Chapter 17

Policy Enforcement in Dynamic Spectrum Sharing

17.1. Introduction

Fully realizing the vision of *dynamic spectrum sharing* (DSS) requires the adoption of fundamentally new spectrum access paradigms. For instance, in DSS, a heterogeneous mix of wireless systems of differing access priorities, QoS requirements, and transmission characteristics need to coexist without causing harmful interference to each other. In these novel paradigms, when different stakeholders share a common resource (such as the case in spectrum sharing), security and enforcement become critical considerations that are essential to the welfare of all stakeholders. Policy enforcement is especially a paramount consideration when sharing government (including military) spectrum with non-government (commercial) systems. Hence, to securely and efficiently employ innovative spectrum access technologies, the spectrum regulatory authorities throughout the world have emphasized the need to adopt new regulatory policies which could be enforced with the help of frameworks, such as a spectrum monitoring system which was discussed in Chapter 16.

In this chapter, we review the critical security and privacy threats to the harmonious and efficient functioning of DSS ecosystems, and their countermeasures. First, a taxonomy for classifying the threats is discussed. The taxonomy considers fundamental mechanisms for enabling coexistence (i.e., spectrum sensing-driven mechanism or database-driven mechanism) as well as the points of attack with respect to the five-layer protocol stack. For each threat category, representative security and privacy threats, and their relation to other types of threats are described. Further, the existing proposals for threat countermeasures and spectrum policy enforcement are discussed. The enforcement mechanisms 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 behavior after a potentially harmful interference event has occurred. The chapter concludes by discussing the research and regulatory challenges that need to be addressed to ensure policy enforcement in DSS.

17.2. Technical Background

In the perspective of policy enforcement, there are three major attributes associated with the DSS model: user, coexistence, and security attributes. These attributes are briefly discussed below. They will be utilized later to present a classification of threats and their countermeasures.

User Attributes. In spectrum sharing, users of different access priorities share a common resource, viz spectrum, within a clearly-defined hierarchy.

On one hand, the Licensed Shared Access (LSA) model adopted in Europe employs a two-tier sharing structure (incumbent tier-1 users and licensee tier-2 users); on the other hand, the Spectrum Access System (SAS) adopted in the United State employs a three-tier structure (incumbent tier-1 users, priority access license tier-2 users, and general authorized access tier-3 users) [51]. For the following discussions in this chapter, we follow the two-tier spectrum sharing model in which users are broadly classified into two categories: *incumbent/primary users* (PUs) and *secondary users* (SUs). The PUs have access priority over the SUs, and may consist of government users and licensed users. The SUs have secondary (i.e., subordinate) rights to spectrum, and typically consist of unlicensed opportunistic users.

Coexistence Attributes. There are two different mechanisms for enabling the harmonious coexistence of heterogeneous wireless systems in a shared spectrum ecosystem: spectrum sensing and geolocation databases. In a sensing-driven spectrum sharing scenario, SUs become cognizant of the surrounding *radio frequency* (RF) environment through either stand-alone or cooperative spectrum sensing [70], and their transmission behavior is dictated by spectrum sensing results. Note that SUs' radios need to have sufficient intelligence to use transmission parameters that are compliant with regulatory spectrum policies. Radios with such capabilities are often referred to as *cognitive radios* (CRs). In a database-driven spectrum sharing application, SUs are required to obtain spectrum availability information from a geolocation database which may also prescribe policies to access the shared spectrum (e.g., maximum allowed transmission power) [33, 52]. In some DSS ecosystems, both geolocation databases and sensing-based mechanisms are utilized in tandem to enable harmonious spectrum sharing between users of different access priorities [23].

Security Attributes. To ensure the viability of spectrum sharing, the following security and enforcement requirements must be met [7, 57].

- *Confidentiality*: The data communicated between users and the database 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.
- *Non-repudiation*: 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 non-compliant behavior causing harmful interference.
- *Access control*: No user should be able to access either the database or the spectrum without proper credentials.
- *Data privacy*: Along with the data stored in the geolocation databases, sensitive data of the users, i.e., PUs and SUs, should be properly protected.
- *Operational privacy*: Sensitive operational attributes (e.g., location) of the users should be preserved.

17.3. Security and Privacy Threats

In the DSS paradigm, SUs may need to employ *software-defined radios* (SDRs) to harmoniously coexist with PUs as well as other SUs. Unlike a legacy radio,

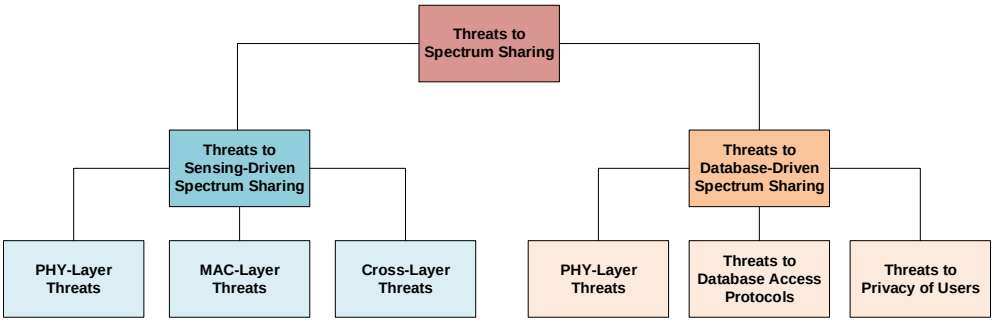

Figure 17.1: Taxonomy of threats to spectrum sharing.

which is hardware or firmware-based, a SDR enables a user to readily reconfigure its transmission parameters, allowing for greater flexibility. However, this "programmability" of SDRs also significantly increases the possibility of "rogue" or malfunctioning SUs. In this section, the security and privacy issues that pose the greatest threats to spectrum sharing are presented.

The threats to spectrum sharing can be classified into two broad categories based on the spectrum sharing approach that the attacks target: threats to sensing-driven spectrum sharing and threats to database-driven spectrum sharing. Based on this classification, a taxonomy of threats is presented in Figure 17.1 to provide a systematic discussion of the topic, and to offer a clear picture of the known security and privacy issues.

