maximize their utilities.
- We propose a two-timescale learning algorithm based on regret learning rule, which converges weakly to the set of correlated equilibria and is shown to outperform the single timescale learning approach in alleviating the system throughput degradation from random power perturbation.

The remainder of the paper is organized as follows. We first discuss the related work in Section II. In Section III, we describe the system model of privacy-preserving spectrum sharing scheme. In Section IV, we present the game theoretic problem formulation and introduce the no-regret based learning rule. We propose the two-timescale learning algorithm for privacy-preserving spectrum sharing in Section V, followed by Section VI which evaluates the effectiveness and performance of the proposed algorithm. Finally, we conclude the paper in Section VII.

II. Related Work

Spectrum management techniques have been widely adopted into smart IIoT designs to meet the high QoS requirement for data communication, which helps to establish strong interconnection among industrial sensor, actuators and systems. For instances, Cao *et al.* in [19] explored opportunistic accessibility of multiple channels to enhance the state estimation performance in a CPS with linear state dynamics. In [20], Chiwewe *et al.* provided an overview of different techniques for spectrum management in cognitive radio based industrial wireless sensor network, and also explored the application of game theoretic modeling for spectrum sharing schemes.

Along a different avenue, industrial cyber-physical security issues have recently garnered much attention by both industry

and academic communities, with great efforts focusing on the cyberattacks over industrial CPS [8]. In [21], the authors proposed a CPS security framework that distinguished the cyber, cyber-physical, and physical components in a CPS system, and surveyed over both potential and reported attacks as well as existing solutions. Particularly, in [22], the authors focused on the data privacy vulnerability of smart meters in smart grid system, and provided a thorough discussion on the state-of-the-art mitigation solutions. And in [23], the authors discussed the the security and privacy challenges within emerging smart city applications such as intelligent healthcare and transportation system.

By contrast, the adversarial localization attack considered in this study is a typical physical-layer attack targeting on wireless sensor networks in general [14]. To combat such threats, one main approach is to obfuscate the physical information of the transmitted signal that can be potentially utilized by adversaries to infer the users' locations. In [14] and [15], mobile devices were designed to strategically reduce their transmission power so as to reduce the number of adversaries that can collaboratively carry out RSS-based localization attacks, or to degrade the accuracy of the adversarial localization. In [24], Wang *et al.* focused on the design of directional antenna to address the physical-layer location privacy attacks. In [25], Gao *et al.* considered the location privacy protection in a cognitive radio network similar to ours. While instead of the RSS-based attack, they considered an attack model that inferred a secondary user's location through her used channels, and the threat was mitigated by choosing channels in favor of the most stable ones.

Different from most of the existing works, in this paper we jointly consider the spectrum management and locational privacy protection. The idea of the proposed two-timescale learning algorithm is inspired by [26], which studied the interference mitigation in decentralized small-cells networks using a reinforcement learning based algorithms. Perhaps The most related work to ours is [1], which investigated the location privacy protection under the scenario of socially-aware dynamic spectrum access by using game theoretic modeling. In this study, we consider a different equilibrium criteria (i.e., correlated equilibrium) which generalizes the Nash equilibrium considered in [1] by relaxing the independence assumption on the players' channel selection strategies. In addition, the IoT devices are designed to adapt strategy following the regret-based rule [27] instead of the Stochastic Fictitious Play dynamics used in [1].

III. System Model for Locational Privacy Preserving Spectrum Sharing

A. Basic Setting

According to the recent ruling by FCC [28], in database-assisted spectrum access, each white-space user will first send a spectrum access request to a database, and the database will reveal the vacant TV channels at a particular location to that user. We consider such a spectrum access network with a set $\mathcal{A} = \{1, 2, \cdots, M\}$ of primary channels (e.g., TV channels). And a set $\mathcal{V} = \{1, 2, \cdots, N\}$ of secondary users (i.e., IoT devices) try to access these channels when the channels are not occupied by licensed users. In particular, each user $n \in \mathcal{V}$ can access a subset of available channels $\mathcal{M}_n \subseteq \mathcal{A}$, as revealed by the database. Apparently, without proper coordination among secondary users, the conflict on channel usage may occur, and the generated interference could severely degrade the network performance. *Accordingly, database-assisted spectrum access boils down to the dynamic channel allocation among secondary users, in a time-varying channel occupancy and interference environment.*

To capture the physical coupling among IoT devices, we assume a physical interference model. Specifically, we denote $a_n \in \mathcal{M}_n$ as the channel that user $n \in \mathcal{V}$ have accessed, and denote the channel gain on her communication link as $g_{nn}^{a_n}$. We then let $g_{mn}^{a_n}$ denote the channel gain of a_n over the interference link between user $m \in \mathcal{V}$ and user n. The noise of channel a_n on the link of user n is denoted as N_{a_n}. The Signal-to-Interference and Noise Ratio (SINR) $\gamma_n(P_n)$ of user n can be written as

$$\gamma_n(P_n) = \frac{P_n g_{nn}^{a_n}}{\sum_{m \in \mathcal{V}/\{n\}} P_m g_{mn}^{a_n} \mathbb{1}_{\{a_m = a_n\}} + N_{a_n}}, \tag{1}$$

where P_n is the transmission power used by user n; the indicator function $\mathbb{1}_{\{a_m = a_n\}}$ is equal to 1 when user m and user n access to the same channel (i.e., $a_m = a_n$), and zero otherwise. We let W denote the bandwidth, and define the individual utility of user n as her throughput with power level P_n,

$$U_n = W \log[1 + \gamma_n(P_n)]. \tag{2}$$

We also assume that all the IoT device can be categorized into different groups according to the functionality or proprietary. In the example of unmanned delivery system shown in Fig. 1, the in-group relationship of unmanned vehicles is illustrated by the different colors. For each user $n \in \mathcal{V}$, we let $\mathcal{N}_n$ denote the set of other users belong to the same group as user n, and define her group utility as her individual utility plus the sum of the utilities of her group neighbors, weighted by a factor $e_n \in [0, 1]$, i.e.,

$$S_n = U_n + e_n \sum_{m \in \mathcal{N}_n} U_m. \tag{3}$$

We use such a group utility model to capture the underlying social coupling among homogeneous IoT devices within the same group. Intuitively, the larger the value of e_n, the stronger the social connection that device n has with respect to the group she is associated with.

