CONTRIBUTED PAPER

A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions

In this paper, both short- and long-term effects of security threats are examined, as well as means of combating them.

By Alireza Attar, Helen Tang, *Senior Member IEEE*, Athanasios V. Vasilakos, *Senior Member IEEE*, F. Richard Yu, *Senior Member IEEE*, and Victor C. M. Leung, *Fellow IEEE*

ABSTRACT | In this survey, we present a comprehensive list of major known security threats within a cognitive radio network (CRN) framework. We classify attack techniques based on the type of attacker, namely exogenous (external) attackers, intruding malicious nodes and greedy cognitive radios (CRs). We further discuss threats related to infrastructure-based CRNs as well as infrastructure-less networks. Besides the short-term effects of attacks over CRN performance, we also discuss the often ignored longer term behavioral changes that are enforced by such attacks via the learning capability of CRN. After elaborating on various attack strategies, we discuss potential solutions to combat those attacks. An overview of robust CR communications is also presented. We finally elaborate on future research directions pertinent to CRN security. We hope this survey paper can provide the insight and the roadmap for future research efforts in the emerging field of CRN security.

KEYWORDS | Cognitive radio (CR); denial of service (DoS); incumbent emulation; security; spectrum sensing data falsification (SSDF)

I. INTRODUCTION AND MOTIVATIONS

The phenomenal growth of cognitive radio (CR) over the past decade has attracted significant research and development efforts in academia and industry. Standardization initiatives such as the IEEE 802.22 [1] and the IEEE SCC41 [2] are now approaching fruition. Several proof-of-concept demonstrations of CR networking have verified the feasibility of this promising technology. On the regulatory side of the equation there has also been a welcome reception toward this innovative concept and the potential implementation of CR networks (CRNs) worldwide.

As CR technologies mature, the issues of operational robustness and security considerations gain increasing importance. Like any other wireless communication technology, a thorough analysis of reliability and security challenges in CRNs is a crucial step toward realization of practical solutions. While several studies on this topic have already appeared in the literature [3]–[6], the fast pace of innovations in this field mandates thorough, up-to-date surveying of security challenges in CRNs with the aim of

Manuscript received April 12, 2011; accepted June 28, 2012. Date of publication September 4, 2012; date of current version November 14, 2012.
A. Attar and **V. C. M. Leung** are with the Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC V6T 1Z4, Canada (e-mail: attar@ece.ubc.ca; vleung@ece.ubc.ca).
H. Tang is with the Secure Mobile Networking Group, Defense R&D Canada, Ottawa, ON, Canada and also with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: Helen.Tang@drdc-rddc.gc.ca).
A. V. Vasilakos is with the Department of Computer and Telecommunications Engineering, University of Western Macedonia, Kozani GR 50100, Greece and also with the Department of Electrical and Computer Engineering, National Technical University of Athens (NTUA), Athens 157 80, Greece (e-mail: vasilako@ath.forthnet.gr).
F. R. Yu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: Richard_Yu@Carleton.ca).
Digital Object Identifier: 10.1109/JPROC.2012.2208211

highlighting open questions and the road ahead. Therefore, the focus of this paper is on providing an insightful round up of existing solutions in the literature as well as highlighting potential challenges in CR communications.

From a high level perspective, two main classes of security issues in CRNs are general (traditional) security concerns, which are similar to other wireless communication systems, and CRN-specific threats. We limit the scope of our study to the latter class of security concerns, and only briefly cover general security issues which have been already investigated to a great extent in traditional wireless communication settings.

The main differentiation point between CRNs and traditional wireless systems is the issue of spectrum (more generally resources) access right. Legacy wireless technologies, whether operating over licensed bands or unlicensed spectrum, have adopted a "horizontal" spectrum access right paradigm. In this paradigm, all the participating nodes in the network are deemed equal in terms of their access rights to the radio spectrum upon which the network operates. For instance, in the unlicensed spectrum case, any transmitting device is allowed to utilize the band for its communication purposes, simultaneous to other similar or different nodes operating over that band. While intranetwork resource allocation and interference management over the unlicensed bands can be managed by specific medium-access protocols (MACs), such as those defined by the IEEE 802.11x standards, there is no intersystem interference mitigation mechanism to guarantee successful transmission and reception of data. Over licensed bands, on the other hand, MAC etiquettes regulate the communications priority of nodes in accessing the available resources.

Cognitive communication is based on a "vertical" spectrum access rights paradigm. In this context, CR nodes are secondary spectrum users authorized to access frequency channels only on a no- or limited-interference manner with respect to the licensed users of the band. This secondary spectrum access (SSA) status makes CRNs particularly vulnerable to attacks aiming to deny the CR nodes from spectrum access, i.e., denial of service (DoS) attacks [7], [8]. We will highlight major attack strategies differentiating between exogenous attackers, intruding malicious nodes and greedy CRs.

Given the central role of spectrum sensing in realization of SSA communication paradigm, studies of robustness of CRNs have mainly focused on robust sensing techniques. In this paper, we cover CRN robustness in a more holistic manner.

We note that the CRN architecture can be infrastructure based, for instance, the IEEE 802.22 standard, or infrastructure-less, such as *ad hoc* CRN. We will elaborate on attacks pertinent to each CRN architecture, as shown in Fig. 1, in the following sections.

The rest of the paper is organized as follows. Given the crucial role of spectrum sensing in various CR-specific security threats, Section II elaborates on the basics of spectrum sensing. Section III focuses on security issues in infrastructure-less CRNs, followed by Section IV, which details attacks in infrastructure-based networks. In Section V, we investigate some nonexclusive CR

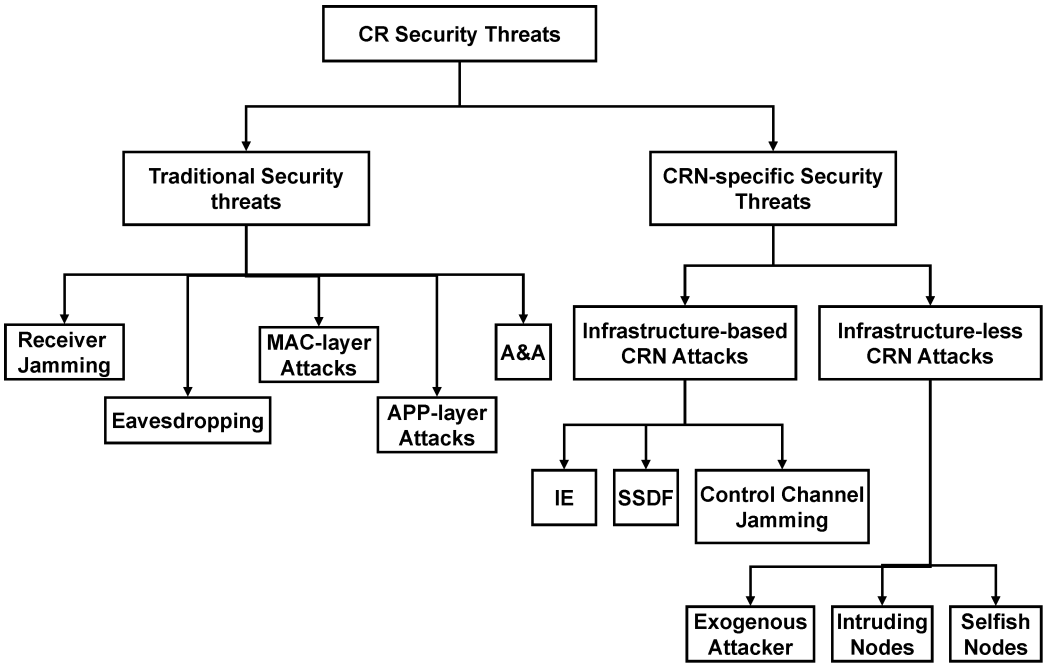

Fig. 1. *Classification of various attack scenarios in a CRN setting.*

security concerns, which are adapted toward a CRN context. Potential solutions to combat various attack techniques are introduced in Section VI. The issue of robust CR operation is covered in Section VII. Future research directions and concluding remarks are discussed in Section VIII.

II. BACKGROUND

There are no dedicated frequency bands for the operation of CRNs. Indeed, CRNs are designed to opportunistically operate over spectrum licensed to other radio networks. However, to safeguard the legacy radios, CRNs can only access those bands in a noninterference basis. This secondary nature of spectrum access by a CRN mandates accurate and reliable spectrum sensing as the first step toward utilizing idle bands.

As such, spectrum sensing plays a crucial role in the operation of CRNs and is a major source of security threats. In this section, we briefly discuss several spectrum sensing approaches, and in particular, present analytic description of the performance of energy-detection spectrum sensing in additive white Gaussian noise (AWGN) and fading channels. By far, energy detection is the most widely used spectrum sensing strategy in CRNs due to its simplicity of implementation as well as flexibility of deployment in both centralized and distributed CRNs. Our focus in this section will be on energy detection strategies in CRNs, which can provide insight into the operation of CRNs and also the attack strategies that are discussed in the following sections. We will also cover strategies to increase the robustness of energy detection schemes.