17.3.1. Sensing-Driven Spectrum Sharing

The following threats exploit the vulnerabilities in the spectrum sensing-based mechanism which is utilized for enabling a spectrum sharing ecosystem.

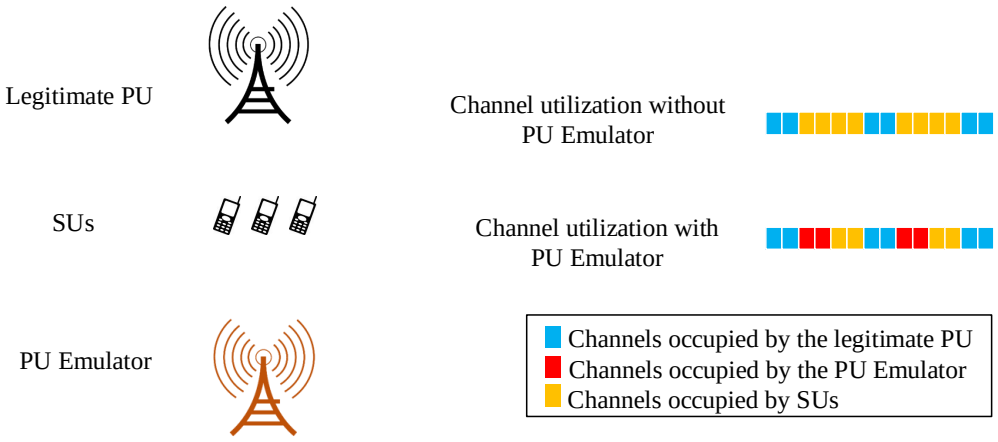

Figure 17.2: Primary user emulation (PUE) attack.

17.3.1.1. PHY-Layer Threats

Threats in this sub-category directly impact the PHY-layer mechanisms, most notably spectrum sensing. Spectrum sensing by SUs can be manipulated by a rogue transmitter to either hijack their spectrum or affect their spectrum sharing decisions, e.g., through *PU emulation* (PUE) attacks [15, 17]. In a PUE attack (shown in Figure 17.2), a malicious SU emulates a PU's transmission characteristics in order to gain illegitimate access to the spectrum and/or prevent other SUs from accessing the spectrum. The PUE attack can also be used as a tool to launch more sophisticated attacks [54].

An approach for enhancing the accuracy of spectrum sensing is to employ cooperative spectrum sensing and centralized decision making [40]. In this approach, multiple users sense and send their observations about the RF environment to a fusion center. The fusion center ingeniously combines the reported information to make the final decision regarding the presence/absence of PU's transmissions. Another approach for collaborative sensing is to employ cooperative spectrum sensing and distributed decision making. In this approach, no fusion center is used, instead each SU makes the decision about the presence

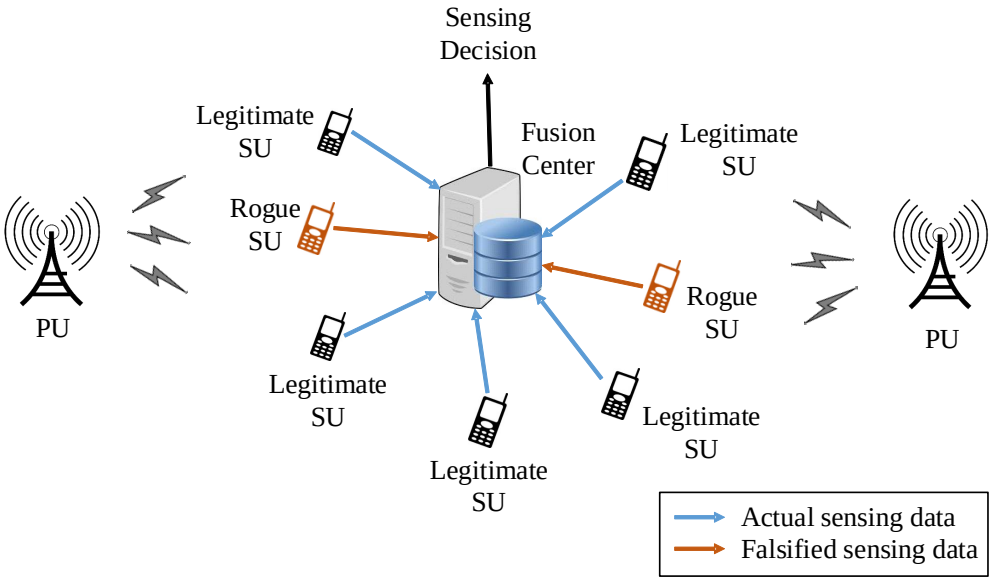

Figure 17.3: Spectrum sensing data falsification (SSDF) attack.

of PU based on its own observations and those shared by other SUs.

Both sensing approaches mentioned above are prone to *spectrum sensing data falsification* (SSDF) attack in which rogue SUs send false observations about the RF environment [14, 20, 60]. An illustration of the SSDF attack is presented in Figure 17.3. Due to the SSDF attack, legitimate SUs in the network may acquire inaccurate perception of the RF environment, and make decisions that may cause interference to PUs. Also, rogue SUs may violate the spectrum sharing policies, and transmit selfishly on convenient channels causing harmful interference to PUs and other SUs [42].

17.3.1.2. MAC-Layer Threats

There are numerous attacks that may compromise the MAC-layer mechanisms of spectrum sharing. In a multi-hop CR network, a pre-defined frequency channel—called the cognitive control channel—is used by SUs to exchange

control information, e.g., channel negotiation and spectrum hand-off. A rogue transmitter may jam this channel with little effort, and cause *denial of service* (DoS) to SUs [72]. This is referred to as *control channel corruption* (CCC) attack. An alternative technique for enabling coexistence of SUs and coordinating the use of channels among SUs is to utilize beacons. Again, in this mechanism, a malicious transmitter can launch a *beacon falsification* (BF) attack which may compromise critical functionalities, such as inter-cell spectrum contention and inter-cell synchronization [12]. Some SUs may also implement a *carrier sense multiple access with collision avoidance* (CSMA/CA) protocol in which a SU backs-off by a random time after sensing the transmission from another SU. If there is a collision of packets transmitted by any two SUs, the SUs double the back-off window before retransmission. In this protocol, a malicious user may utilize a small back-off window, and gain priority over other users [61]. This is called the *small-back-off-window* (SBW) attack.