B. Random Power Perturbation against RSS-based Location Privacy Attack

1) RSS-based Location Privacy Attack: In this study, we consider a PHY-layer adversary model that employs the Received Signal Strength (RSS) based localization technique to compromise target users' location privacy. RSS-based localization captures the transmitted signal and can establish the mapping between the distance and the RSS according to the signal propagation model [14], [15]. As illustrated in Fig. 1, each adversary can collect a sequence of RSS levels of

the transmitted signal from the target user[1], and obtain an estimation of the distance using via Maximum Likelihood estimation [30]. Then an approximate location of the target user can be jointly determined by a trilateration using a set of distance estimations and the corresponding physical positions of the adversary.

2) Random Power Perturbation: To combat RSS-based location privacy attack, we employ a local random power perturbation approach aiming to introduce uncertainties to adversaries' localization outcome [15]. To this end, each user is allowed to dynamically and randomly change her transmission power level on purpose. The noisy measurements of RSS obtained at the adversary could effectively enlarge the uncertainty region of target user's position, which reduces the localization accuracy.

To avoid extra interference to the primary users, we restrict the random power perturbation component to be negative biased. Specifically, the perturbed transmission power of user n is given by $P_n = p + \Delta p_n$, which is the sum of the regular transmission power level $p > 0$ and a perturbation term Δp_n, generated following one-side truncated exponential distribution whose *pdf* is given as

$$f(\Delta p_n|b,\bar{p}) = \frac{\frac{1}{b}\exp(\Delta p_n/b)}{1-\exp(\bar{p}/b)},\ \Delta p_n \in (-\bar{p}, 0], \tag{4}$$

with $\bar{p}$ denotes the maximum perturbation level beyond which the SINR of IoT device might be unacceptable for normal data transmission. The parameter $b > 0$ characterizes the "expected" power perturbation level specified by the user, as will be further discussed in Section VI.

IV. Privacy-preserving Spectrum Sharing

In this section, we cast the spectrum sharing problem as a stochastic channel selection game, and introduce the no-regret matching rule, which can calculate the correlated equilibrium of a non-cooperative game in a distributed manner.

A. Stochastic Channel Selection Game for Spectrum Sharing

In our study, we formulate a stochastic channel selection game where all the IoT users are modeled as self-interested players interacting strategically and repeatedly with each other, aiming to maximize their expected group utilities in the long run[2]. The action space of each player $n \in \mathcal{V}$ is the set of available channels $\mathcal{M}_n$ that user n can access. We let $\boldsymbol{a} = (a_1, a_2, \cdots, a_N) \in \mathcal{M}$ denote the joint spectrum access profile of all the users, where $\mathcal{M} \triangleq \prod_{n=1}^{N} \mathcal{M}_n$. To facilitate the evaluation of each user's long-term expected group utilities, we denote $\Delta\mathcal{M}_n$ as the mixed strategy space of user n, and let $\pi_n = \big(\pi(a_{n,1}), \pi(a_{n,2}), \cdots, \pi(a_{n,|\mathcal{M}_n|})\big) \in \Delta\mathcal{M}_n$ denote user n's mixed strategy, a probability distribution over $\mathcal{M}_n$ with $q(a_{n,i})$ representing the probability of selecting the channel $a_{n,i}$. It follows that the joint mixed-strategy over all players is $\pi = (\pi_1, \pi_2, \cdots, \pi_N) \in \Delta\mathcal{M} \triangleq \prod_{n=1}^{N} \Delta\mathcal{M}_n$, and the joint strategy of players excluding user n can be denoted as $\pi_{-n} = (\pi_1, \cdots, \pi_{n-1}, \pi_{n+1}, \cdots, \pi_N)$ by convention. We further denote $\pi(\boldsymbol{a})$ as the probability of joint action $\boldsymbol{a} \in \mathcal{M}$ being played.

Summarizing, we cast the privacy-preserving spectrum sharing problem as a non-cooperative game denoted by a 3-tuple $\Gamma = \big(\mathcal{V}, \Delta\mathcal{M}, \{S_n\}_{n=1}^{N}\big)$. The equilibrium criteria considered in our study is the *correlated equilibrium*, which generalizes the Nash equilibrium by permitting players' strategies to be dependent. Mathematically, a correlated equilibrium is a convex polytope with its extrema points corresponding to the set of Nash equilibria. Thereby, in general, a better overall performance can be achieved under the correlated equilibrium than that under a Nash equilibrium. The formal definition of correlated equilibrium is given below.

Definition 1 (Correlated Equilibrium)**.** *A probability distribution π^* on $\Delta\mathcal{M}$ is a correlated equilibrium (CE) of game Γ if, $\forall n \in \mathcal{V}$, $\forall a_{n,i}, a_{n,j} \in \mathcal{M}_n$, the expected group utility satisfies the following,*

$$\sum_{\boldsymbol{a}\in\mathcal{M}:a_n=a_{n,i}} \pi^*(\boldsymbol{a})\left[S_n(a_{n,j}, \boldsymbol{a}_{-n}) - S_n(\boldsymbol{a})\right] \le 0. \tag{5}$$

Remarks. To get a concrete sense of the correlated equilibrium herein, one can view π^* as a strategy recommendation provided by the trusted spectrum database. With the implicit assumption that other users' strategies follow the given recommendation, it is of best interest of each user to also follow the recommended strategy. In other words, a user could not obtain a better expected group utility by deviating from the CE unilaterally.

Theorem 1. *(Existence of CE) There exists at least a CE in the stochastic channel selection game Γ.*

Since our channel selection game Γ consists of finite player set and action set, it falls into the category of finite game, which is guaranteed to possess a nonempty set of correlated equilibria [17].

B. No-regret Matching Rule

In this section, we briefly introduce the no-regret matching rule which is developed for searching a correlated equilibrium of a non-cooperative game in a distributed way [27]. By this rule, a regret measure is used to quantify the performance gain or loss of players' action adjustments. The key idea is to let each user learns the regret of playing each particular action, aiming to minimize the average regret over time.

