Security and Enforcement in Spectrum Sharing

To make spectrum sharing successful, incumbent operators must have faith in the enforcement and privacy implications for new technologies. The authors present many of the opportunities and challenges.

By Jung-Min (Jerry) Park, *Senior Member IEEE*, Jeffrey H. Reed, *Fellow IEEE*, A. A. Beex, T. Charles Clancy, *Senior Member IEEE*, Vireshwar Kumar, and Behnam Bahrak

ABSTRACT | When different stakeholders share a common resource, such as the case in spectrum sharing, security and enforcement become critical considerations that affect the welfare of all stakeholders. Recent advances in radio spectrum access technologies, such as cognitive radios, have made spectrum sharing a viable option for significantly improving spectrum utilization efficiency. However, those technologies have also contributed to exacerbating the difficult problems of security and enforcement. In this paper, we review some of the critical security and privacy threats that impact spectrum sharing. We propose a taxonomy for classifying the various threats, and describe representative examples for each threat category. We also discuss threat countermeasures and enforcement techniques, which are discussed in the context of two different approaches: *ex ante* (preventive) and *ex post* (punitive) enforcement.

KEYWORDS | Cognitive radio; dynamic spectrum access; enforcement; security; spectrum sharing

I. INTRODUCTION

The role of spectrum as an important economic growth engine in the United States was brought forth in the National Broadband Plan (NBP) [1] and in the recent President's Council of Advisors on Science and Technology (PCAST) report entitled "Realizing the full potential of government-held spectrum to spur economic growth" [2]. Recommendations in the PCAST report include sharing underutilized federal government spectrum and identifying 1000 MHz of federal spectrum as part of an ambitious endeavor to create "the first shared-use spectrum superhighways."

Regulatory bodies in other countries are also conducting studies, and, in some cases, have established regulations with the aim of improving spectrum utilization efficiency through shared spectrum access. These efforts include the studies and initiatives undertaken by the Office of Communications (Ofcom, a regulatory authority in the United Kingdom) [3], [4], Industry Canada [5], Infocomm Development Authority of Singapore (IDA) [6], Radio Spectrum Policy Group in Europe [7], [8], and the European Communications Office [9].

To realize this vision and meet the spectrum demands of future applications, we need to develop and employ innovative spectrum access technologies as well as adopt new regulatory rules and institutional frameworks that can maximize the efficacy of those technologies. Realizing the foresight described in the PCAST report will require the adoption of fundamentally new spectrum access paradigms, including dynamic spectrum access and spectrum sharing between heterogeneous wireless systems. In the spectrum-sharing paradigm, a heterogeneous mix of wireless systems of differing access priorities, quality-of-service (QoS) requirements, and transmission characteristics need to coexist without causing harmful interference to each other. When different stakeholders share a common resource (such as the case in spectrum sharing), security, privacy, and enforcement become critical considerations that are essential to the welfare of all stakeholders. Security and enforcement are especially paramount considerations related to the recent calls in the United States for sharing of federal government (including military) spectrum with nongovernment systems.

Manuscript received September 23, 2013; revised December 18, 2013; accepted January 15, 2014. Date of publication February 5, 2014; date of current version February 14, 2014.This work was sponsored in part by the National Science Foundation under Grants 0746925, 1314598, 1265886, and 1247928; by Motorola Solutions; and by the industry affiliates of the Broadband Wireless Access & Applications Center and the Wireless @ Virginia Tech group.

The authors are with the Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061 USA (e-mail: jungmin@vt.edu).

Digital Object Identifier: 10.1109/JPROC.2014.2301972

In this paper, we review the critical security and privacy threats in dynamic spectrum access and spectrum sharing. First, we describe a taxonomy for classifying the threats that have been discussed in the literature. The taxonomy considers the fundamental mechanism for enabling coexistence (i.e., spectrum sensing driven versus database driven) as well as the point of attack with respect to the five-layer protocol stack. For each threat category, we describe representative security and privacy threats and their relation to other types of threats. We also discuss threat countermeasures and spectrum rule enforcement. The enforcement techniques are discussed in the context of two distinct approaches: *ex ante* and *ex post* enforcement. The former represents actions that are designed to "prevent" or reduce the likelihood of a potentially harmful interference event, while the latter denotes "punitive" measures designed to punish malicious or selfish behavior after a potentially harmful interference event has occurred. We conclude the paper by discussing the open problems and research challenges that need to be addressed to ensure security and privacy in spectrum sharing.

The rest of the paper is organized as follows. We discuss the spectrum-sharing models and security requirements relevant to spectrum sharing in Section II. In Section III, we propose a taxonomy of security and privacy threats, and describe representative threats in each category. Threat countermeasures and spectrum enforcement techniques are discussed in Section IV. We discuss open research problems and challenges in Section V, and conclude the paper in Section VI.

II. TECHNICAL BACKGROUND

A. Models of Shared Spectrum Access

Most of the security and privacy threats discussed in the literature are intrinsically linked to one of the two fundamental attributes of a spectrum-sharing model: 1) spectrum access user model; and 2) mechanism for enabling the harmonious coexistence of wireless devices/systems. In Section III, we use these attributes to create a taxonomy of threats to spectrum sharing. Here, we briefly review these topics before discussing the threats in the next section.

In spectrum sharing, users of different access priorities share a common resource, viz. spectrum, within a clearly defined hierarchy. Licensed shared access (LSA) is a two-tier spectrum-sharing structure proposed by the European Commission to support the use of idle spectrum in Europe using cognitive radio (CR) technology [7]. In the two-tier user model, users are classified into two categories: incumbent/primary users (PUs) and secondary users (SUs). The PUs have access priority over the SUs, and may consist of federal government users, state/local government users, and licensed users. The SUs have secondary (i.e., subordinate) rights to spectrum, and typically consist of unlicensed opportunistic users. As described in the PCAST report [2] and the U.S. Federal Communications Commission's (FCC) Notice of Proposal Making (NPRM) for the 3.5-GHz band [10], a richer hierarchy of rights is possible with a three-tier user model. In the NPRM, three tiers of users are proposed: incumbent access users, protected access users, and general authorized access users.

Instead of access rights, SUs can be classified based on their capabilities, such as maximum transmit power, geolocation capability, ability to access a database, sensing ability, etc. For example, FCC has defined four classes of TV white space devices: fixed, portable mode II, portable mode I, and sensing only [11]. For details, the reader is referred to [11].

There are two different mechanisms for enabling the harmonious coexistence of heterogeneous wireless systems in a shared spectrum environment: geolocation databases and spectrum sensing. In a database-driven spectrum-sharing scenario, the database provides spectrum availability information and may also prescribe rules for SUs to access the shared spectrum (e.g., transmit spectral mask) [12], [13]. SUs are required to access the database before accessing the spectrum. On the other hand, in a sensing-driven spectrum-sharing application, SUs' transmission behavior is dictated by spectrum sensing results, obtained through either standalone sensing or cooperative sensing [14], [15]. In sensing-driven spectrum sharing, the radios need to be cognizant of the surrounding radio-frequency (RF) environment (through sensing), and need to have sufficient intelligence to use transmission parameters that are compliant with regulatory spectrum rules. Radios with such capabilities are often referred to as CRs [16]. In most situations, both mechanisms are used to realize spectrum sharing.

B. Security and Enforcement Requirements

To protect all stakeholders and ensure the viability of spectrum sharing, certain security and enforcement requirements must be met. Different spectrum-sharing scenarios may have different requirements. Here, we briefly review some of the requirements common to most spectrum-sharing scenarios [17], [18].