17.3.1.3. Cross-Layer Threats

In some scenarios, multiple attacks can be conducted in tandem to exploit vulnerabilities in two or more layers of the protocol stack. These attacks are called cross-layer attacks. For instance, in DSS utilizing the CSMA/CA protocol, a malicious user can launch SSDF attack (at PHY-layer) and SBW attack (at MAC-layer) in a coordinated fashion [64]. This coordination makes it difficult to detect either of the two attacks. Also, this cross-layer attack is more successful than a single-layer attack in diminishing the overall SUs' channel utilization. Another example of a cross-layer attack is known as the *Lion* attack that targets the PHY and transport layers [34]. In a Lion attack, a malicious user launches a PUE attack, and forces the target SUs to carry out frequency

hand-offs. The transmission interruptions caused by the frequency hand-offs lead to very poor throughput at the transport layer since the *transmission control protocol* (TCP) is quite sensitive to variations in delay and bandwidth.

17.3.2. Database-Driven Spectrum Sharing

The threats described in this subsection impinge the security and privacy of users in spectrum sharing enabled by geolocation databases.

17.3.2.1. PHY-Layer Threats

The undesirable interference from rogue transmitters can significantly impact the SUs' spectrum utilization in the database-driven sharing [33]. Specifically, the information about spectrum availability provided by databases can be exploited by a rogue transmitter to amplify its ability to launch targeted jamming attacks, and hide its non-compliant transmissions [71].

17.3.2.2. Threats to the Database Access Protocol

The *database access protocol attacks* (DAPA) refer to the varied set of security threats related to the access control mechanism of the database [8, 58]. In the database-driven sharing without suitable protection mechanisms, different flavours of DAPA can be launched. In a masquerade attack, a rogue SU can listen to registration exchanges between a legitimate SU and the database, and later register with the database by claiming the identity of the legitimate SU. Spoofing a database in order to provide malicious responses to SUs is another type of attack that can disrupt the sharing environment.

Further, the attacker may compromise the integrity of a SU's query and/or

database's response. If an attacker is able to change some of the information in the SU's query (e.g. the location of the SU or its capabilities), the database will respond with incorrect information about available spectrum or maximum allowed transmission power. The attacker may also directly modify the available spectrum or power level information carried in the database response. Additionally, selectively jamming database queries/responses may cause a denial of service to the SUs. Further, if a database includes a mechanism by which spectrum allocated to a SU can be revoked by sending a revoke message, malicious users can pretend to be the database and send a revoke message to that SU terminating or unfairly limiting spectrum access of the SU.

17.3.2.3. Threats to the Privacy of Users

Although using geolocation databases for spectrum sharing has many advantages over the sensing-based approach, it poses a potentially serious privacy problem. There is the possibility that through sophisticated inference techniques, SUs can obtain knowledge beyond what is revealed directly by the database's responses. This type of attack is referred as *database inference attack* (DIA) [6] which compromises the operational privacy of the PUs.

For instance, SUs, through seemingly innocuous queries to the database, can infer various attributes of PUs. Some of these attributes include PU's identity (e.g., the call sign of the transmitter in an FCC's Consolidated Database System), geolocation (i.e., latitude and longitude), antenna parameters, transmission power, transmit protection contours (co-channel and adjacent channel), and times of operation. When the incumbent systems are commercial systems, such as the case in TV spectrum, the inference of these attributes is not an issue. However, when the incumbents are government, possibly military,

Table 17.1: Security features compromised by threats.

Security feature	Threats						
	PUE	SSDF	CCC	BF	SBW	DAPA	DIA
Confidentiality			×			×	
Integrity		×	×	×	×	×	
Availability	×	×	×	×	×	×	
Authentication	×		×	×		×	
Non-repudiation	×			×			
Compliance	×			×			
Access control	×			×		×	
Data privacy						×	
Operational privacy							×

systems, then the information revealed by the databases may result in a serious breach of operational privacy. For instance, the operational privacy of PUs is an especially critical concern for sharing of federal government's spectrum in the 3.5 GHz band with non-government systems in the United States.

Another issue that may arise as a result of using geolocation databases for spectrum sharing is the compromise of operational privacy of SUs. For instance, since SUs 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. An advanced attack on the SU's location privacy is called *spectrum utilization-based location inference* (SULI) attack which allows an attacker to infer the location of the SU from the channels utilized by it [26].

Table 17.1 summarizes the threats to spectrum sharing discussed in this section by highlighting the security features that they compromise (denoted by the notation ×).

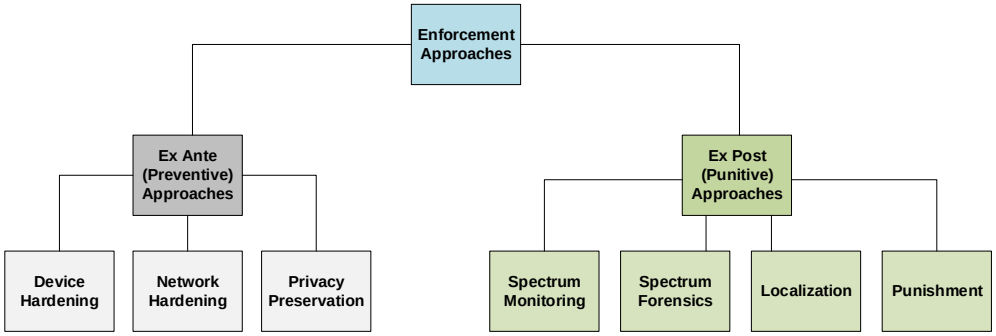

Figure 17.4: Taxonomy of enforcement approaches for spectrum sharing.