Specifically, for each user $n \in \mathcal{V}$, given her opponents' actions $\boldsymbol{a}_{-n}$, the difference between averaged group utility under current action $a_n^t = a_{n,i}$ and that under any other action $a_{n,j} \neq a_{n,i}$ until time t can be measured as

$$D_n^t(a_{n,j}, a_{n,i}) = \frac{\sum_{l\le t} S_n(a_{n,j}, \boldsymbol{a}_{-n}^l)\mathbb{1}_{\{a_n^l = a_{n,i}\}}}{t} - \frac{\sum_{l\le t} S_n(\boldsymbol{a}^l)\mathbb{1}_{\{a_n^l = a_{n,i}\}}}{t}, \tag{6}$$

[1]For instance, through the RF fingerprint technique [29], a receiver can identify a wireless card by analyzing imperfections in the analog components of the signal.

[2]We use the terms "user" and "player" interchangeably throughout the paper.

where the second term quantifies the average group utility perceived by user n under action $a_{n,i}$ until time t, and the first term indicates the average utility she would have obtained if she had chosen $a_{n,j}$ every time when $a_{n,i}$ was played. Then user n's "regret" for not having played action $a_{n,j}$, instead of $a_{n,i}$ in the previous plays, is given as $R_n^t(a_{n,j}, a_{n,i}) = \max\{D_n^t(a_{n,j}, a_{n,i}), 0\}$. Intuitively, user n would regret if an alternate action could have brought her higher utility.

Based on the regret measures at time t, user n adapts her action according to the probabilistic strategy given as follows,

$$\begin{cases} q_n^{t+1}(a_{n,j}) = \frac{1}{\mu} R_n^t(a_{n,j}, a_{n,i}), & \forall a_{n,j} \in \mathcal{M}_n/\{a_{n,i}\}, \\ q_n^{t+1}(a_{n,i}) = 1 - \sum_{a_{n,j} \neq a_{n,i}} q_n^{t+1}(a_{n,j}). \end{cases} \tag{7}$$

Here the probability of changing to an alternate action $a_{n,j} \in \mathcal{M}_n/\{a_{n,i}\}$ is proportional to the corresponding regret measure $R_n^t(a_{n,j}, a_{n,i})$. The parameter μ is chosen to be a large value to guarantee that there is always a positive probability of remaining at the currently selected channel. A higher μ lowers the probability of switching to an alternate channel, therefore can be treated as an 'inertia' parameter. The algorithm then moves on by users updating their regret measures at time step $t+1$. For each joint action $\boldsymbol{a} \in \mathcal{M}$, we let $f^t(\boldsymbol{a}) \in \Delta\mathcal{M}$ denote its empirical distribution by time slot t, expressed as

$$f^t(\boldsymbol{a}) = \frac{1}{t} \sum_{l \leq t} \mathbb{1}_{\{\boldsymbol{a}^l = \boldsymbol{a}\}}. \tag{8}$$

It is well-known that for a non-cooperative game, with players updating their strategies following the no-regret matching rule, the empirical distributions f^t converges (with probability one) to the set of correlated equilibria as $t \to \infty$ [27].

There are two challenges that hinders us from directly using the no-regret matching rule in solving our stochastic channel selection game. Firstly, due to the use of random power perturbation procedure, the group utility of each user is corrupted with random noise, which inevitably leads to inaccurate 'regret' measurements and possibly problematic CE of the game.

Further, according to (6), to compute the regret for not having chosen an alternative channel $a_{n,j}$, user n needs to evaluate her potentially perceivable group utility $S_n(a_{n,j}, \boldsymbol{a}_{-n}^l)$ under $a_{n,j}$ every time when action $a_{n,i}$ was played at time step $l < t$, which is infeasible since user n does not possess the global information of other users' individual utility functions as well as their selected channels $\boldsymbol{a}_{-n}$.

To tackle these two challenges, in the next section, we devise a two-timescale learning algorithm, by which users learn their underlying noisy group utilities in the 'faster' learning process, while adapting their channel selection strategies following a modified regret-based rule in the 'slower' learning process.

V. Distributed Regret-based Learning for Privacy-Preserving Spectrum Sharing

In this section, we introduce the two-timescale distributed algorithm for finding the CE for our channel selection game, and provide a theoretic analysis on the long-run weak convergence of the algorithm under mild conditions.

A. Two-timescale Regret-based Learning Algorithm

The learning algorithm, as outlined in Algorithm 1, consists of a 'faster' and a 'slower' learning process. Specifically, on a faster timescale, each user continuously updates the expected group utility corresponding to each available channel given the noisy utility observation at each time step. Calibrating to the maintained expected group utility, each user adapts her strategy by following the regret-based learning rule at the 'slower' time scale. In what follows, we elaborate further on 'faster' and 'slower' learning processes, respectively.

1) Utility learning on a faster timescale: In the 'faster' learning process, user n maintains a vector $\hat{\mathbf{s}}_\mathbf{n}^\mathbf{t} = \left(\hat{S}_n^t(a_{n,1}), \hat{S}_n^t(a_{n,2}), \cdots, \hat{S}_n^t(a_{n,|\mathcal{M}_n|})\right)$, with each element $\hat{S}_n^t(a_{n,i})$ denoting the estimated group utility under action $a_{n,i}$ at time step t. As time evolves, the estimated group utility is updated as follows:

$$\hat{S}_n^t(a_{n,i}) = (1-\lambda^t)\hat{S}_n^{t-1}(a_{n,i}) + \lambda^t \mathbb{1}_{\{a_n^t = a_{n,i}\}} S_n^t(a_n^t), \tag{9}$$

where $0 < \lambda^t < 1$ denotes the learning rate. Specifically, for each user n, $S_n^t(a_n^t)$ is obtained by first measuring its own received interference $U_n^t(a_n^t)$, querying the U_m^t received by each user $m \in \mathcal{N}_n$ [3], and then conducting the summation according to (3). Note that at each iteration t, only the element $\hat{S}_n^t(a_{n,i})$ of vector $\mathbf{s}_\mathbf{n}^\mathbf{t}$ is actually updated. Through this recursive utility learning process, user n can asymptotically form accurate evaluation of the expected group utility which ensures that the strategy learning on slower timescale can finally reach the set of CE.