- *Confidentiality:* Along with the data stored in the database, the data communicated between the registered users and the database, and among users in the network should not get disclosed to unauthorized users.
- *Integrity:* The data stored in the database and communicated among users should be protected from malicious alteration, insertion, deletion, or replay.
- *Availability:* The users should have access to the database and/or the spectrum when it is required.
- *Authentication:* The network components, including the database, and the mobile terminals should be able to establish and verify their identity.

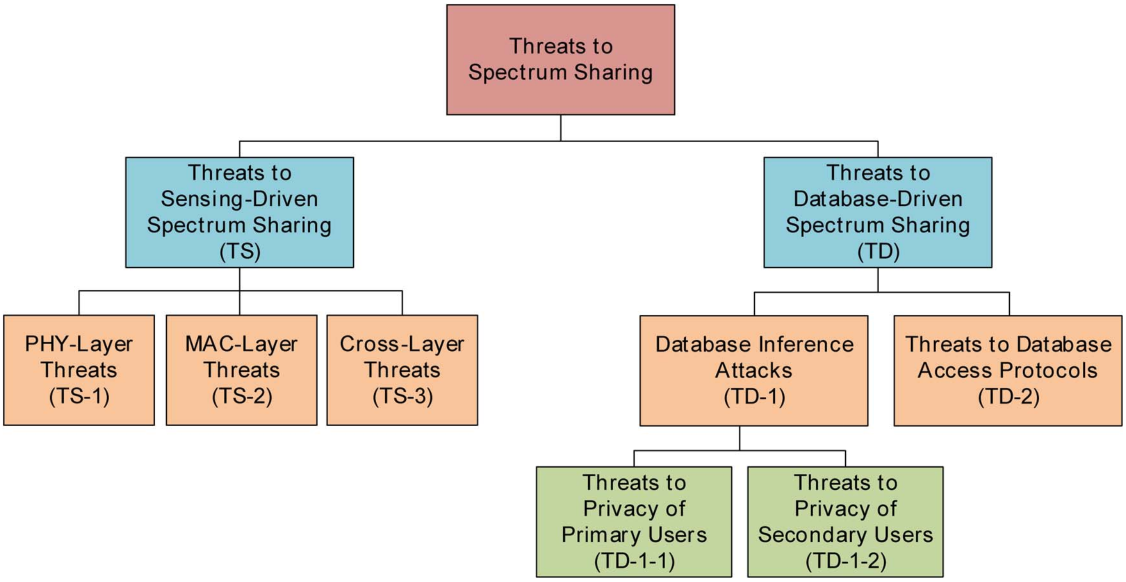
Threats to Spectrum Sharing
Threats to Sensing-Driven Spectrum Sharing (TS)
Threats to Database-Driven Spectrum Sharing (TD)
PHY-Layer Threats (TS-1)
MAC-Layer Threats (TS-2)
Cross-Layer Threats (TS-3)
Database Inference Attacks (TD-1)
Threats to Database Access Protocols (TD-2)
Threats to Privacy of Primary Users (TD-1-1)
Threats to Privacy of Secondary Users (TD-1-2)

Fig. 1. ***Taxonomy of threats to spectrum sharing.***

- *Nonrepudiation:* The users should not be able to deny either having received or sent a message. Also, they should not be able to deny having accessed the spectrum at a specified location and time.
- *Compliance:* The network should be able to detect noncompliant behavior causing harmful interference.
- *Access control:* No user should be able to access either the database or the spectrum without proper credentials.
- *Privacy:* Sensitive or private information of the users, both primary and secondary users, should be properly protected.

III. SECURITY AND PRIVACY THREATS

A. Taxonomy of Threats

In this section, we review some of the security and privacy issues that pose the greatest threats to spectrum sharing. To provide a more systematic discussion of the topic, we first propose a taxonomy that classifies the known threats into a number of categories. Through this taxonomy, our aim is to offer a clear picture of the known security and privacy issues and the related technical challenges. The taxonomy is illustrated in Fig. 1.

All of the known threats (to spectrum sharing) exploit either one of the two mechanisms which enable different wireless systems to coexist, viz., spectrum sensing or geolocation databases. Therefore, all threats can first be classified into two broad categories: threats to sensing-driven spectrum sharing (denoted as class TS) and threats to database-driven spectrum sharing (denoted as class TD). Threats under class TS can be further classified into three subclasses based on which layer of the protocol stack a given threat affects: PHY-layer threat (class TS-1), MAC-layer threat (class TS-2), and cross-layer threat (class TS-3). On the other hand, threats in class TD can be further classified into two subclasses: database inference attacks (class TD-1) and threats to database access protocols (class TD-2).

B. Threats to Sensing-Driven Spectrum Sharing

1) PHY-Layer Threats: Threats in class TS-1 directly impact the PHY-layer mechanisms in spectrum sharing, most notably spectrum sensing. Spectrum sensing by the SUs can be manipulated by a rogue transmitter in order to either hijack their spectrum or affect their spectrum-sharing decisions, e.g., primary user emulation (PUE) attack [19], [20]. In a PUE attack, a malicious user emulates the PU's signals and illegally forces the other SUs to vacate the spectrum. PUE attacks can also be used as a tool to carry out more sophisticated attacks [21].

If SUs fail to sense the presence of PUs' signals in the spectrum of interest, they can cause harmful interference to the PUs. One approach for improving the accuracy of spectrum sensing is to employ cooperative spectrum sensing and centralized decision making. In this approach, a multiple number of users sense their RF environment and send their observations to a fusion center. The fusion center then intelligently combines the reported information to make the final decision regarding the presence or the absence of incumbent transmissions. An alternative approach is to employ cooperative spectrum sensing and distributed decision making. This approach avoids the problems that may arise when a fusion center makes erroneous decisions. In this approach, no fusion center is used, and instead each SU makes its decision based on its own observations and also on observations shared by other SUs. Both sensing approaches described above are vulnerable to spectrum sensing data falsification (SSDF) attacks in which one or more malicious SUs send false observations about the radio environment [22], [23]. A SSDF attack can cause a SU to acquire an incorrect perception of the radio environment leading to transmission decisions that cause harm to others.

2) MAC-Layer and Cross-Layer Threats: There are a number of known attacks that disrupt the MAC-layer mechanisms of spectrum sharing. In a multihop CR network, a predefined frequency channel, called the cognitive control channel (CCC), is used by SUs to exchange control information, e.g., channel negotiation, spectrum handoff, etc. [24]. A rogue transmitter may corrupt the CCC leading to a denial-of-service (DoS) attack [25], [26]. Another method to enable coexistence of SUs and coordinate the use of channels among SUs is to use beacons. In this case, a malicious user can carry out a beacon falsification (BF) attack to disrupt vital network functions, such as intercell spectrum contention and intercell synchronization [27]. The CRs may also utilize a carrier sense multiple access with collision avoidance (CSMA/CA) protocol for spectrum access. In this protocol, after sensing, users back off by a random time before transmission. If there is a collision of transmitted packets by any two users, the users double the backoff window and retransmit. However, a malicious user can use a small backoff window and gain priority over other users [28], [29]. This is called the small-backoff-window (SBW) attack.

A number of attacks can be conducted concurrently to exploit vulnerabilities in two or more layers of the protocol stack. These attacks are often referred to as cross-layer attacks. In a cognitive network utilizing the CSMA/CA protocol, a malicious user can conduct SSDF (PHY-layer) attack and SBW (MAC-layer) attack in a coordinated fashion [30]. Because of the coordination, it becomes difficult to detect either of the two attacks, and, hence, this cross-layer attack is more effective than a single-layer attack in reducing the overall SUs' channel utilization. The Lion attack is another example of a cross-layer attack that targets the PHY and transport layers of a CR network [31]. In a Lion attack, a malicious user launches a PUE attack to force the target nodes to carry out frequency handoffs. Since the transmission control protocol (TCP) is sensitive to variations in delay and bandwidth, the transmission interruptions caused by the frequency handoffs can lead to very poor throughput at the transport layer.

