

# Challenges and New Directions in Securing Spectrum Access Systems

Shanghao Shi, *Graduate Student Member, IEEE*, Yang Xiao<sup>1b</sup>, *Graduate Student Member, IEEE*,  
Wenjing Lou<sup>1b</sup>, *Fellow, IEEE*, Chonggang Wang, *Fellow, IEEE*, Xu Li, Y. Thomas Hou<sup>1b</sup>, *Fellow, IEEE*,  
and Jeffrey H. Reed<sup>1b</sup>, *Fellow, IEEE*

(Invited Paper)

**Abstract**—The spectrum access system (SAS) is being deployed as a key component of the emerging spectrum sharing paradigm to address the spectrum crunch facing the U.S. wireless industry. Ensuring security and privacy of this system against potential attacks is a task of paramount importance. In this article, we first introduce the SAS system, describing its three-tier access model, its functional architecture, and the spectrum management protocol. We then provide a comprehensive analysis of a variety of security and privacy attacks that an SAS is vulnerable to, and discuss their countermeasures. We identify key challenges, formalize threat models, and organize the discussion of SAS security into four categories: 1) SAS server security and privacy; 2) citizens broadband radio service device security; 3) security of environment sensing capability; and 4) communication protocol security. Finally, we suggest future research directions for spectrum management security.

**Index Terms**—Citizens broadband radio service (CBRS), security and privacy, spectrum access system (SAS), spectrum management.

## I. INTRODUCTION

WIRELESS technologies have been an important enabler for economic growth. As mobile devices become increasingly more powerful, they will be at the heart of a transformation in communication and computing applications, and there are numerous reports with projections that Internet traffic from mobile devices will become the primary form of communication traffic in the near future. As the total volume of mobile communications increases, there will be an inevitable crunch placed on wireless spectrum, which ultimately threatens the long-term viability of such economic growth [1]–[4].

Manuscript received December 14, 2020; revised January 25, 2021; accepted February 19, 2021. Date of publication March 8, 2021; date of current version April 7, 2021. This work was supported in part by the U.S. National Science Foundation under Grant 2037777 and Grant 1916902; in part by the Army Research Office under Grant W911NF-20-1-0141; in part by the Virginia Commonwealth Cyber Initiative (CCI); and a gift from InterDigital. (Corresponding author: Wenjing Lou.)

Shanghao Shi and Wenjing Lou are with the Department of Computer Science, Virginia Polytechnic Institute and State University, Blacksburg, VA 24060 USA (e-mail: shanghaos@vt.edu; wjlou@vt.edu).

Yang Xiao, Y. Thomas Hou, and Jeffrey H. Reed are with the Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA 24060 USA (e-mail: xiaoy@vt.edu; thou@vt.edu; reedjh@vt.edu).

Chonggang Wang and Xu Li are with the InterDigital Communications, Inc., Princeton, NJ, USA (e-mail: chonggang.wang@interdigital.com; xu.li@interdigital.com).

Digital Object Identifier 10.1109/IJOT.2021.3064583

In contrast to the exclusive use or licensed use of wireless spectrum, *spectrum sharing* has emerged as a key technology to address this spectrum shortage dilemma [5]–[10]. Spectrum sharing technology allows unlicensed or secondary users (SUs) to opportunistically access the licensed bands, as long as they do not cause harmful interference to licensed or primary users (PUs). Spectrum sharing fundamentally requires that SUs know what bands of spectrum are under-utilized and hence available for usage. This is usually done by spectrum sensing [11] or inquiry to a spectrum database [12].

Realizing spectrum sharing is a collaborative effort, involving not only scientific research, but also policy, regulation, and operations in key economic sectors. In the United States, the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) jointly manage the wireless spectrum. The NTIA is responsible for managing the federal use of spectrum, while the FCC is responsible for managing the nonfederal use of spectrum. Since the release of the President's Council of Advisors on Science and Technology (PCAST) report entitled "Realizing the full potential of government-held spectrum to spur economic growth" in July 2012 [1], the FCC, the NTIA, and other government agencies have worked together and have identified and repurposed a number of federally owned spectrum bands for shared use or unlicensed use to allow more efficient spectrum usage through dynamic spectrum sharing and to support the upcoming 5G operations [5], [6].

Of particular interest is the citizens broadband radio service (CBRS) band, i.e., the 3.55–3.7-GHz spectrum band, which was adopted for shared commercial use by the FCC in 2015 and has entered commercial deployment recently. The FCC also defined an innovative three-tiered sharing framework for the CBRS band that allows three tiers of user access [13], namely, incumbent users (tier-1), priority access license (PAL) users (tier-2), and general authorized access (GAA) users (tier-3). The highest priority incumbent users, in this case the U.S. Navy radar system and the fixed satellite services (FSSs), require strict interference protection in the CBRS band while users of lower tiers enjoy spectrum access opportunities. Among two lower tier users, PAL users obtain licenses through an auction and have higher priority than nonlicensed GAA users. This three-tiered access paradigm is enforced by dedicated spectrum management systems that coordinate spectrum allocation for all users of the CBRS band. These systems

rely on spectrum databases for making spectrum decision on a query basis and are generally referred to as the spectrum access system (SAS). In the United States, several companies have been approved by the FCC as SAS administrators and full-scale commercial deployment of SAS is under way for the CBRS band.

SAS is a critical component in the emerging spectrum sharing paradigm. SAS dynamically manages the spectrum access of a multitude of spectrum users and the success of SAS is the key to the agility and efficiency of dynamic spectrum sharing. Despite that the current implementation is focused on the CBRS band, the concept, the architecture and the functionalities of SAS are fundamental and could be instrumental for future spectrum management systems which are expected to accommodate a larger variety of spectrum users and more and wider spectrum bands. Therefore, in this article, we will use the CBRS SAS as a vehicle to demonstrate how a spectrum management system works. We provide an academic-style introduction of SAS, which we summarize from technical specifications and standards released by the Wireless Innovation Forum (WinnForum) and the CBRS Alliance, the industrial consortium, including SAS administrators (e.g., Google, CommScope, Federated Wireless, and Sony), mobile network operators (MNOs) (e.g., AT&T and Comcast), device manufacturers (e.g., Ericsson) and other stakeholders (e.g., Microsoft). We will then focus on the security and privacy aspects of SAS, highlighting important challenges facing a spectrum management system, reviewing the state-of-the-art defense mechanisms, and identifying new directions for future research.

We consider a wide range of attacks toward SAS alongside with discussions on state-of-the-art defense mechanisms. We examine the potential attacks on critical components of the SAS functional architecture, including SAS servers, CBRS devices (CBSDs), and environment sensing capability (ESC). We also address the security of communication protocols running among different entities within SAS. In the remaining part of the section we provide a glimpse of the corresponding attacks and defenses.

SAS server is at the heart of a spectrum management system. Every SAS server is operated by an SAS administrator. The current implementation of an SAS server maintains several databases that keep track of all spectrum users along with their current and planned activities in the local area. CBSDs send requests for spectrum use to an SAS server and obtain permissions before they transmit in the requested spectrum band(s). A critical concern in the database-driven SAS server is the security and privacy of spectrum database, which often store sensitive information about federal or military incumbent users. To pry into such sensitive information, an outsider attacker can launch inference attack [14] or reidentification attack [15] from outside entities; while a “honest but curious” insider attacker, which has legitimate access to the server and database, can retrieve sensitive information directly from the database [16], [17]. Privacy protection techniques, such as anonymization [15], [18], [19] and homomorphic encryption (HE) [16], [17], [20] are among potential defense schemes against those attacks. Another critical concern lies in the trusted execution of spectrum

assignment in SAS server. In the case SAS server is compromised or not trusted by the participating spectrum users, a hardware-assisted trusted execution environment (TEE) can be used to instantiate spectrum assignment functionalities and provide integrity proof via remote attestation. Alternatively, a decentralized blockchain-based spectrum management system can be a promising workaround, as it generates assignment decisions through consensus and does not rely on an individual SAS server nor assume trust among the participating entities [21], [22].

CBRS radio devices are wireless devices whose transmissions must comply with the dynamic spectrum sharing policies in the CBRS band. CBRS radio devices include end user devices (EUDs), such as mobile phones and laptops, and CBSDs, such as indoor small cell access points and outdoor base stations. A critical concern for CBRS radio devices is how to enforce their transmission compliance with the spectrum sharing rules. They need to follow the spectrum assignments made by SAS servers for RF operation in order to avoid harmful mutual interference. An important security measure is the accurate and timely detection of spectrum use violations, which captures digital forensic evidences that are reliable and un-deniable, so that the violators can be held accountable. There are a number of research efforts that aim to address policy enforcement [23], radio device operational integrity verification [24], [25], spectrum anomaly detection [26]–[28], as well as jamming attacks [29].

The ESC is an important subsystem in an SAS system. The ESC is composed of a network of dedicated sensors deployed in the protected areas that cooperatively perform spectrum sensing to detect moving incumbents. A big threat to ESC security is the falsified sensing reports that may lead to erroneous decisions made at the server, given it is possible that Byzantine sensors may exist in the ESC sensor network [30]. Prior wisdom has demonstrated various techniques that distinguish false sensing reports from genuine ones [31]–[37]. Recent development in machine learning technologies has enabled more effective attacks to the ESC system. Carefully crafted adversarial examples (AE) could deceive the decision system in a more stealthy way [38], renewing the concern on robustness of the decision-making process.

Previous research has tackled one or more aspects of the security and privacy issues of the spectrum sharing systems. Attacks and defense mechanisms in cooperative spectrum sensing are surveyed in [30] and [39]–[42]. Security threats and enforcement methods in both spectrum sensing-driven and database-driven cognitive radio networks (CRNs) are discussed in [23]. The operational security requirements for incumbents users within the CBRS band are described in [43]. The location privacy issues in CRNs are introduced in [44]. However, little attention was paid to the SAS systems that are currently being deployed and will continue to evolve as a key component for dynamic spectrum management. Although there are some overlaps with respect to techniques surveyed, our article is the first comprehensive review focusing on the security and privacy of SAS and more generally the spectrum management system.

In summary, we make the following contributions in this article.

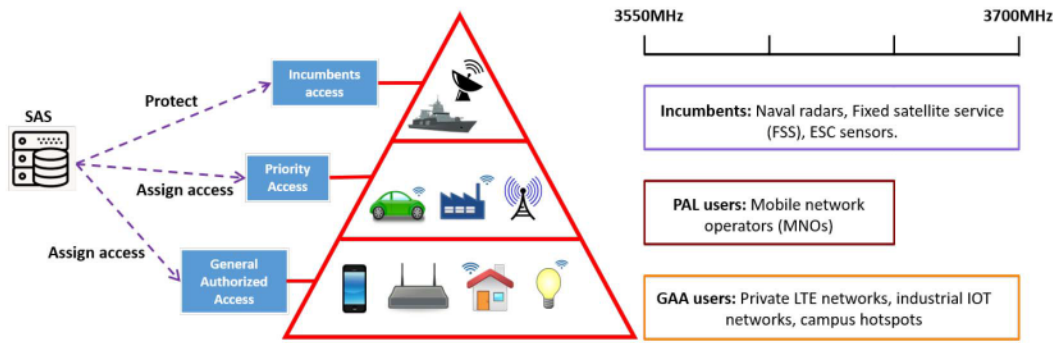


Fig. 1. Three-tier SAS for the CBRS band.