A. Single-Node (Local) Sensing

Let us denote the received samples at the sensing node i by

$$x_i[l] = \begin{cases} n_i[l], & H_0 \\ n_i[l] + |h_i[l]|^2 s[l], & H_1 \end{cases} \quad (1)$$

where l denotes the sample index, $n_i[l]$ is the lth AWGN sample, $|h_i[l]|^2$ represents the sampled channel gain from primary transmitter to sensing node i, and $s[l]$ denotes the primary signal sample. H_0 and H_1 represent the hypothesis of idle and busy channels, respectively. Energy detector adds the energy of L samples together and compares the output with a certain detection threshold γ_0 as follows:

$$y_i = \sum_{l=1}^{L} x_i[l] \underset{H_1}{\overset{H_0}{\gtrless}} \gamma_0. \quad (2)$$

Several studies in the literature have calculated the detection and false-alarm probability using the model described by (1) and (2) and have developed closed-form analytical results [9]–[11]. In particular, for AWGN channel, we have

$$P_{d,\text{local}} = Q_L(\sqrt{2L\gamma_i}, \sqrt{\gamma_0}) \quad (3)$$

where γ_i is the received signal-to-noise ratio (SNR) at sensing node i, and $Q_L(a,b)$ is the generalized Marcum Q-function defined as

$$Q_L(a,b) = \int_b^\infty \frac{x^L}{a^{L-1}} e^{-\frac{x^2+a^2}{2}} I_{L-1}(ax)\,dx$$

and $I_m(.)$ denotes modified Bessel function of order m. Similarly, the false-alarm probability is given by

$$P_{f,\text{local}} = \frac{\Gamma\left(L, \frac{\gamma_0}{2}\right)}{\Gamma(L)} \quad (4)$$

where $\Gamma(.,.)$ and $\Gamma(.)$ denote incomplete and complete gamma functions, respectively. Note that the false-alarm probability is only a function of detection threshold γ_0 and the number of samples L. However, as demonstrated in the literature, it is not feasible to enhance the detection probability arbitrarily by further sampling due to the uncertainty of the noise, a phenomenon referred to as SNR walls [12]. This lack of robustness can be improved by combining energy detection at several nodes in a CRN setting, i.e., cooperative spectrum sensing.

In Rayleigh fading channels, the false-alarm probability remains the same as (4). The detection probability has a random nature due to variability of the received SNR at the sensing node. Therefore, average detection probability is usually used and is given by

$$\overline{P}_{d,\text{local}} = \frac{\Gamma\left(L-1, \frac{\gamma_0}{2}\right)}{\Gamma(L-1)} + e^{-\frac{\gamma_0}{2(1+L\bar{\gamma}_i)}} \left(1 + \frac{1}{L\bar{\gamma}_i}\right)^{L-1} \times \left[1 - \frac{\Gamma\left(L-1, \frac{\gamma_0 L\bar{\gamma}_i}{2(1+L\bar{\gamma}_i)}\right)}{\Gamma(L-1)}\right] \quad (5)$$

where $\bar{\gamma}_i$ is the average received SNR at sensing node i.

B. Cooperative Spectrum Sensing

In many practical CRN scenarios and in order to improve the reliability of primary detection, sensing results of several nodes are taken into account to make the final spectrum sensing decision. The cooperative spectrum sensing technique can be exploited in both centralized (such as the IEEE 802.22 standard) and *ad hoc* CRNs. Although technically it is possible to aggregate the raw spectrum sampling data from various nodes, to reduce the overhead usually only the binary local detection decision is exchanged. Furthermore, there are many sensing fusion rules that can be exploited in order to arrive at the final spectrum sensing decision. A general sensing data fusion rule is the k-out-of-n rule whereby at least k local spectrum sensing decisions, out of the total n sensors, should be "busy" to declare the channel "busy." In this setting, if the probability of detection at local node i is given by (3) [or in the case of fading channels by (5)], the cooperative probability of detection can be calculated as

$$P_{d,\text{global}} = 1 - \sum_{i=1}^{k-1} \binom{n}{i} P_{d,\text{local}}^{i} \left(1 - P_{d,\text{local}}^{i}\right)^{n-i}. \qquad (6)$$

In this model, the AND rule is defined as the case when $k = n$ and the OR rule is defined as $k = 1$. The global probability of the false alarm can be calculated from local false-alarm probabilities in a similar manner. In Section II-C, we will use the derived probabilities of detection and false alarm in this section to explain various CR attacks and their possible combat techniques.

C. Other Spectrum Sensing Techniques

In the interest of completeness, we also briefly cover some other spectrum sensing techniques developed in the literature. The interested reader can refer to [13] and [14] for the more comprehensive surveys of spectrum sensing approaches.

1) Feature Detection: A more sophisticated spectrum sensing strategy is to detect the primary signal based on known characteristics of the primary waveform. Features such as cyclostationary signal measures, pilot pattern, or detection of signal modulation are among possible detection criteria [15]. The tradeoff in this case is the higher sensing decision delay due to the required complex signal processing techniques on the one hand, and a higher probability of primary detection on the other hand.

2) Change Detection: The underlying phenomenon utilized in change detection schemes is the switching between the distribution of sequential samples of a stochastic process before and after a known change happens. In a CRN setting, the spectrum samples before the return of primary transmitter will follow noise-like statistics, as noted in (1). Several studies in the literature have developed Bayesian or minmax strategies for change detection [16], [17].

3) Consensus Schemes: A number of distributed spectrum sensing techniques follow consensus formation, whereby individual CR nodes make local spectrum sensing decision without the need of a fusion center [18]–[20]. Some of these consensus algorithms are biologically inspired based on the self-organizing behavior of animal groups such as birds, fish, ants, or honeybees.

III. INFRASTRUCTURE-LESS CRN-SPECIFIC ATTACKS

We start investigating CRN-specific security threats from infrastructure-less CR settings. The main source of security threats in a distributed CRN setting is manipulation of a spectrum sensing process by the adversaries. As discussed in Section II, two main classes of distributed spectrum sensing (DSS) solutions are with "data collection" node or "consensus-based" algorithms.

The sophistication of attack strategy depends on factors such as the spectrum sensing technique exploited by the CRN and possibility/simplicity of intrusion to the CRN, among other factors. To provide an insightful description of infrastructure-less CRN attacks, we proceed by differentiating attackers as exogenous attackers, intruding nodes and greedy CRs.

A. Exogenous Attackers

An external adversary node is not part of the CRN and thus not part of the CRN's spectrum sensing decision making. However, such exogenous attackers can affect the successful operation of an *ad hoc* CRN through jamming attacks. The target of jamming attack can be the DSS process or else it can affect the common control channel of the CRN. Furthermore, if the CRN utilizes a feature-detection spectrum sensing strategy, the exogenous attacker can follow incumbent emulation (IE) attacks.

1) Jamming: Using energy detection for spectrum sensing in *ad hoc* CRNs opens the network to CRN-specific sensor-jamming attacks where an attacker floods the sensed channel with white/colored noise. The jamming signal will increase the received SNR at the local energy-detection sensing nodes. For instance, in AWGN channel model given by (3), and assuming no primary signal over the targeted channel is present, $\gamma_i = \gamma_{i,\text{attack}}$ should be used as the received SNR at the local sensing node, where $\gamma_{i,\text{attack}}$ denotes the received attacker's signal strength at the sensing node. The resulting detection probability in presence of sensor jammers is denoted by $P_{d,\text{attack}}$. Similarly, for fading channels, we have $\bar{\gamma}_i = \bar{\gamma}_{i,\text{attack}}$, where $\bar{\gamma}_{i,\text{attack}}$ represents the average received SNR from the

attacker at the local sensing node. Thus, the total probability of the false alarm in presence of an attacker will increase to

$$P_{f,\text{attack}} = P_{f,\text{local}} + P_{d,\text{attack}} \tag{7}$$

in the AWGN channel model. A similar increase in false-alarm probability for a fading channel is expected.

The effect of a considerable increase in the local false-alarm probability, as denoted by (7), on the overall performance of the *ad hoc* CRN can be significant. In data-collection schemes, such as given by (6), as well as consensus-based algorithms, the increased false-alarm probability at local sensing nodes might force the entire *ad hoc* CRN to abandon a given sensed channel in the false belief of the availability of the primary's signal in that channel.