C. Threats to Database-Driven Spectrum Sharing

The threats discussed in this section exploit the security or privacy vulnerabilities inherent to employing geolocation databases for spectrum sharing.

1) Threats to the Privacy of Primary Users: The FCC ruling on TV white spaces proposes relying on a database of the incumbents' spectrum usage information as the primary means of determining white space availability at any white space device (WSD) [34]. The database is required to house an up-to-date repository of incumbents including television stations, and in certain cases, wireless microphones, and use this information to determine white space availability at a white space device's location. It has been shown that sensing-only devices do not generally utilize spectrum as efficiently as geolocation-enabled devices, due to the large margins in incumbent detection thresholds that must be built into sensing-only devices [12]. Geolocation-enabled devices have knowledge of the specific interference protection requirements of each licensed incumbent, which allows varying levels of protection to be applied, and thus maximize utilization of the spectrum.

Although using geolocation databases for spectrum sharing has many advantages, it poses a potentially serious privacy problem. For instance, SUs, through seemingly innocuous queries to the database, can determine the types and locations of incumbent systems operating in a given region of interest; we refer to this as the operational privacy of the incumbents. In other words, operational privacy of PUs is the confidentiality of information regarding the primary users' operational characteristic. When the incumbent systems are commercial systems, such as the case in TV spectrum, this is not an issue. However, when the incumbents are federal government, possibly military, systems, then the information revealed by the databases may result in a serious breach of operational privacy. Moreover, there is the possibility that SUs can obtain knowledge beyond that revealed directly by the database's query replies by using sophisticated inference techniques; we refer to this as a database inference attack.

The operational privacy of primary users is an especially critical concern related to the recent calls in the United States for sharing of federal government (including military) spectrum in the 3.5-GHz band with nongovernment systems.

Below, we list some of the operational attributes of incumbent transmitters that may need to be protected if those transmitters are being used in military or intelligence gathering applications:

- transmitter identity [e.g., the call sign of the transmitter in an FCC consolidated database system (CDBS)];
- geolocation (i.e., latitude and longitude);
- antenna parameters (HAAT, etc.);
- power (Max EIRP, average operation power, etc.);

Table 1 Mapping of Threats to the Security and Privacy Requirements

Threat	Class	Confidentiality	Integrity	Availability	Authentication	Non-repudiation	Compliance	Access Control	Privacy
PUE [19], [20]	TS-1			☠	☠	☠	☠	☠	
SSDF [22], [23]	TS-1		☠	☠					
CCC [25], [26]	TS-2	☠	☠	☠	☠				
BF [27]	TS-2		☠	☠	☠	☠	☠	☠	
SBW [28], [29]	TS-3		☠	☠					
SULI [32]	TD-1-2								☠
DAP [33]	TD-2	☠	☠	☠	☠			☠	☠

- transmit protection contours (cochannel, adjacent channel, etc.);
- times of operation.

The problem of operational privacy of PUs cannot be addressed by tightly controlling access to the database, since all SUs need access to it to enable spectrum sharing. A more viable approach is to "obfuscate" the information revealed by the database in an intelligent manner such that a certain level of privacy is assured while supporting efficient use of the spectrum.

2) *Threats to the Privacy of Secondary Users:* Another privacy issue that arises as a result of using geolocation databases for spectrum sharing is the problem of location privacy of the secondary users. Since the secondary users need to send their location information to the database to receive information on the set of available channels in their region, their location privacy may be threatened by an untrustworthy database. In [32], Gao *et al.* present a new kind of location privacy attack, named the spectrum-utilization-based location inferring (SULI) attack, which allows an attacker to infer the location of an SU from the channels s/he has used.

3) *Threats to the Database Access Protocol (DAP):* In addition to the aforementioned privacy issues, there are other security concerns related to using a geolocation database for spectrum sharing. The latest Internet Engineering Task Force (IETF) draft of the protocol to access white space database (PAWS) contains a section that focuses on security issues [33]. Some of those security issues are listed as follows.

- *Modifying a device to masquerade as another certified device:* Without suitable protection mechanisms, devices can listen to registration exchanges, and later register with the database by claiming the identity of another device.
- *Spoofed database:* Spoofing a database in order to provide malicious responses to a WSD (master device) is another type of attack that can be used to cause interference to the primary user of the spectrum.
- *Modifying or jamming a query:* If an attacker is able to change some of the information in the WSD's query (e.g., the location of the device or its capabilities), the database responds with incorrect information about available spectrum or maximum transmit power allowed which can result in interference to the primary user of the spectrum. Also, jamming the queries may cause a DoS to the master device if the attacker can prevent the query from reaching the database.
- *Modifying or jamming a database response:* An attacker may modify the available spectrum or power level information carried in the database response which can result in interference to the primary users.
- *Malicious individual acts as a database to terminate or unfairly limit spectrum access of devices:* If a database includes a mechanism by which spectrum allocated to a master device can be revoked by sending a revoke message, malicious users can pretend to be the database and send a revoke message to that device and cause a DoS attack.

In Table 1, we summarize the threats discussed in this section, and also map them to the security and enforcement requirements that they infringe.

IV. THREAT COUNTERMEASURES AND ENFORCEMENT

We classify attack countermeasures and spectrum rule enforcement into two broad categories: *ex ante* (preventive) and *ex post* (punitive) enforcement. The objective of *ex ante* enforcement is to prevent or reduce the probability of harmful interference events. On the other hand, the objective of *ex post* enforcement is to identify and/or punish malicious or selfish users after an interference event has occurred.

A. *Ex Ante* (Preventive) Approaches

1) *Preventive Measures for Rogue Transmissions:* Enforcing spectrum access control in legacy radios (e.g., cellular phones) is relatively straightforward since the spectrum access policies are an inseparable part of the radio's firmware and platform. Making controlled changes to a legacy radio's transmission behavior would require an adversary to have very specialized expertise in the radio's

firmware and hardware, and would also require specialized equipment. Unfortunately, manipulating the transmission behavior of software-defined radios (SDRs) and CRs is easier. The reconfigurability of a SDR/CR makes it vulnerable to unauthorized modification. Such modifications can result in harmful interference. Illegally modified radios can even be used to launch very sophisticated jamming attacks, as shown in [35].

One approach for enforcing spectrum access control in spectrum sharing is to employ policy-based CRs. Policy-based CRs cope with evolving spectrum access policies and constantly changing application requirements by decoupling the policies from device-specific implementations and optimizations. These radios can invoke situation-appropriate adaptive actions based on policy specifications and the current spectrum environment [36]. Enforcing spectrum access policies by mandating the use of policy-based CRs is one effective approach for mitigating rogue transmissions.

In order to regulate and enforce proper transmission behavior, policy-based CRs need mechanisms to enforce spectrum access policies. Most of these mechanisms are carried out by specialized software modules called policy conformance components (PCCs) [37]. To enforce spectrum policies, the policies themselves first need to be interpreted, and then a CR's transmission strategies need to be evaluated against those policies to determine the legality of the transmission strategies. Within a policy-based CR, the aforementioned tasks are carried out in real time by a software module called the policy reasoner.

Our previous work [38], [39] as well as that of others [37], [40], [41] has shown that rule-based policy reasoners can be used to enforce policy conformance in CRs. Rule-based policies use logic programming techniques to encode the axioms and rules in a straightforward way [42]. Using rule-based spectrum policies simplifies the design of the policy reasoner because the reasoning complexity is sufficiently low in most applications to meet the real-time processing requirements of the radio. However, rule-based policies have a number of critical drawbacks. The most serious drawbacks are policy management overhead and limited interoperability. With rule-based policies, complex spectrum policies are difficult to specify and manage. Moreover, rule-based policies do not support the sharing of the policy structure among different policy authors (i.e., regulation authorities), and thus limit interoperability of the policy-based radios across different regulatory policy domains.