- 1) We elaborate on the technical background of the current SAS paradigm, including its service model, system architecture, and functionalities.
- 2) We analyze security threats toward the critical components of the SAS paradigm, namely, the SAS servers, CBSDs, ESC and communication protocols, then identify and review the potential defense approaches, respectively.
- 3) We identify several key research challenges and new research directions that may inspire further research in this area.

The remainder of this article is organized as follows. In Section II, we introduce the basic structure and core functionalities of SAS. From Section III to Section VI, we review and discuss SAS server security, CBSD security, ESC security, and communication protocol security, respectively. After that, we introduce additional research challenges and new research directions in Section VII, followed by conclusion in Section VIII. The most frequently used acronyms are listed in Table I.

## II. SAS OVERVIEW

In this section, we describe how the SAS works, laying the foundation for later security discussions. We first introduce the three-tiered spectrum access model adopted by the FCC and services provided to each tier and then present the SAS functional architecture and explain how subscribed entities function in this architecture. We also elaborate on the spectrum management protocol, demonstrating how it coordinates practical communications and spectrum assignment process between CBSDs and SAS servers. Finally, we discuss the security requirements of SAS.

### A. Three-Tiered Hierarchical Spectrum Access

Following the standards specified by the Wireless Innovation Forum (WInnForum), SAS is envisioned to provide a three-tier hierarchical spectrum access service for all users in the CBRS band. The WInnForum is a nonprofit organization that publishes technical specifications for all commercial operations within the CBRS band. These specifications serve as the baseline standards for this spectrum sharing system. The WInnForum does not involve in any commercial implementation of SAS. The CBRS Alliance is an industry consortium consisting of more than a hundred wireless and telecommunication organizations who are interested in rolling out CBRS

TABLE I  
TABLE OF ACRONYMS

| Acronym   | Full Name                                                  |
|-----------|------------------------------------------------------------|
| CBRS      | Citizens Broadband Radio Service                           |
| CBSD      | Citizens Broadband Radio Service Devices                   |
| CRN       | Cognitive Radio Network                                    |
| DP        | Domain Proxy                                               |
| EIRP      | Effective Isotropic Radiated Power                         |
| ESC       | Environment Sensing Capability                             |
| EUD       | End User Device                                            |
| FCC       | Federal Communications Commission                          |
| GAA       | General Authorized Access                                  |
| IDS       | Intrusion Detection System                                 |
| NTIA      | National Telecommunications and Information Administration |
| PAL       | Priority Access License                                    |
| SAS       | Spectrum Access System                                     |
| TEE       | Trusted Execution Environment                              |
| WInnForum | Wireless Innovation Forum                                  |

commercial services. The member companies in the Alliance deploy their SAS systems in compliance with the released technical specifications and standards, and provide the three-tier hierarchical spectrum access service. Fig. 1 illustrates the three tiers of spectrum access privileges in the CBRS band. The incumbents (i.e., tier 1) include naval radars, FSSs, dedicated ESC sensors, etc. They are the current users of the CBRS band and mostly locate in coastal area as part of the federal infrastructures or military equipment. They do not participate in commercial operations in this promulgated CBRS band and only require for strict interference protection from lower tier civilian users when they are using the spectrum. Incumbents users have no usage restriction and can get access to spectrum band(s) any time they want.

The PAL users (i.e., tier 2) obtain transmission licenses through competitive bidding on a county-by-county basis. When a PAL user wins a license for a specific location, it has a higher priority to use the licensed spectrum band(s) than the GAA users, when incumbents are not present or the PAL user can limit the interference to the incumbent below a certain level. In practical commercial bidding, the CBRS band is divided into 15 channels with each covering a 10 MHz spectrum chunk; and according to the WInnForum's working documents, a PAL user could use up to 7 out of the first 10 channels in a single geolocation [43]. This restriction leaves at least 80 MHz spectrum resource available for GAA users. Typical PAL users include MNOs and industrial companies.

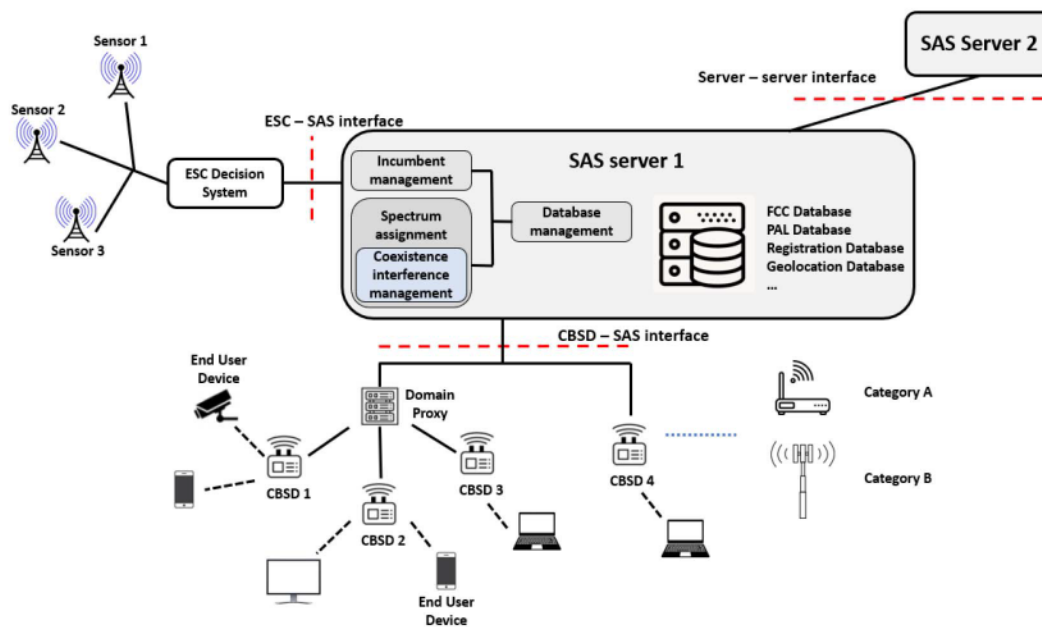


Fig. 2. SAS functional architecture.

The GAA tier (i.e., tier 3) is licensed-by-rule to permit open, flexible access to the CBRS band. GAA users have the lowest priority and can only get access to spectrum channels when they do not cause harmful interference to both incumbents and PAL users. GAA users are allowed to access all 15 channels in the whole CBRS band. PAL and GAA tiers together provide flexible access opportunities for a broad range of daily spectrum users and both could be used to support diverse network applications, such as private LTE networks, IoT networks, campus hotspots, etc.

In summary, SAS provides a hierarchical spectrum access service for multiple users in the CBRS band. This spectrum management service allows harmonic coexistence of three tiers of users and improves the spectrum utilization and efficiency of the CBRS band.

### B. SAS Functional Architecture

Fig. 2 shows the SAS functional architecture. There are four main entities in an SAS system, namely, CBSDs, CBSD domain proxies (DPs), ESC, and SAS servers. In a nutshell, SAS can be seen as a “client-server” system where CBSDs and DPs are “clients” while SAS servers, with support from the ESC, act as an abstract “server” that provides spectrum allocation service to the requesting clients.

CBSDs are PAL or GAA tiers of user devices. CBSDs function as the clients of SAS by sending spectrum requests to an SAS server and can transmit only if the SAS server replies with an spectrum use authorization. Note that CBSDs are usually not EUDs (e.g., mobile phones and laptops). The concept of CBSD is the same as base station in 4G-LTE network and wireless access point in WiFi technology. According to the WInnForum’s working documents [43], CBSDs are categorized into two types: category-A and category-B. Category-A CBSDs are deployed indoor with a maximum EIRP of 30 dBm while category-B CBSDs are deployed outdoor with

a maximum EIRP of 47 dBm, where EIRP stands for effective isotropic radiated power.

DP is an intermediary entity engaging in communications with the SAS servers on behalf of multiple individual CBSDs or networks of CBSDs, when requesting spectrum allocation service. Due to its similar interaction routine with SAS servers to that of normal CBSDs, DP can be perceived as an extended CBSD concept.

ESC is a network of dedicated sensors deployed primarily along the Pacific, Atlantic, and Gulf coasts to detect moving incumbents, such as naval ships in the CBRS band. According to the FCC’s rules, ESC is deployed by nongovernment entities designated by FCC [43]. ESC sensors inform SAS servers about the appearance of incumbents in one geolocation and SAS servers will correspondingly calculate and activate protection zones and exclusive zones to protect incumbents from aggregate harmful interference in that area. Here, the protection zone and the exclusive zone are two *ex ante* (preventive) enforcement methods for sound SAS operation [45]. The protection zone refers to an area in which servers limit CBSDs’ operation to reduce interference level with respect to incumbents’ specific requirements; while the exclusive zone refers to an area where only authorized entities are allowed to operate. According to the WInnForum’s specification [43], mutual interference is calculated based on the Longley-Rice propagation model.

SAS servers are the core spectrum management entity in the CBRS band and provide multiple high-level functions for the three-tiered spectrum access service model. We summarize the high-level functions of the SAS servers as follows.

- 1) *Incumbent Management*: An SAS server must obtain incumbents’ spectrum activity information in order to control the interference to the incumbents effectively. An SAS server get incumbents’ operating information, such as location, time, transmission frequency band(s),

and power level, through either inquiring a FCC database or performing incumbent detection. The FCC database contains information about incumbent activities which are mostly static in location and time. It is accessible through SAS server's database management function. More dynamic incumbent detection tasks are accomplished by the ESC. The incumbent management function at an SAS server is responsible for gathering that information and providing it as input to other functions, such as the spectrum assignment function which further enforces interference protection by activating exclusive zones and protection zones in a certain area.

- 2) *Database Management*: Each SAS server manages several databases, such as the FCC database, PAL information database, user registration information database and geolocation information database. SAS server makes inquiries to these databases to get information for other spectrum management operations. Database management is a fundamental component that provides services to other high-level functions.
- 3) *Spectrum Assignment*: An SAS server is responsible for assigning spectrum resources to PAL users or GAA users via the spectrum assignment function. This function can be viewed as a two-step request-and-response process. A CBSD or a DP, be it PAL user or GAA user, starts the process by sending a spectrum request message to the SAS server. A spectrum request message can be either a spectrum inquiry or a spectrum grant message. Upon receiving the request message, the SAS server will follow a spectrum management protocol to generate a response and send the response, which is either an inquiry response or a spectrum allocation decision, back to the requesting CBSD or DP. The details of the spectrum management protocol will be elaborated in Section II-C.
- 4) *Coexistence Interference Management*: Coexistence interference management is a core function in spectrum assignment. SAS servers implement this function to ensure the safe and nonconflicting operation of all subscribed users. This function takes as input the new spectrum requests, priority levels, the existing spectrum allocations, incumbents' information, interference thresholds, etc., and outputs a spectrum assignment schedule for each request in a local area. This schedule shall meet all interference thresholds and also maximize spectrum band utilization rate.