17.4. Enforcement Approaches

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. Also, making controlled changes to a legacy radio's behavior would require an adversary to have very specialized technical expertise in the radio's firmware and hardware. Unfortunately, the reconfigurability of SDRs/CRs not only makes them vulnerable to unauthorized modifications, but also makes it difficult to enforce spectrum policies.

Considering the wide landscape of the threats, we discuss a battery of countermeasures for spectrum policy enforcement by classifying them into two broad categories: *ex ante* (preventive) and *ex post* (punitive) enforcement. The taxonomy of enforcement approaches is illustrated in Figure 17.4. The objective of ex ante enforcement is to prevent or reduce the probability of a policy violation causing harmful interference or loss of user privacy. On the other hand, the objective of ex post enforcement is to identify and/or punish malicious or selfish users after a policy violation has occurred. A real-world policy enforcement framework may need to employ a combination of specific ex ante and ex post enforcement approaches.

17.4.1. Ex Ante (Preventive) Approaches

The ex ante approaches can be classified into three classes which include device hardening, network hardening and privacy preservation.

17.4.1.1. Device Hardening

The device hardening is an important step in ensuring policy enforcement in DSS. It follows the concept of target hardening, i.e., strengthening the security of SDRs/CRs to deter or delay the threats. This technique is discussed below by differentiating between software and/or hardware-based approaches.

Software-Based Approach. The most prominent software-based approach for enforcing policy control is to employ *policy-based* CRs. Policy-based CRs adapt with evolving spectrum access policies and constantly changing application requirements by decoupling the policies from device-specific implementation and optimization. These radios can invoke situation-appropriate adaptive actions based on policy specifications and the current spectrum environment [28]. In order to regulate and enforce proper transmission behavior, policy-based CRs need mechanisms to interpret and enforce spectrum access policies. Each transmission from the policy-based CRs needs to be evaluated against those policies to determine the legality of the transmission parameters. Within a policy-based CR, the aforementioned tasks are carried out in real time by a software module called the *policy reasoner*. There are two major types of policy reasoners: rule-based and ontology-based policy reasoners.

The rule-based policy reasoners utilize logic programming techniques to encode the axioms and rules, and enforce policy conformance [4, 58, 59, 62]. Using the rule-based approach simplifies the design of the policy reasoner be-

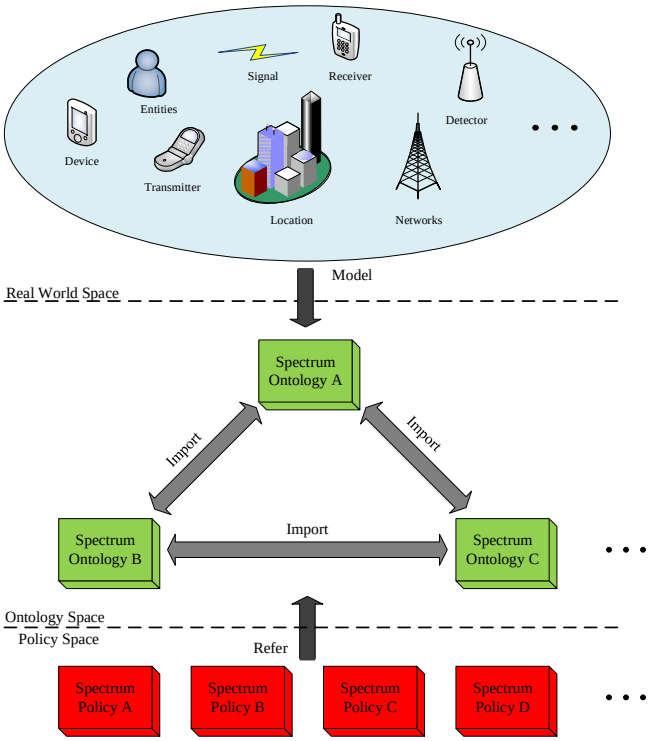

Figure 17.5: Components of an ontology-based policy reasoner.

cause the reasoning complexity is sufficiently low in most applications to meet the real-time processing requirements of the radio. However, they do not support the sharing of the policy structure among different policy authors (i.e., regulatory authorities) limiting the interoperability of the policy-based CRs across different regulatory policy domains. Also, complex spectrum policies are difficult to specify and manage with rule-based policies.

To overcome these limitations of rule-based policy reasoners, the IEEE 1900.5 Standard for Policy Language Requirements and System Architectures for Dynamic Spectrum Access Systems prescribes the use of an ontology-based policy language for managing the functionality and behavior of DSS networks [1, 5, 39]. Managing ontologies to support the formal representation of spectrum policies in the ever changing DSS ecosystem is significantly easier than man-

aging rule-based policy enforcement. Figure 17.5 illustrates the components of an ontology-based policy reasoner utilized for spectrum access policies.

Middleware-Based Approach. A *secure radio middleware* (SRM) layer can be implemented between the operating system and the hardware [46]. 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, and type of modulation, conform with policies in a policy database. Unlike a software-based policy reasoner that provides feedback to the radio's software, the SRM layer simply discards non-conforming requests.

Hardware-Based Approach. An effective hardware-based approach is to use tamper resistance techniques to protect a radio's software against unauthorized modifications [67]. The tamper resistant module 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). This approach is also effective in enforcing countermeasures against rogue transmission [42, 43].

In addition to tamper resistance techniques, the integrity assessment of a SDR can also be performed by a hardware dedicated for power fingerprinting [30]. This mechanism is able to detect the execution of a tampered routine by closely monitoring the power consumption of the radio platform. Also, an independent power-check module can be implemented at the hardware of the SDR transceiver to control its maximum transmission power [47]. These hardware-based approaches are designed to prevent transmissions that cause harmful interference to PUs/SUs even if the radio's software is compromised.