To overcome the limitations of rule-based spectrum policies, there is growing interest in using ontology-based policies for prescribing spectrum access rules [44]. In fact, the IEEE 1900.5 Standard, Standard for Policy Language Requirements and System Architectures for Dynamic Spectrum Access Systems, published in 2012, prescribes the use of an ontology-based policy language for managing the functionality and behavior of dynamic spectrum access networks [45]. Using ontologies to support the formal representation of spectrum policies and its usage in dynamic spectrum access networks is expected to benefit all stakeholders in this ever changing environment. In [43], we introduced an ontology-based policy reasoner to enforce ontology-based spectrum access policies in a policy-based CR. Fig. 2 illustrates an ontology space for spectrum access policies.

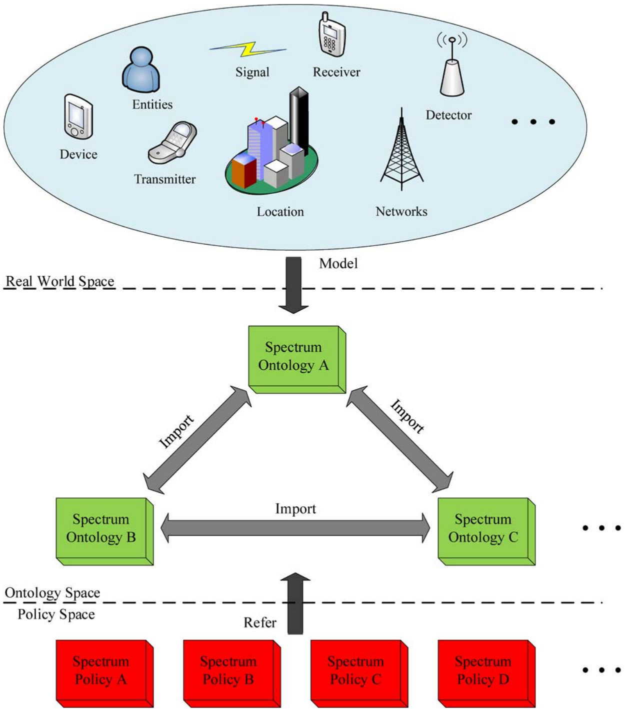

Fig. 2. ***Ontology space. Ontology-based spectrum policies offer a number of significant advantages, including facilitating the specification and management of complex spectrum policies, flexible knowledge representation, support for interoperability, flexible querying, and self-awareness [43].***

In [46], Li *et al.* propose an *ex ante* enforcement technique that is based on a secure radio middleware (SRM) layer. This layer is implemented in software and resides between the operating system and the hardware. The SRM layer checks all software transmission requests that are sent to the hardware layer to make sure that configurations such as transmission power, frequency, type of modulation, etc., conform with policies in a policy database. Unlike a policy reasoner that provides feedback to the radio's software, the SRM layer simply discards nonconforming requests.

Another *ex ante* approach is to use tamper resistance techniques to protect a radio's software against unauthorized modifications. Such a technique for protecting SDR/CR software is proposed in [47]. The proposed scheme is designed to thwart static attacks (i.e., static information extracted by examining the software code) and to protect partially against dynamic attacks (i.e., dynamic information extracted while the software code executes).

In [48], Aguayo González and Reed proposed an *ex ante* approach that employs power fingerprinting to perform integrity assessment of an SDR. This mechanism is able to detect the execution of a tampered routine by closely monitoring the power consumption of the radio platform.

In [49], a hardware-based method is proposed to control the maximum transmission power of an SDR through a module implemented at the hardware of the SDR transceiver. This independent self-check module is designed to prevent transmissions that cause harmful interference to primary users even if the radio's software is compromised.

In terms of regulatory approaches, a simple *ex ante* approach is to employ exclusion zones [50]. An exclusion zone is a spatial region in which no in-band emissions from SUs would be permitted in its interior. To prevent interference to PUs, the PUs and the SUs would agree on a spatial database that defines these exclusion zones.

2) Preventive Measures for Privacy Violations: As we mentioned in Section III-C1, obfuscating the contents of the query replies from the geolocation database is one approach for preserving the privacy of primary users in spectrum sharing. Because privacy is an important concern in many database applications, privacy-preserving data management techniques [51] is an area of active research. Although there is very little, if any, existing work on privacy-preserving databases for spectrum sharing, there is an abundance of existing work on the topic in the context of other applications. In this section, we review some of the existing work on privacy-preserving databases, focusing on techniques that may have applications to database-driven spectrum sharing with some modifications.

Probably the most widely used method for privacy-preserving databases is perturbation [52]. The perturbative masking method (also knows as the randomization method) is a technique for privacy-preserving databases that uses data distortion in order to mask the attribute values of records. In this method, sufficiently large noise is added to individual record values to prevent recovery of those values by an adversary. One key advantage of the randomization method is that it is relatively simple, and does not require knowledge of the distribution of other records in the data.

Other well-known privacy protection techniques such as k-anonymity [53], l-diversity [54], and t-closeness [55] use generalization and suppression to increase the granularity of data representation in order to preserve the privacy of sensitive data. The concept of k-anonymity was originally introduced in the context of relational data privacy [56] to address the following problem: "How can a data holder release its private data with guarantees that the individual subjects of the data cannot be identified while the data remain practically useful?" [53]. The l-diversity model was designed to address the weaknesses in the k-anonymity model when there is homogeneity of sensitive values within a group [54]. The t-closeness model is a further enhancement on the concept of l-diversity [55].

Differential privacy [57] is another emerging privacy-preserving paradigm that has recently gained considerable attention. Unlike the aforementioned privacy-preserving techniques that use generalization (i.e., k-anonymity, l-diversity, and t-closeness) to provide a syntactic model, differential privacy provides a semantic privacy model with strong protection guarantees. In other words, differential privacy is able to capture the amount of disclosure that occurs due to the publication of sensitive data in addition to mandating how the published data should look.

The vast majority of the existing literature on location privacy focuses on preserving the privacy of the users' location from an untrusted database (or service provider) in location-based services. The location-based services rely on accurate, continuous, and real-time streams of the users' location data. However, if such information is mishandled by the database, location-based services pose a significant privacy risk to the users. Techniques for mitigating such a risk include sending a space- or time-obfuscated version of the users' actual locations [58], hiding some of the users' locations by using mix zones [59], sending fake queries, indistinguishable from real queries, issued from fake locations to the database [60], and applying k-anonymity to location privacy [61].

In [32], a scheme called *PriSpectrum* is proposed that protects the secondary users' location information in database-driven spectrum sharing. However, to the best of our knowledge, there is no existing work that addresses the problem of the primary users' operational privacy in the context of database-driven spectrum sharing.

B. *Ex Post* (Punitive) Approaches

We define *ex post* enforcement as measures designed to remediate malicious or selfish behavior, after a potentially harmful interference event has occurred, by enacting punitive actions. We divide the *ex post* enforcement process into three stages: identification, localization, and punishment.

1) Identification of Noncompliant Transmitters: The logical first step in *ex post* enforcement is for a regulator (e.g., FCC's Enforcement Bureau) to uniquely identify or authenticate malfunctioning or "rogue" transmitters. Ideally, the regulator would want to carry out the identification using some sort of a PHY-layer authentication procedure because it enables a receiver to quickly distinguish between compliant and rogue transmitters without having to complete unnecessary higher layer processing. For this approach to be viable, all SU radios must be required to incorporate a mechanism for authenticating their waveforms and employ tamper-resistant mechanisms to prevent hackers from circumventing the mechanism.

