Attack Prevention for Collaborative Spectrum Sensing in Cognitive Radio Networks

Lingjie Duan, *Member, IEEE*, Alexander W. Min, *Member, IEEE*, Jianwei Huang, *Senior Member*, IEEE, and Kang G. Shin, *Fellow, IEEE*

***Abstract*—Collaborative spectrum sensing is vulnerable to data falsification attacks, where malicious secondary users (attackers) submit manipulated sensing reports to mislead the fusion center's decision on spectrum occupancy. This paper considers a challenging attack scenario, where multiple attackers cooperatively maximize their aggregate spectrum utilization. Without attack-prevention mechanisms, we show that honest secondary users (SUs) are unable to opportunistically transmit over the licensed spectrum and may even get penalized for collisions caused by attackers. To prevent such attacks, we propose two attack-prevention mechanisms with direct and indirect punishments. Our key idea is to identify collisions with the primary user (PU) that should not happen if all SUs follow the fusion center's decision. Unlike prior work, the proposed simple mechanisms do not require the fusion center to identify and exclude attackers. The direct punishment can effectively prevent all attackers from behaving maliciously. The indirect punishment is easier to implement and can prevent attacks when the attackers care enough about their long-term reward.**

***Index Terms*—Cognitive radios, Collaborative spectrum sensing, and Data falsification attacks.**

I. Introduction

COGNITIVE radios enable secondary (unlicensed) users (SUs) to opportunistically access licensed spectrum bands underutilized by primary licensed users (PUs), and can thus effectively improve spectrum utilization [1], [20]. As a key technology for realizing this opportunistic spectrum access, spectrum sensing aims to detect the presence/absence of a PU with high accuracy. To ensure sufficient protection, researchers have proposed *collaborative spectrum sensing* to improve detection performance by exploiting sensor location diversity [2], [3].

Collaborative sensing, however, is vulnerable to critical attacks, such as sensing data falsification attacks, especially in cognitive radio networks (CRNs) where sensors may likely operate unattended. If they are compromised, the sensors can report distorted sensing results to the fusion center in order to disrupt the incumbent detection process [4]–[6]. Such attacks can be easily launched due to the openness of the low-layer protocols stacks of cognitive radio devices [7]. However, it is challenging for the fusion center to validate the integrity of sensing reports because of the two unique features in spectrum sensing: unpredictability in wireless channel signal propagation and lack of coordination between PUs and SUs. The sensing data falsification attack will result in a waste of spectrum opportunities (due to false alarms) and excessive interference to the PU communications (due to missed detections). This poses a significant threat to the realization of cognitive radio technology, and thus calls for efficient attack detection and prevention mechanisms.

In this paper, we consider an attack scenario in which multiple attackers (i.e., compromised SUs/sensors) *cooperate* to maximize their aggregate spectrum utilization in CRNs. Despite the serious threat posed by collaborative attacks, this aspect has not yet been fully considered in CRNs. We focus on a very challenging attack scenario in which attackers can overhear all honest SUs' sensing reports, whereas the honest SUs are unaware of the existence of attackers. This information asymmetry gives the attackers the maximum capability to launch attacks and achieve their goals. We design attack-prevention mechanisms that safeguard collaborative sensing in such a challenging scenario.

We consider two different attack scenarios: (1) "attack-and-run" where attackers only care about an immediate reward, and (2) "stay-with-attacks" where attackers care about their long-term reward. We first analyze the impact of attacks on honest SUs in the absence of attack-prevention mechanisms. Then, we propose two attack-prevention mechanisms: a *direct* punishment scheme that can effectively prevent attacks in both scenarios, and an *indirect* punishment scheme that is easier to implement and effectively prevents attacks in the "stay-with-attacks" scenario. The key idea of both mechanisms is to discourage attackers from launching attacks by designing efficient attack detection and punishment strategies.

The key contributions of this paper are summarized as follows.

- *A spectrum-sharing model with collision penalty:* In Section II, we introduce the collision penalty, which aims to protect the PU's exclusive spectrum usage and provides incentives for the PU to open its spectrum for sharing.
- *Understanding cooperative attackers' optimal behaviors:* In Section III, we theoretically show that in the absence of attack-prevention mechanisms, attackers will utilize all

Manuscript received 14 February 2011; revised 21 July 2011. This work is supported by the General Research Funds (Projects CUHK 412710 and CUHK 412511) established under the University Grant Committee of Hong Kong. The work at the University of Michigan was supported in part by the US National Science Foundation under Grant CNS 0905143 and by the US Air Force Office of Scientific Research under Grant FA9550-10-1-0393.

L. Duan is with the Engineering Systems and Design Pillar, Singapore University of Technology and Design (e-mail: swing.dlj@gmail.com).

J. Huang is with the Network Communications and Economics Lab, Department of Information Engineering, The Chinese University of Hong Kong (e-mail: jwhuang@ie.cuhk.edu.hk).

A. W. Min is with the Circuits and System Research, Intel Labs, USA (e-mail: alexander.w.min@intel.com).

K. G. Shin is with the Real-Time Computing Laboratory, Dept. of EECS, The University of Michigan (e-mail: kgshin@eecs.umich.edu).

Digital Object Identifier 10.1109/JSAC.2012.121009.

TABLE I
KEY RESULTS FOR DIFFERENT ATTACK SCENARIOS

Attack Scenarios	Attack-and-run	Stay-with-attacks
No Punishment (Section III)	Attacks happen and honest SUs always lose transmission opportunities	
Direct Punishment (Section IV)	Completely prevent attacks	
Indirect Punishment (Section V)	Cannot prevent attacks	If attackers focus on long-term reward: completely prevent attacks; If attackers focus on short-term reward: partially prevent attacks.

spectrum opportunities exclusively, whereas honest SUs cannot transmit and may even suffer from the collision penalty caused by attackers (see Table I).

- *Effective direct punishment:* In Section IV, we design a direct punishment mechanism that can detect attacks and punish the attackers. The proposed mechanism can *prevent all attacks* in both "attack-and-run" and "stay-with-attacks" scenarios. We show that a single attacker makes the network most vulnerable under this mechanism.
- *Effective indirect punishment:* In Section V, we propose an indirect attack-prevention mechanism that is easy to implement when direct punishment is infeasible. The key idea is to terminate collaborative sensing upon detection of an attack. The proposed mechanism can prevent all attacks if the attackers care enough about their long-term reward. Unlike the direct punishment, a larger number of attackers may make the network more vulnerable.