17.4.1.2. Network Hardening

The concept of network hardening refers to the preventive measures required to protect PUs from interference, SUs from denial-of-service, and geolocation databases from threats to the access protocol.

Protecting PUs from Interference. As discussed in Chapters 2 and 4, a popular ex ante approach to protect the PU from undesirable interference is to employ the concept of *exclusion zones* [66]. An exclusion zone is a spatial region in which no in-band emissions from SUs are permitted. This protection boundary can also be dynamically adjusted based on the radio environment, network conditions and the corresponding PU interference protection requirement [9]. The dynamic exclusion zones can be realized with the help of a dedicated/crowd-sourced network with spectrum *environmental sensing capability* (ESC) [55]. Dynamically adjusting the PU's protection boundary allows more SUs to operate closer to the PU thereby resulting in an improvement in spectrum utilization efficiency while also ensuring that the PU is adequately protected from interference.

Protecting SUs from Jamming. The traditional well-known anti-jamming techniques, such as *direct-sequence spread spectrum* (DSSS) and *frequency hopping spread spectrum* (FHSS), are insufficient for preventing jamming attacks in spectrum sharing ecosystem. This is because the spectrum information disseminated in either the sensing-based or the database-based sharing mechanism is available to all SUs including rogues SUs/jammers. Hence, novel countermeasures must complement the traditional techniques by considering dynamic channel allocation mechanisms and jammer inference mechanisms [71].

Protecting Geolocation Databases. The access control mechanism of the geolocation databases must be protected using state-of-the-art cryptographic primitives for encryption and authentication [8, 35, 37]. Additionally, a distributed architecture for storing and disseminating information is an essential aspect for securing the database-driven DSS [2].

17.4.1.3. Privacy Preservation

The application of the DSS paradigm in many scenarios is limited by the privacy concerns of PUs and SUs. These concerns can be mitigated by employing the following measures which thwart an adversary from directly gaining or inferring such information that could compromise the privacy of users.

Protecting PU's Privacy. In the database-driven sharing mechanism, the 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 its responses to the SUs' queries [6, 11, 18]. For instance, to infer the location of the PU, a rogue SU may exploit the *allowed transmission power* values which are inherently provided by the database in response to SU's queries. The true power values can be masked using two obfuscation strategies: perturbation with *additive noise* and *transfiguration* [6]. In perturbation with additive noise, the database adds random noise values to the actual power values, and responds with these modified power values. In perturbation with transfiguration, the database modifies the structure of the exclusion zone by employing randomly shaped contours in place of the actual circular contour, and then responds with the power values corresponding to these randomly shaped contours.

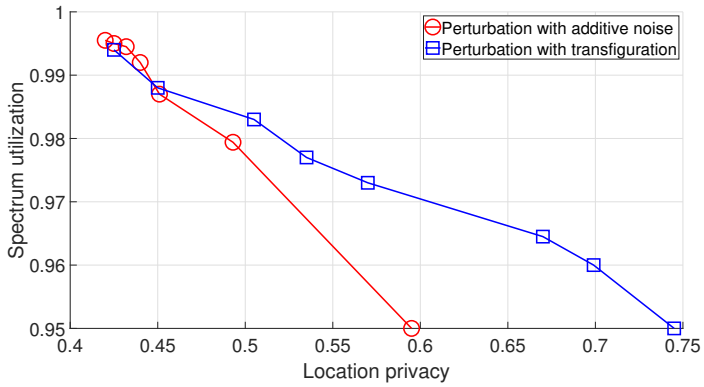

Figure 17.6: Trade-off between location privacy of the PU and spectrum utilization of SUs [6].

Figure 17.6 presents an illustration of the impact of perturbation with additive noise and transfiguration on the normalized values of location privacy of the PU and the spectrum utilization of SUs. The location privacy is measured by the metric called *inaccuracy* which is defined as the expected distance between the estimate of the PU's location inferred through queries and the PU's true location. The spectrum utilization is measured by the metric called *area sum capacity* which is defined as the sum of channel capacity values of the SUs in the region served by the database. Figure 17.6 illustrates that the obfuscation strategies need to be performed in an intelligent manner such that a certain level of privacy is assured to the PU while supporting an efficient use of the spectrum. For instance, the database may keep track of the information revealed through its past responses so that it can leverage such a history to compute an optimal response to the current query.

Another approach is to utilize the attribute-based encryption for the responses [48]. In this approach, the PU obtains attribute credentials based on its operational specifications, and then utilizes these credentials for encrypting the responses. The encrypted responses can only be decrypted by the SU with

qualified attribute credentials. This approach is computationally expensive, but it does not adversely affect the spectrum utilization.

Protecting SU's Privacy. The location-based services, such as DSS, rely on accurate, continuous, and real-time streams of the users' location data. However, with the potential of mishandling of such information by an untrusted database, these services pose a significant privacy risk to the SUs. Techniques for mitigating such a risk include sending a space or time-obfuscated version of the users' actual locations [26, 32], hiding some of the users' locations by using mix zones [24], sending fake queries which are indistinguishable from real queries and issued from fake locations to the database [16], applying k-anonymity to location privacy [27], and utilizing private information retrieval techniques [31]. Again, these privacy-preserving techniques for SUs bring forth the delicate trade-off between privacy and efficient spectrum utilization.

17.4.2. Ex Post (Punitive) Approaches

To counter threats which may bypass ex ante enforcement approaches, it is crucial to deploy a multi-pronged ex post enforcement approach for detection and remedy [25]. The ex post enforcement procedure can be divided into four stages: spectrum monitoring, spectrum forensics, localization, and punishment.

17.4.2.1. Spectrum Monitoring

The logical first step in ex post enforcement for an enforcement entity (e.g., FCC's Enforcement Bureau) is to perform data collection by spectrum monitoring which refers to the procedure of recording spectral RF emissions. Spectrum monitoring helps in verifying policy compliance in DSS by detecting interfer-

ence events. It can be practically realized by combining interference detection results from dedicated sensors [25, 55] and crowd-sourced sensors [21, 45]. A detailed discussion on spectrum monitoring is presented in Chapter 16.