### C. Spectrum Management Protocol

Spectrum management protocol refers to the communication protocols running among SAS entities that collectively accomplish the spectrum management tasks. The communications between the ESC and SAS server and between SAS servers are mainly for information sharing. Important spectrum assignment functions are carried out between CBSDs and SAS servers. In this section we focus on the interactive protocol between CBSDs and SAS servers, which is referred to as SAS-CBSD Interface in the WInnForum specification [46].

This protocol defines how individual CBSDs interact with SAS servers to inquire spectrum availability or acquire transmission grants and authorizations. According to [46], SAS-CBSD Interface contains seven procedures as follows.

- 1) *Prerequisite Procedures*: Before the commencement of SAS-CBSD communication, four prerequisite procedures need to take place in advance, including user registration, PAL right management, installation parameter uploading and communication security setup. User registration requires a user to register its basic information, such as legal identity and mailing address with an SAS server. The SAS server will reply with a unique UR-ID for each registered user. PAL right management helps users to indicate their PAL priority level. Installation parameter uploading procedure requires users to pass the installation parameters of their CBSDs to the servers. Finally, users and SAS servers negotiate the security parameters needed for building a secure communication channel, including those of a cipher suite.
- 2) *SAS Discovery*: SAS administrators, such as Google and CommScope need to publish a URL for CBSD users and DPs to connect to their proprietary SAS servers. The publication process is subject to the SAS administrator's discretion and out of the scope of the spectrum management protocol.
- 3) *CBSD Registration*: CBSD registration is a procedure for a CBSD to register itself with the SAS server. After discovering an SAS server's URL, a CBSD first connects to the server and performs mutual authentication with the server. If successful, the CBSD will register itself in the SAS server's user registration database. The registration information includes the CBSD's category, location information, device specific parameters, etc. For DPs, they will aggregate all the registration requests from subscribed CBSDs and then interact with SAS servers to have every subscribed CBSDs registered.
- 4) *CBSD Spectrum Inquiry*: The CBSD spectrum Inquiry procedure is to allow a CBSD to inquire the spectrum usage information of interested frequency band(s). In this procedure, a CBSD first sends an inquiry request that includes its interested frequency band(s) to the SAS server. The SAS server checks the availability of the requested frequency band(s) and sends back the inquiry response. The SAS server does not reserve any spectrum resource for CBSDs or DPs.
- 5) *CBSD Grant Procedure*: The CBSD Grant procedure is used by CBSDs to obtain transmission grant from the server. In this procedure, the CBSD first initiates a grant request to the server with operational parameters, including the maximum EIRP and desired frequency band(s). The SAS server executes the coexistence interference management function and determines whether this frequency range is available for the CBSD. If so, SAS server grants this request by sending back a response with a grant-ID, a grant expiration time, and a heartbeat interval. If SAS server determines that the desired frequency band(s) is not available, the grant request will be denied and SAS server may include a

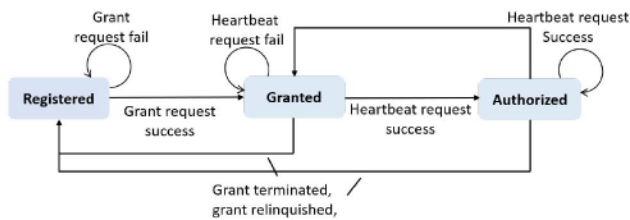


Fig. 3. Spectrum management protocol state diagram.

recommendation about potential operation parameters in the response. Fig. 3 illustrates the state transitions of CBSD grant procedure. To begin with, a CBSD is in the registered state. If a grant request is approved, the CBSD will transit to the granted state; if denied, it will remain in the registered state. Note that the CBSD cannot perform transmission when in the granted state. Only in the authorized state can a CBSD use the granted frequency band(s).

- 6) *CBSD Heartbeat*: CBSD Heartbeat procedure is used by CBSDs to obtain the transmission authorizations to start or to continue to use the granted spectrum band(s). After reaching the granted state, a CBSD sends the SAS server a heartbeat request and the server responds with the authorization for the CBSD to start using the granted spectrum band(s). To maintain continuous use of the spectrum band(s), a CBSD needs to periodically send heartbeat requests to the SAS server. The SAS server responds to the CBSD with heartbeat response messages on whether they can begin or continue to use the granted spectrum band(s), according to the real-time result of coexistence interference management function. Essentially, this procedure allows an SAS server to authorize, suspend, or terminate existing grants. To check the liveness of a CBSD, the SAS server sets a timer for the CBSD Heartbeat procedure and the CBSD needs to start the Heartbeat procedure at any time prior to the expiration of this timer. If the CBSD fails to do so, its transmission grant will be suspended or revoked.
- 7) *CBSD Grant Relinquishment*: CBSD Grant Relinquishment procedure is used by CBSDs to relinquish transmission grants. SAS servers will revoke the grants when receiving relinquish requests.

#### D. Threats and Security Requirements

With the fledgling of the CBRs ecosystem and the increasing number of spectrum users, a well-defined security framework is needed to facilitate the discussion of security challenges and solutions in SAS-based spectrum management. We define the following types of attacks based on information available to attackers, attacker's capability, and attacker's behavior.

- 1) *Insider and Outsider Attacks*: We distinguish between insider attacks and outsider attacks based on the access right and available information to the attacker. Insider attacks are launched by insiders who are authorized constituents of the victim system. While outsider attacks are launched by outsiders who try to gain protected

information without the privilege to access internal information of the victim system.

- 2) *Curious-but-Honest and Malicious Attacks*: We distinguish between curious-but-honest attacks and malicious attacks based on the attackers' behaviors. Curious-but-honest attackers are legitimate components in a system who follow the prescribed procedures honestly but attempt to learn all possible information. Malicious attackers violate the operation requirements in order to jeopardize the normal operation of the victim system.
- 3) *Individual and Colluding Attacks*: Individual attack is carried out by an individual attacker, while colluding attacks refer to attacks that need multiple attackers to collaborate.
- 4) *Byzantine Failures and Attacks*: Byzantine failure is a condition in distributed computing systems, where nodes may arbitrarily deviate from their normal routine and send contradicting or false information to peer nodes. Byzantine failure can be caused by either component malfunctioning or adversarial influence. Corresponding to the second case, Byzantine attack refers to the scenario where the attackers, either act individually or in collusion, maliciously control a number of nodes which are configured to behave arbitrarily or maliciously (in a stealthy manner) in order to disrupt the normal operation of the distributed system.

We identify the following security requirements for the secure operation of SAS.

- 1) *Data Confidentiality*: Sensitive data stored on SAS servers or exchanged between SAS components across the network are protected from unauthorized access.
- 2) *Information Integrity*: Integrity protection mechanisms are needed to maintain the correctness, consistency, and completeness of databases and other information on SAS servers and messages exchanged between SAS components. Information should be protected from unauthorized alteration, insertion, and deletion.
- 3) *Service Availability*: SAS should ensure timely and uninterrupted services to authorized users.
- 4) *Mutual Authentication*: Rigorous authentication systems/protocols are needed in SAS to enable different types of entities to mutually authenticate each other.
- 5) *User Data Privacy*: SAS should protect unauthorized disclosure or misuse of spectrum users' data that could be used to derive sensitive user information that may or may not be relevant to spectrum access.
- 6) *Information Freshness*: SAS should keep all information updated in the system in time to realize near real-time control and accurate decision making.
- 7) *Device Compliance and Policy Enforcement*: SAS should ensure the compliance of access rules and radio configurations in all CBSDs and be able to enforce the prescribed access policies for different tiers of spectrum users.

In the next four sections of the article, we will examine critical security and privacy attacks targeted at various SAS components, from SAS servers, CBSDs, ESC system, and communication protocols. We will review potential

countermeasures, examining how those mechanisms could help to address these security and privacy needs of SAS.

### III. SAS SERVER SECURITY

SAS servers are the core of a spectrum management system that fulfill the critical role of spectrum assigner and coordinator. Different entities in the SAS ecosystem interact with SAS servers to accomplish spectrum management functions from incumbent management to spectrum allocation. SAS servers are the most densely connected component in the functional architecture of a spectrum management system, and therefore a high risk target to various attacks. In this section, we focus on the security and privacy of SAS server operation. Following the attack taxonomy in Section II-D, we identify three types of security attacks on SAS server and review the corresponding solutions. We first consider outsider attacks which aim at inferring sensitive information of SAS server operation through either inference attack with database queries (Section III-A) or linkage attack on public disclosed data (Section III-B). Then we move to insider attacks wherein SAS servers themselves are not fully trusted. Honest-but-curious servers that extract sensitive user device information are considered (Section III-C). Finally, we consider the worst case scenario—Byzantine attacker, who can maliciously manipulate the SAS servers or administrators in order to disrupt the normal functioning of the SAS ecosystem. In response, we review solutions based on the TEE technology (Section III-D) and the blockchain-based decentralized SAS paradigm (Section III-E).

#### A. Inference Attack With Database Queries

With the development of sophisticated data analytic tools, an outsider attacker has been shown to have the capability of inferring sensitive information from a database through legitimate inquiries to the servers [47]. One prominent example of inference attacks on SAS databases is the privacy attack on incumbent user locations. The attacker leverages the seemingly innocuous spectrum inquiry procedure to infer the precise locations of victim incumbents.

An inference attack targeting the location of incumbent users in a protection zone is illustrated in [14] and [48]. This attack assumes that the attacker possesses the capability of sending a large amount of spectrum inquiry requests with the target incumbents' frequency band(s) to SAS servers from different locations. The response from the SAS servers will indicate whether the specified band(s) is available at specified locations. This information could be used to infer whether the specified locations are within the incumbent's protection zone or not. By continuing the queries with carefully selected new locations, the attacker cumulatively gains more information about the location of incumbents' protection zone and could effectively narrow down the incumbents' possible location to several small areas. The article shows that with a limited number of inquiries, the attacker could derive the precise location of a target incumbent, breaching the incumbent user's location privacy. Similar attacks targeted at SUs' location privacy have been reported in the traditional TV bands [49], where

the attacker can derive an SU's location through the analysis of spectrum inquiries and responses.

In order to defend such kind of location privacy attacks, several defense mechanisms have been proposed. Vaka *et al.* [14] proposed several heuristic methods, including enlarging the protection zone, controlling working patterns of incumbents, and randomly inhibiting transmissions. Clark and Psounis [50] addressed the spectrum information database privacy problem using two obfuscation methods—one by inserting false entries to the database and the other by parameters randomization. Zhang *et al.* [51] applies  $k$ -anonymity-based obfuscation to spectrum inquiry responses in order to preserve PUs' location privacy. While [52] proposes an  $\epsilon$ -differential privacy mechanism on urban sensing data to avoid location inference.

It is worth noting that such inference attacks generally get closer to the ground truth (or yield a higher success probability) as the number of inquiries increases. Therefore, in practice it is recommended that servers limit the number of inquiries a user can send in a certain time interval. Users who demonstrate suspicious behaviors by making excessive inquiries shall be suspended or banned from making spectrum inquiries.