There has been a growing interest in attack-resilient collaborative spectrum sensing in CRNs (e.g., [4]–[6], [8]).This prior work mainly focused on mechanisms for detecting and filtering out abnormal sensing reports. Our work is different from existing approaches in three aspects. First, we consider *cooperation* among attackers, so the attacks are much more challenging to prevent. Second, unlike the previous work which focused on sensing data falsification attacks, we also consider the case where the attackers violate the fusion center's decision regarding spectrum access. Finally, our proposed attack-prevention mechanisms can easily prevent attacks without differentiating attackers from honest SUs.

II. PRELIMINARY

A. CRN Model and Assumptions

We consider an infrastructure-based secondary CRN, which consists of a single fusion center and a set of SUs (or sensors). The fusion center coordinates SUs' collaborative spectrum sensing and their access to a licensed PU channel. We assume that the fusion center is maintained by a trusted network administrator and has high computation power. For collaborative spectrum sensing, all SUs measure the primary signal strength on the same target channel, then make local binary decisions on the presence or absence of the primary signal, and finally report the binary decisions to the fusion center [9]. Based on the reported sensing results, the fusion center makes a global decision and broadcasts it to the SUs.

There is a set of $\mathcal{N} = \{1, \ldots, N\}$ SUs in the network, M of which are attackers as shown in Fig. 1. We assume that there is at least one honest SU in the network, i.e., $N - M \geq 1$; otherwise, it would be infeasible to defeat attacks. The honest SUs fairly share the licensed channel among themselves when the channel is available (i.e., it is not being used by the PU).

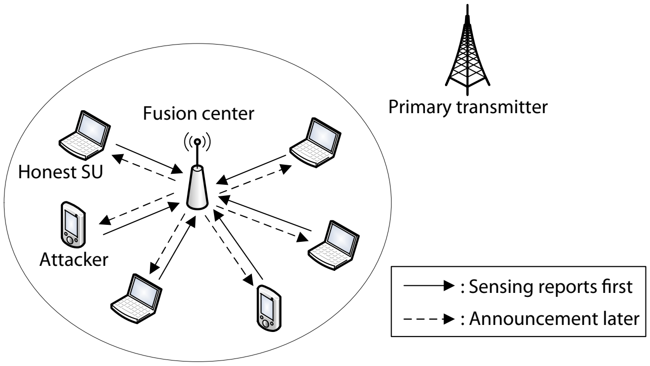


Fig. 1. **An illustration of cooperative spectrum sensing in cognitive radio networks**: The figure shows a secondary network with $N = 6$ SUs including $M = 2$ malicious SUs (i.e., attackers). The SUs periodically perform spectrum sensing and report the local (binary) decisions to the fusion center (the solid arrows). The fusion center makes a final decision and announces it to the SUs (the dotted arrows).

The attackers (i.e., malicious or compromised SUs), on the other hand, behave to maximize their own aggregate reward (e.g., achievable throughput) by manipulating their sensing reports so that the fusion center makes a wrong decision. In particular, we focus on the case that attackers can overhear all honest SUs' sensing reports to the fusion center before they collaboratively manipulating their sensing results. We assume that attackers can communicate with each other (and thus know the number of attackers), while the honest SUs only communicate with the fusion center. The honest SUs do not have to be strategic, and they do not need to make decisions by considering other honest SUs and attackers' decisions.

To make the analysis tractable and obtain useful engineering insights, we make three assumptions throughout the paper:

A1. All SUs have the same detection performance in terms of primary false alarm (P_f) and missed detection (P_m) probabilities.[1]

A2. The PU's spectrum occupancy is the same for all SUs and is independent across different time slots.[2]

A3. All SUs have the same transmission rate in utilizing the licensed channel.

In our online technical report [11], we relax both assumptions **A1** and **A3** by studying SUs' heterogeneous detection

[1] A false alarm occurs when an SU detects an idle channel as busy, and a missed detection occurs when an SU detects a busy channel as idle. The detection performance depends on the SU's physical location (relative to the primary transmitter) and fading environment.

[2] This assumption is frequently used in the literature (e.g., [6], [10]), and is reasonable when we approximate the case where PU's traffic changes fast (e.g., wireless microphones) and the time slot is relatively long. We need to study the correlation between spectrum occupancies when PU's traffic changes slowly over time (e.g., TV transmitters). Analyzing the correlated case requires a much more complicated Markov decision process (MDP) model than the one we used in Section V, and we consider this as a future direction.

performances and heterogeneous transmission rates. Our proposed attack-prevention mechanisms still apply in these cases.

Regarding the PU's temporal channel usage statistics, we denote P_I as the probability that the channel is *actually* idle. Thus, the channel is busy with the probability $1 - P_I$. We assume that SUs (including attackers and fusion center) know the probability P_I [6], [10]. This is reasonable if SUs and fusion center can collect PU's activity information from PU side and calculate P_I using various methods as in [12]. Such information collection is possible for SUs by examining PU's published historical activity report or purchasing the history report from PU directly.

B. Spectrum Sensing and Opportunistic Access Model

We assume a time-slotted model for opportunistic spectrum access. Such time-slotted channel access model has been widely assumed in the literature [13]–[15], including the IEEE 802.22 standard draft [16]. Each time slot includes two phases:

- Phase I (*Collaborative Spectrum Sensing*): As shown in Fig. 1, each SU senses individually and makes a local binary decision on channel occupancy: 1 if it detects the PU's signal (i.e., busy), and 0 otherwise (i.e., idle). All honest SUs truthfully report their sensing decisions to the fusion center. The attackers overhear the sensing reports from the honest SUs before sending their own reports (which may be different from their actual local sensing decisions) to the fusion center. Based on the reports from all SUs (including the attackers), the fusion center makes a global decision and broadcasts it to all SUs in the network. We assume that the sensing reports and announcements are communicated via a dedicated and reliable control channel with no communication errors.[3]
- Phase II (*Spectrum Sharing*): If the fusion center announces the channel to be idle, then honest SUs will transmit in Phase II. If it announces the channel to be busy, then honest SUs will wait. The attackers may transmit or wait in both cases. We assume that SUs who transmit in Phase II equally share the transmission time. More advanced link scheduling and power control may improve the overall network performance in Phase II, but is not the focus of this paper. Let us normalize the total transmission rate of the channel to 1.[4] More specifically, X SUs transmitting together leads to $1/X$ rate for each involved SU by using TDMA mode.