The learning capability of CRs, while essential in performing cognitive tasks, amplifies the effect of sensor-jamming attacks well beyond the instance of an attack. Various machine learning techniques including reinforcement learning and Q-learning have been studied to provide the CR nodes with a mechanism to interact with their radio-frequency (RF) environment [21]. In most machine learning solutions, there is a well-known tradeoff between exploration (jumping to new channels for sensing and determining their probability of being idle/busy) versus exploitation (staying over those channels that are known to have a high probability of being idle) [22]. When after several sensing attempts a certain channel is wrongly determined as busy by the DSS process due to sensor-jamming attack, the local sensing node will return to that channel in the future with a much lower probability. Therefore, even a short-term sensor-jamming attack limits the operation of an *ad hoc* CRN in a long term by preventing the network from accessing otherwise idle bands. We explore the long-term effect of the CRN attack with more detail in Section V.

Moreover, *ad hoc* CRN nodes require a common control channel to identify their peers and coordinate their resource access [23], [24]. Therefore, an exogenous attacker can also disrupt the operation of a CRN by transmitting jamming signals over such common control channel. We refer to this type of an attack as "*control channel jamming*."

2) Incumbent Emulation (IE): As discussed in Section III, feature detection can provide a more reliable primary detection strategy, which makes it more difficult for a sensor jammer to mount a DoS attack on the CRN. Instead, the adversary node(s) can deter the *ad hoc* CRN from accessing a given primary channel by transmitting a signal closely mimicking the primary's waveform. This type of attack is generally known as IE in the literature [25]. We note that due to the complexity of feature detection schemes, these spectrum sensing methods are more suitable in infrastructure-based CRNs. As such, IE attacks are expected to be more frequent in such centralized settings.

B. Intruding Attackers

Ad hoc CRNs are vulnerable to attacks from intruding adversary nodes which can penetrate into the network posing as legitimate nodes. The infiltrated malicious node can influence the overall spectrum sensing decision of CRN mainly via reporting misleading local sensing data. This class of CRN-specific security issue is known as the spectrum sensing data falsification (SSDF) [26]–[32].

The simplest type of SSDF attacks is performed by always reporting a channel busy or idle [9]. More complex attackers selectively provide false spectrum sensing reports so as to keep their attack strategy more difficult to identify [8].

However, we need to differentiate intruding nodes from greedy CRs, which might also follow sensing data falsification with the aim of skewing the legitimate resource access competition within a CRN. The reason to separate the intruding nodes from the greedy CRs, from security analysis perspective, is the difference in the motivation of attacks in each case, which in turn mandates different security solutions, as will be discussed in Section VII.

C. Greedy CRs

In *ad hoc* CRNs, a degree of competition in utilizing the available spectrum resources exists [22]. This competition might motivate some greedy CRs, which unlike intruding nodes are authenticated and authorized members of the CRN, to misbehave in order to increase their chances of reserving the medium. In its natural extent, greedy behavior of CR nodes is known to reduce the total network capacity compared to a cooperative networking strategy [33], [34]. What constitutes a security concern in *ad hoc* CRNs is the possibility of untruthful behavior within the adopted MAC framework.

As an example, if the CRN MAC scheme follows ALOHA-style handshaking with random backoff mechanism, a greedy CR can manipulate the backoff window so as to increase its probability of access to the spectrum. Note that as CRs are built upon software-defined radio (SDR) platforms, tweaking MAC parameters based on observation and learning from the RF environment is potentially feasible.

IV. INFRASTRUCTURE-BASED CRN-SPECIFIC ATTACKS

The development of infrastructure-based CRNs has been investigated in academia and industry in the past several years. A good example is the IEEE 802.22 standard which

follows a cellular architecture. Given that the deployment of an infrastructure-based network is time consuming and costly, it is expected that such CRNs will mainly be tuned toward frequency bands with considerable secondary spectrum stability. As an example, the IEEE 802.22 standard is expected to deliver broadband wireless access over unused TV bands in rural areas.

The spectrum regulators, such as the U.S. Federal Communications Commission (FCC), have stipulated stringent spectrum sensing accuracy targets in conjunction with the possibility of exploiting geolocation databases to ensure primary users, such as digital TV receivers, are not affected by SSA of any CRN. Thus, spectrum sensing constitutes the main source of CRN-specific security threats in infrastructure-based networks as well. Similar to Section III, we elaborate here on attack strategies differentiated by the executor entity.

A. Exogenous Attackers

Similar to *ad hoc* CRNs, the two classes of spectrum sensing attacks might be implemented by external adversary nodes. An exogenous attacker can mount IE or sensor-jamming attacks on an infrastructure-based CRN. For instance, in the IEEE 802.22 standard, user devices known as consumer premises equipment (CPE) form a DSS network. The IEEE 802.22 base station (BS) coordinates quite periods for coarse and fine local spectrum sensing by CPEs [1], the results of which are fed back to the BS. Therefore, similar to an *ad hoc* CRN, the attacker can increase the local false-alarm probability in order to skew the decision of the IEEE 802.22 BS regarding the availability of a given band.

Given the centralized processing capability of an infrastructure-based CRN, feature detection schemes are more likely to be developed in such CRNs. As such, the more sophisticated IE attacks by exogenous adversaries are more possible in centralized CRN architectures. Nevertheless, efficient combat strategies against IE attacks have been developed in the literature [25] and will be presented in Section VII.

Furthermore, exogenous attackers can degrade the operation of a centralized CRN architecture, perhaps to the point of DoS, via common control channel jamming. Besides general wireless communication operations, the common control channel in an infrastructure-based CRN can be utilized to orchestrate the spectrum sensing process, as for instance discussed in the IEEE 802.22 setting. Therefore, disrupting the access to the control channel will severely affect a CRN.

Consider a scenario where in total N channels are available for secondary spectrum access. It is generally assumed that the channels follow an independent availability pattern with a probability density function (pdf) $f^n(\boldsymbol{\theta})$, where $n \in \{1, 2, \ldots\}$ denotes the index of a resource access period and $\boldsymbol{\theta} = [\theta_1\ \theta_2\ \ldots\ \theta_N]$, where θ_i is the probability of the availability of the ith channel. The utility of the CRN at period n is denoted by $U[n]$, which can depend on the availability pattern of licensed channels and the MAC protocol of the CRN. The CRN follows an expected utility maximization policy in general. The MAC protocol in any CRN architecture consists of spectrum sensing before data transmission and the feasible utility is directly proportional to the availability of primary channels. If $\boldsymbol{\theta}$ is *a priori* known, the optimal strategy is to choose the channel that satisfies

$$i^* = \arg\max_i \theta_i .$$

In the absence of the knowledge of $\boldsymbol{\theta}$, the optimal resource access strategy is to strike a balance between short-term and long-term gains. In short term, sensing those channels that are already known to have a high probability of being idle provides immediate transmission opportunities. This greedy strategy is also known in the literature as "exploitation." Further, by choosing to sense less tested channels, the CRN updates its estimate of $f^n(\boldsymbol{\theta})$, after $n-1$ observations, which is known in the literature as "exploration" [22].

Several published studies have investigated the optimal spectrum sensing and access strategy in a distributed CRN architecture [22], [36], [37]. The underlying stochastic process governing the availability or occupancy of a given channel can be assumed as a two-state Markovian process, following the Gilbert–Elliot channel model [38]. Whereas traditional wireless communication systems perceive the quality of radio channel as a continuous random variable, the Gilbert–Elliot channel model better matches the "binary" perception of frequency channels in CR settings, as CR transmission is conditioned upon the availability of the primary channel, irrespective of its quality.

As the CRN might not be able to simultaneously scan all available channels (due to delay and processing power limitations), it should select a subset of channels to explore at any given resource allocation period. It is imperative that the state (availability or occupancy) of not-selected channels will also evolve over time, therefore, the cognitive spectrum access problem can naturally be modeled as a multiarmed bandit problem [39]. In [36] and [37], partially observed Markov decision process (POMDP) models have been developed to study this problem. Given the prohibitive complexity of determining the optimal spectrum sensing and access strategy, especially as the number of available channels grows, Zhao *et al.* [36] and Haji Ali Ahmad *et al.* [37] establish conditions upon which a myopic strategy of selecting the channel with the highest availability probability for the next access period is optimal.

A jamming attack in resource access period n will then have both short-term and long-term effects. If the jammed

channel is the chosen channel to be sensed at period n by the CRN, the exogenous attacker might succeed in skewing the overall CRN sensing decision on the attacked channel to *busy* and thus unfairly deny the network from accessing that channel. This DoS effect results in a short-term exploitation loss whereby $U[n] = 0$. Furthermore, depending on how the CRN updates its belief of the spectrum occupancy probability, the jammed channel will be less likely to be selected by the CRN over the longer time horizon. In the following, we provide two specific examples, a Bayesian approach and a Q-learning model, to highlight how the long-term learning process of CRNs is affected by short-term jamming attacks.