PHY-layer authentication schemes can be broadly divided into two categories: intrinsic and extrinsic approaches. Schemes in the first category utilize the "intrinsic" characteristics of the waveform or communication medium (e.g., transmitter-unique RF signal characteristics) as unique signatures to authenticate/identify transmitters. They include RF fingerprinting, and electromagnetic signature identification [62]–[67]. Although these intrinsic approaches have been shown to work in controlled lab environments, their sensitivity to environmental factors, such as temperature changes, channel conditions, and interference, limit their efficacy in real-world scenarios. Moreover, they have been shown to be vulnerable to impersonation attacks [68].

Schemes in the second category enable a transmitter to "extrinsically" embed an authentication signal [e.g., message authentication code (MAC) or digital signature] in the message signal and enable a receiver to extract it. Such schemes include PHY-layer watermarking [69]–[72] and transmitter authentication [73]–[81].

Although extrinsic PHY-layer authentication looks promising, some of its drawbacks need to be addressed before it can be considered a viable technique for *ex post* enforcement. Most of the schemes proposed in the literature for extrinsic PHY-layer authentication add the authentication signal to the message signal in such a way that the former is treated as noise by the latter and *vice versa*; this is referred to as "signal superposition" [71]. Hence, there is a fundamental, unavoidable tradeoff between the message signal's signal-to-noise ratio (SNR) and the authentication signal's SNR. More importantly, this implies that signal superposition requires the transmitter to significantly increase its transmission power to achieve acceptable performance; however, this is a serious impediment to deployment in spectrum-sharing environments because such an environment is severely interference constrained.

Another drawback of extrinsic PHY-layer authentication is that it requires the SNR at the receiver to be sufficiently high for correct demodulation and decoding of the authentication signal. In *ex post* enforcement scenarios, the regulator that is attempting to identify the noncompliant transmitter is *not* the intended receiver. This means that the regulator may be at a location where the SNR is very low with significant multipath fading. Moreover, the regulator may not even know precisely the PHY-layer parameters needed to properly demodulate and decode the detected signal. Because of these distinguishing challenges associated with *ex post* enforcement, we coin the term blind transmitter identification to denote the identification of noncompliant transmitters. Ideally, a scheme for blind transmitter identification should enable a regulator to uniquely identify (or authenticate) a transmitter under low SNR and high multipath fading conditions while not requiring the regulator to have complete knowledge of the PHY-layer transmission parameters.

2) Localization of Noncompliant Transmitters: After the identification of the malfunctioning or rogue transmitter (by analyzing its signal), the logical next step in *ex post* enforcement is to localize the noncompliant transmitter. The location of an authorized user who may be required to report its location can be verified by the regulatory framework once its identity is established. On the other hand, a rogue transmitter may fake its location information. Hence, location verification could be used to differentiate among compliant and noncomplaint transmitters. However, it is unlikely that the rogue transmitter would provide any cooperation for its location estimation. Thus, the localization in CR networks has to be achieved via a noninteractive technique, e.g., by measuring the received signal strength (RSS) [19], [82], [83]. The RSS is an indicator of the link distance between a transmitter and a receiver. Hence, the information about the distances measured between the rogue transmitter and a set of receivers through RSS measurements can be merged at the regulator to localize the rogue transmitter.

3) Punishment of Noncompliant Transmitters: The aim of punishment/penalty is to impose a cost for the noncompliant behavior [84], [85]. Therefore, the efficacy of deterrence against rogue transmissions not only depends on the probability of a bad actor getting caught, but also on the severity of punishment when the perpetrator is caught. To be effective, the penalty has to be sufficiently large to offset the benefits from noncompliance. We also need to ensure a proportional penalty for a harm caused due to noncompliance by measuring the cost of the harm. Additionally, we need to take into account the implications of imperfect enforcement as the risk of punishing compliant users may deter the prospects of spectrum sharing.

According to the literature, there are two methods for punishing noncompliant transmitters [84], [86].

- *No access to spectrum:* The rogue transmitter is not allowed to access the spectrum for an amount of time that is commensurate with the severity of the infraction. This can be achieved by revoking the license/permit of the rogue transmitter or modifying its operating rights.
- *Economic penalties:* The other way is to economically handle the punishment. Those causing the harm are charged commensurately with the severity of the harm. The collected amount can be paid to those who suffered due to the rogue transmitter. In this way, it can be observed as one of the benefits for compliant behavior by legitimate SUs.

In Table 2, we summarize the countermeasures discussed in this section, and also map them to the security and enforcement threats that they counter.

V. OPEN PROBLEMS AND RESEARCH CHALLENGES

Traditional *ex ante* enforcement techniques for wireless systems relied on transmitter/receiver specifications and white spaces to prevent harmful interference. Transmission specifications include transmission power and antenna parameters, while receiver specifications include

Table 2 Threat Countermeasures and Enforcement Strategies

Countermeasure	Class	PUE	SSDF	BF	SBW	SULI	DAP
Policy Reasoner [37]–[41]	Ex ante	⊘		⊘			
Tamper Resistance [47]	Ex ante	⊘	⊘	⊘	⊘		
Data Obfuscation [32], [51]	Ex ante					⊘	
Cryptographic Primitives [87]	Ex ante						⊘
PHY-layer Authentication [69]–[81]	Ex post	⊘		⊘			
Localization [19], [82], [83]	Ex post	⊘		⊘			
Punishment [84]	Ex post	⊘	⊘	⊘	⊘		

parameters such as bandwidth and sensitivity. Also, most of these traditional approaches assume that transmitters are fixed, which makes punitive enforcement easier. For mobile systems, *ex ante* measures that are based on transmitter specifications are less effective [85]. Mobility also hinders *ex post* techniques such as detection and reputation-based enforcement.

The intelligence, efficiency, and programmability of SDRs and CRs enable us to employ spectrum sharing to fundamentally improve the efficiency of spectrum utilization. However, these advantages also exacerbate the enforcement problem. For example, dynamic spectrum access enhances the dynamic flexibility of radios, allowing them to have greater mobility. This increased mobility, however, makes spectrum enforcement more challenging.

Another important open problem in spectrum enforcement is the development of a flexible and descriptive policy language, which can be used to specify spectrum access policies for dynamic spectrum access systems. Such a language can be used to not only prescribe the transmission behavior of an individual radio (which is a form of *ex ante* enforcement), but can also be used to manage the functionality and behavior of a dynamic spectrum access network.

There are a number of other challenges related to spectrum policies, including the development of advanced algorithms for executing policy inference and reasoning tasks carried out by policy-based CRs. Despite the great potential of ontology-based spectrum policies, there is slow progress in integrating this concept into policy-based CRs because of the complexity of policy inference and reasoning when the policies are ontology based. The primary challenge in using ontology-based policies is meeting the real-time processing requirements of the radio. To date, ontology-based policies have been successfully applied to interactive, non-real-time applications, but not to real-time applications. Most of the policy inference and reasoning tasks carried out by a policy-based CR need to be executed within a very tight time window.

In *ex post* enforcement, locus of adjudication is another critical problem that remains unaddressed [50]. The adjudicating entity must have jurisdiction to adjudicate interference events. At present, there is no clearly defined process for resolving certain types of interference events. For example, for an event that occurs in the 1695–1710-MHz band in the United States, a civil court may refer the matter to the FCC for resolution, but the FCC has no jurisdiction over federal bands and the National Telecommunications and Information Administration (NTIA) is ill-equipped to deal with civil disputes.

Metrics can be an effective tool to discern the effectiveness of various components of a security system. Metrics can also help to identify the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions. However, defining meaningful metrics is very challenging. Some of the important metrics that need to be defined to quantify security/privacy in spectrum sharing include a metric for quantifying harmful interference, metrics for quantifying the operational privacy of PUs and SUs, and metrics for measuring spectrum utilization efficiency.