C. Collision Penalty

In order to increase social welfare, the government regulatory bodies (e.g., FCC in the U.S. and Ofcom in the U.K.) are pushing new spectrum-sharing schemes to allow the coexistence of PUs and SUs. There are two main obstacles in persuading PUs to share their licensed spectrum bands: (i) PUs' fear of interference or service disruption caused by SUs, and (ii) lack of economic incentives to PUs for spectrum sharing. To achieve these goals while efficiently preventing attacks, we adopt the notion of "collision penalty", similar in [17], as an incentive mechanism to allow for an efficient PU-SU coexistence. When a collision happens, we assume that the PU will charge a collision penalty C_p to *all* SUs in the network. This collision penalty will compensate PUs for potential performance loss due to collisions.[5] The reasons why PU charges all SUs can be found in [11].

We now define the PU's expected utility in one time slot as the sum of the PU's successful transmission rate and collision penalty collected from N SUs, i.e.,

$$U_{PU}(C_p) = (1-\gamma(C_p))V(r_{PU}) + \gamma(C_p)NC_p, \tag{1}$$

where $\gamma(C_p)$ is the collision probability of the PU's transmission due to SUs' aggressive access and is decreasing in C_p, r_{PU} is the PU's transmission rate, and $V(r_{PU})$ is PU's utility of achieving rate r_{PU}. A larger C_p makes SUs more conservative in spectrum access and leads to a lower $\gamma(C_p)$. Hence, a larger C_p achieves a high successful transmission rate (in the first term in Eq. (1)), but may also lead to a low compensation from SUs (the second term in Eq. (1)).

D. Decision Fusion Rule

At the end of Phase I in each time slot, the fusion center collects a binary sensing report $D_i \in \{0\,(\text{idle}), 1\,(\text{busy})\}$ from each SU $i \in \mathcal{N}$, and makes a decision using the following n-out-of-N rule [2]:

$$\begin{cases} \mathcal{H}_0 \text{ (primary signal does not exist) : if } \sum_{i\in\mathcal{N}} D_i < n. \\ \mathcal{H}_1 \text{ (primary signal exists) : if } \sum_{i\in\mathcal{N}} D_i \geq n \end{cases} \tag{2}$$

According to Eq. (2), the fusion center infers the channel to be busy $\mathcal{H}_1$ when at least n-out-of-N SUs report 1 (busy); otherwise, it infers the channel to be idle $\mathcal{H}_0$. The optimal selection of the threshold n depends on the system parameters and the reward functions of the SUs [9]. When $n = 1$, we have the OR-rule.

Of the general n-out-of-N rules, We adopt OR-rule throughout this paper. Ghasemi and Sousa [19] showed that the OR-rule performs better than other rules in many cases of practical interest. We further show the following theoretical result.

Theorem 1: At the fusion center, the OR-rule outperforms the other n-out-of-N rules ($n > 1$) when the collision penalty C_p satisfies the following condition.

$$\begin{aligned} \texttt{Condition.I}: &\frac{P_I}{1-P_I}\left(\frac{1-P_f}{P_m}\right)^N \frac{1}{N}\frac{P_m P_f}{(1-P_m)(1-P_f)} \\ &< C_p < \frac{P_I}{1-P_I}\left(\frac{1-P_f}{P_m}\right)^N \frac{1}{N}. \end{aligned} \tag{3}$$

The lower-bound of C_p in Condition.I discourages the SUs from transmitting when at least one SU reports 1 (busy). The upper-bound of C_p in Condition.I encourages SUs to transmit when all N SUs report 0 (idle). In the rest of the paper, we assume that C_p always satisfies Condition.I. More discussion of Condition.I can be found in [11].

[3] Under this one-hop network configuration, the attackers can overhear the control channel and easily decode honest SUs' reports like the fusion center.

[4] If the total transmission rate of the channel is $r\ (\neq 1)$, we can change C_p and C_b (defined later) to C_p/r and C_b/r and all results will go through.

[5] The penalty C_p can be in the form of monetary payments from SUs, or reduced transmission opportunities of SUs, or cooperative transmission by SUs to improve the PU's performance [17], [18].

For the ease of reading, we denote the following two conditional probabilities depending on SUs' sensing reports:

$$P^{I}_{N,k} := Pr\left(\texttt{idle}|\sum_{i\in\mathcal{N}} D_i = k\right) = \frac{P_I(1-P_f)^{N-k}P_f^k}{P_I(1-P_f)^{N-k}P_f^k + (1-P_I)(P_m)^{N-k}(1-P_m)^k}, \quad (4)$$

$$P^{B}_{N,k} := Pr\left(\texttt{busy}|\sum_{i\in\mathcal{N}} D_i = k\right) = 1 - P^{I}_{N,k}. \quad (5)$$

III. Attackers' Behaviors Without Punishment

In this section, we analyze the behavior of cooperative attackers when the system lacks attack-prevention mechanisms. The results in this section will serve as a benchmark for the proposed attack-prevention mechanisms in Sections IV and V.

We first define some useful notations.

- *State set $\mathcal{S}$:* A state $\boldsymbol{s} \in \mathcal{S}$ describes the local sensing decisions of the honest SUs and attackers: $(\sum_{i\in\mathcal{N}\setminus\mathcal{M}} D_i, \sum_{i\in\mathcal{M}} D_i)$. The size of set $\mathcal{S}$ is $(N-M+1)(M+1)$.[6] The attackers know the exact state in a particular time slot by overhearing the honest SUs' reports to the fusion center.
- *Attackers' action set $\mathcal{A}$:* The action $\boldsymbol{a}_m$ of an attacker $m \in \mathcal{M}$ is a tuple, (report to the fusion center in Phase I, spectrum access decision in Phase II), which has 4 possibilities: (idle, wait), (busy, wait), (idle, transmit), and (busy, transmit). Define $\boldsymbol{a} = \{\boldsymbol{a}_m, \forall m \in \mathcal{M}\}$ as all attackers' action vector, and $\mathcal{A}$ includes all possible $\boldsymbol{a}$.
- *Attackers' expected aggregate reward $R(\boldsymbol{a}, \boldsymbol{s})$:* This reward depends on the state $\boldsymbol{s}$ and the attackers' actions $\boldsymbol{a}$ in one time slot. It denotes the difference between the attackers' aggregate transmission rate and their expected payment to PU due to usage collision in one time slot.