Algorithm 1 Two-timescale Distributed Learning Algorithm

initialization: For each user n,
Initialize $\mathbf{s}_\mathbf{n}^\mathbf{0}$, and the regret measures $R_n^0(a_{n,j}, a_{n,i}), \forall a_{n,i}, a_{n,j} \in \mathcal{M}_n$.
Randomly select a channel $a_{n,i} \in \boldsymbol{a}_n$ with initial probability $q_n^0(a_{n,i}) = \frac{1}{|\mathcal{M}_n|}$.
Set the learning rate λ^0 and ϵ^0; set the parameter γ.
end initialization
loop for each user $n \in \mathcal{V}$ in parallel:
'Faster' learning process:
Measure the received interference and compute the personal throughput $U_n^t(a_n^t)$ by (2).
Enquiry the individual utility of neighbors and compute instantaneous group utility $S_n^t(a_n^t)$ by (3).
Update the estimation of expected utility $\hat{S}_n^t(a_n^t)$ by (9).
'Slower' learning process:
Calculate the instantaneous regret $Q_n^t(a_{n,j}, a_{n,i})$ according to (11), and compute the regret measures $D_n^t(a_{n,j}, a_{n,i})$ according to (10).
Update the channel selection strategy $\{q_n^t(a_n)\}$ according to (12), and randomly select a channel a_n^{t+1} based on $\{q_n^t(a_n)\}$.
$t \leftarrow t+1$.
end loop

[3]The information exchange among two users within a same group could be fulfilled via a common control channel.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2019.2938491, IEEE Transactions on Industrial Electronics

2) Strategy adaptation on a slower timescale: At the slower timescale, we implement a modified regret-based learning procedure developed based on the standard no-regret rule as introduced in Section IV-B.

In particular, each user n updates the averaged group utility difference $D_n^t(a_{n,j}, a_{n,i})$ between each alternative action $a_{n,j} \in \mathcal{M}_n/\{a_{n,i}\}$ and the current action $a_{n,i}$ recursively as follows,

$$D_n^t(a_{n,j}, a_{n,i}) = (1-\epsilon^t) D_n^{t-1}(a_{n,j}, a_{n,i}) + \epsilon^t Q_n^t(a_{n,j}, a_{n,i}), \tag{10}$$

where $Q_n^t(a_{n,j}, a_{n,i}) \triangleq [S_n(a_{n,j}, \boldsymbol{a}_{-n}^t) - S_n(\boldsymbol{a}^t)]\mathbb{1}_{\{a_n^t = a_{n,i}\}}$ is defined as the instantaneous regret for not playing actions $a_{n,j}$ instead of $a_{n,i}$ at time t. The learning rate $0 < \epsilon^t < 1$ determines the timescale of the regret-based strategy learning, and should be set in accordance with the value of λ^t to guarantee the convergence to the CE, to be discussed next. Note that (10) generalizes (6) and can reduce to (6) with learning rate ϵ^t being set to $1/t$.

As mentioned in the previous section, the perceivable utility under an alternate action $a_{n,j} \neq a_{n,i}$ at time t, $S_n(a_{n,j}, \boldsymbol{a}_{-n}^t)\mathbb{1}_{\{a_n^t = a_{n,i}\}}$, is challenging to compute without the knowledge of other users' actions $\boldsymbol{a}_{-n}^t$ and their individual utility functions. Thus, we resort to the modified no-regret matching rule [18], and replace the explicit perceivable utility with an estimated term $\frac{q_n^t(a_{n,i})}{q_n^t(a_{n,j})}\mathbb{1}_{\{a_n^t = a_{n,j}\}} S_n(\boldsymbol{a}^t)$, where $q_n^t(a_{n,j})$ and $q_n^t(a_{n,i})$ are the probabilities of choosing the two actions being considered. In particular, user n calculates her instantaneous regret at time t according to the following equation:

$$Q_n^t(a_{n,j}, a_{n,i}) \triangleq \left[\frac{q_n^t(a_{n,i})}{q_n^t(a_{n,j})}\mathbb{1}_{\{a_n^t = a_{n,j}\}} - \mathbb{1}_{\{a_n^t = a_{n,i}\}}\right] \hat{S}_n^t(a_{n,i}). \tag{11}$$

And we again define the "regret" measure for not having played $a_{n,j}$ instead of $a_{n,i}$ as $R_n^t(a_{n,j}, a_{n,i}) = \max\{D_n^t(a_{n,j}, a_{n,i}), 0\}$. Simply put, the regret measure characterizes the difference of the averaged group utility between $a_{n,j}$ and $a_{n,i}$. And the weight $\frac{q_n^t(a_{n,i})}{q_n^t(a_{n,j})}$ is employed to normalize the instantaneous group utility to make the two terms in the brackets comparable.

With the regret measure $R_n^t(a_{n,j}, a_{n,i})$, each user updates her strategy as follows:

$$\begin{cases} q_n^t(a_{n,j}) = & (1-\delta^t)\min\left\{\frac{R_n^t(a_{n,j},a_{n,i})}{\mu}, \frac{1}{|\mathcal{M}_n|-1}\right\} + \frac{\delta^t}{|\mathcal{M}_n|}, \\ & \forall a_{n,j} \neq a_{n,i}, \\ q_n^t(a_{n,i}) = & 1 - \sum_{a_{n,j} \neq a_{n,i}} q_n^t(a_{n,j}), \end{cases} \tag{12}$$

where $\mu > 2S_{max}(|\mathcal{M}| - 1)$ with S_{max} denotes an upper bound on a user's group utiltiy. Since $\frac{q_n^t(a_{n,i})}{q_n^t(a_{n,j})}$ can go unbounded, to guarantee that $q_n^t(a_{n,i}) \geq 0$, we take the minimum of the weighted regret term and $\frac{1}{|\mathcal{M}_n|-1}$. Given the updated strategy, each user then adjusts her channel selection and proceeds to update her regret measures in the next time step.