There is an interesting tradeoff between enforcement and privacy that exists in the context of shared spectrum access. The collaboration of wireless nodes to monitor and "tattle" about neighboring nodes can help detect regulation-violating transmitters as well as locate and punish those violators. However, privacy considerations need to be addressed before such solutions can be adopted.

There is a fundamental tradeoff between spectrum regulations and enforcement. Tighter regulations can reduce the need for enforcement, but such an approach incurs a significant cost—tighter regulations can create a regulatory environment that discourages investment in research and deployment of wireless innovation. Finding an optimal tradeoff between regulations and enforcement is a challenge that the regulatory community will need to struggle with over the coming years.

VI. CONCLUSION

In this paper, we focused on the engineering aspects of spectrum enforcement and security. However, as emphasized in [85], building an optimal enforcement framework will require a combination of *ex ante* and *ex post*, centralized and decentralized, and general and application-specific enforcement components that coevolve with markets and regulatory policy frameworks within a complex ecosystem. Building such a complex enforcement framework will require a greater understanding of not only the engineering challenges, but also of the ramifications of the enforcement solutions in terms of legal, economic, and regulatory policy aspects. ■

REFERENCES

[1] U.S. Federal Communications Commission (FCC), "National broadband plan: Connecting America," 2010. [Online]. Available: http://www.broadband.gov/plan/

[2] President's Council of Advisors on Science and Technology (PCAST), "Report to the President: Realizing the full potential of government-held spectrum to spur economic growth," Jul. 2012. [Online]. Available: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_spectrum_report_final_july_20_2012.pdf

[3] U.K. Office of Communications (Ofcom), "Geolocation for cognitive access: A discussion on using geolocation to enable license-exempt access to the interleaved spectrum," Jul. 2009.

[4] U.K. Office of Communications (Ofcom), "Implementing geolocation: Summary of consultation responses and next steps," Sep. 2011.

[5] Industry Canada, "Consultation on a policy and technical framework for the use of non-broadcasting applications in the television broadcasting bands below 698 MHz," SMSE-012-11, Aug. 2011.

[6] Infocomm Development Authority of Singapore (IDA), "Trial of white space technology accessing VHF and UHF bands in Singapore," Jul. 2010.

[7] European Parliament and Council, "Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multiannual radio spectrum policy programme." [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX: 32012D0243: EN:NOT

[8] European Commission, "Commission implementing Decision of 23 April 2013 defining the practical arrangements, uniform formats and a methodology in relation to the radio spectrum inventory established by Decision No 243/2012/EU of the European Parliament and of the Council Establishing a Multiannual Radio Spectrum Policy Programme, 2013/195/EU." [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX: 32013D0195:EN:NOT

[9] ECC, "Technical and operational requirements for the possible operation of cognitive radio systems in the white spaces of the frequency band 470–790 MHz," Jan. 2011.

[10] U.S. Federal Communications Commission (FCC), "Enabling innovative small cell use in 3.5 GHz band NPRM & Order (FCC 12-148)," Dec. 2012.

[11] T. Baykas, M. Kasslin, M. Cummings, H. Kang, J. Kwak, R. Paine, A. Reznik, and R. Saeed, "Developing a standard for TV white space coexistence: Technical challenges and solution approaches," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 10–22, Feb. 2012.

[12] D. Gurney, G. Buchwald, L. Ecklund, S. Kuffner, and J. Grosspietsch, "Geo-location database techniques for incumbent protection in the TV white space," in *Proc. IEEE Symp. New Frontiers Dyn. Spectrum Access Netw.*, 2008, DOI: 10.1109/DYSPAN.2008.31.

[13] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl, "Senseless: A database-driven white spaces network," *IEEE Trans. Mobile Comput.*, vol. 11, no. 2, pp. 189–203, 2012.

[14] D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proc. Asilomar Conf. Signals Syst. Comput.*, 2004, vol. 1, pp. 772–776.

[15] 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.

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

[17] G. Baldini, T. Sturman, A. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Commun. Surv. Tut.*, vol. 14, no. 2, pp. 355–379. 2nd Qtr., 2012.

[18] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey," *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 1691–1708, 2012.

[19] R. Chen, J.-M. Park, and J. 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.

[20] T. Clancy and N. Goergen, "Security in cognitive radio network: Threats and mitigation," in *Proc. Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun.*, May 2008, DOI: 10.1109/CROWNCOM.2008.4562534.

[21] T. Newman, T. Clancy, M. McHenry, and J. Reed, "Case study: Security analysis of a dynamic spectrum access radio system," in *Proc. IEEE Global Telecommun. Conf.*, 2010, DOI: 10.1109/GLOCOM.2010.5683726.

[22] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE Conf. Comput. Commun.*, 2008, pp. 1876–1884.

[23] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, Feb. 2011.

[24] C. Cormio and K. R. Chowdhury, "A survey on MAC protocols for cognitive radio networks," *Ad Hoc Netw.*, vol. 7, no. 7, pp. 1315–1329, 2009.

[25] K. Bian and J.-M. Park, "MAC-layer misbehaviors in multi-hop cognitive radio networks," in *Proc. US-Korea Conf. Sci. Technol. Entrepreneurship*, 2006.

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

[27] K. Bian and J.-M. Park, "Security vulnerabilities in IEEE 802.22," in *Proc. 4th Annu. Int. Conf. Wireless Internet*, 2008, article 9.

[28] A. Toledo and X. Wang, "Robust detection of selfish misbehavior in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 6, pp. 1124–1134, Aug. 2007.

[29] M. Raya, I. Aad, J.-P. Hubaux, and A. El Fawal, "DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots," *IEEE Trans. Mobile Comput.*, vol. 5, no. 12, pp. 1691–1705, Dec. 2006.

[30] W. Wang, Y. Sun, H. Li, and Z. Han, "Cross-layer attack and defense in cognitive radio networks," in *Proc. IEEE Global Telecommun. Conf.*, 2010, DOI: 10.1109/GLOCOM.2010.5684069.

[31] J. Hernandez-Serrano, O. León, and M. Soriano, "Modeling the lion attack in cognitive radio networks," *EURASIP J. Wireless Commun. Netw.*, Jan. 2011, DOI: 10.1155/2011/242304.

[32] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and counter measures," in *Proc. IEEE INFOCOM*, 2013, pp. 2751–2759.

[33] B. Patil, "Protocol to access white space database: Problem statement, use cases and requirements," Jul. 2012. [Online]. Available: http://tools.ietf.org/html/draft-ietf-paws-problem-stmt-usecases-rqmts-06

[34] U.S. Federal Communications Commission (FCC), "Third order and memorandum opinion and order, in the matter of unlicensed operation in the TV broadcast bands, additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band," Apr. 2012.

[35] N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, "Attacks on public WLAN-based positioning," in *Proc. 7th Int. Conf. Mobile Syst. Appl. Services*, 2009, pp. 29–40.

[36] A. Ginsberg, W. D. Horne, and J. D. Poston, "Community-based cognitive radio architecture: Policy-compliant innovation via the semantic web," in *Proc. 2nd IEEE Int. Symp. New Frontiers Dyn. Spectrum Access Netw.*, 2007, pp. 191–201.

[37] F. Perich and M. McHenry, "Policy-based spectrum access control for dynamic spectrum access network radios," *Web Semantics, Sci. Services Agents World Wide Web*, vol. 7, pp. 21–27, 2009.

[38] B. Bahrak, A. Deshpande, M. Whitaker, and J. Park, "BRESAP: A policy reasoner for processing spectrum access policies represented by binary decision diagrams," in *Proc. IEEE Int. Symp. New Frontiers Dyn. Spectrum Access Netw.*, 2010, DOI: 10.1109/DYSPAN.2010.5457867.