For each state $\boldsymbol{s}$, the attackers choose $\boldsymbol{a}$ to maximize the expected aggregate reward in a single time slot, i.e.,

$$\max_{\boldsymbol{a}\in\mathcal{A}} R(\boldsymbol{a}, \boldsymbol{s}). \quad (6)$$

We discuss the solution to Eq. (6) in the three following cases. Due to the page limit, we skip all proofs here which can be found in our online technical report [11].

A. All SUs sense the channel idle

Proposition 1: Given the state $\boldsymbol{s} = \left(\sum_{i\in\mathcal{N}\setminus\mathcal{M}} D_i = 0, \sum_{i\in\mathcal{M}} D_i = 0\right)$, the cooperative attackers' optimal actions are: at least one attacker adopts the action (busy, transmit) and the other attackers (if any) adopt the action (idle, transmit). That is, at least one attacker will report the channel busy in Phase I and all attackers will transmit exclusively over the channel in Phase II. The fusion center will announce a wrong decision $\mathcal{H}_1$ in this case. The attackers' expected aggregate reward is:

$$R(\boldsymbol{a}, \boldsymbol{s}) = P^{I}_{N,0} - MP^{B}_{N,0}C_p > 0, \quad (7)$$

where the definitions of $P^{I}_{N,0}$ and $P^{B}_{N,0}$ are given in Eqs. (4) and (5), respectively. An honest SU does not transmit, but may suffer from the collision penalty caused by attackers and receives a negative expected reward

$$R_{honestSU}(\boldsymbol{s}) = -P^{B}_{N,0}C_p < 0. \quad (8)$$

Proposition 1 shows that an attack always happens when all SUs sense the channel idle.

B. All honest SUs sense the channel idle, but some attacker(s) senses the channel busy

Here we define the attackers' aggregate sensing result $\sum_{i\in\mathcal{M}} D_i$ as $\bar{M}$.

Proposition 2: Given the state $\boldsymbol{s} = \left(\sum_{i\in\mathcal{N}\setminus\mathcal{M}} D_i = 0, \sum_{i\in\mathcal{M}} D_i = \bar{M} \geq 1\right)$, the cooperative attackers' optimal actions are as follows.

- *If* $P^{I}_{N,\bar{M}} < MP^{B}_{N,\bar{M}}C_p$, then at least one attacker adopts the action (busy, wait) and the other attackers (if any) adopt the action (idle, wait). This leads to a correct announcement $\mathcal{H}_1$ (busy) at the fusion center. Since no one transmits, the attackers and the honest SUs all get zero reward,
$$R(\boldsymbol{a}, \boldsymbol{s}) = R_{honestSU}(\boldsymbol{s}) = 0. \quad (9)$$
- *If* $P^{I}_{N,\bar{M}} \geq MP^{B}_{N,\bar{M}}C_p$, then at least one attacker adopts the action (busy, transmit) and the other attackers (if any) adopt the action (idle, transmit). This leads to a correct announcement $\mathcal{H}_1$ (busy) at the fusion center. Only attackers will transmit exclusively in Phase II, their expected aggregate reward is:
$$R(\boldsymbol{a}, \boldsymbol{s}) = P^{I}_{N,\bar{M}} - MP^{B}_{N,\bar{M}}C_p > 0. \quad (10)$$
An honest SU does not transmit in Phase II, but may suffer from the collision penalty caused by attackers' transmissions and receives a negative expected reward
$$R_{honestSU}(\boldsymbol{s}) = -P^{B}_{N,\bar{M}}C_p < 0. \quad (11)$$

Proposition 2 indicates that an attack only happens when the benefit of exclusive transmission is large enough to compensate the potential collision penalty for the attackers.

C. Some honest SUs sense the channel busy

Proposition 3: Given the state $\boldsymbol{s} = \left(\sum_{i\in\mathcal{N}\setminus\mathcal{M}} D_i = K \geq 1, \sum_{i\in\mathcal{M}} D_i = \bar{M} \geq 0\right)$,[7] the announcement at the fusion center is always correct with $\mathcal{H}_1$ (busy), and the attackers' optimal actions are as follows.

- *If* $P^{I}_{N,K+\bar{M}} < MP^{B}_{N,K+\bar{M}}C_p$, then each attacker can either take the action (busy, wait) or (idle, wait). Since no one transmits, the attackers and the honest SUs all get zero reward,
$$R(\boldsymbol{a}, \boldsymbol{s}) = R_{honestSU}(\boldsymbol{s}) = 0. \quad (12)$$
- *If* $P^{I}_{N,K+\bar{M}} \geq MP^{B}_{N,K+\bar{M}}C_p$, then each attacker can either take the action (busy, transmit) or (idle, transmit). As only attackers will transmit in Phase II, their expected aggregate reward is:
$$R(\boldsymbol{a}, \boldsymbol{s}) = P^{I}_{N,K+\bar{M}} - MP^{B}_{N,K+\bar{M}}C_p. \quad (13)$$

[6] The value of D_i can be either 0 or 1, thus $\sum_{i\in\mathcal{N}\setminus\mathcal{M}} D_i$ ranges from 0 to $N-M$ and $\sum_{i\in\mathcal{M}} D_i$ ranges from 0 to M.

[7] Note that this state includes the case that all honest SUs sense the channel busy and (some) attackers sense idle.

- An honest SU does not transmit in Phase II, but may suffer from the collision penalty caused by attackers' transmissions and receives a negative expected reward

$$R_{honestSU}(\boldsymbol{s}) = -P^{B}_{N,K+\bar{M}}C_p < 0. \tag{14}$$

Propositions 1-3 indicate that, without any attack-prevention mechanism, the attackers will utilize the spectrum opportunities exclusively, whereas the honest SUs will never transmit regardless of their sensing decisions. What is worse, the honest SUs may suffer from the collision penalty caused by the attackers.

Note that our current analytical results focus on one time slot, where the attackers want to maximize their expected aggregate reward in the current time slot (i.e., the "attack-and-run" scenario). Since attackers' behaviors are independent over time slots, the above analytical results also hold for the "stay-with-attacks" scenario.

IV. Attack-Prevention Mechanism: A Direct Punishment

In this section, we consider the case in which the fusion center can directly charge a punishment to the SUs when attacks are identified. We focus on the "attack-and-run" scenario in a single time slot. The analysis also applies to the "stay-with-attacks" scenario as in Section III. With the proper choice of punishment, the proposed mechanism ensures that no attack will happen and no one will be punished.