#### B. Inference Attack on Public Disclosed Data

Besides spectrum inquiries, the mandatory information disclosure of SAS servers may also pose a privacy threat. Per WInnForum's working document on the requirements for commercial operation of the CBRS band, the designated SAS administrators shall provide means to make nonfederal, non-proprietary information available to the public in a reasonably accessible fashion [43]. This regulation places the SAS administrators in an auditable position to ensure their conformation to public interests. However, this information disclosure mechanism may also be taken advantage by the attacker to extract private and sensitive information of spectrum users. For example, in [53], a class of statistical deanonymization attacks against high-dimensional microdata, such as individual preferences, recommendations and transaction records is proposed. Pseudonymous data can be easily reidentified and expose private information with this introduced attacks. The results in this article shows that an adversary who has only a little knowledge about an individual subscriber can easily identify this subscriber's record in real-life Netflix data set.

To reduce the risk of linkage attack, SAS administrators should be cautious on the type of data to be disclosed to the public. If an SAS administrator must disclose certain data for regulation compliance, obfuscation methods, such as  $k$ -anonymity [15],  $t$ -closeness [18], and  $l$ -diversity [19] can be enforced to perturb the exact value of data entries before disclosure.

#### C. Privacy Leakage Due to Honest-but-Curious SAS Server

SAS servers are typically managed by third party companies, such as Google, CommScope, Federal Wireless, and Sony. User data privacy is a common concern when information is managed by those companies. There are numerous cases that tech companies monetize on user data without proper user consent. At the same time, cyberattack is another

cause of private data leakage. In both cases, the SAS servers may not be as trustworthy as we assumed in the previous sections. A dishonest employee of the SAS administrator, or a cyberattacker who managed to break into the SAS server, may quietly extract users' sensitive information without disrupting spectrum sharing service.

In this section, we discuss challenges related to protecting user privacy against semihonest SAS servers. Semihonest means that the servers function normally but are curious about inferring users' private information, i.e., they are honest-but-curious. The challenge of providing such protection lies in maintaining the normal utility of the server function while preserving the privacy of sensitive data involved in the function computation. If the sensitive information is available to the server all in plaintext format, server utility will not be affected but extracting user private information become extremely easy for such dishonest servers. On the other hand, encrypted data will protect user data privacy, but how to make use of the data in its encrypted form to fulfill the SAS utility, i.e., spectrum allocation function, is a big challenge the SAS servers have to solve.

Protection of user data privacy against semihonest servers has been addressed extensively in the context of information security and privacy in cloud computing [54]–[58]. There are generally two main directions to address this problem. The first one is software-only solutions in which cryptographic tools, such as secure multiparty computation and HE are employed to ensure privacy-preserving spectrum negotiation at the server. Examples of this approach include [16], [17], [20], where the authors build up spectrum management functions in ciphertext domain with the help of various HE primitives, such as Paillier cryptography system to keep server agnostic about users' information. However, the downside of this approach is the computation complexity when implementing all operations over ciphertext. For example, HE-based spectrum management scheme in [16], denoted  $p^2$ -SAS, requires more than fifty times longer spectrum operations processing time and a hundred times larger communication messages size than traditional SAS at server side, making it hardly acceptable for practical deployment. A recent work to address HE-based scheme's large communication and computation overhead is to combine differential privacy technique with HE-based scheme [20]. The scheme proposed in [20], denoted *PeDSS*, requires only incumbents to encrypt their message with HE primitives. The SUs communicate with servers in plaintext messages with uncertainty noise added to location attribute of messages to preserve location privacy. In this way, *PeDSS* partially avoids the unacceptable complexity introduced by fully HE computation. This work successfully reduces the level of the computation and communication overhead per message to millisecond and kilo bytes, making it more suitable for practical deployment.

The other direction to ensure privacy-preserving operations at a semitrusted server is to leverage the advancement in hardware-assisted TEE, such as Intel software guard extensions (SGX) [59]. The idea of using the hardware-assisted solution is to process the sensitive information in a secure container known as enclave in the SGX technology. Sensitive information is stored on the server in encrypted form and will

only be decrypted and used for function computation inside the protected enclave. Examples of this approach include [25], [60]–[62]. We will discuss more on TEE-based secure computation in Section III-D, as TEE technology not only ensures data privacy but also guarantees program integrity when executing in an untrusted server. Comparing to crypto-based privacy-preserving function computation techniques, such as HE, the TEE-based solution is much more flexible. It can be applied to arbitrary computation function although there is a size limit, while crypto-based privacy-preserving schemes have to be customized for each type of function for efficiency purpose as the complexity of a general fully HE scheme is forbiddingly high to be useful in any practical system. The TEE-based solution could also achieve more predictable performance in terms of execution time, very often comparable to plaintext operations [60], [63].

#### D. Hardware-Assisted Security Enhancement Against Compromised SAS Server

In the current SAS framework for CBRS, a CBSD interacts with one SAS server for spectrum inquiry and assignment. A compromised SAS server is considered either under malicious influence or arbitrarily deviating from normal functioning (i.e., Byzantine). For instance, an malicious SAS server may intentionally issue conflicting spectrum grants to different CBSDs; a Byzantine SAS server may arbitrarily suspend a CBSD's grant during the Heartbeat procedure. Such server behaviors would be devastating to the operation of CBSDs that subscribe to its spectrum service.

In the computer architecture community, there have been continuing research endeavors on realizing trusted computing in an untrusted or even adversarial hosting system. To this regard, the hardware-assisted TEE technology stands out as a promising solution. TEE technology limits the trusted computing base (TCB) to hardware only; secure containers containing sensitive routines can be instantiated in isolated, protected memory regions. Intel SGX [59] and ARM TrustZone [64] are well-known TEE solutions in the market. Here, we focus on SGX, since TrustZone is primarily used in embedded systems. Among the key functionalities enabled by TEE is *remote attestation*, the process of making a claim about the properties of a target by having a prover supply evidence to a verifier remotely. It is originally used to protect software execution by verifying the software integrity or detecting abnormal software behaviors [65]–[67].

Back to our SAS case, a TEE enclave containing the FCC-ratified spectrum scheduling routine can be bootstrapped in each SAS server. The integrity and authenticity of the enclave routine as well as the SGX-enabled hardware can be proved via the remote attestation process, to any spectrum user (i.e., attester) who knows the enclave routine's checksum and has access to the Intel Attestation Service (IAS). In a likely deployment case, every spectrum allocation grant issued by an SAS server shall be accompanied by an attestation report, including measurement on the enclave routine and a SGX hardware authenticity report returned from IAS. Once the attestation report passes, spectrum users can entrust the SAS server's

enclave routine for calculating the grant assignment, regardless of trustworthiness of the server's host platform.

Promising as it seems, TEE technology faces two major challenges before been considered for large-scale SAS deployment. The first challenge is the lack of diversity in TEE hardware vendor. For SGX, which is proprietary to Intel, the validity of remote attestation depends on the integrity and availability of IAS, which poses risks of single point failure. Second, the TEE technology itself is hardly vulnerability free from system security perspective. Several recent high-profile attacks have demonstrated that the SGX implementation is susceptible to side channel attacks which exploit the speculative execution feature of the hosting processor [68], [69].

### E. Blockchain-Based Decentralized SAS

Another direction of providing resilient, fault-tolerant spectrum service is leveraging service provider redundancy. We identify two different models of realizing redundancy in a multiserver system: 1) *distributed* and 2) *decentralized*. Though conceptually similar at a first glance, the two models have major differences in system scale and autonomy of participants.

**Server Replication:** In classical distributed systems, server replication has been widely used for providing client computing services in the presence of server failures. For the worst case scenario—Byzantine servers, state machine replication (SMR) is heralded as the *de facto* solution for achieving Byzantine fault tolerance (BFT) [70]. Classical BFT-SMR schemes, such as PBFT [71] mandates that a server consortium, consisting of one leader and replicas, answers to user requests in a collective manner. The leader receives requests from users and starts a SMR scheme which ensures that all nonfaulty servers in the consortium execute the requests in the correct order and output the same result, under the security assumption that fewer than one third of servers are Byzantine. Setting in the spectrum allocation scenario, a consortium of SAS servers, under the management of one SAS administrator, may operate a BFT-SMR scheme for the execution of spectrum requests (i.e., assignment decision). Spectrum users can regard the decision of the server consortium as authoritative as long as the SAS administrator is trusted.

However, the BFT-SMR scheme only works on a small scale (i.e., under one administrator) and requires intensive interserver communication as well as centralized synchronization service. When one SAS administrator is not trusted for managing its proprietary server consortium, CBSD users need to subscribe to spectrum services from multiple SAS administrators. A challenge arises in that CBSDs need to decide which SAS administrator/server's assignment is fair and policy compliant. On the other hand, WINnForum specifications [43], [72] dictate that any individual SAS server, under a certain SAS administrator, should communicate and synchronize service information with other SAS servers regardless of their SAS administrators. Though this procedure guarantees consistent spectrum management service nationwide, it allows malicious SAS administrators/servers to disseminate false information that jeopardizes the entire ecosystem.

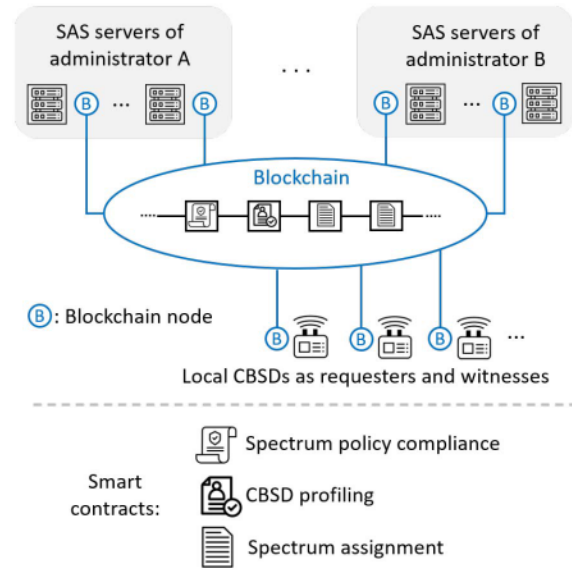


Fig. 4. Conceptual blockchain-based SAS. Three core SAS functions are encoded in the form of smart contract.

In face of these operational and informational challenges, a decentralized, collectively governed SAS solution becomes desirable.

**Blockchain-Based SAS:** Blockchain emerged as a secure-by-design technology for enabling fully decentralized payment networks. With the cryptography-hardened transaction model and consensus-based validation mechanism, blockchain enables trusted transaction processing and ledger keeping among mutually distrustful participants, given a certain portion of them may behave maliciously (i.e., Byzantine) [70]. The decentralized and zero-trust nature, consensus-based security, and irreversible ledger keeping make blockchain system an ideal candidate for decentralized SAS.

The FCC has indicated its interest in employing blockchain technology for future spectrum sharing systems [73]. Several papers in the recent literature also alluded or explored the use of blockchain for spectrum management systems. Readers are referred to [22], [74] for general discussions on application scenarios, economic models, and policy compliance of blockchain-based spectrum sharing systems. In [75], a token-based spectrum sharing concept is proposed in that a blockchain smart contract system is used as a trusted third-party service. In [21], a hierarchical blockchain system called TrustSAS is proposed to enable efficient and privacy-preserving spectrum sharing among SUs. Local blockchain networks are established among SUs for spectrum query aggregation and response distribution while a global blockchain is used for general policy compliance and records keeping. A blockchain-enhanced spectrum sharing system is proposed for the CBRS band [76]. The PAL users are responsible for establishing local blockchain networks which help a central regulator reduce its workload in spectrum sharing coordination. However, these proposals all assume absolute trust on individual SAS servers and do not consider the consistency of inter-SAS communication.