Notice that by introducing the parameter δ, the strategy update rule (12) strikes an exploration-exploitation trade-off. On one hand, an alternate action with a larger 'regret' will have a larger probability of being chosen, which can be regarded as the exploitation process for a better strategy. On the other hand, each of the alternate actions will be selected with a probability of at least $\frac{\delta^t}{|\mathcal{M}_n|}$, enabling the exploration of the strategy space. As a result, each action could be visited for enough amount of times, which is the necessity for the convergence of both strategy adaptation and utility learning. By standard, we set a diminishing weight $\delta^t = 1/t^\rho$ with $\rho < 1/4$ in order to guarantee the convergence of the strategy adaptation. For clarification, we use Fig. 2 to illustrate the coupling of the two learning processes at an arbitrary time step t. Simply put, in the proposed regret-based two-timescale learning algorithm, users synchronously learn their long-term group utilities in parallel to the adaptation of their strategies in favor of channels with higher 'regret'. At each iteration, each user makes use of her maintained average regret matrix to calculate the instantaneous regret measure, leading to a computational complexity of $O(|\mathcal{M}_n|)$. Next, we evaluate the convergence performance of our proposed learning algorithm.

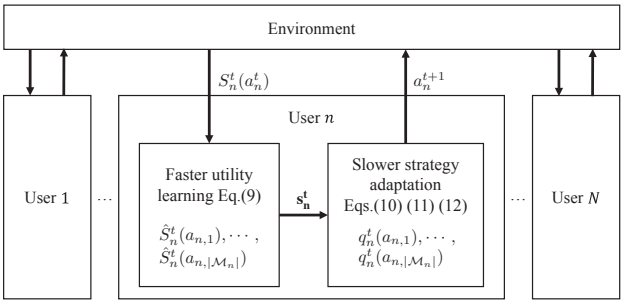


Fig. 2: Illustration of the coupling of utility learning (on faster timescale) and strategy adaptation (on slower timescale) at time t.

B. Convergence Analysis

In this section, we analyze the convergence behavior of Algorithm 1. We resort to the two-timescale extension of standard Stochastic approximation theory to show the weakly convergence of game Γ to the set of correlated equilibria. The idea is to let the utility learning and regret-based strategy adaptation proceed simultaneously with different step-size schedules so that the regret-based strategy learning runs on a slower effective timescale and sees the utility learning as quasi-static. Our main result is given in the following theorem.

Assumption 1. *For each user $n \in \mathcal{V}$, the conditions **C1-C3** are satisfied,*

$$\textbf{\textit{C1}}: \lim_{t\to\infty}\sum_{t\geq 0}\lambda_n^t = +\infty, \quad \lim_{t\to\infty}\sum_{t\geq 0}(\lambda_n^t)^2 < +\infty. \tag{13}$$

$$\textbf{\textit{C2}}: \lim_{t\to\infty}\sum_{t\geq 0}\epsilon_n^t = +\infty, \quad \lim_{t\to\infty}\sum_{t\geq 0}(\epsilon_n^t)^2 < +\infty. \tag{14}$$

$$\textbf{\textit{C3}}: \lim_{t\to\infty}\frac{\epsilon_n^t}{\lambda_n^t} = 0. \tag{15}$$

Theorem 2. *(Convergence of Algorithm 1) Let $f^t \in \Delta\mathcal{M}$ be the empirical distribution as defined in (8). With $\epsilon^t = 1/t$ in (10) and Assumption 1 being satisfied, Algorithm 1 converges*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIE.2019.2938491, IEEE Transactions on Industrial Electronics

almost surely to the set of CE $\{\pi^*\}$ *of the game* Γ *with* $\pi^* = (\pi_1^*, \pi_2^*, \cdots, \pi_N^*) \in \Delta\mathcal{M}$. *In particular, we have,*

$$\lim_{t\to\infty} \hat{S}_n^t(a_{n,i}) = \bar{S}_n(a_{n,i}, \pi_{-n}^*),\ \forall n \in \mathcal{V},\ \forall i = 1, \cdots, |\mathcal{M}_n|, \tag{16}$$

$$\text{and}\quad f^t \xrightarrow{a.s.} \{\pi^*\}\ \text{as}\ t \to \infty. \tag{17}$$

where $\bar{S}_n(a_{n,i}, \pi_{-n}^*)$ *is the expected group utility of user* n *with action* $a_{n,i}$ *and others' strategies* π_{-n}^*.

The main idea of the proof is to first introduce the continuous time interpolated process of the discrete learning process (9) and (10), which can be shown to be the asymptotic pseudotrajectory of the semiflow corresponding to the differential inclusion defined by the two learning dynamics [31]. Thus the limiting behaviors of the sequences $\{S_n(\boldsymbol{a})\}$ and $\{\pi(\boldsymbol{a})\}$ can be studied via the differential inclusion. By combining the asynchronous stochastic approximation framework [32], and under the Assumption 1, we can obtain the asymptotic weak convergence result of the two concurrent learning processes. Due to the lack of space, we leave the detailed proof to the online appendix [33].

VI. Performance Evaluation

In this section, we evaluate the performance of the proposed two-timescale distributed learning algorithm for the privacy-preserving spectrum sharing.

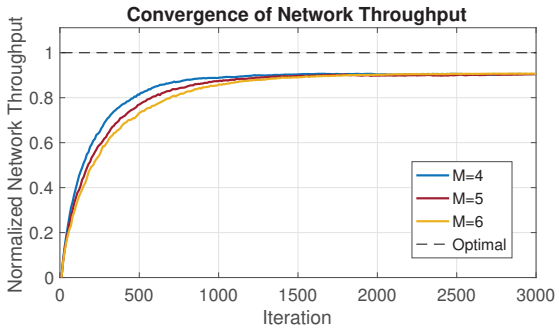
A. Simulation Setup

We consider a database-assisted spectrum access network consisting of $N = 80$ IoT devices that are randomly scattered in a square area of 1 km $\times$ 1 km and are categorized into either one of two groups with equal probability. For each secondary user n, we set the transmission power before being perturbed as $P_n = 100$ mW [28] and the available channel set $\mathcal{M}_n = \mathcal{A}$ with $M = 5$ by default. We consider a Rayleigh fading channel environment where the channel gain between user n and m is inversely proportional to their physical distance powered by the path-loss factor $\alpha = 4$. The background interference power N_{a_n} for each user n using channel a_n is uniformly assigned in the interval of [-100,-90] dBm. The weight factor e_n for each user n in either group is generated following a uniform distribution $\mathcal{U}(e_{min}, 1)$ with $e_{min} = 0.5$ by default.