Let us denote the direct punishment as C_b, which is different from the collision penalty C_p introduced in Section II-C. The fusion center will only charge the punishment to all SUs when the PU detects an attack. Let us consider the following scenario:

- When the announcement at the fusion center is $\mathcal{H}_1$ (busy) in Phase I and a collision happens in Phase II, the fusion center knows that an attack happens (as honest SUs will not transmit in Phase II). In this case, all SUs are charged a direct punishment C_b by the fusion center (in addition to the collision penalty C_p charged by the PU).[8]

Note that when the announcement at the fusion center is $\mathcal{H}_0$ (idle) in Phase I, no direct punishment will be triggered even if there is a collision in Phase II. This is because attackers will not share the spectrum access opportunity with honest SUs as in Proposition 1, and such collision can only the result of the missed detections of spectrum sensing.

The effectiveness of the attack-prevention mechanism depends on the choice of the punishment C_b. Theorem 2 shows that a large enough C_b can prevent all possible attacks.

Theorem 2: For M attackers in the network, there exists a threshold $C_b^{th}(M)$, i.e.,

$$C_b^{th}(M) = \max\left(\frac{P_f P_m}{(1-P_f)(1-P_m)}\frac{1}{M} - C_p, \left(\frac{1}{M} - \frac{1}{N}\right)\right) \times \frac{P_I}{1-P_I}\left(\frac{1-P_f}{P_m}\right)^{N}, \quad \forall M \geq 1, \tag{15}$$

such that any value $C_b > C_b^{th}(M)$ can prevent all attack scenarios described in Section III.

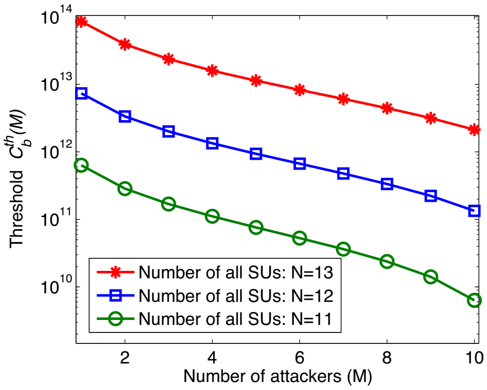


Fig. 2. Direct punishment threshold $C_b^{th}(M)$ for different M and N cases with (P_I, P_f, P_m, C_p)=$(0.6, 0.08, 0.08, 6e+10)$.

The proof of Theorem 2 is given in [11]. Next, we examine how the numbers of honest SUs and attackers affect the threshold $C_b^{th}(M)$.

Observation 1: $C_b^{th}(M)$ is decreasing in the number of attackers M and increasing in the number of honest SUs $N-M$. If the fusion center does not know the number of attackers, it should set the threshold to be $C_b^{th}(1) = \max_{M\geq 1} C_b^{th}(M)$ to prevent all attacks.

Figure 2 shows the value of threshold $C_b^{th}(M)$ as a function of M for different values of N.[9] When the number of attackers increases, the total penalty to the group of attackers also increases when an attack is confirmed (while the total transmission rate does not change), which discourages the attacks to happen.

Figure 2 also shows that $C_b^{th}(M)$ increases with the number of honest SUs $N-M$ for any fixed M. This is because the more honest SUs' sensing reports are overheard by the attackers, the more accurately the attackers can estimate the actual channel state, and thus more likely the attackers will launch an attack. As a result, a higher C_b is required to prevent attackers from manipulating their sensing reports. Thus, the single attacker scenario (i.e., $M=1$) is the most challenging case for this attack-prevention mechanism.

Observation 2: The threshold $C_b^{th}(1)$ is increasing in the idle probability P_I and non-increasing in collision penalty C_p.

V. Attack-Prevention Mechanism: An Indirect Punishment

The direct punishment scheme may be difficult to enforce for certain types of networks due to practical constraints, such as implementation overhead and complexity. For example, if the direct punishment is in the form of monetary payments from SUs to the fusion center, the fusion center needs to have reliable channels to collect and monitor such payments [18]. In this section we propose an indirect punishment scheme that can effectively prevent attacks in the "stay-with-attacks" scenario as long as the attackers care enough about future rewards. The key idea is to terminate collaborative sensing

[8] The way for the fusion center to realize the punishment C_b is similar to the way to realize the collision penalty C_p. See footnote 5 for details.

[9] Since P_f and P_m must be less than 10% in 802.22 WRAN standard draft, thus the probability to trigger direct punishment is very small under this choice of P_f and P_m. As a result, high $C_b^{th}(M) = C_b^{th}(M)/r$ value is determined in Fig. 2 to eliminate the attack benefit.

once the fusion center detects an attack, which forces the attackers to rely on their own sensing results in the future. This prevents attackers from overhearing honest SU sensing reports, and results in an increase in missed detection probability for attackers. Therefore, such indirect punishment will reduce the attackers' incentives to attack.

The indirect punishment works as follows:

- When the fusion center announces $\mathcal{H}_1$ (busy) in Phase I and a collision happens in Phase II, the indirect punishment is triggered and there is no collaborative sensing in future time slots.[10]

Note that when the fusion center announces $\mathcal{H}_0$ (idle) in Phase I, no indirect punishment will be triggered even if there is a collision in Phase II.

Similar to the direct punishment mechanism in Section IV, no indirect punishment will be triggered if all SUs behave honestly. The effectiveness of the indirect punishment depends on the attackers' performance when they are isolated from the honest SUs.

In the rest of the section, we make the following assumption:

$$\textbf{A4}: \qquad C_p > \frac{P_I}{1-P_I}\frac{1-P_f}{P_m}. \tag{16}$$

A4 is derived from $P^I_{1,0} - P^B_{1,0}C_p < 0$, which implies that a single SU will not transmit based on its own sensing decision (since it can be quite unreliable after the collaborative sensing breaks down) even without interference from the other SUs. **A4** is quite mild. When the number of SUs is reasonable (i.e., $N > 7$), $\texttt{Condition.I}$ in Eq. (3) directly guarantees the satisfaction of **A4** in Eq. (16). Note that **A4** only applies to this section.

To analyze the attackers' dynamic decisions in the long-term "stay-with-attacks" scenario, we formulate the problem as a Markov decision process (MDP). More specifically, we consider an infinite horizon Markov decision process $(\mathcal{S}', \mathcal{A}', P, R)$, where the group of cooperative attackers is the only decision-maker (collectively) over time.