To support spectrum sharing in the CBRS ecosystem without assuming trust on individual SAS administrators/servers or

their intercommunication, we provide a conceptual blockchain solution, as is illustrated in Fig. 4. A blockchain network can be established in a local area for providing inter-SAS communication and consensus-based spectrum assignment and records keeping. A major divergence from the traditional server replication solutions is that the blockchain network contains SAS servers across SAS administrations as the consensus committee and sanctioned local CBSDs as witnesses for validation purposes; the leader-initiated SMR procedure is thus replaced by decentralized consensus for ensuring consistent network operation. Both SAS-to-CBSD interaction and SAS-to-SAS communication happen in the form of blockchain transactions which are subject to consensus-based validation and finalization. Smart contract, an important functionality enabled by blockchain, can be used for encoding spectrum management policies/routines and enforcement. Specifically, three types of contracts can be instantiated for different SAS functionalities: 1) spectrum policy compliance; 2) CBSD profiling (including registration of RF context); and 3) spectrum assignment. When a CBSD invokes a spectrum assignment contract, the execution of the assignment will be fulfilled by all SAS servers through consensus. The assignment records are attached to the contract execution history and stay in the blockchain ledger in an irreversible manner.

Despite its appealing features, blockchain-based SAS faces several challenges primarily in processing cost (due to replication) and scalability. Large-scale permissionless blockchain networks overlaying on the Internet and running a Nakamoto-style consensus protocol, such as Bitcoin [77] and Ethereum [78], tend to have low transaction throughput—typically capped 25 transactions per second (TPS)—and large transaction confirmation delays [79]. This is far from satisfactory for time-sensitive spectrum management. BFT-style consensus protocols, on the other hand, yield much higher throughput (hundreds to thousands TPS) but constrain the network size to subhundred [70]. Scaling up blockchain system in both transaction capacity and network size is still an ongoing effort in the blockchain research community [79]–[81]. We identify a solution with the help of the aforementioned TEE technology. It is worth noting that blockchain and TEE are complementary technologies in providing trusted execution for spectrum requests. Recent work in the blockchain community has demonstrated that functions of a smart contract can be offloaded to a TEE enclave for efficient and confidential execution [82]–[86]. In the blockchain-based SAS, harmonizing of TEE and smart contract stands a promising method to reduce on-chain execution cost and scale up overall capacity of the system in processing spectrum requests.

Readers are referred to Section VII-E for discussion on the enforcement challenges of blockchain-based SAS and Section VII-F for vision on blockchain-based secondary spectrum markets.

#### IV. CBSD SECURITY

CBRS radio devices include both CBSDs and EUDs. In this section we focus on the security threats on both the hardware and operation of CBRS radio devices. We first introduce physical-layer attack and defense under the premise

that attackers' capability is limited to leveraging outsider wireless devices to jeopardize victim CBRS radio devices (Section IV-A). Then we further consider the attackers' capability of being able to seize the control of victim CBRS radio devices to violate their compliance to SAS servers' spectrum management instructions, through leveraging either software or hardware vulnerabilities. An attacker can both jeopardize innocuous spectrum sharing services and endanger SAS servers if he gains control of CBRS radio devices to perform abnormal behaviors. How to reliably verify the operation integrity of CBRS radio devices becomes an urgent security requirement for SAS. In response to this concern, we review promising solutions in CBRS radio device integrity verification (Section IV-B) and spectrum sensing-based anomaly detection (Section IV-C) and discuss potential challenges.

##### A. Jamming and Defense

Jamming is one of the major security threats to modern wireless communication and sensing systems. Jamming attacks can disturb communication between different entities and cause throughput degradation, protocol failure, and even loss of connectivity. In spectrum sharing systems, the spectrum sensing capability and highly programmable cognitive radio devices make jamming attacks, particularly reactive jamming, much easier to launch. A reactive jammer will continuously sense the activities of victim devices and only launch the attack when he detects the victim's activities in the target channel. This property makes reactive jamming a stealthy and energy-efficient attack and difficult to detect because of the overlap of user and attackers' activities [87], [88]. The feasibility and effectiveness of practical reactive jamming schemes have been discussed in [29] and [89].

CBRS radio devices also face the threat of reactive jamming. Fortunately, defense techniques proposed in previous works provide mitigation to this attack. In [29] and [90], a jamming-resilient OFDM communication scheme using MIMO interference cancelation (IC) technology is introduced. The defense mechanism leverages signal enhancing rotation and message feedback techniques to enable effective cancelation of jamming signals. The mechanism is designed to safeguard both forwarding frame transmissions and feedback messages. In [91], a jammer detection method leveraging channel diversity is proposed for database-driven spectrum sharing system. This method enables database servers to infer whether a SU (i.e., CBSD in SAS) is a jammer. After a jammer is detected, the administration can impose a three-step *ex post* (punitive) enforcement framework to enact punishments [23]. The three steps include identification, localization, and punishment of noncompliant transmitters. The identification step requires the administration to clearly identify the attackers. The localization step requires the administration to determine where the attacker is. Finally, the punishment step leverages two punitive measures—rejecting all access to spectrum and imposing economic penalty [92], [93].

##### B. EUD and CBSD Operational Integrity

The dynamic spectrum sharing paradigm of SAS allows radio devices, namely, EUDs and CBSDs, to operate in shared

frequency band(s) using domain-specific wireless access technologies, such as Wi-Fi and LTE. The increased flexibility in both hardware and software is the foundation for efficient spectrum utilization. In the meantime, successful spectrum sharing relies on the cooperation from all participants in the RF domain. For instance, an SAS server's spectrum assignment service depends on CBSDs for accurately reporting of their device status and radio capabilities; a CBSD's customized operation requires its subscribing EUDs to operate under the designated radio settings. Unfortunately, self-reported device information may not always be reliable. The risk of user device misconfiguration cannot be ruled out. And malicious spectrum users may deliberately modify radio software and parameters in order to gain unfair advantage or disrupt network service. For example, a selfish CBSD may misreport information, such as identities, locations, priority levels to gain excessive transmission spectrum. An attacker can also leverage a CBSD bot net to launch Denial-of-Service (DoS) attack by having a large number of zombie CBSDs continuously sending requests to SAS servers. A compromised EUD may also cause mutual interference to other devices by using unauthorized channels. Therefore, there needs a solution for ensuring operational integrity of EUDs and CBSDs in the RF domain, which is critical to the performance and reputation of the CBRS ecosystem.

To this regard, a novel remote radio context attestation protocol called ROSTER is proposed in [24] to verify the radio operational integrity in spectrum sharing systems. As is introduced in Section III-D, remote attestation is originally used to protect software execution via detecting abnormal software behaviors. It is suggested that the compliance of a radio transmission depends on the software configuration, radio configuration as well as location and time of the device transmitting, which are collectively define as *radio context*. In the ROSTER protocol, attesting the radio context of cognitive radio devices, i.e., EUDs in SAS, ensures the compliance of large number of EUDs in the CBRS network. The network attestation procedure includes three phases: 1) attestation request propagation; 2) radio context measurement and attestation report generation; and 3) attestation report aggregation and verification. ROSTER allows a network appraiser, such as a trusted base station or SAS server, to remotely attest the operational integrity of EUDs through verifying the integrity and authenticity of radio context reports generated by the attestation routines inside the TEE of EUDs, using the ARM TrustZone technology.

A follow-up attestation scheme called PriROSTER is proposed in [25] to further address the concern of EUD users' privacy leakage to untrusted verifier (called "appraiser" in the article), which corresponds to CBSD in our case. PriROSTER accomplishes privacy-preserving radio contest attestation by leveraging the Intel SGX trusted hardware platform [59] at the verifier side. PriROSTER requires edge base stations (i.e., CBSDs) to set up an Intel SGX enclave to serve as the local appraiser. A trusted SAS server assumes the role of global appraiser. PriROSTER requires each EUD to verify the trustworthiness of its local appraiser before sending its radio context attestation report to the latter. Since attestation is a far

more expensive process comparing to cryptographic key-based authentication, PriROSTER also includes a trust transfer protocol in which the trustworthiness of local appraiser is attested by the global appraiser and transferred to all EUDs' associated with that local appraiser through authentication. Although authentication provides only identity verification, a weaker trust level comparing to attestation which provides additional radio context compliance verification, the amount of computation and communication overhead involved is significantly reduced.

Both ROSTER and PriROSTER focus on attesting the operational integrity of EUDs. From the perspective of spectrum management, enforcing the compliance of CBSDs in the RF domain is also an indispensable task. The WInnForum specification on CBRS communication security (June 2020 version) [94] suggests using TEE technology, such as ARM TrustZone to establish certified software system in CBSD. In Fig. 5 we describe a two-layer radio context attestation paradigm which includes the first layer for EUD attestation and the second layer for CBSD attestation. Each CBSD sets up an Intel SGX enclave serving as a local appraiser for EUD radio contexts and an SAS server fulfills as the global appraiser (verifier). The EUD radio context attestation process follows the PriROSTER protocol. CBSD needs to justify its operation compliance, on authenticity and integrity of both appraiser functionality and radio context, through remote attestation to the global verifier.

### C. Spectrum Sensing-Based Anomaly Detection

Remote radio attestation verifies the operational compliance of radio transmission configurations at CBSDs and EUDs, serving as a first line of defense to secure the spectrum sharing paradigm. As a typical second line of defense, an anomaly detection system can be set up to detect spectrum anomalies. Spectrum anomaly refers to a fault or misuse in spectrum, such as intentional spectrum misuse, misconfigured transmitters, RF leakage, etc. These problems will grow in severity and scale in the near future due to the advances in reconfigurable hardware, spectrum sharing policies, and cellular interfaces for IoT systems. Anomalies may appear anywhere in the physical network which necessitates a large-scale and distributed detection system.

Liu *et al.* [26] formalizes the fundamental framework for the spectrum anomaly detection problem. The spectrum anomaly detection system takes spectrum sensing data as input and outputs a decision on whether a spectrum anomaly is present. A binary classifier based on support vector machine (SVM) is trained to detect the spectrum anomalies. However, SVM is a relatively lightweight machine learning technique and only suitable for classifier training on small data sets, rather than the streaming data generated from unstable wireless environments.

To address this problem, [27] proposes a deep autoencoder-based anomaly detection system. This system preprocesses the wireless signal with short-time Fourier transform (STFT) as the input to a multilayer deep autoencoder model. With preprocessed data as input, the multilayer autoencoder model outputs a reconstruction error as the indicator for spectrum anomaly.