Example 1: Following the approach in [22], denote by $s[n]$ the selected channel by CRN for sensing and possible access in time slot n. Further, define the outcome of sensing $s[n]$ at that instance by $Z_{s[n]}[n] \in \{0, 1\}$, where "0" and "1" represent busy and available, respectively. Then, after the channel sensing decision at time slot n is finalized by the CRN, the estimated joint probability density function of channel availability should be updated in a Bayesian manner, as follows [22]:

$$f^{n+1}(\boldsymbol{\theta}) = \begin{cases} \dfrac{\theta_{s[n]} f^n(\boldsymbol{\theta})}{\int \theta_{s[n]} f^n(\boldsymbol{\theta}) d\boldsymbol{\theta}}, & \text{if } Z_{s[n]}[n] = 1 \\ \dfrac{(1-\theta_{s[n]}) f^n(\boldsymbol{\theta})}{\int (1-\theta_{s[n]}) f^n(\boldsymbol{\theta}) d\boldsymbol{\theta}}, & \text{if } Z_{s[n]}[n] = 0. \end{cases}$$

A jamming-induced false alarm in channel sensing, where $Z_{s[n]}[n]$ is set to 0 instead of 1, will alter the network's belief on the availability of specific channels in the long term.

Example 2: Among various reinforcement learning schemes proposed in the literature, Q-learning is a widely used technique which has also been adopted in many wireless communication applications, including CRNs [40]. In particular, Q-learning provides a mapping framework from the space of action states to the space of rewards [41], [42]. In a CRN context, the space of states S involves the availability or occupancy of primary channels, i.e., the Gilbert–Elliot channel model [38]. The space of actions A can involve staying over a given channel or jumping to another channel. The decision to jump to a new channel can be triggered by the return of a primary transmitter to that channel or as part of the exploration strategy of the CRN. The space of rewards R can be composed of short-term exploitation gains or a combination of short-term and long-term exploration gains.

At time slot n, denote by $s[n]$ and $a[n]$ the current state and action, which results in changing the state to $s[n+1]$ and observing a reward of $R(s[n+1])$. Then, function $Q(s[n], a[n])$, which returns the quality of the state–action combination, needs to be updated to

$$Q(s[n], a[n]) \leftarrow Q(s[n], a[n]) + \alpha_n(s[n], a[n]) \times \left[R\left(s[n+1] + \gamma \times \max_a Q(s[n+1], a) - Q(s[n], a[n]) \right) \right.$$

where $\alpha_n(.,.)$ represents the learning rate and $0 \leq \gamma < 1$ is a discount factor to allow infinite time horizon analysis. In this setting, the long-term effect of the jamming attack, which propagates through the Q-learning mechanism, depends on the learning rate α_n. By setting $\alpha_n(s[n], a[n]) = 0$, the CRN stops the learning process. Alternatively, choosing $\alpha_n(s[n], a[n]) = 1$ results in a "short-memory" effect, whereby the CRN only learns based on its most recent action–space choice.

Based on the above examples, as well as the earlier discussion on POMDP approach to modeling CRN spectrum access strategy, upon several attempts to sense a given channel i, which is under the jamming attack, the availability probability will be estimated much lower than another uncompromised channel j, such that $E[\theta_i] \ll E[\theta_j]$, where $E[.]$ denotes statistical expectation. Then, whether the CRN follows a myopic sensing/access strategy or aims for longer term returns via Q-learning, for instance, it will be highly unlikely that channel i is selected over j, even after the jamming attack is terminated.

B. Intruding Attackers

Similar to *ad hoc* CRNs, an intruding attacker can initiate an SSDF-style attack by providing the central decision making entity within an infrastructure-based CRN with misleading sensing data. Given the centralized process of authorization and authentication (A&A) of nodes in an infrastructure-based CRN, however, it is more challenging for an adversary node to infiltrate the CRN network.

C. Greedy CRs

In infrastructure-based CRNS, unlike the infrastructureless counterparts, the medium-access rights are allocated by the centralized BS. However, in order to perform the scheduling, the CR BS relies on the feedback from CR nodes, such as pertinent to the channel state information (CSI), their buffer size, or application QoS requirements, among other possible parameters. Therefore, the SDR capabilities of CR nodes provide the greedy nodes with the opportunity of misbehavior by reporting false CSI or similar manipulations of the feedback signaling. The nature of untruthful feedback information to a great extent depends on the scheduling policy of CR BS. For instance, in opportunistic scheduling, the BS selects the CR node with the highest channel gain in each frequency channel to be served in a given time slot. Therefore, by exaggerating its

true channel gain, a greedy CR can enhance the probability of being served unlawfully.

Before elaborating on other security issues, which are also commonplace in traditional wireless systems, we cover a unique aspect of CRs, i.e., their learning capability, as it provides a framework to extend the effect of CRN attacks beyond the instance of the attack.

V. NON-CRN-EXCLUSIVE ATTACKS

In Sections III and IV, we elaborated on various attack strategies that were specifically developed for CRNs. However, the array of potential security threats to CRNs is not limited to those discussed in Sections III and IV. In this section, we briefly cover other potential threats which are also commonplace in traditional wireless systems in a CRN context.

A. Receiver Jamming

CR receivers, similar to other wireless technologies, require a minimum received SNR when trying to decode the signal from their corresponding transmitters. One of the oldest and most widely used attack strategies is then to reduce the received SNR below the required threshold by transmitting noise over the received channel [43], [44]. We refer to this attack technique as "*receiver jamming*" to distinguish it from other possible jamming techniques discussed before.

B. Eavesdropping

Another type of security threat which is commonplace in most wireless systems is the privacy of the data communicated over those systems. An eavesdropper might get access to the content of exchanged data over wireless links, such as in CRNs [45], and then exploit this information against the end users or the network.

C. MAC-Layer Attacks

CRs are usually built over an SDR platform so as to facilitate the necessary reconfigurability characteristics of its transmission. The ability of cognitive nodes to alter their transmission specification can potentially pose security threats when a malicious node takes advantage of this flexibility for its benefit. As an example, Zhu and Zhou [46] introduce several such greedy misbehaviors in an *ad hoc* CRN setting. In particular, the channel negotiations between two CR nodes in a multihop network can include three types of MAC frames, namely, free channel list (FCL, which contains available channels at the transmitting node), SELection (SEL, which denotes the receiving node's channel choice), and REServation (RES, which is broadcast to the network to reserve the communication channel).

It is then possible for an intruding node to create forged control channel messages so as to saturate a common control channel of the *ad hoc* CRN. This strategy constitutes a DoS attack against the CRN. Further, it is possible for a greedy CR node to report a fraudulent SEL to the requests of a source node, for instance, indicating no available channel toward a destination node. The greedy node then utilizes those available channels for its own communications rather than relaying. Such greedy nodes will enjoy an unfair level of access to the shared channel compared with truthful CR nodes.

D. Authorization and Authentication

Whether CRN architecture is centralized or distributed, the issue of authentication of network nodes is of utmost importance. Failure to establish the identity of sensing nodes facilitates intrusion of malicious nodes within the network, which, as already discussed, can result in SSDF or other attacks. Therefore, the authentication of sensing terminals and the spectrum sensing data are closely related in a CRN setting [5]. Authorization of CR nodes in accessing the secondary spectral resources also has crucial security implications. Protecting the primary receivers is a precondition of accessing the resources by the CRN. Thus, if prohibitive interference toward primary system is observed, it will be necessary to determine if such misbehavior is due to an authorized but faulty CR transmitter or an unauthorized malicious node.

E. Application-Layer Security

As the processing power of wireless handsets increases, so does the number of applications that can be accessed over mobile devices. CRNs inherently require a higher processing power and memory capacity than traditional user equipment such as smartphones so as to accommodate the need for extra tasks such as spectrum sensing and learning. It is expected that mobile devices will be the target of software viruses and malware in the same fashion as those observed in computer networks in the past [50], [51].

In the CRN setting in particular, to support the reconfigurability of the underlying SDR platform, it might be required to implement a mass upgrade of the PHY-layer software of nodes in a given locale [52] or on an individual bases, as provisioned by the IEEE P1900.B standard [53]. Such on-the-fly software download poses a security challenge in the sense that a malicious code might be transferred to legitimate CR nodes forcing unpredictable misbehaviors.

Before proceeding to discuss solutions to combat particular CRN security threats, we summarize the attacks in terms of their impact, long- or short-term effect, and probability of occurrence in Table 1.

VI. COMBATTING CRN ATTACKS

Several papers in the literature have covered an array of potential CRN threats and have also discussed certain solutions to such threats in a broad sense, such as those

Table 1 Impact and Probability of CRN Attacks

Attack type	*Impact*	*Time Horizon of Impact*	*Probability*
Receiver Jamming	Moderate to High	Short and Long Term	High
Eavesdropping	Low to Moderate	Long Term	Low
Mac-Layer Attacks	High	Short Term	High
App-Layer Attack	High	Long Term	Low
A&A	Moderate to High	Long Term	Low
IE	High	Short and Long Term	Low
SSDF	Moderate	Short and Long Term	Moderate
Control Channel Jamming	High	Short Term	Low

reported in [3]–[5] and [31]. In this section, we present a number of proposed solutions pertinent to specific CRN attacks, which were discussed in Sections III–V. In order to keep the consistency of the presented material, we follow the attacker classification approach of the previous sections. We elaborate on the implication of combating strategies for infrastructure-based and infrastructure-less CRNs in each case.