- *State set* $\mathcal{S}'$*:* A state $\boldsymbol{s} \in \mathcal{S}'$ describes the attackers' knowledge of honest SUs' sensing decisions, their own sensing decisions, and whether the indirect punishment is triggered: $(\sum_{i\in\mathcal{N}\setminus\mathcal{M}} \bar{D}_i$, $\sum_{i\in\mathcal{M}} D_i$, $\texttt{Punishment})$. When $\texttt{Punishment} = \texttt{off}$, $\sum_{i\in\mathcal{N}\setminus\mathcal{M}} \bar{D}_i = \sum_{i\in\mathcal{N}\setminus\mathcal{M}} D_i$. When $\texttt{Punishment} = \texttt{on}$, $\sum_{i\in\mathcal{N}\setminus\mathcal{M}} \bar{D}_i = \texttt{Unknown}$ as the attackers do not know the honest SUs' sensing decisions. The size of set $\mathcal{S}'$ is $[(N-M+1)(M+1)+(M+1)]$. The attackers know the state during each time slot.
- *Attackers' action set* $\mathcal{A}'$*:* The action $\boldsymbol{a}_m$ of an attacker $m \in \mathcal{M}$ is a tuple: (report to the fusion center, spectrum access decision). When the indirect punishment is not triggered, there are four possible actions: (idle, wait), (busy, wait), (idle, transmit), and (busy, transmit). When the indirect punishment is triggered, an attacker's action can be (N/A, transmit) or (N/A, wait), where N/A means that the attackers do not report. We define $\boldsymbol{a} = \{\boldsymbol{a}_m, \forall m \in \mathcal{M}\}$ as the action vector of all attackers and $\mathcal{A}'$ contains all feasible values of $\boldsymbol{a}$.
- *Transition probability* $P(\boldsymbol{a}, \boldsymbol{s}, \boldsymbol{s}')$*:* The transition probability that actions $\boldsymbol{a}$ in a state $\boldsymbol{s}$ at time slot t will lead to state $\boldsymbol{s}'$ in time slot $t+1$ is $P(\boldsymbol{a}, \boldsymbol{s}, \boldsymbol{s}') = Pr(\boldsymbol{s}_{t+1} = \boldsymbol{s}' | \boldsymbol{s}_t = \boldsymbol{s}, \boldsymbol{a}_t = \boldsymbol{a})$. This depends on both state $\boldsymbol{s}$ and actions $\boldsymbol{a}$, and is independent of time t.
- *Attackers' expected aggregated reward* $R(\boldsymbol{a}, \boldsymbol{s})$*:* The attackers' received reward after taking actions $\boldsymbol{a}$ in state $\boldsymbol{s}$ of a time slot.

Compared to the reward in the current time slot, the attackers may value future rewards less. This can be captured by a discount factor $\delta \in (0,1)$. We further define a stationary policy $\boldsymbol{u}$ as a mapping between the set of states $\mathcal{S}'$ to the action set $\mathcal{A}'$. In other words, a policy defines what action to take in each possible state. The attackers' objective is to choose a policy $\boldsymbol{u}$ from policy set $\mathcal{U}$ to maximize the long-term expected aggregate reward:

$$\max_{\boldsymbol{u}\in\mathcal{U}} \sum_{t=0}^{\infty} \delta^t R(\boldsymbol{u}(\boldsymbol{s}), \boldsymbol{s}), \tag{17}$$

Let us denote the attackers' optimal long-term expected aggregate rewards by LR^H and LR^{DH} if they behave honestly and dishonestly, respectively.

Since attackers' behaviors and rewards before and after the indirect punishment are quite different, we need to study them separately. Here we first consider the attackers' behaviors before the punishment. Let us consider the case where at least one SU senses the channel busy, i.e., $\sum_{i\in\mathcal{N}} D_i = K \geq 1$. The attackers' optimal behaviors can be classified into two cases:

- *Non-aggressive Transmission:* The attackers will not attack for any $K \geq 1$, which is true if
$$\texttt{Case.NT}: P^I_{N,1} - MP^B_{N,1}C_p < 0, \tag{18}$$
where the attackers' exclusive transmission opportunity does not compensate their collision penalty.
- *Aggressive Transmission:* The attackers may attack even if $K \geq 1$, which is true if
$$\texttt{Case.AT}: P^I_{N,1} - MP^B_{N,1}C_p \geq 0. \tag{19}$$

In the rest of this section, we focus on $\texttt{Case.NT}$ with $M \geq 1$ attackers. The discussion for $\texttt{Case.AT}$ with $M \geq 1$ is given in [11].

We analyze the conditions under which attacks can be completely prevented via an indirect punishment. We first need to understand the attackers' performance degradation once the indirect punishment is triggered. Since the attackers are cooperative, they can always exchange sensing information among themselves. Depending on whether the attackers will transmit after the indirect punishment, we have two cases:

- *Weak Cooperation:* The attackers will not transmit even when all attackers sense the channel idle,
$$\texttt{Case.WC}: \quad P^I_{M,0} - MP^B_{M,0}C_p \leq 0. \tag{20}$$
This means that the attackers feel that their own sensing results are not reliable enough (with a high missed detection probability). $\texttt{Case.WC}$ also implies that the attackers will definitely not transmit if one or more attackers sense the channel busy. Due to assumption **A4**, the reward

[10] The fusion center can achieve this by broadcasting to all SUs that there is no need to report local sensing decisions in the future.

in Eq. (20) is an increasing function of the number of attackers M. Then we can also write Eq. (20) as an upper bound of M, i.e., Case.WC corresponds to a small number of attackers M.

- *Strong Cooperation:* The attackers will transmit when all attackers sense the channel idle,

$$\texttt{Case.SC}: \ P^I_{M,0} - MP^B_{M,0}C_p > 0. \tag{21}$$

This means that the attackers feel that their own sensing results (collectively) are accurate enough (with a low missed detection probability) even taking the collision penalty C_p into consideration. We can also write Eq. (21) as a lower bound of M, i.e., Case.SC corresponds to a large number of attackers M.

Obviously, it is more challenging to prevent attacks in Case.SC than Case.WC. However, we can show that in Case.SC the attackers' expected aggregate reward in one time slot with punishment triggered is always less than their reward when they always behave honestly. In other words, as long as the attackers care enough about future reward (i.e., the discount factor δ is high enough), we can still prevent attacks even in Case.SC (and thus in Case.WC as well).