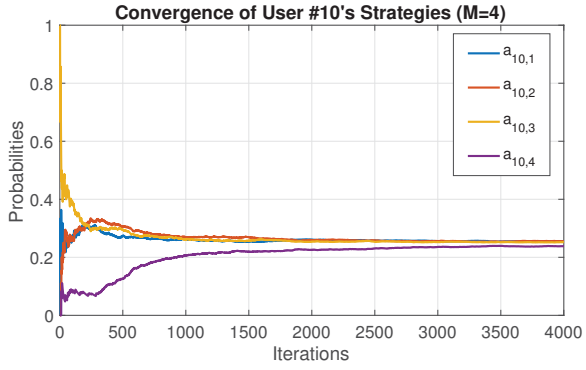
In our experiment, we let each user randomly perturb her transmission power level to combat the RSS based localization attack (as introduced in Section III-B), where each user's privacy protection level is quantified by the expected value of power perturbation $E(\Delta p_n)$. According to (4), we can derive the expression for the expected value of power perturbation term as $E(\Delta p_n) = b\left[\frac{1-(k+1)\exp(-k)}{1-\exp(-k)}\right]$, where $k = \bar{p}/b > 0$. We fix $\bar{p} = 15$mW and set $b = 12$ by default such that the mean perturbation level is about -6mW. For the two-timescale learning algorithm, we set the learning rate $\lambda^t = t^{-0.5}$ and $\epsilon^t = t^{-0.2}$ in Algorithm 1. The value of hyperparameters are determined through a tuning process so that the conditions **C1-C3** are satisfied. In addition, we let $\rho = 1/8$ as it is used in [18].

B. Results and Discussions

1) Convergence performance: We first examine the convergence performance of our algorithm. We adjust the value of b so that the mean value of power perturbation magnitude is -5 mW and the minimum group-relationship strength $e_{min} = 0.5$. We first run the experiment with different number of available channels, $M = 4, 5, 6$. The network throughput $T = \frac{1}{N}\sum_{n\in\mathcal{V}} T_n$ is used as the performance metric, where T_n denotes the average throughput of user n. From Fig. 3a, we observe that the proposed algorithm converges within 1500 iterations in general with increased number of channels leading to longer convergence time. It can be observed that changing the size of channel set does not impact the maximum achievable network throughput, which accounts for about 90% of the optimal network throughput. For an arbitrary selected user #10, we further evaluate the convergence of her strategies over each of the available channels, as shown in Fig. 3b.



(a)



(b)

Fig. 3: Convergence performance of two-timescale distributed learning algorithm.

2) Comparative studies on the throughput-privacy tradeoff: We next investigate the tradeoffs between network throughput and location privacy under different levels of power perturbation. We use the default setting of $M = 5$, $e_{min} = 0.5$, and run the experiment under different levels of power perturbation. Specifically, we change the value of parameter b so that the mean value of perturbation power level varies from 0mW to -9mW. For the comparative study, we consider two benchmarks: (a) the single timescale learning algorithm that merely consists of strategy adaptation based on modified regret based learning (RBL) as introduced in Section V-A2; (b) the

two-timescale learning algorithm involving a utility learning as well as a strategy adaptation following the Stochastic Fictitious Play (SFP) [1].

As shown in Fig. 4, in general, the system throughput decreases as expected with the increase of mean power perturbation level. Meanwhile, it is clear that the throughput of single timescale learning using RBL degrades much faster as the privacy preserving level increases, compared with other two approaches that involve both utility learning and strategy adaptation. This indicates the effectiveness of using a parallel utility learning to calibrate the noisy utility observation, which helps balance the location privacy protection with the network performance (i.e., system throughput).

It can also be seen that the throughput obtained by our proposed algorithm outweighs the one obtained using the two-timescale learning approach introduced in [1] by 5% in average. This can be explained by the different Equilibrium criteria used in the two studies. By definition, Nash equilibrium uses an underlying assumption that players' strategies are mutually independent. While the correlated equilibrium considered in this study generalizes the Nash equilibrium by allowing the strategies to be dependent among players. As the correlated equilibrium is mathematically equivalent to a convex polytope with its extrema points corresponding to the set of Nash equilibria, it is likely to exhibits better performance in general.

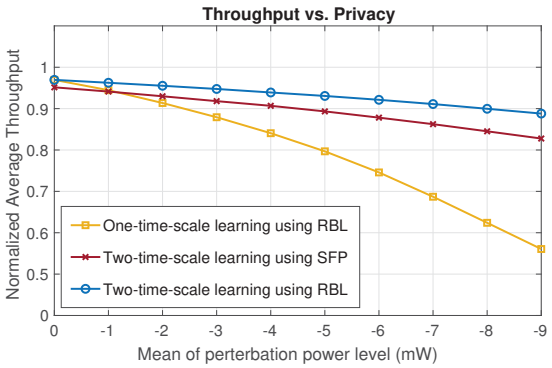


Fig. 4: Performance comparisons among different learning algorithms under varying power perturbation level.

3) The impact of system scale and group-relationship strength: We finally examine the network impact to the system performance. We run the experiment with increasing e_{min} from 0.5 to 0.9 for three cases with different network scale, i.e., $N = 80, 100, 120$. As illustrated in Fig. 5, the network throughput grows in general as the system scale enlarges. Also, it can be seen that the throughput experiences a monotonically increase as the strength of in-group relationship increases. For the cases with $N = 80, 100, 120$, approximately 14.5%, 15%, and 16.4% performance gains are achieved, respectively, when e_{min} is increased from 0.5 to 0.9, which indicates that the system would benefit from users behaving more altruistically.

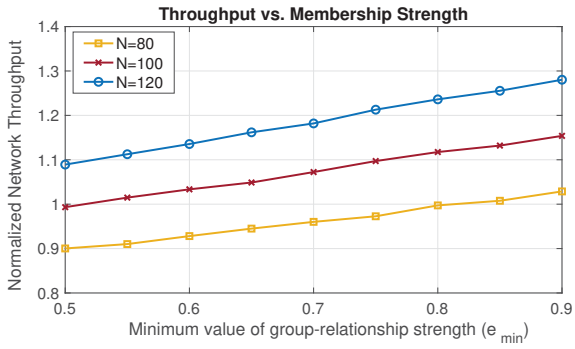


Fig. 5: Impact of total number of users N and minimum in-group relationship strength μ_{min} on network throughput.