A. Exogenous Attacker

1) Sensor Jamming: There have been relatively fewer research efforts to address sensor-jamming attacks in the literature so far, compared with SSDF attacks, which are discussed next. The cooperative spectrum sensing policies such as DSS, initially developed to overcome the effect of local channel uncertainty, inherently provides a safeguard mechanism against sensor jamming by providing a spatially distributed sampling of the sensed frequency channels. It is likely that at any given time a number of sensing nodes fall outside the coverage area of the sensor jammer and thus can provide reliable sensing data. It is thus necessary to identify those sensing nodes affected by jamming in order to remove their sensing data from fusion rules or consensus algorithms.

One potential solution, proposed in [26] and [47], is a shadow-fading correlation-based filter that allows sensing nodes within a cluster to detect abnormal sensing reports. While the main application of this technique is to combat SSDF attacks (see Section VI-B1), it can potentially be utilized to determine if certain areas within a cluster are facing jamming signals. Further, such cluster-based cooperative sensing techniques improve the primary detection probability and thus make the network more resilient toward sensor jamming.

2) Common Control Channel Jamming: There have been very few studies so far that propose countermeasures toward control channel jamming, particularly in CRNs. In *ad hoc* CRNs, due to the point-to-point nature of communications, the network can adopt a noncommon control channel strategy whereby nodes stay on each available channel for a certain time to identify any other node operating on that band in their proximity. Each node continues to jump between channels in order to develop a table of existing neighboring nodes and their operating channel. Such noncommon control channel strategy can be part of multihop routing strategies widely studied in the mobile *ad hoc* network (MANET) framework [48].

In infrastructure-based CRNs, a common control channel is also widely used [23]. Usage of interference-resilient waveforms, such as spread-spectrum (SS) techniques, and exploitation of error detection and correction coding are among potential solutions to combat control channel jamming. Due to frequency agility of CR nodes, it might also be possible to switch the control channel of the network from time to time in an attempt to safeguard signaling packets against interferes.

3) Receiver Jamming: Combating receiver jamming has been studied for many years in wireless communications, as such jamming attacks are among the most widely used threats in practice. The first issue to combat receiver jamming is to identify the existence of a jammer. In other words, the wireless network, for instance a CRN, should conclusively determine if the poor performance of a receiving node is due to natural causes, including channel ailments and network congestion, or due to prohibitive interference from a jamming attacker. The presented results in [43] verify that measuring signal strength and carrier sensing time is not sufficient to determine existence of a jammer. The authors propose two consistency checking parameters to detect an attacker. Upon detection of a receiver jammer, anti-jamming techniques must be exploited to overcome its interfering effect. SS communication techniques, such as direct sequence SS and frequency hopping SS, are among the most widely used anti-jamming solutions due to their superior performance in the presence of interference. Further, employing powerful error detection and correction coding can enhance the receiver performance in presence of jamming.

CRNs, due to their inherent frequency agility and the potential of PHY-layer reconfigurability, have some extra weapons in their defense arsenal to resist receiver-jamming attacks. However, few studies in the literature so far have focused on this security aspect of CR communications. Yue *et al.* [54] have developed two coding techniques, namely rateless coding and piecewise coding, to

protect CRNs against receiver jamming. A game-theoretic framework to combat jamming in CRNs is developed in [55], whereby the CRN observes the state of available channels, the quality of these channels, and the strategy of jammer, and makes decisions accordingly. Utilizing a Q-learning policy, the CRN can learn the optimal channel utilization strategy, including how many channels to use for data and control packets as well as the channel switching strategy. Also, Altman *et al.* [44] develop power distribution strategies over multiple channels in the face of uncertainty of a jamming attack. The proposed zero-sum game in [44] can be further utilized to help wireless receivers determine those channels which are more likely to be jammed by an attacker.

4) Incumbent Emulation: An effective defense technique against IE attacks is based on verifying *a priori* known information regarding the primary transmitter such as the location of transmitters (e.g., when the primary system is TV broadcasting towers) [25], [31]. As discussed previously, FCC has proposed to develop geolocation databases to enhance reliability of communications over TV white spaces, which can serve as a verification source to identify real versus fake primary transmitters.

B. Intruding Node

1) Spectrum Sensing Data Falsification: Combating falsified sensing data in CRNs has received considerable research attention in the past. A number of studies in the literature propose to identify outlier reports. Besides the already discussed cross checking by shadow fading correlation-based filter in [26] and [47], a trustworthiness score is proposed in [27] to develop a reputation weight for sensing nodes. In a similar approach, Wangz *et al.* [28] also develop a trust-value indicator to detect malicious CRs through evaluating a suspicious level of nodes. An outlier detection scheme based on prefiltering the sensing data is proposed in [29]. Other studies with similar reputation-based sensing data fusion include [30]–[32] and [49] among others.

2) MAC-Layer Attacks: Potential defense mechanisms against CRN MAC-layer attacks mainly involve identifying intruding/misbehaving nodes. In a centralized CRN architecture, such as the IEEE 802.22 standard, monitoring the behavior of CR nodes can be the responsibility of the central BS. If the BS notes in excessive control packets from a limited number of CR nodes saturate the control channel, it can block those nodes by not allocating any signaling and communication resources to those nodes. In a distributed CRN, a clustering strategy can be exploited whereby cluster members can crosscheck the behavior of other member nodes.

The above strategy is also effective against other MAC-layer misbehaviors, such as incorrect SEL data or abnormal access rate of certain nodes, implying a backoff window manipulation.

3) Authentication and Authorization: Implementing effective mechanisms to secure the authentication and authorization process in CRNs, especially in distributed network architectures, can prevent intruding malicious nodes and serve as a corner stone to enhance the security of PHY-MAC layer operations as well. We have developed several distributed authentication techniques in the general framework of MANET that can readily be extended to distributed CRN architectures as well [56]–[58].

4) Eavesdropping: Unauthorized accessing of the exchanged data over a wireless link, such as in CRNs, can take place by intruding nodes as well as exogenous attackers, both in centralized and distributed network architectures. A number of information-theoretic studies have tried to determine the secrecy capacity of a wireless channel, i.e., the maximum transmission rate between two legitimate parties while an eavesdropper tries to decode the exchanged data. An interesting result, reported in [59], demonstrates that fading in the communication channel (as opposed to Gaussian channels) can help the legitimate nodes achieve a secure communication due to outage probability at the eavesdropper receiver. Further studies in the literature examined the wiretap channel, including [45] and [60]–[62].

It is, therefore, possible to envision secure communication techniques in CRN context to achieve the developed secrecy channel capacity in practical scenarios. As an example, for distributed communications networks, Saad *et al.* [63] propose a coalition formation approach whereby neighboring nodes form disjoint coalitions with the aim of maximizing their secrecy rate.

C. Greedy CRs

1) Misreporting: The main misbehavior pertinent to legitimate but greedy CRs is the employment of untruthful approaches, such as misreports, so as to place such nodes in advantage compared with truthful CRs. A number of schemes to prevent such greedy misbehavior can be envisioned. Monitoring the behavior of CR nodes, by a centralized BS or the peer nodes, depending on the network architecture and provisioning punishment schemes to penalize detected greedy behavior, is one possible way to explore.

Another approach is misbehavior incentive reduction. For instance, in [8], we developed an incentive elimination strategy to combat SSDF by greedy nodes based on minimizing the difference in the utility of truthful and falsifying nodes in a DSS setting. As another example utilizing fairness measures in scheduling, CR nodes in a centralized architecture can also reduce the motivation to report exaggerated CSI information.

A further possible method to combat untruthfulness can be realized through "mechanism design" [65], [66]. In essence, mechanism design aims to devise a framework to ensure the outcome of a given game, based on the rationality assumption of players, converged to a desired equilibrium. This method, for instance, has successfully been implemented in auction design in the literature and can be adapted to specific CRN scenarios as required.

VII. ROBUSTNESS OF CRNs

Robust communication (and more generally robustness in computer science) examines the effect of errors on execution of certain algorithms (e.g., optimization) and aims to develop a solution to improve the processing capability of a system in face of inaccurate or erroneous input data. For instance, traditional wireless communication models assumed that timely and accurate information of a radio channel is available at both transmitter and receiver sides. Such simplifying assumptions, while increasing the tractability of the problem at hand, result in suboptimal operational efficiency. Recent wireless communication studies improve upon "perfect" information assumptions by considering the effect of lack of channel information at the transmitter side, for example, [67] and [68].