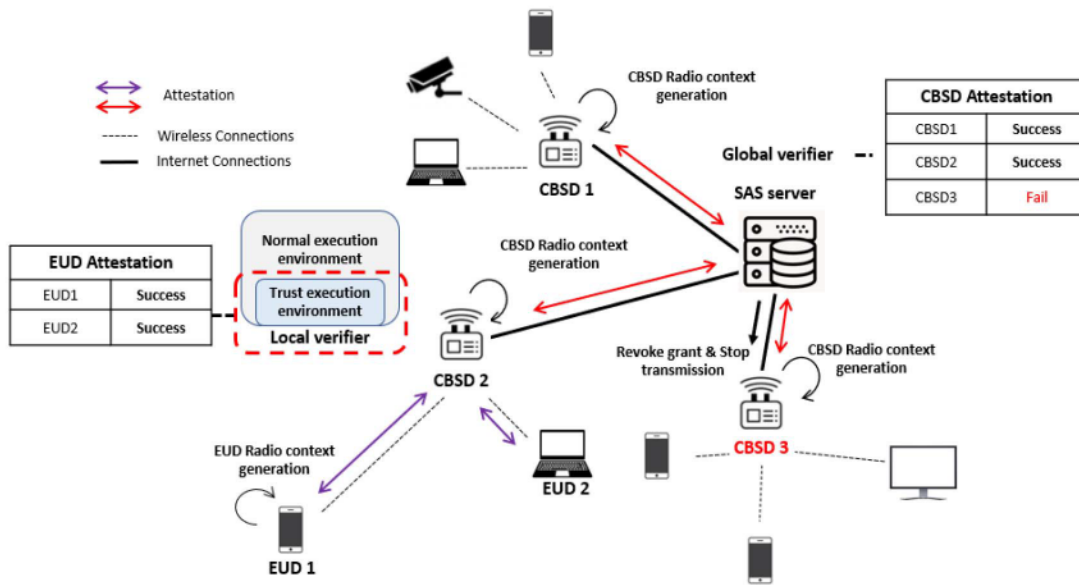


Fig. 5. Example of two-layer radio context attestation paradigm.

If this error exceeds a threshold which is obtained through model training phases, the system will flag the input sample as an anomaly. Experimental results in this work show that this system achieves excellent performance on Gaussian noise detection tasks. However, time series information of wireless signals is not considered in this feedforward network.

To further leverage the time-series property of spectrum signals, in [28], a recurrent neural network (RNN)-based model for spectrum anomaly detection is proposed. The model assumes a scalable, distributed spectrum monitoring system with both static and mobile observers. Anomaly detection is based on measurements from both a dedicated spectrum monitoring infrastructure and spectrum crowdsensing [95]. In particular, a long short-term memory (LSTM) model is trained as the DNN-based anomaly detection model with the help of their collected large-scale LTE sensing data set in the form of time-frequency spectrogram. For the optimal performance, this LSTM anomaly detection model is configured to take 25.6 ms of measured signal spectrogram as input and output a predicted 6.4 m signal. The root-mean-square error (RMSE) between the predicted signal and the ground-truth sensing signal is calculated as the model prediction error, indicating the difference between true signal and predicted signal. Similar with the usage of reconstruction error in [27], for the RNN-based model in [28], if the RMSE exceeds a certain threshold, which was determined from the training process, the model will flag the input signal as an anomaly.

A common concern for a DNN-based spectrum anomaly detection model is whether it is transferable to other spectrum anomaly detection scenarios of different LTE bands, locations, and time. In [28], model transferability across different cells and LTE bands is analyzed. The article applies transfer learning techniques to address this concern by leveraging the similarity of LTE signal characteristics between different scenarios. With transfer learning, a teacher model trained for a specific location and LTE band can be used to

quickly bootstrap student models for other anomaly detection scenarios.

## V. ESC SECURITY

In this section, we discuss the security and privacy threats of ESC. ESC can be viewed as a cooperative spectrum sensing system in which constituent sensors individually perform spectrum sensing to detect moving incumbents' activities, while ESC decision system integrates sensors' reports to reach a final determination about incumbents' presence information. This critical information about incumbents' presence is conveyed to SAS servers through the ESC-Server interface, and servers rely on this information to manage spectrum allocation services. In Section V-A we consider the scenario that part of the sensors are compromised and act Byzantine, individually or in collusion, reporting false data to seduce the ESC decision system into making wrong decisions. In Section V-B we consider strategic attackers who control a portion of sensors may launch adversarial machine-learning-based attacks to bypass detection or poison the ESC decision model. Finally, considering the information sensitivity of incumbent users whom ECS serves, we discuss the privacy requirements for ESC operation Section V-C.

### A. Byzantine Data Falsification Attacks and Defenses

The performance of cooperative spectrum sensing can be significantly degraded if part of the subscribed sensors act Byzantine. Those Byzantine sensors may generate false reports to confuse the ESC decision system and impair its capability of detecting the advent of incumbents. For example, a Byzantine sensor can flip the result made by the ESC decision system about the presence of incumbents and cause confusion at SAS servers. This confusion may cause problem in interference control because SAS servers without correct information about

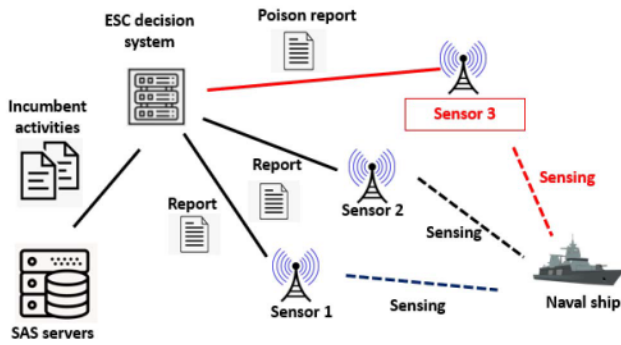


Fig. 6. ESC Byzantine attacks.

incumbents' activities may start to authorize CBSD transmissions even when the incumbents are still using the spectrum band(s).

In spectrum sharing systems, this kind of Byzantine attacks is also referred to as spectrum sensing data falsification (SSDF) attack, commonly known as one of the severest adversarial attacks on cooperative spectrum sensing operations [30]. Fig. 6 illustrates an example of Byzantine attacks toward ESC operation.

One way to defend against such Byzantine data falsification attacks is to label false data as anomalous and employ anomaly detection techniques to distinguish abnormal nodes from innocuous ones. Several detection methods have been introduced to mitigate this attack by leveraging the underlying characteristics and patterns of sensory data. Here, we classify them into three categories.

- 1) *Statistical Inference on Byzantine Data*: This type of defense distinguishes malicious nodes from innocuous ones based on the statistical measures derived from the sensing report history. Statistical consistency, which indicates whether the statistics of current sensing data report, such as covariance and deviation, are consistent with those of historical data [96]. This indicator can be used to detect malicious nodes because most malicious nodes have to inevitably exhibit data inconsistency for they need to occasionally or intermittently send poisonous data whose statistics are usually not consistent with normal data. Besides using straightforward statistical indicators, sophisticated statistical methods, such as Kruskal–Wallis statistical test [31], Conover–Inman statistical test [31], Neyman–Pearson test [97], and belief propagation and Bayes inference [32], can also be used to derive exquisite statistics of different orders and detect the outliers in the sensing data with subtlety.
- 2) *Machine-Learning-Based Byzantine Detection*: Compared to statistical inference methods, ML-based Byzantine detection takes data of large size and diverse features. It assumes data from malicious nodes and data from innocuous nodes follow different intrinsic patterns and ML tools can discern and classify these patterns. Defenders need to use a carefully curated data set with manually labeled malicious samples to train a binary classifier to learn these intrinsic data patterns, before using the models to detect malicious nodes [37], [98].

- 3) *Reputation-Based Defense*: Reputation based defense schemes define a trust metric and assign a trust value to each sensor node based on the “trustworthiness” of its reported data. The trust value at individual sensors is updated after each decision round, by checking the conformation of this sensor's report and the final decision, the node's trust value increases when the reported data is consistent with the system's final decision, otherwise its trust value decreases. In a long-term sensing operation, a malicious node's falsified data has a higher probability to be inconsistent with final decision comparing to innocuous ones. A malicious node's trust value will therefore gradually decrease and the weight of its input to the system will also decrease accordingly. The malicious node will eventually be eliminated from data fusion process if the malicious behavior continues. Most reputation-based defense schemes leverage statistics computed from sensing data to measure the conformation degree and derive metric assignment matrix [33]–[36].

### B. Adversarial Machine-Learning-Based Attacks and Defense

Recent advance in machine learning research, especially the development of adversarial machine learning introduces more security threats to wireless systems. Adversarial machine learning tools have been used to infer sensitive information, deceive decision system and poison spectrum data in spectrum sharing systems [99], [100].

A new adversarial machine-learning-based attack targeting ESC, called learn-evaluate-beat (LEB) attack, is proposed in [38]. This attack contains three steps: 1) learning step, in which the attacker leverages the machine learning technology to build its surrogate model to approximate decision system's fusion model; 2) evaluating step, in which the attacker evaluates whether the surrogate model is accurate enough to launch an attack; and if the attacker decides that the surrogate model is accurate enough, he performs the next step; and 3) beating step, in which the attacker leverages fine tuned surrogate model to craft final AEs to poison the sensing system. The concept of AE is first introduced by [101] and [102] by adding small perturbations to normal examples to cause misclassification of deep learning models. One important property of AEs is that the perturbations are usually norm bounded [103] and hardly distinguishable from benign examples. The LEB attack leverages this AEs' property and can carry out data poison attack in a very stealthy way. The article's experimental result shows the devastating effect of LEB attack as it achieves high attack successful rate up to 82%.

Potential defense mechanism against this powerful new attack is discussed in [38]. This article proposed a defense scheme called influence limiting policy, in which an upper bound is set to restrict the decision influencing capability of any subset of sensing nodes, in order to protect decision process from being dominant by certain node subset. Because malicious nodes are considered minority in the sensing system, their capability of manipulating sensing input to dominant and flip over the final decision is prohibited.

AEs is the key technique that enables this type of powerful but stealthy attacks. More defense mechanisms against AE attacks can be found in general adversarial machine learning literature. Feinman *et al.* [104] and Carlini and Wagner [105] propose effective AE detection methods to distinguish AEs from benign ones. While [106]–[109] propose defense methods, such as network distillation and adversarial training to build an AE resistant robust machine learning model against malicious crafted AEs.

### C. Incumbents Privacy

As most of the incumbents are federal governments' infrastructure or military facilities, privacy is particularly important for ESC operations. The WinnForum specification [110] requires ESC to preserve incumbents privacy from multiple aspects.

1) *Data Privacy*: To prevent compromised sensors from leaking sensitive information, ESC sensors do not store long-term time series data on detected incumbents' signals. Instead, they only store the most recent sensing data and incumbent radars' basic signal characteristics to meet the minimum requirement for incumbent activity determination.

2) *Intrusion Detection*: ESC sensors shall deploy intrusion detection system (IDS) to protect their software and hardware from tampering. For example, each sensor can instantiate a TEE and integrate an IDS routine in it to monitor its working status and report anomaly behaviors timely to avoid devastating results.