Lemma 1: The attackers' optimal long-term expected aggregate rewards in Case.WC and Case.SC are

$$\begin{aligned} LR^H_{WC} &= LR^H_{SC} \\ &= Pr\left(\sum_{i\in\mathcal{N}} D_i = 0\right)\left(P^I_{N,0}\frac{1}{N} - P^B_{N,0}C_p\right)\frac{M}{1-\delta}, \end{aligned} \tag{22}$$

$$LR^{DH}_{WC} = \frac{Pr(\sum_{i\in\mathcal{N}} D_i = 0)(P^I_{N,0} - MP^B_{N,0}C_p)}{1-\delta(1-Pr(\sum_{i\in\mathcal{N}} D_i = 0)P^B_{N,0})}, \tag{23}$$

and LR^{DH}_{SC} in

$$\begin{aligned} LR^{DH}_{SC} &= LR^{DH}_{WC} + \frac{\delta}{1-\delta}Pr\left(\sum_{i\in\mathcal{N}} D_i = 0\right) \\ &\cdot \frac{P^B_{N,0}Pr(\sum_{i\in\mathcal{M}} D_i = 0)(P^I_{M,0} - MP^B_{M,0}C_p)}{1-\delta(Pr(\sum_{i\in\mathcal{N}} D_i > 0) + Pr(\sum_{i\in\mathcal{N}} D_i = 0)P^I_{N,0})}. \end{aligned} \tag{24}$$

Here the superscripts "*H*" and "*DH*" indicates honest and dishonest behaviors of attackers, respectively.

The proof of Lemma 1 is given in [11], where we can show that $LR^{DH}_{WC} < LR^H_{WC}$ and $LR^{DH}_{SC} < LR^H_{SC}$ when δ goes close to 1. This leads to the following result.

Theorem 3: The indirect punishment can prevent all attack in "stay-with-attacks" scenario if the discount factor δ satisfies the following condition:

- *Weak cooperation (*Case.WC*):* for any $1 \le M < N$, we need $\delta > \delta^{th}_{WC}(M)$ where

$$\delta^{th}_{WC}(M) = \frac{1}{1 + \frac{P_I(1-P_f)^N\frac{1}{N} - (1-P_I)(P_m)^N C_p}{\frac{1}{M}-\frac{1}{N}}\frac{1-P_I}{P_I}\left(\frac{P_m}{1-P_f}\right)^N}. \tag{25}$$

- *Strong cooperation (*Case.SC*):* for any $1 \le M < N$, we need $\delta > \delta^{th}_{SC}(M)$ where δ^{th}_{SC} is given in Eq. (26).

If the fusion center does not know the number of attackers, M, it can choose $\delta > \max_{0<M<N} \delta^{th}_{WC}(M)$ and $\delta > \max_{0<M<N} \delta^{th}_{SC}(M)$ for the two cases, respectively.

Although it is not shown in Theorem 3, we want to mention that the indirect punishment can still partially prevent attacks even δ is less than the discount factor threshold. Intuitively, attackers do not want to trigger indirect punishment and lose the opportunity to overhear honest SUs' sensing results. Thus they will behave more conservatively compared to the case with no indirect punishment. For example, if some SUs' sensing results indicate a busy channel state, the attackers will not attack to trigger the long-term punishment.

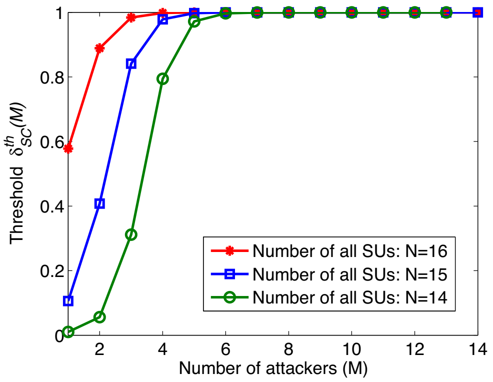


Fig. 3. Discount factor threshold $\delta^{th}_{SC}(M)$ with $(P_I, P_f, P_m, C_p) = (0.6, 0.08, 0.08, 3e+18)$.

We have the following interesting observations.

Observation 3: (*Impact of network size:*) Both $\delta^{th}_{WC}(M)$ in Case.WC and $\delta^{th}_{SC}(M)$ in Case.SC are increasing in the number of the honest SUs $N-M$. Threshold $\delta^{th}_{WC}(M)$ is decreasing in the number of the attackers M, while $\delta^{th}_{SC}(M)$ is increasing in the number of the attackers M.

Figure 3 plots $\delta^{th}_{SC}(M)$ as a function of N and M in Case.SC. The corresponding result in Case.WC can also be obtained based on Eq. (25).

With more honest SUs $N-M$, attackers have a less incentive to share the spectrum with honest SUs in the long-term and a higher incentive to attack and transmit exclusively. Thus a higher δ is needed to prevent attacks.

A larger number of attackers M has two effects: (a) a higher total collision penalty (whenever a collision happens), and (b) attackers' better estimation of channel condition (once the punishment is triggered). It turns out that effect (a) dominates in Case.WC and effect (b) dominates in Case.SC, which explains why the δ threshold decreases in M in Case.WC and increases in M in Case.SC. In Fig. 3, the most attack-vulnerable case happens when almost all SUs are attackers ($M \to N$), in which case $LR^{DH}_{SC} \to LR^H_{SC}$ and $\delta^{th}_{SC}(M)$ in (26) is close to 1.

Observation 4: (*Impact of collision penalty C_p:*) $\delta^{th}_{WC}(M)$ in Case.WC is increasing in the collision penalty C_p, while $\delta^{th}_{SC}(M)$ in Case.SC is decreasing in C_p.

In Case.WC, the collision penalty C_p only affects the time slots before the punishment is triggered. A higher C_p means a smaller long-term expected reward as a conservative honest SU (by comparing LR^H_{WC} in Eq. (22) to LR^{DH}_{WC} in Eq. (23)), and thus more incentives to attack. In Case.SC, a larger C_p hurts the reward of attackers more after punishment than before punishment. This is because the transmission probability before punishment is $Pr(\sum_{i\in\mathcal{N}} D_i = 0)$ (i.e., all SUs sense idle), which is smaller than the transmission probability after punishment $Pr(\sum_{i\in\mathcal{M}} D_i = 0)$ (i.e., all attackers sense idle). Thus a larger C_p discourages the attacks in Case.SC.

$$\delta_{SC}^{th}(M) = \left(1 + \frac{(P_I(1-P_f)^N \frac{1}{N} - (1-P_I)(P_m)^N C_p) - (P_I(1-P_f)^M \frac{1}{M} - (1-P_I)(P_m)^M C_p)}{\frac{1}{M} - \frac{1}{N}} \frac{1-P_I}{P_I} \left(\frac{P_m}{1-P_f}\right)^N\right)^{-1}. \tag{26}$$

VI. Conclusion

Collaborative spectrum sensing is vulnerable to sensing data falsification attacks. In this paper, we focused on a challenging attack scenario in which multiple cooperative attackers can overhear the honest SU sensing reports, but the honest SUs are unaware of the existence of attackers. We proposed two attack-prevention mechanisms with direct and indirect punishments. Both mechanisms do not require identification of the attackers. The direct punishment can effectively prevent all attacks in both "attack-and-run" and "stay-with-attacks," and the indirect punishment can prevent all attacks in the long-run if the attackers care enough about their future rewards.