With the same token, studies of CRNs are evolving to consider the effect of errors, intentionally induced by an attacker or otherwise, on the performance of primary and secondary users. CRs face similar robustness challenges as traditional wireless systems, such as in synchronization, precoding, beamforming, and transmit power control among others.

Robust transmit power control for the CR is studied in [69], where the worst case interference scenario is considered in a dynamic framework, and both equilibrium and dis-equilibrium (transient) behaviors of the CR network are studied. Wang *et al.* [70] study a robust CR system with imperfect CSI. A strategic noncooperative game is used to model the SU network. The imperfectness of PU CSI is taken into account through the robust interference constraints, which limit the interference generated by an SU to a PU.

In a multiple-input–multiple-output (MIMO) CRN, linear precoding needs to deal with imperfect CSI. Islam *et al.* [71] develop a robust precoding solution, given a fixed orthogonal space-time block code (OSTBC). Similarly, Gong *et al.* [72] study transceiver optimization for cognitive MIMO communication systems. Robust beamforming for MIMO CRNs is also studied in [73] and [73].

In distributed CRNs, robustness becomes more important as there is no central coordinator to manage the consequences of input data or processing errors. A stochastic transmit power control approach based on utilizing incumbent user outage information is proposed in [75], which enhances CRN performance compared to worst case analysis models commonly used in the literature to achieve robustness. In the context of *ad hoc* CRNs, Li and Gross [76] propose a clustering mechanism to deal with the changing availability of radio channels and thus CRN connectivity. By focusing on intraconnectivity and interconnectivity of CR clusters, the proposed scheme achieves a degree of robustness when a given channel suddenly is redeemed by the primary user.

Robustness of cognitive communications in presence of malicious nodes is another critical aspect pertaining reliability of CRNs. Li and Han analyze an incumbent emulation attack where the channel availability statistics is unknown to both the CRN and the attacker [77]. The developed defense mechanisms are thus more robust than most studies in the literature. Similarly, Li and Han [78] improve upon Bayesian schemes of detecting falsifying CR nodes in a cooperative spectrum sensing setting, by relaxing the assumption that the data fusion center knows the strategy of the attacker. Another study, in [79], deals with unintentional orthogonal frequency-division modulation (OFDM) transmission power leakage to neighboring frequency channels in a CRN and provides a robust transmission scheme to improve the system performance.

The issue of robustness of cognitive communications has not been addressed sufficiently in the literature yet. The challenge of developing cognitive processing algorithms (pertaining to all aspects of cognitive cycle [21]) that can cope under possibility of error, and adversarial attacks, needs further attention from the research community.

VIII. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

The security considerations in a CRN setting are still in their infancy phase and require a more thorough analysis by the research community. A number of threats specifically pertains to cognitive communications, most notably to secure the spectrum sensing process against exogenous and insider malicious nodes. While an array of solutions, mainly based on trust ranking of cooperating nodes, have been developed to combat SSDF attacks, it is further crucial to more closely examine other attacks including IE and sensor jamming. The far reaching effect of isolated attacks against CRNs, due to the learning-based interaction CR nodes with their RF environment, is another key issue to be more vigorously investigated. In the following, a number of potential research directions are introduced.

A. A Cross-Layer Approach to CRN Security

Different layers in the CRN need the authentication for their different functionalities. It is then possible to integrate the authentication from higher layers into the MAC-PHY layer. This approach will save the cost of communication and provide a unifying framework to address the authentication of sensing nodes as well as the sensing data, among other possibilities.

B. Distributed CRN Monitoring

Irrespective of the architecture of the CRN, local nodes share certain channel characteristics due to shadowing and fading correlation. Observation of such correlated parameters within a certain locale can unearth misbehavior of greedy CR nodes as well as intruding adversary nodes. Besides the radio channel, nodes in geographic proximity can also follow clustering schemes to detect anomaly in the performance of neighboring nodes such as those executed via manipulation of PHY-MAC-layer characteristics.

C. Joint Link and System Level Learning

A critical issue in defense against attacks on CRNs is to address the long-term effect of such attacks due to the RF environment learning of CR nodes. Each node will interact with and learn from its surrounding at a local level. Further, the overall CRN will also learn and try to optimize its performance in the face of collaboration or competition of its nodes as well as the effect of adversary nodes. It is therefore of utmost importance to develop adaptive strategies based on CRN learning capability to align the link and the system level requirements and to improve the overall network performance.

D. Incentive-Based Security Mechanisms

We classified the agents posing security threats in a CRN into three categories, namely exogenous adversaries, intruding malicious nodes, and greedy CRs. Each group will follow a different attack strategy. It is interesting to address the incentives for misbehaviors and attacks against a CRN so as to adopt incentive-minimization schemes. As an example, a greedy CR is seeking to further enhance its own performance at the expense of other network nodes. Thus, fair resource allocation strategies will ensure that no single node can sustain superior performance in the network, which in turn eliminates the opportunity of misbehavior based on fraudulent reports. Further, if such greedy CRs know that upon detection of their misbehavior the network will devise punishment strategies, it might decide not to act greedily.

E. Reliable Spectrum Sensing Schemes

Perhaps solutions to combat attacks against DSS schemes have been studied more than any other CR security issue. Still a thorough analysis to compare and contrast existing techniques, such as trust-weight fusion versus consensus-based algorithms, can provides further insights into pros and cons of each scheme and might lead future researchers toward developing more robust DSS solutions.

F. Anti-Jamming CR Techniques

As discussed in this paper, an exogenous attacker can cause CRN service disruption through emitting jamming signals geared toward sensors, control channels, or receivers. A common trait in all these attacks is the need for more interference-resilient communications schemes, for instance, to decode the received signals in very low SNR regimes or to detect the primary signal buried in the jammer's signal. Further studies are needed to target specific solutions regarding various jamming attacks within a CRN framework.

G. Robust Cognitive Communications

The algorithms that govern the behavior of CRNs generally fall into two categories: observing/learning the radio environment (e.g., spectrum sensing) and controlling the environment (e.g., interference management through transmit power control). There have been very few studies that examine the robustness of the above processes. Reliable spectrum sensing, efficient learning algorithms, and effective transmission strategies, especially under the presumption of input information error/inaccuracy/manipulation, should be vigorously studied. ■

REFERENCES

[1] C. Stevenson, G. Chouinard, L. Zhongding, W. Hu, S. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag.*, vol. 47, no. 1, pp .130–138, Jan. 2009.

[2] R. V. Prasad, P. Pawelczak, J. A. Hoffmeyer, and H. S. Berger, "Cognitive functionality in next generation wireless networks: Standardization efforts," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 72–78, Apr. 2008.

[3] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," *Mobile Net. Appl.*, vol. 13, no. 5, pp. 516–532, Oct. 2008.

[4] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun.*, Singapore, May 15–17, 2008, DOI: 10.1109/CROWNCOM.2008.4562534.

[5] J. L. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *Proc. Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun.*, Singapore, May 15–17, 2008, DOI: 10.1109/CROWNCOM.2008.4562536.

[6] A. N. Mody, R. Reddy, T. Kiernan, and T. X. Brown, "Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard," in *Proc. IEEE Military Commun. Conf.*, Boston, MA, Oct. 18–21, 2009, DOI: 10.1109/MILCOM.2009.5380058.

[7] Y. Tan, S. Sengupta, and K. P. Subbalakshmi, "Coordinated denial-of-service attacks in IEEE 802.22 networks," in *Proc. IEEE Int. Conf. Commun.*, Cape Town, South Africa, May 23–27, 2010, DOI: 10.1109/ICC.2010.5502431.

[8] S. Sodagari, A. Attar, V. Leung, and S. Bilen, "Denial of service attacks in cognitive radio networks through channel eviction triggering," in *Proc. IEEE Global Telecommun. Conf.*, Miami, FL, Dec. 6–10, 2010, DOI: 10.1109/GLOCOM.2010.5683177.

[9] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. IEEE Int. Conf. Commun.*, Istanbul, Turkey, Jun. 2006, vol. 4, pp. 1658–1663.

[10] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Trans. Commun.*, vol. 55, no. 1, pp. 21–24, Jan. 2007.

[11] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: The cooperation-processing tradeoff," *Wireless Commun. Mobile Comput.*, vol. 7, no. 9, pp. 1049–1060, May 2007.

[12] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Sel. Areas Commun.*, vol. 2, no. 1, pp. 4–17, Feb. 2008.

[13] D. Noguet *et al.*, "Sensing techniques for cognitive radio—State of the art and trends," in *IEEE SCC41- P1900.6 White Paper*, Apr. 2009.

[14] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surv. Tut.*, vol. 11, no. 1, pp. 116–130, First Quarter, 2009.

[15] A. Attar, A. Sheikhi, and A. Zamani, "Communication system recognition by modulation recognition," in *Proc. 11th Int. Conf. Telecommun.*, Fortaleza, Brazil, Aug. 1–7, 2004, pp. 106–113, DOI: 10.1007/978-3-540-27824-5_16.