17.4.2.2. Spectrum Forensics

Spectrum forensics refers to the procedure of leveraging the data obtained from spectrum monitoring to gather actionable evidence (that may be tenable in a court of law) of rogue transmission by a SU. This can be performed by uniquely identifying or authenticating rogue transmitters. Ideally, the enforcement entity would want to carry out the identification using a PHY-layer scheme because it is not the intended recipient of the transmitted signals, and it has little or no knowledge of the higher-layer parameters of the SU. Also, a PHY-layer scheme enables the enforcement entity to quickly distinguish between compliant and rogue transmitters without having to complete higher-layer processing.

Spectrum forensic schemes can be broadly divided into two categories: identification and authentication 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 identify transmitters. They include RF fingerprinting, and electromagnetic signature identification [13, 36]. Although these identification 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 [19]. Hence, more mature and refined detection/identification techniques, such as those based on machine leaning [41, 50], are needed for robust spectrum forensics.

Schemes in the second category enable a transmitter to *extrinsically* embed an authentication signal (e.g., message authentication code or digital signature) in the message signal and enable a receiver to extract it. Such schemes include PHY-layer watermarking [22, 29, 38] and transmitter authentication [43, 44, 68, 69]. For this approach to be viable, all SU radios must incorporate a mechanism for authenticating their waveforms, and employ tamper resistant mechanisms to prevent hackers from circumventing the mechanism.

17.4.2.3. Localization

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 non-compliant 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, it is unlikely that the rogue transmitter would provide any cooperation for its location estimation. Thus, the localization in DSS has to be achieved via a non-interactive technique, e.g., by measuring the *received signal strength* (RSS) and time difference of arrival (TDOA) [15, 21, 49, 63]. The information about the distances measured between the rogue transmitter and the receivers in the spectrum monitoring system can be merged at the regulator to localize the rogue transmitter.

17.4.2.4. Punishment

The aim of punishment is to impose a *penalty* for the non-compliant behavior [3, 20, 25, 53, 65]. 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 non-compliance [25]. It should also be proportional to the harm caused due to non-compliance. Additionally, the implications of imperfect enforcement mechanisms need to be taken into account as the risk of punishing compliant users may deter the prospects of spectrum sharing.

In a spectrum sharing ecosystem, there are two methods for penalizing non-compliant transmitters: restricting access to spectrum, and charging economic penalties. In the first method, the resource allocation strategy takes into account the compliance behavior of the SU. A rogue SU may not be 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, and curtailing its operating rights [25]. The second method 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 act as one of the benefits to legitimate SUs for their compliance.

17.5. Open Problems

To motivate future work, we briefly discuss important open research and regulatory challenges in realizing a secure and efficient DSS ecosystem.

17.5.1. Research Challenges

Challenges in Ex Ante Approaches. The development of a flexible and descriptive policy language, which can be used to specify spectrum access poli-

cies for DSS, is a challenge that needs the attention of the research community. Another important challenge related to spectrum policies includes the development of advanced algorithms for executing policy inference and reasoning tasks carried out by policy-based cognitive radios. Another open problem is to utilize ontology-based policies for enforcement while meeting the real-time processing requirements of the radio.

Challenges in Ex Post Approaches. Traditional ex post enforcement techniques for wireless systems relied on transmitter specifications (transmission power, antenna parameters, bandwidth and sensitivity) to detect and prevent harmful interference. However, these traditional approaches are less effective in DSS since the dynamic spectrum access enables the flexibility/mobility of radios in time, space and spectral domains, which exacerbate the problem of security and enforcement [10, 56, 65]. Hence, novel mechanisms need to be developed for monitoring, forensics, and localization of transmitters in DSS.

17.5.2. Regulatory Challenges

Enforcement and Privacy. 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 the neighboring nodes can help detect, locate and punish policy-violating transmitters. However, privacy considerations need to be addressed before such solutions can be adopted.

Adjudication. In the ex post enforcement, the locus of adjudication is another critical problem that remains unaddressed [66]. 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.

Regulation and Enforcement. 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 ecosystem 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.

17.6. Summary

In this chapter, we focused on the engineering aspects of spectrum enforcement and security. Going forward, we believe that building an optimal policy enforcement framework will require a skillful combination of ex ante and ex post, centralized and decentralized, and general and application-specific enforcement components that co-evolve 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.

Bibliography

1. IEEE standard for policy language requirements and system architectures for dynamic spectrum access systems. IEEE Std 1900.5, 2012.

2. G. Aggarwal, M. Bawa, P. Ganesan, et al. Two can keep a secret: A distributed architecture for secure database services. In *The Second Biennial Conference on Innovative Data Systems Research (CIDR)*, 2005.

3. G. Atia, A. Sahai, V. Saligrama, et al. Spectrum enforcement and liability assignment in cognitive radio systems. In *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–12, 2008.

4. B. Bahrak, A. Deshpande, M. Whitaker, and J. Park. BRESAP: A policy reasoner for processing spectrum access policies represented by binary decision diagrams. In *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–12, 2010.

5. B. Bahrak, J. Park, and H. Wu. Ontology-based spectrum access policies for policy-based cognitive radios. In *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 489–500, 2012.

6. B. Bahrak, S. Bhattarai, A. Ullah, et al. Protecting the primary users' operational privacy in spectrum sharing. In *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 236–247, 2014.

7. G. Baldini, T. Sturman, A. R. Biswas, et al. Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead. *IEEE Communications Surveys & Tutorials*, 14(2):355–379, 2012.

8. E. Bertino and R. Sandhu. Database security-concepts, approaches, and

challenges. *IEEE Transactions on Dependable and Secure Computing*, 2 (1):2–19, 2005.

9. S. Bhattarai, A. Ullah, J. Park, et al. Defining incumbent protection zones on the fly: Dynamic boundaries for spectrum sharing. In *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 251–262, 2015.

10. S. Bhattarai, J. Park, B. Gao, et al. An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research. *IEEE Transactions on Cognitive Communications and Networking*, 2(2): 110–128, 2016.