3) *Location Uncertainty*: ESC should be able to detect the presence of stationary or moving incumbents in one area but not their precise location. In specific, ESC sensors only report quantized signal strength to ESC decision system to prevent the latter from inferring the precise location of incumbents. Sensors are also required not to deploy highly directional antennas which would allow them to perform Angle-of-Arrival (AoA) estimation, such as MUSIC [111] and ESPRIT [112] algorithms to derive incumbent location.

4) *Supply Chain Security*: ESC sensors' supply chain security shall be taken into consideration when choosing sensor manufacturers. Potential cyber security and privacy risks (e.g., exploits, backdoors) should be thoroughly assessed during the manufacturing process.

## VI. COMMUNICATION PROTOCOL SECURITY

Overlaying upon the Internet, communications between SAS entities are subject to various network level threats, such as eavesdropping, impersonation, message modification, message replay, DoS attack, etc. These attacks aim to compromise one or multiple SAS security requirements, such as confidentiality and integrity of information when in transit, user/device authentication, and service availability. Violation of such security requirements will certainly lead to system malfunction or complete disruption. Securing a network protocol against such attacks is typically done by incorporating security measures, such as user authentication, message encryption, message authentication code (MAC) and digital signature into the protocol suite. In this section, we will

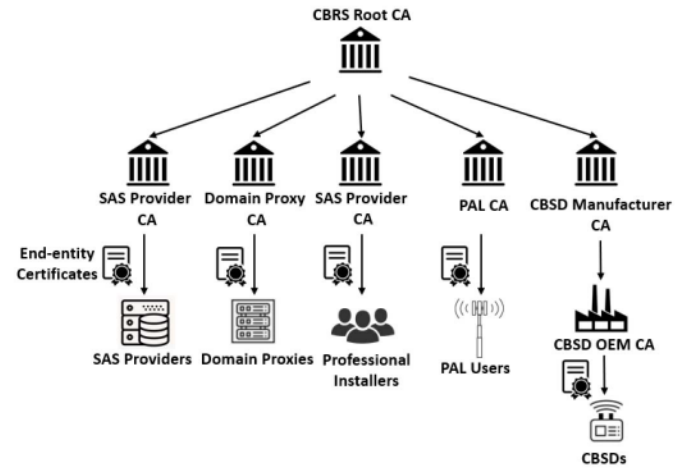


Fig. 7. CBRS PKI hierarchy structure.

briefly discuss the WinnForum proposed public key infrastructure (PKI) for CBRS [113] (Section VI-A) that provides key management service to support transport layer protocol (TLS) (Section VI-B) which enables message authentication and encryption within SAS ecosystem.

### A. CBRS PKI

Fig. 7 illustrates the structure of the WinnForum proposed CBRS PKI. It takes a top-down tree structure with possibly multiple Root certification authorities (CAs) on top. Root CAs sign certificates of intermediate CAs, and then intermediate CAs sign certificates of lower level CAs, till end-entity certificates in the CBRS ecosystem.

1) *CBRS Root CA*: CBRS root CAs are trusted entities in the CBRS ecosystem and their sets of public/private key pairs serve as the trust anchor of all certificate chains in the CBRS ecosystem. The role of root CA is to qualify intermediate CAs to issue end-entity certificates through a certificate signature. The WinnForum's specification discusses the selection of Root CAs [94]. It is expected that the root CA key materials are generated and maintained by organizations designated by the WinnForum. Those organizations shall be capable of securely generating keys under audited conditions, storing them on secure hardware, operating them to sign intermediate CAs as needed, and ensure that the key custody can be transferred in a manner that conforms to the WinnForum's guidelines. Currently, the WinnForum has approved three root CA operators, including INSTA, KYRIO, and CommScope.

2) *CBRS Intermediate CA*: CBRS intermediate CAs serve as the subordinate CAs certified by root CAs to issue end-entity certificates. They generate and maintain their keys under auditable conditions and follow all operating procedures required by the Web Trust Principles and Criteria for CAs 2.0 [114]. CBRS intermediate CAs include SAS Provider CAs, domain proxy CAs, professional installer CAs, PAL CAs, CBSD manufacturer CAs and CBSD original equipment manufacturer (OEM) CAs.

An SAS provider CA issues end-entity certificates to SAS providers, such as Google, CommScope, Federated Wireless,

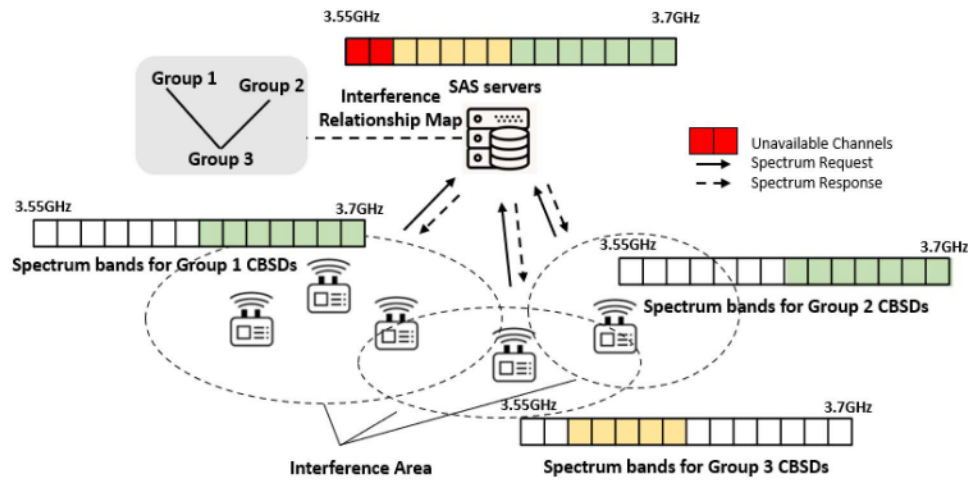


Fig. 8. Intratier interference management mechanism.

and Sony. The trust responsibility of an SAS provider is to provide correct transmission authorizations to subscribed CBSDs and DPs, and also notify spectrum usage information to its peers in time.

A domain proxy CA issues end-entity certificates to domain proxy operators. The trust responsibility of a domain proxy operator is to provide assurance of the compliance of its subscribed CBSDs to the transmission authorizations from SAS servers, to which the domain proxy communicates.

A professional installer CA issues digital certificates to a professional installer after he finished the installer training program. Professional installers install Category-B CBSDs and some Category-A CBSDs. They are responsible and accountable to convey accurate installation configurations to SAS servers with their certificates.

CBSD manufacturer CA is an intermediate CA that signs next level subordinate CBSD OEM CAs. A CBSD OEM can include its product CBSDs into CBRS trust boundary through issuing them end-entity certificates after it is certified as a CBSD OEM CA. Authorized OEMs include Samsung, Cisco, Ericsson, etc.

3) *End-Entity Certificate*: End-entity certificate is an X.509 certificate signed by each of its parent CAs in the tree. It contains the issuer's information, version, serial number, certificate validation date, key information, algorithms type and other extension information. They are used during TLS protocols to build a secure and authentication communication channel between entities in the CBRS ecosystem.

### B. Transport Layer Security

The Internet is already equipped with security protection mechanism, including IPsec at the IP level and SSL/TLS at the transport layer. Securing SAS management protocol at the application level can follow similar principles of secure network protocol design as long as the key management is properly arranged.

Different entities in the CBRS ecosystem communicate with each other through the Internet. The WinnForum recommends that transport layer security (TLS), i.e., HTTP over TLS, to be

used in conjunction with the CBRS PKI in order to protect the security of all interfaces between entities. TLS is a widely used network security protocol that provides authentication, confidentiality, and data integrity for connections over a computer network on the Internet. It was proposed by Internet engineering task force (IETF) in 1999 [115] and the latest version is TLS 1.3. In the CBRS ecosystem, different entities authenticate each other with their issued end-entity certificates to build a secure communication channel via TLS. WinnForum Specification requires that SAS servers shall be configured to support both TLS 1.2 and TLS 1.3 [113].

## VII. FUTURE DIRECTIONS AND CHALLENGES

Continuing improvements in spectrum sharing technologies, especially successful dynamic spectrum management, allocation and access, will ensure that the wireless spectrum is used in the most efficient way, maximizing the benefits of services that rely on those spectrum bands and enabling the harmonic coexistence of heterogeneous wireless applications. At the same time, with the sophistication of spectrum sharing technologies, additional security and privacy challenges will continue to emerge. In this section, we discuss additional challenges and identify potential future research directions for securing spectrum sharing.

### A. Intratier Spectrum Coordination

The current interference management design in SAS server anticipates the harmonious coexistence of intertier user devices in the same geolocation. However, how to coordinate spectrum use to avoid harmful interference among devices in the same priority tier, for example in the most commonly used GAA tier, is still unclear. We refer to this unsolved problem as the intratier spectrum coordination problem.

The WinnForum recommends three approaches in their working documents [116]–[118] to address this problem. Their fundamental mechanisms, which are illustrated in Fig. 8, are to assign spectrum band(s) without overlapping to different individual or group of CBSDs with respect to their mutual interference relationships in order to avoid harmful

interference. More specifically, when nearby groups of GAA-tier CBSDs in the same local area governed by an SAS server request for spectrum allocation simultaneously, the SAS server will use interference threshold and terrain information to calculate the interference area of each group, and then build up an interference relationship map in which groups are taken as vertex and overlapping interference areas are taken as edges to indicate the mutual interference relationship between different groups. According to this map, the server assigns spectrum band(s) without overlapping to each two vertexes connected by an edge to avoid harmful mutual interference. However, one key concern of these recommended approaches is that they only build up theoretical models to address the intratier spectrum coordination problem without experimental validation. Particularly, the performance of these approaches is unclear when the network scale is very large.

In addition to the model-based scheduling approach, machine-learning-based approaches, such as reinforcement learning-based automatic spectrum decision scheme has been proposed to address this problem [119]. In the SAS paradigm, ML approaches can be instantiated in each SAS server taking inputs from CBSDs to resolve potential interference. The recent DARPA's spectrum collaboration challenge (SC2) [120] aimed for a highly dynamic spectrum access network where radio devices autonomously collaborate and reason about how to share the RF spectrum, thereby avoiding interference and jointly exploiting opportunities to achieve the most efficient use of the available spectrum. This is accomplished by taking advantage of recent advances in artificial intelligence and especially reinforcement learning [121]. It is believed that novel spectrum coexistence methods that go beyond sensing and database management methods used today are much desired and machine learning would be an important technology leveraged to accomplish such goals with near real-time spectrum awareness and automated spectrum decision making. Currently, a big challenge for machine-learning-based automatic spectrum coordination mechanism is the scarcity of high-quality, large-scale SAS operating data sets, especially for the CBRS band. These data sets are essential to building and validating the data-driven machine learning models, and therefore in great demand.

### B. Spectrum Anomaly Detection

Spectrum anomalies refer to the unauthorized or misconfigured transmission in the shared spectrum band(s). They cause harmful interference to innocuous users and jeopardize the normal spectrum sharing paradigms. As discussed in Section IV-C, one promising solution to this problem is using the strong representative learning capability of deep learning models to capture features of spectrum signal, and then leverage these features to classify spectrum anomalies from innocuous ones. However, training those DNN models requires high-quality, curated data sets with established baselines of normal user behavior, which are still in great scarcity.