VII. Conclusion

In this paper, we studied database-assisted spectrum sharing in the system of Industrial Internet of Things (IIoT). To address the RSS-based location privacy attack, a random power perturbation approach is applied to reduce the localization accuracy of adversaries. We cast the privacy-preserving spectrum sharing as a stochastic channel selection game among socially coupled IoT devices. Based on no regret dynamics, we develop a two-timescale distributed learning algorithm in which each device continuously estimates her group utility and adapts her strategy in favor of reduced regrets. Our proposed algorithm is shown to weakly converge towards the set of correlated equilibria and exhibits significant outperformance against the single timescale learning approach involving only strategy adaptation. Thereby, our approach helps to strike a balance between location privacy protection and enhancing network performance in IIoT system.

References

[1] "Privacy-preserving database assisted spectrum access: A socially-aware distributed learning approach," in *Proceedings of IEEE GLOBECOM*, pp. 1–6, 2015.

[2] J. Lee, B. Bagheri, and H.-A. Kao", "A cyber-physical Systems architecture for industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18 – 23, 2015.

[3] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[4] J. Fu, Y. Liu, H. Chao, B. K. Bhargava, and Z. Zhang, "Secure data storage and searching for industrial iot by integrating fog computing and cloud computing," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4519–4528, 2018.

[5] P. K. Sahoo, S. Mohapatra, and J. Sheu, "Dynamic spectrum allocation algorithms for industrial cognitive radio networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, Jul. 2018.

[6] T. M. Chiwewe, C. F. Mbuya, and G. P. Hancke, "Using cognitive radio for interference-resistant industrial wireless sensor networks: An overview," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, Dec. 2015.

[7] B. Wang, K. Liu, and T. Clancy, "Evolutionary cooperative spectrum sensing game: How to collaborate?" *IEEE Transactions on Communications*, vol. 58, no. 3, pp. 890–900, 2010.

[8] A. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, 2015.

[9] Z. Li, Z. Xiao, Y. Zhu, I. Pattarachanyakul, B. Y. Zhao, and H. Zheng, "Adversarial localization against wireless cameras," in *Proceedings of the 19th ACM HotMobile*, pp. 87–92, 2018.

[10] J. Lategahn, M. Muller, and C. Rohrig, "TDoA and RSS based Extended Kalman Filter for indoor person localization," in *Proc. IEEE 78th Vehicular Technology Conference (VTC Fall)*, pp. 1–5, Sep. 2013.

[11] S. Gezici, "A survey on wireless position estimation," *Wirel. Pers. Commun.*, vol. 44, no. 3, pp. 263–282, Feb. 2008.

[12] T. Wang and Y. Yang, "Location privacy protection from RSS localization system using antenna pattern synthesis," in *2011 Proceedings IEEE INFOCOM*, pp. 2408–2416, 2011.

[13] S. Oh, T. Vu, M. Gruteser, and S. Banerjee, "Phantom: Physical layer cooperation for location privacy protection," in *Proceedings of IEEE INFOCOM*, pp. 3061–3065, 2012.

[14] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless LANs," in *Proceedings of ACM MobiSys*, pp. 246–257, 2007.

[15] R. El-Badry, A. Sultan, and M. Youssef, "HyberLoc: Providing physical layer location privacy in hybrid sensor networks," in *Proceedings of IEEE ICC*, 2010.

[16] X. Chen, X. Gong, L. Yang, and J. Zhang, "Exploiting social tie structure for cooperative wireless networking: A social group utility maximization framework," *IEEE/ACM Transactions on Networking*, vol. 24, no. 6, pp. 3593–3606, Dec. 2016.

[17] S. Lasaulce and H. Tembine, *Game Theory and Learning for Wireless Networks: Fundamentals and Applications*. Academic Press, 2011.

[18] S. Hart and A. Mas-colell, "A reinforcement procedure leading to correlated equilibrium," *In: Debreu, G., Neuefeind, W., Trockel, W. (Eds.), Economic*, pp. 181–200.

[19] X. Cao, P. Cheng, J. Chen, S. S. Ge, Y. Cheng, and Y. Sun, "Cognitive radio based state estimation in cyber-physical systems," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 489–502, 2014.

[20] T. M. Chiwewe, C. F. Mbuya, and G. P. Hancke, "Using cognitive radio for interference-resistant industrial wireless sensor networks: An overview," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1466–1481, 2015.

[21] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[22] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2820–2835, 2017.

[23] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[24] T. Wang and Y. Yang, "Location privacy protection from RSS localization system using antenna pattern synthesis," in *Proceedings of IEEE INFOCOM*, pp. 2408–2416, Apr. 2011.

[25] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *Proceedings of IEEE INFOCOM*, pp. 2751–2759, Apr. 2013.

[26] M. Bennis, S. M. Perlaza, P. Blasco, Z. Han, and H. V. Poor, "Self-organization in small cell networks: A reinforcement learning approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3202–3212, 2013.

[27] Hart and A. Mas-colell, "A simple adaptive procedure leading to correlated equilibrium," *Econometrica*, pp. 1127–1150, 2000.

[28] FCC, *THIRD MEMORANDUM OPINION AND ORDER*, FCC Std., April 5, 2012.

[29] Y. Shu, Y. Huang, J. Zhang, P. Coué, P. Cheng, J. Chen, and K. G. Shin, "Gradient-based fingerprinting for indoor localization and tracking," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 4, pp. 2424–2433, 2016.

[30] M. R. Gholami, R. M. Vaghefi, and E. G. Ström, "RSS-based sensor localization in the presence of unknown channel parameters," *IEEE Transactions on Signal Processing*, vol. 61, no. 15, pp. 3752–3759, Aug. 2013.

[31] H. Kushner and G. Yin, *Stochastic Approximation and Recursive Algorithms and Applications*. Springer, 2003.

[32] V. S. Borkar, "Stochastic approximation with two time scales," *Systems & Control Letters*, vol. 29, no. 5, pp. 291 – 294, 1997.