11. S. Bhattarai, P. R. Vaka, and J. Park. Thwarting location inference attacks in database-driven spectrum sharing. *IEEE Transactions on Cognitive Communications and Networking*, 4(2):314–327, 2018.

12. K. Bian and J. Park. Security vulnerabilities in IEEE 802.22. In *Proceedings of the 4th Annual International Conference on Wireless Internet*, pages 1–9, 2008.

13. V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom)*, pages 116–127, 2008.

14. R. Chen, J. Park, and K. Bian. Robust distributed spectrum sensing in cognitive radio networks. In *IEEE International Conference on Computer Communications (INFOCOM)*, pages 1876–1884, 2008.

15. R. Chen, J. Park, and J. H. Reed. Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37, 2008.

16. R. Chow and P. Golle. Faking contextual data for fun, profit, and privacy. In *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society (WPES)*, pages 105–108, 2009.

17. T. C. Clancy and N. Goergen. Security in cognitive radio networks: Threats and mitigation. In *International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pages 1–8, 2008.

18. M. A. Clark and K. Psounis. Trading utility for privacy in shared spectrum access systems. *IEEE/ACM Transactions on Networking (TON)*, 26(1): 259–273, 2018.

19. B. Danev, H. Luecken, S. Čapkun, and K. Defrawy. Attacks on physical-layer identification. In *Proceedings of the Third ACM Conference on Wireless Network Security (WiSec)*, pages 89–98, 2010.

20. L. Duan, A. W. Min, J. Huang, and K. G. Shin. Attack prevention for collaborative spectrum sensing in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 30(9):1658–1665, 2012.

21. A. Dutta and M. Chiang. "See something, say something" crowdsourced enforcement of spectrum policies. *IEEE Transactions on Wireless Communications*, 15(1):67–80, 2016.

22. C. Fei, D. Kundur, and R. H. Kwong. Analysis and design of secure watermark-based authentication systems. *IEEE Transactions on Information Forensics and Security*, 1(1):43–55, 2006.

23. V. Frascolla, A. J. Morgado, A. Gomes, et al. Dynamic licensed shared access-a new architecture and spectrum allocation techniques. In *IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pages 1–5, 2016.

24. J. Freudiger, R. Shokri, and J. P. Hubaux. On the optimal placement of mix zones. In *International Symposium on Privacy Enhancing Technologies*, pages 216–234, 2009.

25. C. Galiotto, G. K. Papageorgiou, K. Voulgaris, et al. Unlocking the deployment of spectrum sharing with a policy enforcement framework. *IEEE Access*, 6:11793–11803, 2018.

26. Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao. Location privacy in database-driven cognitive radio networks: Attacks and countermeasures. In *IEEE International Conference on Computer Communications (INFOCOM)*, pages 2751–2759, 2013.

27. B. Gedik and L. Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7(1):1–18, 2008.

28. A. Ginsberg, W. D. Horne, and J. D. Poston. Community-based cognitive radio architecture: Policy-compliant innovation via the semantic web. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 191–201, 2007.

29. N. Goergen, T. C. Clancy, and T. R. Newman. Physical layer authentication watermarks through synthetic channel emulation. In *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–7, 2010.

30. C. R. A. González and J. H. Reed. Power fingerprinting in SDR integrity assessment for security and regulatory compliance. *Analog Integrated Circuits and Signal Processing*, 69(2-3):307–327, 2011.

31. M. Grissa, B. Hamdaoui, and A. A. Yavuz. Unleashing the power of multi-server PIR for enabling private access to spectrum databases. *IEEE Communications Magazine*, 56(12):171–177, 2018.

32. M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys)*, pages 31–42, 2003.

33. D. Gurney, G. Buchwald, L. Ecklund, et al. Geo-location database techniques for incumbent protection in the TV white space. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 1–9, 2008.

34. J. Hernandez-Serrano, O. León, and M. Soriano. Modeling the lion attack in cognitive radio networks. *EURASIP Journal on Wireless Communications and Networking*, 2011:1–10, 2011.

35. M. Jakobi, C. Simon, N. Gisin, et al. Practical private database queries based on a quantum-key-distribution protocol. *Physical Review A*, 83(2): 022301, 2011.

36. K. Kim, C. M. Spooner, I. Akbar, and J. H. Reed. Specific emitter identification for cognitive radio with application to IEEE 802.11. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–5, 2008.

37. S. Kirrane, A. Mileo, and S. Decker. Access control and the resource description framework: A survey. *Semantic Web*, 8(2):311–352, 2017.

38. J. E. Kleider, S. Gifford, S. Chuprun, and B. Fette. Radio frequency watermarking for OFDM wireless networks. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, volume 5, pages 397–400, 2004.

39. M. M. Kokar and L. Lechowicz. Language issues for cognitive radio. *Proceedings of the IEEE*, 97(4):689–707, 2009.

40. A. Kortun, T. Ratnarajah, M. Sellathurai, et al. On the performance of eigenvalue-based cooperative spectrum sensing for cognitive radio. *IEEE Journal of Selected Topics in Signal Processing*, 5(1):49–55, 2011.

41. M. Kulin, T. Kazaz, I. Moerman, and E. De Poorter. End-to-end learning from spectrum data: A deep learning approach for wireless signal identification in spectrum monitoring applications. *IEEE Access*, 6:18484–18501, 2018.

42. V. Kumar, J. Park, and K. Bian. Blind transmitter authentication for spectrum security and enforcement. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 787–798, 2014.

43. V. Kumar, J. Park, and K. Bian. PHY-layer authentication using duobinary signaling for spectrum enforcement. *IEEE Transactions on Information Forensics and Security*, 11(5):1027–1038, 2016.

44. V. Kumar, J. Park, and K. Bian. Transmitter authentication using hierarchical modulation in dynamic spectrum sharing. *Journal of Network and Computer Applications*, 91:52–60, 2017.