[39] B. Bahrak, A. Deshpande, and J. Park, "Spectrum access policy reasoning for policy-based cognitive radios," *Comput. Netw.*, vol. 56, no. 11, pp. 2649–2663, Jul. 2012.

[40] G. Denker, D. Elenius, R. Senanayake, M. O. Stehr, and D. Wilkins, "A policy engine for spectrum sharing," in *Proc. IEEE Int. Symp. New Frontiers Dyn. Spectrum Access Netw.*, 2007, pp. 55–65.

[41] F. Perich, R. Foster, P. Tenhula, and M. McHenry, "Experimental field test results on feasibility of declarative spectrum management," in *Proc. IEEE Int. Symp. New Frontiers Dyn. Spectrum Access Netw.*, 2008, DOI: 10.1109/DYSPAN.2008.28.

[42] A. Toninelli, J. Bradshaw, L. Kagal, and R. Montanari, "Rule-based and ontology-based policies: Toward a hybrid approach to control agents in pervasive environments," in *Proc. Semantic Web Policy Workshop*, Sep. 2005, pp. 42–54.

[43] B. Bahrak, J. Park, and H. Wu, "Ontology-based spectrum access policies for policy-based cognitive radios," in *Proc. IEEE Int. Symp. New Frontiers Dyn. Spectrum Access Netw.*, 2012, pp. 489–500.

[44] M. Kokar and L. Lechowicz, "Language issues for cognitive radio," *Proc. IEEE*, vol. 97, no. 4, pp. 689–707, Apr. 2009.

[45] *IEEE Standard for Policy Language Requirements and System Architectures for Dynamic Spectrum Access Systems*, IEEE Std. 1900.5, Jan. 2012.

[46] C. Li, A. Raghunathan, and N. Jha, "An architecture for secure software defined radio," in *Proc. Design Autom. Test Eur.*, 2009, pp. 448–453.

[47] S. Xiao, J. Park, and Y. Ye, "Tamper resistance for software defined radio software," in *Proc.*

33rd Annu. IEEE Int. Comput. Softw. Appl. Conf., 2009, pp. 383–391.

[48] C. R. Aguayo González and J. H. Reed, “Power fingerprinting in SDR integrity assessment for security and regulatory compliance,” *Analog Integr. Circuits Signal Process.*, vol. 69, no. 2–3, pp. 307–327, Dec. 2011.

[49] X. Li, J. Chen, and F. Ng, “Secure transmission power of cognitive radios for dynamic spectrum access applications,” in *Proc. Conf. Inf. Sci. Syst.*, 2008, pp. 213–218.

[50] M. Weiss, M. Altamimi, and M. McHenry, “Enforcement and spectrum sharing: A case study of the 1695–1710 MHz band,” in *Int. Conf. Cogn. Radio Oriented Wireless Netw. (CROWNCOM)*, 2013.

[51] E. Bertino and S. Ravi, “Database security-concepts, approaches, and challenges,” *IEEE Trans. Depend. Secure Comput.*, vol. 2, no. 1, pp. 2–19, Jan.–Mar. 2005.

[52] L. Li, M. Kantarcioglu, and B. Thuraisingham, “The applicability of the perturbation based privacy preserving data mining for real-world data,” *Data Knowl. Eng.*, vol. 65, no. 1, pp. 5–21, 2008.

[53] L. Sweeney, “k-anonymity: A model for protecting privacy,” *Int. J. Uncertainty Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[54] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, “L-diversity: Privacy beyond k-anonymity,” in *Proc. Int. Conf. Data Eng.*, 2006, DOI: 10.1109/ICDE.2006.1.

[55] N. Li, T. Li, and S. Venkatasubramanian, “t-closeness: Privacy beyond k-anonymity and l-diversity,” in *Proc. Int. Conf. Data Eng.*, 2007, pp. 106–115.

[56] P. Samarati and L. Sweeney, “Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression,” in *Proc. IEEE Symp. Res. Security Privacy*, 1998.

[57] C. Dwork, “Differential privacy,” in *Proc. Int. Conf. Automata Lang. Programm.*, 2006, pp. 1–12.

[58] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” in *Proc. 1st Int. Conf. Mobile Syst. Appl. Services*, 2003, pp. 31–42.

[59] J. Freudiger, R. Shokri, and J. Hubaux, “On the optimal placement of mix zones *Privacy Enhancing Technologies*, vol. 5672, Berlin, Germany: Springer-Verlag, 2009, pp. 216–234.

[60] R. Chow and P. Golle, “Faking contextual data for fun, profit, and privacy,” in *Proc. 8th ACM Workshop Privacy Electron. Soc.*, 2009, pp. 105–108.

[61] B. Gedik and L. Liu, “Protecting location privacy with personalized k-anonymity: Architecture and algorithms,” *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, pp. 1–18, Jan. 2008.

[62] J. Hall, M. Barbeau, and E. Kranakis, “Detecting rogue devices in Bluetooth networks using radio frequency fingerprinting,” in *Proc. Int. Conf. Commun. Comput. Netw.*, Oct. 2006.

[63] O. Ureten and N. Serinken, “Wireless security through RF fingerprinting,” *Can. J. Electr. Comput. Eng.*, vol. 32, no. 1, pp. 27–33, 2007.

[64] K. Kim, C. Spooner, I. Akbar, and J. Reed, “Specific emitter identification for cognitive radio with application to IEEE 802.11,” in *Proc. IEEE Global Telecommun. Conf.*, 2008, DOI: 10.1109/GLOCOM.2008.ECP.404.

[65] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless device identification with radiometric signatures,” in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, 2008, pp. 116–127.

[66] B. Danev and S. Capkun, “Transient-based identification of wireless sensor nodes,” in *Proc. Int. Conf. Inf. Process. Sensor Netw.*, Apr. 2009, pp. 25–36.

[67] K. A. Remley, C. A. Grosvenor, R. T. Johnk, D. R. Novotny, P. D. Hale, M. D. Mckinley, A. Karygiannis, and E. Antonakakis, “Electromagnetic signatures of WLAN cards and network security,” in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol.*, Dec. 2005, pp. 484–488.

[68] B. Danev, H. Luecken, S. Čapkun, and K. Defrawy, “Attacks on physical layer identification,” in *Proc. 3rd ACM Conf. Wireless Netw. Security*, 2010, pp. 89–98.

[69] I. Cox, M. Miller, and A. McKellips, “Watermarking as communication with side information,” *Proc. IEEE*, vol. 87, no. 7, pp. 1127–1141, Jul. 1999.

[70] C. Fei, D. Kundur, and R. Kwong, “Analysis and design of secure watermark-based authentication systems,” *IEEE Trans. Inf. Forens. Security*, vol. 1, no. 1, pp. 43–55, Mar. 2006.

[71] N. Goergen, T. Clancy, and T. Newman, “Physical layer authentication watermarks through synthetic channel emulation,” in *Proc. IEEE Symp. New Frontiers Dyn. Spectrum*, Apr. 2010, DOI: 10.1109/DYSPAN.2010.5457897.

[72] J. Kleider, S. Gifford, S. Chuprun, and B. Fette, “Radio frequency watermarking for OFDM wireless networks,” in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, May 2004, vol. 5, pp. 397–400.

[73] X. Wang, Y. Wu, and B. Caron, “Transmitter identification using embedded pseudo random sequences,” *IEEE Trans. Broadcast.*, vol. 50, no. 3, pp. 244–252, Sep. 2004.