References

[1] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, 2005.

[2] K. B. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proc. IEEE*, vol. 97, no. 5, pp. 878–893, 2009.

[3] A. W. Min and K. G. Shin, "An optimal sensing framework based on RSS-profile in cognitive radio networks," in *Proc. IEEE SECON*, 2009.

[4] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM*, 2008.

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

[6] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3554–3565, 2010.

[7] W. Xu, P. Kamat, and W. Trappe, "TRIESTE: A trusted radio infrastructure for enforcing spectrum etiquettes," in *Proc. IEEE Workshop on SDR*, 2006.

[8] O. Fatemieh, R. Chandra, and C. A. Gunter, "Secure collaborative sensing for crowdsourcing spectrum data in white space networks," in *Proc. IEEE DySPAN*, 2010.

[9] E. Peh and Y.-C. Liang, "Optimization for cooperative sensing in cognitive radio networks," in *Proc. IEEE WCNC*, 2007.

[10] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE GLOBECOM*, 2009.

[11] L. Duan, A. W. Min, J. Huang, and K. G. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks," Tech. Rep. [Online]. Available: http://arxiv.org/abs/1109.1021

[12] A. Azzalini, "A note on the estimation of a distribution function and quantiles by a kernel method," *Biometrika*, vol. 68, no. 1, pp. 326–238, 1981.

[13] Y.-C. Liang, Y. Zeng, E. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, April 2008.

[14] L. Duan, J. Huang, and B. Shou, "Investment and pricing with spectrum uncertainty: A cognitive operator's perspective," *IEEE Trans. Mobile Computing*, vol. 10, no. 11, pp. 1590-1604, 2011.

[15] A. W. Min and K. G. Shin, "On sensing-access tradeoff in cognitive radio networks," in *Proc. IEEE DySPAN*, 2010.

[16] C. Cordeiro, K. Challapali, and D. Birru, "IEEE 802.22: An introduction to the first wireless standard based on cognitive radios," *J. Commun.*, vol. 1, no. 1, pp. 38–47, 2006.

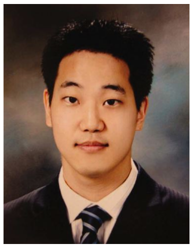
[17] S. Huang, X. Liu, and Z. Ding, "Optimal sensing-transmission structure for dynamic spectrum access," in *Proc. IEEE INFOCOM*, 2009.

[18] C. Courcoubetis and R. Weber, *Pricing Communication Networks: Economics, Technology and Modelling*. Wiley, 2003.

[19] A. Ghasemi and E. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," *J. Commun.*, vol. 2, no. 2, pp. 71–82, 2007.

[20] X.Wang, Z. Li, P.Xu, Y.Xu, X.Gao, H. Chen, "Spectrum Sharing in Cognitive Radio Networks – An Auction based Approach," inIEEE Trans. Syst. Man Cybern. B, Cybern.,vol40, no. 3, pp. 587–596, 2010.

Lingjie Duan (S'09–M'12) received his Ph.D. degree in Information Engineering at The Chinese University of Hong Kong, Hong Kong in 2012. He is currently an Assistant Professor in Engineering Systems and Design, Singapore University of Technology and Design, Singapore. His research interests are in the area of research allocation and game theoretical analysis of communication networks. He has been on the technical program committees (TPC) for IEEE VTC, PIMRC, and WCNC.



Alexander W. Min (M'11) received the BS degree in Electrical Engineering from Seoul National University, Korea, in 2005 and the Ph.D. degree in Electrical Engineering and Computer Science from the University of Michigan, Ann Arbor, in 2011. He is currently a Research Scientist in the Circuits and Systems Research at Intel Labs. His research interests are in the areas of cognitive radio and dynamic spectrum access networks, wireless security, low power mobile platforms, and mobile sensing. He is a member of the ACM and IEEE.

Jianwei Huang (S'01-M'06-SM'11) is an Assistant Professor in the Department of Information Engineering at the Chinese University of Hong Kong. He leads the Network Communications and Economics Lab (ncel.ie.cuhk.edu.hk), with main research focuses on network economics, cognitive radio networks, and smart grid. He is the recipient of the IEEE Marconi Prize Paper Award in Wireless Communications in 2011, the IEEE GLOBECOM Best Paper Award in 2010, the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2009, and Asia-Pacific Conference on Communications Best Paper Award in 2009. Dr. Huang serves as Editor of *IEEE Journal on Selected Areas in Communications - Cognitive Radio Series* and *IEEE Transactions on Wireless Communications*. Dr. Huang is the Chair of IEEE Multimedia Communications Technical Committee.

Kang G. Shin is the Kevin & Nancy O'Connor Professor of Computer Science in the Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor. His current research focuses on computing systems and networks as well as on embedded real-time and cyber-physical systems. He has supervised the completion of 72 PhDs, and authored/coauthored more than 780 technical articles (more than 280 of these are in archival journals), one a textbook and more than 20 patents or invention disclosures, and received numerous best paper awards, including the Best Paper Awards from the 2011 IEEE International Conference on Autonomic Computing, the 2010 and 2000 USENIX Annual Technical Conferences, as well as the 2003 IEEE Communications Society William R. Bennett Prize Paper Award and the 1987 Outstanding IEEE Transactions of Automatic Control Paper Award. He has also received several institutional awards, including the Research Excellence Award in 1989, Distinguished Faculty Achievement Award in 2001, and Stephen Attwood Award in 2004 from The University of Michigan (the highest honor bestowed to Michigan Engineering faculty); a Distinguished Alumni Award of the College of Engineering; 2003 IEEE RTC Technical Achievement Award; and 2006 Ho-Am Prize in Engineering (the highest honor bestowed to Korean-origin engineers).