[16] Q. Zhao and J. Ye, "Quickest detection in multiple ON-OFF processes," *IEEE Trans. Signal Process.*, vol. 58, no. 12, pp. 5994–6006, Dec. 2010.

[17] V. Krishnamurthy, *Quickest Time Herding and Detection for Optimal Social Learning*, 2010. [Online]. Available: http://arxiv.org/abs/1003.4972/

[18] F. R. Yu, M. Huang, and H. Tang, "Biologically inspired consensus-based spectrum sensing in mobile Ad Hoc networks with cognitive radios," *IEEE Networks*, vol. 24, no. 3, pp. 26–30, May–Jun. 2010.

[19] B. Atakan and O. B. Akan, "Biologically-inspired spectrum sharing in cognitive radio networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Hong Kong, Mar. 11–15, 2007, pp. 43–48.

[20] Z. Li, F. R. Yu, and M. Huang, "A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 383–393, Jan. 2010.

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

[22] L. Lifeng, H. El Gamal, J. Hai, and H. V. Poor, "Cognitive medium access: Exploration, exploitation, and competition," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 239–253, Feb. 2011.

[23] O. Holland, A. Attar, N. Olaziregi, N. Sattari, and A. H. Aghvami, "A universal resource awareness channel for cognitive radio," in *Proc. IEEE Pers. Indoor Mobile Radio Commun.*, Helsinki, Finland, Sep. 11–14, 2006, DOI: 10.1109/PIMRC.2006.254338.

[24] G. A. Safdar and M. O'Neill, "Common control channel security framework for cognitive radio networks," in *Proc. IEEE Veh. Technol. Conf. Spring*, Barcelona, Spain, Apr. 26–29, 2009, DOI: 10.1109/VETECS.2009.5073450.

[25] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[26] A. W. Min, K. G. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *Proc. 17th IEEE Int. Conf. Netw. Protocols*, Princeton, NJ, Oct. 13–16, 2009, pp. 294–303.

[27] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," *ACM Mobile Comput. Commun. Rev.*, vol. 13, no. 2, pp. 86–95, Apr. 2009.

[28] W. Wangz, H. Liy, Y. Sunz, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. Conf. Inf. Sci. Syst.*, Baltimore, MD, Mar. 2009, pp. 130–134.

[29] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, May 2008, pp. 3406–3410.

[30] F. Gao, W. Yuan, W. Liu, W. Cheng, and S. Wang, "A robust and efficient cooperative spectrum sensing scheme in cognitive radio networks," in *Proc. IEEE Int. Conf. Commun.*, Cape Town, South Africa, May 23–27, 2010, DOI: 10.1109/ICCW.2010.5503968.

[31] R. Chen, J.-M. Park, Y. T. Hou, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008.

[32] F. R. Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile Ad Hoc networks with cognitive radios," in *Proc. IEEE Military Commun. Conf.*, Boston, MA, Oct. 2009, DOI: 10.1109/MILCOM.2009.5379832.

[33] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 517–528, Apr. 2007.

[34] A. Attar, M. R. Nakahi, and A. H. Aghvami, "Cognitive radio game for secondary spectrum access problem," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 2121–2131, Apr. 2008.

[35] S.-S. Byun, I. Balasingham, and A. V. Vasilakos, "A market-clearing model for spectrum trade in cognitive radio networks," in *Proc. 12th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Paris, France, May 2011, DOI: 10.1145/2107502.2107513.

[36] Q. Zhao, L. Tong, A. Swami, and Y. Chen, "Decentralized cognitive MAC for opportunistic spectrum access in Ad Hoc networks: A POMDP framework," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 3, pp. 589–600, Apr. 2007.

[37] S. Haji Ali Ahmad, M. Liu, T. Javidi, Q. Zhao, and B. Krishnamachari, "Optimality of myopic sensing in multichannel opportunistic access," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4040–4050, Sep. 2009.

[38] A. Laourine and L. Tong, "Betting on Gilbert-Elliot channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 723–733, Feb. 2010.

[39] K. Liu and Q. Zhao, "Distributed learning in multi-armed bandit with multiple players," *IEEE Trans. Signal Process.*, vol. 58, no. 11, pp. 5667–5681, Nov. 2010.

[40] E. Hossain, D. Niyato, and Z. Hun, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*. New York: Cambridge Univ. Press, 2009.

[41] C. J. C. H. Watkins, "Learning from delayed rewards," Ph.D. dissertation, Faculty Comput. Sci. Technol., Univ. Cambridge, Cambridge, U.K., 1989.

[42] C. J. C. H. Watkins and P. Dayan, "Q-learning," *Mach. Learn.*, vol. 8, pp. 279–292, 1992.

[43] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Urbana, IL, May 25–28, 2005, pp. 46–57.

[44] E. Altman, K. Avrachenkov, and A. Garnaev, "Jamming in wireless networks under uncertainty," *Mobile Netw. Appl.*, vol. 16, no. 2, pp. 246–254, Nov. 2010.

[45] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[46] L. Zhu and H. Zhou, "Two types of attacks against cognitive radio network MAC protocols," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, Wuhan, China, Dec. 2008, vol. 4, pp. 1110–1113.

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

[48] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl.*, New Orleans, LA, Feb. 25–26, 1999, pp. 90–100.

[49] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proc. IEEE*, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.

[50] D. Dagon, T. Martin, and T. Starner, "Mobile phones as computing devices: The viruses are coming!" *IEEE Pervasive Comput.*, vol. 3, no. 4, pp. 11–15, Oct.–Dec. 2004.

[51] P. Wang, M. C. González,, C. A. Hidalgo, and A.-L. Barabási, "Understanding the spreading patterns of mobile phone viruses," *Science*, vol. 32, no. 5930, pp. 1071–1076, May 2009.

[52] O. Holland and A. H. Aghvami, "Dynamic scalable software downloads for mobile terminal mass-upgrades," in *Proc. IST Mobile Wireless Commun. Summit*, Budapest, Hungary, Jul. 2007, DOI: 10.1109/ISTMWC.2007.4299035.

[53] M. Muck, S. Buljore, P. Martigne, A. Kousaridas, E. Patouni, M. Stamatelatos, K. Tsagkaris, J. Yang, and O. Holland, "IEEE P1900.B: Coexistence support for reconfigurable, heterogeneous air interfaces," in *Proc. IEEE Int. Symp. New Frontiers Dynamic Spectrum Access Netw.*, Dublin, Ireland, Apr. 2007, pp. 381–389.

[54] G. Yue, X. Wang, and M. Madihian, "Design of anti-jamming coding for cognitive radio," in *Proc. IEEE Global Telecommun. Conf.*, Washington, DC, Nov. 26–30, 2007, pp .4190–4194.

[55] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 877–889, Apr. 2011.

[56] H. Tang and M. Salmanian, "Lightweight integrated authentication for tactical MANETS," in *Proc. IEEE 9th Int. Conf. Young Comput. Sci.*, Zhangjiajie, China, Nov. 18–21, 2008, pp. 2266–2271.

[57] F. R. Yu and H. Tang, *Distributed Node Selection for Threshold Key Management With Intrusion Detection in Mobile Ad Hoc Networks*. New York: ACM/Springer Wireless Networks, Apr. 2010.

[58] F. R. Yu, H. Tang, P. C. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile Ad Hoc networks," *IEEE Trans. Netw. Services Manage.*, vol. 7, no. 4, pp. 1932–4537, Dec. 2010.

[59] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, Jul. 9–14, 2006, pp. 356–360.

[60] P. K. Gopala, L. Lifeng, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[61] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 6–11, 2008, pp. 524–528.

[62] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 24–29, 2007, pp. 1301–1305.

[63] W. Saad, Z. Han, T. Basar, M. Debbah, and A. Hjørungnes, "Distributed coalition formation games for secure wireless transmission," *Mobile Netw. Appl.*, vol. 16, no. 2, pp. 231–245, Nov. 2010.

[64] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile Ad Hoc networks," *IEEE Commun. Surv. Tut.*, vol. 11, no. 1, pp. 116–130, First Quarter, 2009.

[65] J. W. Huang and V. Krishnamurthy, "Game theoretic issues in cognitive radio systems," *J. Commun.*, vol. 4, no. 10, pp. 790–802, Nov. 2009.

[66] R. K. Dash, A. Rogers, N. R. Jennings, S. Reece, and S. Roberts, "Constrained bandwidth allocation in multisensor information fusion: A mechanism design approach," in *Proc. IEEE Inf. Fusion Conf.*, Philadelphia, PA, Jul. 2005, pp. 1185–1192.

[67] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Pers. Commun.*, vol. 6, pp. 311–335, 1998.