[74] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Using the physical layer for wireless authentication in time-variant channels,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[75] P. Yu, J. Baras, and B. Sadler, “Physical-layer authentication,” *IEEE Trans. Inf. Forens. Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[76] P. Yu, J. Baras, and B. Sadler, “Multicarrier authentication at the physical layer,” in *Proc. Int. Symp. World Wireless Mobile Multimedia Netw.*, Jun. 2008, DOI: 10.1109/WOWMOM.2008.4594926.

[77] X. Tan, K. Borle, W. Du, and B. Chen, “Cryptographic link signatures for spectrum usage authentication in cognitive radio,” in *Proc. 4th ACM Conf. Wireless Netw. Security*, Jun. 2011, pp. 79–90.

[78] R. Miller and W. Trappe, “ACE: Authenticating the channel estimation process in wireless communication systems,” in *Proc. 4th ACM Conf. Wireless Netw. Security*, 2011, pp. 91–96.

[79] Y. Liu, P. Ning, and H. Dai, “Authenticating primary users’ signals in cognitive radio networks via integrated cryptographic and wireless link signatures,” in *Proc. IEEE Symp. Security Privacy*, May 2010, pp. 286–301.

[80] L. Yang, Z. Zhang, B. Y. Zhao, C. Kruegel, and H. Zheng, “Enforcing dynamic spectrum access with spectrum permits,” in *Proc. 13th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2012, pp. 195–204.

[81] V. Kumar, J.-M. Park, T. C. Clancy, and K. Bian, “PHY-layer authentication by introducing controlled inter symbol interference,” in *Proc. IEEE Conf. Commun. Netw. Security*, Oct. 2013, pp. 27–35.

[82] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, “Non-interactive localization of cognitive radios based on dynamic signal strength mapping,” in *Proc. 6th Int. Conf. Wireless On-Demand Netw. Syst. Services*, 2009, pp. 77–84.

[83] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, “Range-free localization schemes for large scale sensor networks,” in *Proc. 9th Annu. Int. Conf. Mobile Comput. Netw.*, 2003, pp. 81–95.

[84] K. Woyach, A. Sahai, G. Atia, and V. Saligrama, “Crime and punishment for cognitive radios,” in *Proc. 46th Annu. Allerton Conf. Commun. Control Comput.*, 2008, pp. 236–243.

[85] M. B. Weiss, W. H. Lehr, L. Cui, and M. Altamaimi, “Enforcement in dynamic spectrum access systems,” in *Proc. Telecommun. Policy Res. Conf.*, Sep. 2012.

[86] K. Ren, X. Liu, W. Liang, M. Xu, X. Jia, and K. Xing, “Enforcing spectrum access rules in cognitive radio networks through cooperative jamming,” in *Wireless Algorithms, Systems, and Applications*, vol. 7992. Berlin, Germany: Springer-Verlag, 2013, pp. 440–453.

ABOUT THE AUTHORS

Jung-Min (Jerry) Park (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, USA, in 2003.

He is currently an Associate Professor in the Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, and the Site Director of a National Science Foundation (NSF) Industry-University Cooperative Research Center (I-UCRC) called Broadband Wireless Access & Applications Center (BWAC). As the Site Director of BWAC at Virginia Tech, he leads several sponsored research projects on wireless networks and network security. He is widely recognized for his pioneering work on enforcement and security problems in cognitive radio networks. His research interests include cognitive radio networks, spectrum-sharing technologies, network security and privacy, and applied cryptography. Current or recent research sponsors of his work include the National Science Foundation (NSF), the National Institutes of Health (NIH), the Defense Advanced Research Projects Agency (DARPA), the U.S. Office of Naval Research (ONR), the SysAdmin, Audit, Network Security (SANS) Institute, Motorola Solutions, Samsung Electronics, and SCA Techniques.

Prof. Park is a recipient of the 2008 NSF Faculty Early Career Development (CAREER) Award, the 2008 Hoeber Excellence in Research Award, and the 1998 AT&T Leadership Award. He is a Senior Member of the Association for Computing Machinery (ACM) and a member of the Korean-American Scientists and Engineers Association (KSEA).

Jeffrey H. Reed (Fellow, IEEE) received the B.S.E.E., M.S.E.E., and Ph.D. degrees from the University of California Davis, Davis, CA, USA, in 1979, 1980, and 1987, respectively.

Currently, he serves as Director of Wireless@ VT, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA. He is the Founding Faculty member of the Ted and Karyn Hume Center for National Security and Technology and served as its interim Director when founded in 2010. He is the author of the book *Software Radio: A Modern Approach to Radio Design* (Englewood Cliffs, NJ, USA: Prentice-Hall, 2002). He is cofounder of Cognitive Radio Technologies (CRT), a company commercializing the cognitive radio technologies; Allied Communications, a company developing technologies for 5G systems; and Power Fingerprinting, a company specializing in security for embedded systems.

Dr. Reed became Fellow to the IEEE for contributions to software radio and communications signal processing and for leadership in engineering education, in 2005. He is also a Distinguished Lecturer for the IEEE Vehicular Technology Society. In 2013, he was awarded the International Achievement Award by the Wireless Innovations Forum. In 2012, he served on the President's Council of Advisors of Science and Technology Working Group that examines ways to transition federal spectrum to allow commercial use and improve economic activity

A. A. (Louis) Beex received the Ir. degree (M.S. equivalent) from the Technical University Eindhoven, Eindhoven, The Netherlands, and the Ph.D. degree from Colorado State University, Fort Collins, CO, USA, both in electrical engineering.

Currently, he is Professor of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University, Blacksburg, VA, USA and Director of the DSP Research Laboratory, affiliated with Wireless@VT. His research interests lie in stochastic, digital, and adaptive signal processing, as in, for example, Doppler and multipath mitigation for acoustic communication channels; analysis and exploitation of nonlinear effects in adaptive signal processing; multipath modeling and mitigation; robust interference mitigation; adaptive sensor array processing, for direction finding in reverberant environments; (spectral) analysis, (adaptive) modeling, and coding of signals (EEG, speech, communications) for detection of specific characteristics. He has been teaching in the signals, systems, controls, and communications areas for well over three decades. His industrial experience includes serving as a Staff Research Engineer at Starkey Labs, Eden Prairie, MN, USA, working on applications of digital signal processing for the design of advanced hearing instruments, and for their automated evaluation. He has taught short courses for various companies and organizations, as well as served as a consultant on DSP-oriented power measurements of undersampled signals containing harmonics, on adaptive channel equalization, on DSP related review, on AGC analysis, on analysis of nonlinear dynamic behavior of filter weights for control of nonlinear antenna arrays, on signal analysis and decomposition, on multipath mitigation for satellite communications, and on noise mitigation for system identification.

T. Charles Clancy (Senior Member, IEEE) received the M.S. degree in electrical engineering from the University of Illinois, Chicago, IL, USA, and the Ph.D. degree in computer science from the University of Maryland, College Park, MD, USA.

Currently, he is an Associate Professor of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, VA, USA, and is Director of the Hume Center for National Security and Technology. His current research interests include resilient wireless communications and electronic warfare. Prior to joining Virginia Tech in 2010, he worked for the Laboratory for Telecommunications Sciences, a federal research laboratory at the University of Maryland. There he led government research programs in wireless communications, with an emphasis on military applications of software-defined and cognitive radio. He is the author to over 100 peer-reviewed publications.

Vireshwar Kumar received the B.S. degree in electrical engineering from Indian Institute of Technology, Delhi, India, in 2009. He is currently working toward the Ph.D. degree at the Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA.

His research interests include security issues in cognitive radio networks and spectrum-sharing, PHY-layer authentication, and wireless networks.

Behnam Bahrak received the B.S. and M.S. degrees in electrical engineering from Sharif University of Technology, Tehran, Iran, in 2006 and 2008, respectively, and the Ph.D. degree from the Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, in 2013.

His research interests include cryptography, network security, and dynamic spectrum access.