[33] Tech. Rep., 9 2018. [Online]. Available: https://www.dropbox.com/s/xx62327sov64uub/TIE_appendix.pdf?dl=0

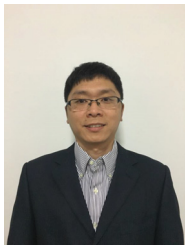
Mengyuan Zhang received the B.S. degree in optical science and engineering at Zhejiang University, Hangzhou, China, in 2011, and the M.S. degree from School of photovoltaic and renewable energy engineering at the University of New South Wales, Sydney, Australia, in 2012. He is currently working toward the Ph.D. degree with the Department of Control Science and Engineering, Zhejiang University.

His research interest include network economics, mechanism design, security and privacy in mobile social network and crowdsourcing network.

Jiming Chen (M'08, SM'11, F'19) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University in 2000 and 2005, respectively.

He is a Changjiang Scholars Professor with College of control science and engineering, Zhejiang University. He is currently vice Dean of Faculty of Information Technology, deputy Director of the State Key laboratory of Industrial Control Technology, Director of Industrial Process Control. He was a visiting researcher at University of Waterloo from 2008 to 2010. His current research interests include networked control, sensor networks, cyber security, IoT.

Prof. Chen is a Fellow of the IEEE, and a Distinguished Lecturer of IEEE Vehicular Technology Society (2015-2018). He also received the IEEE Comsoc Asia-pacific Outstanding Young Researcher Award 2011. He serves/served associate editors for for several international journals, including ACM TECS, IEEE TPDS, IEEE Network, IEEE TCNS, IEEE TII, etc.



Shibo He (M'13) received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2012.

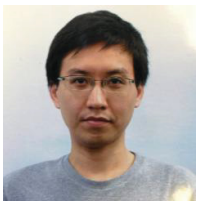
He is currently a Professor with College of control science and engineering, Zhejiang University. From 2010 to 2011, he was a visiting scholar with the University of Waterloo, Waterloo, ON, Canada. He was an Associate Research Scientist from March 2014 to May 2014, and a postdoctoral scholar from May 2012 to February 2014, with Arizona State University, Tempe, AZ, USA. His research interests include wireless sensor networks, crowdsensing, and big data analysis.

Dr. He serves on the editorial board of the IEEE Transactions on Vehicular Technology, Springer Peer-to-Peer Networking and Application, KSII Transactions on Internet and Information Systems, and is a Guest editor of Elsevier Computer Communications, and Hindawi International Journal of Distributed Sensor Networks. He served as Publicity Chair of the IEEE SECON 2016, TPC Co-Chair for IEEE ScalCom in 2014, TPC Vice Co-Chair for ANT from 2013-2014, etc. Dr. He coauthored two papers that won the best paper award of IEEE PIRMC 2012 and the IEEE WCNC 2017. He is a recipient of the IEEE Asia-Pacific Outstanding Researcher Award in 2015.

Lei Yang (M'13) received the B.S. and M.S. degrees in electrical engineering from Southeast University, Nanjing, China, in 2005 and 2008, respectively, and the Ph.D. degree from the School of Electrical Computer and Energy Engineering, Arizona State University, Tempe, AZ, USA, in 2012.

He is currently an Assistant Professor with the Department of Computer Science and Engineering, University of Nevada, Reno, NV, USA. He was a Postdoctoral Scholar with Princeton University, Princeton, NJ, USA, and an Assistant Research Professor with the School of Electrical Computer and Energy Engineering, Arizona State University. His research interests include big data analytics, edge computing and its applications in IoT and 5G, stochastic optimization and modeling in smart cities and cyber-physical systems, data privacy and security in crowdsensing, and optimization and control in mobile social networks.

Prof. Yang was a recipient of the Best Paper Award Runner-up at the IEEE INFOCOM 2014. He is currently associate editor for IEEE Access.



Xiaowen Gong received his BEng degree in electronics and information engineering from Huazhong University of Science and Technology in 2008, his MSc degree in communications from the University of Alberta in 2010, and his PhD degree in electrical engineering from the Arizona State University in 2015.

He is currently an Assistant Professor in the Department of Electrical and Computer Engineering at Auburn University. From 2015 to 2016, he was a postdoctoral researcher in the Department of Electrical and Computer Engineering at The Ohio State University. His research interests are in the area of computer communication networks with focuses on mobile social networks, crowdsourcing, fog networking and computing, privacy in mobile networks.

Junshan Zhang (M'00-SM'06-F'12) received the Ph.D. degree from the School of ECE at Purdue University in 2000.

He joined the School of ECEE, Arizona State University in August 2000, where he has been Fulton Chair Professor since 2015. His research interests fall in the general field of information networks and data science, including communication networks, Internet of Things (IoT), Fog Computing, social networks, smart grid. His current research focuses on fundamental problems in information networks and data science, including Fog Computing and its applications in IoT and 5G, IoT data privacy/security, optimization/control of mobile social networks, cognitive radio networks, stochastic modeling and control for smart grid.

Prof. Zhang is a Fellow of the IEEE, and a recipient of the ONR Young Investigator Award in 2005 and the NSF CAREER award in 2003. He received the IEEE Wireless Communication Technical Committee Recognition Award in 2016. His papers have won a few awards, including the Kenneth C. Sevcik Outstanding Student Paper Award of ACM SIGMETRICS/IFIP Performance 2016, the Best Paper Runner-up Award of IEEE INFOCOM 2009 and IEEE INFOCOM 2014, and the Best Paper Award at IEEE ICC 2008 and ICC 2017. Prof. Zhang was TPC co-chair for a number of major conferences in communication networks, including IEEE INFOCOM 2012 and ACM MOBIHOC 2015. He was the general chair for ACM/IEEE SEC 2017, WiOPT 2016, and IEEE Communication Theory Workshop 2007. He was a Distinguished Lecturer of the IEEE Communications Society. He was an Associate Editor for IEEE Transactions on Wireless Communications, an editor for the Computer Network journal, and an editor IEEE Wireless Communication Magazine. He is currently serving as an editor-at-large for IEEE/ACM Transactions on Networking and an editor for IEEE Network Magazine.