[68] Y. Li, L. J. Cimini, and N. R. Sollenberger, "Robust channel estimation for OFDM systems with rapid dispersive fading channels," *IEEE Trans. Commun.*, vol. 46, no. 7, pp. 902–915, Jul. 1998.

[69] P. Setoodeh and S. Haykin, "Robust transmit power control for cognitive radio," *Proc. IEEE*, vol. 97, no. 5, pp. 915–939, May 2009.

[70] J. Wang, G. Scutari, and D. P. Palomar, "Robust cognitive radio via game theory," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2073–2077.

[71] M. H. Islam, Y.-C. Liang, and R. Zhang, "Robust precoding for orthogonal space-time block coded MIMO cognitive radio networks," in *Proc. IEEE 10th Workshop Signal Process. Adv. Wireless Commun.*, Perugia, Italy, Jun. 2009, pp. 86–90.

[72] X. Gong, A. Ishaque, G. Dartmann, and G. Ascheid, "MSE-based linear transceiver optimization in MIMO cognitive radio networks with imperfect channel knowledge," in *Proc. 2nd Int. Workshop Cogn. Inf. Process.*, Elba Island, Italy, Jun. 2010, pp. 105–110.

[73] G. Zheng, S. Ma, K.-K. Wong, and T.-S. Ng, "Robust beamforming in cognitive radio," *IEEE Trans. Wireless Commun*, vol. 9, no. 2, pp. 570–576, Feb. 2010.

[74] H. Du, T. Ratnarajah, M. Pesavento, and C. B. Papadias, "Joint transceiver beamforming in MIMO cognitive radio network via second-order cone programming," *IEEE Trans. Signal Process.*, vol. 60, no. 2, pp. 781–792, Feb. 2012.

[75] O. Durowoju, K. Arshad, and K. Moessner, "Distributed power control for cognitive radio networks, based on incumbent outage information," in *Proc. IEEE Int. Conf. Commun.*, Kyoto, Japan, Jun. 2011, DOI: 10.1109/icc.2011.5962937.

[76] D. Li and J. Gross, "Robust clustering of ad-hoc cognitive radio networks under opportunistic spectrum access," in *Proc. IEEE Int. Conf. Commun.*, Kyoto, Japan, Jun. 2011, DOI: 10.1109/icc.2011.5963426.

[77] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems—Part II: Unknown channel statistics," *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 274–283, Jan. 2011.

[78] 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, Nov. 2011.

[79] A. Ghassemi, L. H.-J. Lampe, A. Attar, and T. A. Gulliver, "Joint sidelobe and peak power reduction in OFDM-based cognitive radio," in *Proc. IEEE Veh. Technol. Conf. Fall*, San Francisco, CA, Sep. 5–8, 2011, DOI: 10.1109/VETECF.2010.5594133.

ABOUT THE AUTHORS

Alireza Attar received the Ph.D. degree in telecommunications from King's College London, London, U.K., in 2008, where he was awarded the Mobile VCE scholarship.

He was a Postdoctoral Fellow at the University of British Columbia, Vancouver, BC, Canada, during 2009–2011.

Dr. Attar had been an active IEEE member, serving in various capacities including reviewer for various Communications and Signal Processing Society journals, Technical Program Committee (TPC) member for major ComSoc conferences, as well as Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY special issues.

Helen Tang (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Carleton University, Ottawa, ON, Canada, in 2005.

She is a Defence Scientist at Defence R&D Canada—Ottawa (DRDC-Ottawa), Ottawa, ON, Canada. She is also an Adjunct Professor at the Department of System and Computer Engineering, Carleton University. From 1999 to 2005, she worked in several R&D organizations in Canada and the United States, including Alcatel-Lucent, Mentor Graphics, and Communications Research Center Canada. In October 2005, she joined DRDC as a Defence Scientist. Her research interests include architectural and protocol design for computer networks, with a current focus on wireless network security.

Dr. Tang has served as technical program chair, reviewer, and session chair for numerous conferences. She received the Best Paper Award at the 2009 IEEE/IFIP International Symposium on Trusted Computing and Communications, the Outstanding Contribution Award at DRDC-Ottawa in 2009, and the Outstanding Leadership Award at the 2010 IEEE/IFIP International Symposium on Trusted Computing and Communications.

Athanasios V. Vasilakos (Senior Member, IEEE) received the Ph.D. degree in computer engineering from the University of Patras, Patras, Greece, in 1988.

He is currently Professor at the Department of Computer and Telecommunications Engineering, University of Western Macedonia, Kozani, Greece, and visiting Professor at the Graduate Program of the Department of Electrical and Computer Engineering, National Technical University of Athens (NTUA), Athens, Greece. He has authored or coauthored over 200 technical papers in major international journals and conferences. He is author/coauthor of five books and 20 book chapters in the areas of communications.

Dr. Vasilakos served as General Chair, Technical Program Committee (TPC) Chair, and Symposium Chair for many international conferences. He served or is serving as an Editor or/and Guest Editor for many technical journals, i.e., the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is the founding Editor-in-Chief of the *International Journal of Adaptive and Autonomous Communications Systems* (IJAACS, http://www.inderscience.com/ijaacs) and the *International Journal of Arts and Technology* (IJART, http://www.inderscience.com/ijart). He is Chairman of the European Alliance for Innovation.

F. Richard Yu (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of British Columbia (UBC), Vancouver, BC, Canada, in 2003.

From 2002 to 2004, he was with Ericsson (Lund, Sweden), where he worked on the research and development of 3G cellular networks. From 2005 to 2006, he was with a startup in California, where he worked on the research and development in the areas of advanced wireless communication technologies and new standards. He joined Carleton School of Information Technology and the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, in 2007, where he is currently an Associate Professor. His research interests include cross-layer design, security, and quality-of-service (QoS) provisioning in wireless networks.

Dr. Yu received the Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly Premier's Research Excellence Award) in 2011, the Excellent Contribution Award at the 2010 IEEE/IFIP International Symposium on Trusted Computing and Communications, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009, and the Best Paper Awards at the 2009 IEEE/IFIP International Symposium on Trusted Computing and Communications and the 2005 International Conference on Networking. He serves on the editorial boards of several journals, including the IEEE Transactions on Vehicular Technology, *IEEE Communications Surveys and Tutorials*, *ACM/Springer Wireless Networks*, *EURASIP Journal on Wireless Communications Networking*, *Ad Hoc and Sensor Wireless Networks*, *Wiley Journal on Security and Communication Networks*, and the *International Journal of Wireless Communications and Networking*, and a Guest Editor for the IEEE Systems Journal for the Special Issue on Smart Grid Communications Systems. He has served on the Technical Program Committee (TPC) of numerous conferences, as the TPC Co-Chair of IEE Globecom'13, CCNC'13, INFOCOM-CCSES'2012, ICC-GCN'2012, VTC'2012S, Globecom'11, INFOCOM-GCN'2011, INFOCOM-CWCN'2010, IEEE IWCMC'2009, VTC'2008F, and WiN-ITS'2007, as the Publication Chair of ICST QShine 2010, and the Co-Chair of ICUMT-CWCN'2009.

Victor C. M. Leung (Fellow, IEEE) received the B.A.Sc. (honors) degree in electrical engineering from the University of British Columbia (UBC), Vancouver, BC, Canada, in 1977, and was awarded the APEBC Gold Medal as the head of the graduating class in the Faculty of Applied Science. He attended graduate school at UBC on a Natural Sciences and Engineering Research Council Postgraduate Scholarship and received the Ph.D. degree in electrical engineering in 1981.

From 1981 to 1987, he was a Senior Member of Technical Staff at MPR Teltech Ltd., specializing in the planning, design, and analysis of satellite communication systems. In 1988, he was a Lecturer in the Department of Electronics, Chinese University of Hong Kong, Hong Kong, . He returned to UBC as a faculty member in 1989, where he is currently a Professor and the inaugural holder of the TELUS Mobility Research Chair in Advanced Telecommunications Engineering in the Department of Electrical and Computer Engineering. He has coauthored more than 600 technical papers in international journals and conference proceedings, several of which had been selected for best paper awards. His research interests are in the broad areas of wireless networks and mobile systems.

Dr. Leung is a registered professional engineer in the Province of British Columbia, Canada. He is a Fellow of the Engineering Institute of Canada and the Canadian Academy of Engineering. He has served on the editorial boards of the IEEE Journal on Selected Areas in Communications—Wireless Communications Series, the IEEE Transactions on Wireless Communications, and the IEEE Transactions on Vehicular Technology, and is serving on the editorial boards of the IEEE Transactions on Computers, the IEEE Wireless Communications Letters, the *Journal of Communications and Networks*, *Computer Communications*, as well as several other journals. He has guest-edited many journal special issues, and served on the technical program committee of numerous international conferences. He has chaired or cochaired many conferences and workshops. He was the recipient of the IEEE Vancouver Section Centennial Award and the 2011 UBC Killam Research Prize.