45. Vireshwar Kumar, He Li, Jung-Min (Jerry) Park, and Kaigui Bian. Enforcement in spectrum sharing: Crowd-sourced blind authentication of co-channel transmitters. In *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2018.

46. C. Li, A. Raghunathan, and N. K. Jha. An architecture for secure software defined radio. In *Design, Automation and Test in Europe (DATE)*, pages 448–453, 2009.

47. X. Li, J. Chen, and F. Ng. Secure transmission power of cognitive radios for dynamic spectrum access applications. In *Conference on Information Sciences and Systems (CISS)*, pages 213–218, 2008.

48. J. Liu, C. Zhang, H. Ding, et al. Policy-based privacy-preserving scheme for primary users in database-driven cognitive radio networks. In *IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2016.

49. S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein. Non-interactive localization of cognitive radios based on dynamic signal strength mapping. In *Sixth International Conference on Wireless On-Demand Network Systems and Services*, pages 85–92, 2009.

50. K. Merchant, S. Revay, G. Stantchev, and B. Nousain. Deep learning for RF device fingerprinting in cognitive communication networks. *IEEE Journal of Selected Topics in Signal Processing*, 12(1):160–167, 2018.

51. M. D. Mueck, S. Srikanteswara, and B. Badic. Spectrum sharing: Licensed shared access (LSA) and spectrum access system (SAS). *Intel White Paper*, 2015.

52. R. Murty, R. Chandra, T. Moscibroda, and P. Bahl. Senseless: A database-driven white spaces network. *IEEE Transactions on Mobile Computing*, 11(2):189–203, 2012.

53. V. Muthukumar and A. Sahai. Fundamental limits on ex-post enforcement and implications for spectrum rights. *IEEE Transactions on Cognitive Communications and Networking*, 3(3):491–504, 2017.

54. T. R. Newman, T. C. Clancy, M. McHenry, and J. H. Reed. Case study: Security analysis of a dynamic spectrum access radio system. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–6, 2010.

55. T. T. Nguyen, A. Sahoo, M. R. Souryal, and T. A. Hall. 3.5 GHz environmental sensing capability sensitivity requirements and deployment. In *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–10, 2017.

56. J. Park, J. H. Reed, A. A. Beex, et al. Security and enforcement in spectrum sharing. *Proceedings of the IEEE*, 102(3):270–281, 2014.

57. S. Parvin, F. K. Hussain, O. K. Hussain, et al. Cognitive radio network security: A survey. *Journal of Network and Computer Applications*, 35(6): 1691–1708, 2012.

58. B. Patil, A. Mancuso, and S. Probasco. Protocol to access white space (PAWS) databases: Use cases and requirements, 2013. URL `https://tools.ietf.org/html/rfc6953`. Accessed: November 1, 2018.

59. F. Perich and M. McHenry. Policy-based spectrum access control for dynamic spectrum access network radios. *Web Semantics: Science, Services and Agents on the World Wide Web*, 7(1):21–27, 2009.

60. A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney. Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks. *IEEE Transactions on Signal Processing*, 59(2):774–786, 2011.

61. M. Raya, I. Aad, J-P. Hubaux, and A. E. Fawal. DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots. *IEEE Transactions on Mobile Computing*, 5(12):1691–1705, 2006.

62. 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 *Semantic Web and Policy Workshop*, pages 42–54, Sept. 2005.

63. H. Wang, Z. Gao, Y. Guo, and Y. Huang. A survey of range-based localization algorithms for cognitive radio networks. In *2012 2nd international conference on consumer electronics, communications and networks (CECNet)*, pages 844–847, 2012.

64. W. Wang, Y. Sun, H. Li, and Z. Han. Cross-layer attack and defense in cognitive radio networks. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–6, 2010.

65. M. B. H. Weiss, W. H. Lehr, L. Cui, and M. Altamaimi. Enforcement in dynamic spectrum access systems. In *Telecommunications Policy Research Conference*, 2012.

66. M. B. H. Weiss, M. Altamimi, and M. McHenry. Enforcement and spectrum sharing: A case study of the 1695–1710 MHz band. In *8th International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM)*, pages 7–12, 2013.

67. S. Xiao, J. Park, and Y. Ye. Tamper resistance for software defined radio software. In *33rd Annual IEEE International Computer Software and Applications Conference (COMPSAC)*, pages 383–391, 2009.

68. L. Yang, Z. Zhang, B. Y. Zhao, et al. Enforcing dynamic spectrum access with spectrum permits. In *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 195–204, 2012.

69. P. L. Yu, J. S. Baras, and B. M. Sadler. Physical-layer authentication. *IEEE Transactions on Information Forensics and Security*, 3(1):38–51, 2008.

70. T. Yucek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Communications Surveys & Tutorials*, 11(1):116–130, 2009.

71. H. Zhu, C. Fang, Y. Liu, et al. You can jam but you cannot hide: Defending against jamming attacks for geo-location database driven spectrum sharing. *IEEE Journal on Selected Areas in Communications*, 34 (10):2723–2737, 2016.

72. L. Zhu and H. Zhou. Two types of attacks against cognitive radio network MAC protocols. In *International Conference on Computer Science and Software Engineering*, volume 4, pages 1110–1113, 2008.

Acronyms

BF	Beacon Falsification
CCC	Control Channel Corruption
CR	Cognitive Radio
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DAPA	Database Access Protocol Attack
DIA	Database Inference Attack
DoS	Denial of Service
DSS	Dynamic Spectrum Sharing
DSSS	Direct-Sequence Spread Spectrum
ESC	Environmental Sensing Capability
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
MAC	Medium Access Control
NTIA	National Telecommunications & Information Administration
PHY	Physical
PU	Primary User
PUE	Primary User Emulation
RF	Radio Frequency

RSS	Received Signal Strength
SBW	Small-Back-off-Window
SDR	Software Defined Radio
SRM	Secure Radio Middleware
SSDF	Spectrum Sensing Data Falsification
SU	Secondary Users
SULI	Spectrum Utilization based Location Inference
TCP	Transmission Control Protocol