From another perspective, one key drawback of DNN-based anomaly detection models is that they often require the system to possess considerable large computational and

memory resource. This may not be an issue for machine learning workstations, but for wireless devices this requirement can be prohibitive. It is a tradeoff to balance deep learning model's size and practical wireless deployment capability, which entails lightweight anomaly detection algorithms with high accuracy and low resource consumption.

Additional challenges lie in public acceptance of the potentially intrusive sensing and monitoring mechanism, trustworthiness of the learning process against increasingly sophisticated adversarial attacks on machine learning, privacy protection, and feasibility of generalizing the machine learning models to different frequency bands and different locations. Efficient and effective spectrum anomaly detection is an important capability that deserves more research endeavor.

### C. Forensics

Spectrum is a critical and valuable resource. Disruption of proper spectrum sharing, or interruption of critical services that rely on such spectrum, may lead to significant financial loss or infringement to national security. Once a spectrum use violation is detected, an important next step capability is to identify and localize the offender, and collect sound evidences with respect to the violation that are admissible at a court.

Not much work has been done along this line, yet it is an important research direction. To ensure the collected evidence is indisputable, unique physical layer characteristics, such as the carrier frequency difference, phase shift difference, received signal amplitude, cyclostationary signal features, might be leveraged to establish a unique device fingerprint for each wireless device at the physical layer.

### D. Heterogeneous Spectrum Management Services

Future spectrum management system is expected to manage diverse types of spectrum users. RF spectrum is not only used by wireless communications. Other spectrum users, such as radio astronomy, which quietly monitors the RF spectrum to conduct scientific observations/discoveries, and atmospheric remote sensing, who has a variety of ground-based and airborne remote sensing radars that need to use RF spectrum. When the spectrum management is extended to cover many different types of spectrum services across large geographical areas, how to minimize the amount of information to be exchanged and how to ensure the exchange of such information in a secure way and with an appropriate level of privacy protection against different types of attackers will be a key research challenge. Lessons learned from securing SAS for the CBRS band could be useful and used to inform security design for future spectrum management system.

### E. Policy Enforcement in Blockchain-Based SAS

The centralized SAS framework relies on regulatory means to mandate spectrum policies and react to misbehaving spectrum users in hindsight, with the help of forensic tools. In the blockchain-based SAS introduced in Section III-E, this top-down enforcement approach is no-longer feasible due to the lack of trust on individual SAS administrator/server

and localized nature of spectrum allocation. We identify three challenges toward automatic policy enforcement in blockchain-based SAS.

The first challenge is the replication of spectrum policies across local spectrum sharing areas, as it is impossible for regulators to participate in every local blockchain network. A potential solution is to adopt a global-scale blockchain network between regulators and SAS administrators, with the latter being responsible for replicating policy requirements in their proprietary servers. How to encode spectrum policy in blockchain smart contract without software vulnerability is also worth exploring.

The second challenge is the detection and response on spectrum violations at the local-scale. While violation detection mechanisms can be instantiated in smart contract, the actionable sensory data which likely comes from outside the blockchain system through crowdsensing, may not be trusted in the first place. To this regard, a partial solution is the smart contract oracle mechanism proposed in [122] and [123], which helps extract sensory data from outside sources. This however needs to assume the outside sources are trustworthy. In the case they are not trusted, data analytic approaches, such as truth discovery [124] can be used to extract trustworthy information from multisourced data. On the downside, since on-chain operation is generally very costly due to the mandatory consensus procedure, how to incorporate such data analytic mechanisms into smart contract securely and efficiently while keeping the blockchain system decentralized entails innovative solutions.

The third challenge is the stringent delay requirement due to the dynamic nature of spectrum sharing. For example, the consensus-based validation of spectrum assignment against spectrum policy should be done with seconds. This boils down to the design of efficient consensus protocol and smart contract platform.

#### F. Secondary Spectrum Market

The 2016 FCC ruling [125] suggests the feasibility of secondary markets for trading spectrum access rights held by PAL users. The underlying vision is that market forces, in addition to the SAS model, would drive the development of creative and dynamic spectrum usage scenarios. For instance, a PAL user may lease its licensed spectrum bands to GAA users for temporary, uninterrupted use; multiple PAL users may sign a service cooperation agreement that allows their customers to use either side's spectrum bands in the wandering mode. Challenges remain on how to establish such market mechanisms in a secure and efficient manner.

The functions of a conceptual spectrum trading market is first discussed in [126], prior to the inception of CBRS. A central spectrum exchange, emulating a traditional security exchange, matches buy and sell offers of spectrum usage rights. The trade, i.e., the transfer of money and spectrum usage rights between buyers and sellers, is facilitated by the exchange. A regulator is responsible for monitoring the trading market and enforcing government policies. Speculative entities, such as market makers are allowed to tackle liquidity problems in spectrum trading and pricing. Despite its resemblance to traditional security exchange (more closely, futures

exchange), the spectrum exchange concept faces a unique challenge on the securitization of spectrum usage right and trade settlement. Wireless spectrum bands, unlike physical or financial assets, are self-existent and not subject to custody. Misbehaving spectrum users are only punishable from the hindsight. How to enforce the trade in a timely manner and prevent the seller from violating the trade is essential to solving this challenge, which expects solutions from the policy domain (e.g., incentive or punitive mechanisms) and the physical domain (e.g., attestable wireless configuration using software radio technologies).

In the case that centralized exchanges are not trustworthy, similar to the blockchain-based SAS discussed in Section III-E, blockchain can also provide a decentralized, self-organized platform for spectrum trading [22]. With the establishment of a smart contract environment and a built-in transaction model, spectrum usage rights (of certain band, local, time) and derivative spectrum contracts of complex logic can publicly traded. The blockchain platform essentially realizes a decentralized exchange. However, challenges remain in aligning the business model of spectrum trading with blockchain's decentralized finances. More specifically, market mechanisms, such as orders matching, commission fee assessment, and even financial derivatives of spectrum trading (if desired) need to be fulfilled by the blockchain's native currency minting process and transactional model. This is a potential multidisciplinary research involving distributed systems, game theory, and economics. Another challenge of the blockchain-based decentralized spectrum exchange lies in its efficiency. The maximum trade volume per second and trade finalization speed are influenced by the underlying blockchain consensus process and network infrastructure.

#### VIII. CONCLUSION

In this article, we focused on the security aspect of the SAS. We discussed the security and privacy threats that might violate the security requirements for the seamless spectrum sharing service and the harmonious coexistence of different tier of users and their countermeasures. More specifically, we considered server security, CBSD security, ESC security, and communication protocol security, according to the SAS functional architecture. For server security, privacy leakage attacks and malicious insider attacks are among the main concerns against current centralized spectrum management server system. We described a blockchain-based spectrum management system operating in a secure and decentralized manner to address it. For CBRS radio devices, we introduced both TEE-based remote attestation and DNN-based spectrum anomaly detection as two defense lines to safeguard radio devices' operation integrity. For the ESC, we considered Byzantine data falsification attack and more sophisticated adversarial machine-learning-based attack as two main adversaries against cooperative spectrum sensing. Moreover, for the protocols among entities within the CBRS ecosystem, we demonstrated the existing mature cryptographic tool, namely, CBRS PKI and TLS as the paradigm to protect communication security. Last but not least, we positioned several future research directions for SAS security and applications.

The commercial success of SAS has drawn broad attention from the industry and academia. New spectrum bands other than the CBRS band are being promulgated to accommodate future proliferation of spectrum sharing services. Therefore, it is anticipated that more spectrum sharing paradigms and commercial applications are on the horizon. We hope our survey and discussions on security and privacy issues of dynamic spectrum sharing are helpful in designing robust SAS solutions and also shed light on future database-driven multilayer spectrum sharing paradigms.

## REFERENCES

- [1] *Report to the President: Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth*, President's Council Advisors Sci. Technol., Washington, DC, USA, Jul. 2012.
- [2] *Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future*, Nat. Telecommun. Inf. Admin., Washington, DC, USA, Oct. 2018.
- [3] "5G white paper," Frankfurt, Germany, NGMN Alliance, White Paper, 2015.
- [4] "Cisco visual networking index: Global mobile data traffic forecast update 2017–2022," San Jose, CA, USA, Cisco, White Paper, 2019.
- [5] *Research and Development Priorities for American Leadership in Wireless Communications*, Executive Office President United States, Washington, DC, USA, May 2019.
- [6] *Emerging Technologies and Their Expected Impact on Non-Federal Spectrum Demand*, Executive Office President United States, Washington, DC, USA, May 2019.
- [7] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: Requirements, challenges and design trade-offs," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 32–39, Apr. 2008.
- [8] A. B. MacKenzie et al., "Cognitive radio and networking research at Virginia Tech," *Proc. IEEE*, vol. 97, no. 4, pp. 660–688, Apr. 2009.
- [9] M. M. Sohel, M. Yao, X. Ma, E. Y. Imana, V. Marojevic, and J. H. Reed, "Next generation public safety networks: A spectrum sharing approach," *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 30–36, Mar. 2016.
- [10] A. M. Wyglinski, M. Nekovee, and T. Hou, *Cognitive Radio Communications and Networks: Principles and Practice*. Burlington, MA, USA: Academic, 2009.
- [11] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, 1st Quart., 2009.
- [12] D. Gurney, G. Buchwald, L. Ecklund, S. L. Kuffner, and J. Grosspietsch, "Geo-location database techniques for incumbent protection in the TV white space," in *Proc. 3rd IEEE Symp. New Front. Dyn. Spectr. Access Netw.*, 2008, pp. 1–9.
- [13] M. D. Mueck, S. Srikanteswara, and B. Badic, "Spectrum sharing: Licensed shared access (LSA) and spectrum access system (SAS)," Santa Clara, CA, USA, Intel, White Paper, 2015.
- [14] P. R. Vaka, S. Bhattarai, and J.-M. Jerry, "Location privacy of non-stationary incumbent systems in spectrum sharing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2016, pp. 1–6.
- [15] L. Sweeney, "k-anonymity: A model for protecting privacy," *Int. J. Uncertainty Fuzziness Knowl. Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.
- [16] Y. Dou et al., " $p^2$ -SAS: Privacy-preserving centralized dynamic spectrum access system," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 1, pp. 173–187, Jan. 2017.
- [17] C. Guan, A. Mohaisen, Z. Sun, L. Su, K. Ren, and Y. Yang, "When smart TV meets CRN: Privacy-preserving fine-grained spectrum access," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2017, pp. 1105–1115.
- [18] N. Li, T. Li, and S. Venkatasubramanian, "t-Closeness: Privacy beyond k-anonymity and l-diversity," in *Proc. IEEE 23rd Int. Conf. Data Eng.*, 2007, pp. 106–115.
- [19] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkatasubramanian, "l-Diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Disc. Data*, vol. 1, no. 1, p. 52, 2007.
- [20] H. Li, Y. Yang, Y. Dou, J.-M. J. Park, and K. Ren, "PeDSS: Privacy enhanced and database-driven dynamic spectrum sharing," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2019, pp. 1477–1485.
- [21] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "TrustSAS: A trustworthy spectrum access system for the 3.5 Ghz CBRS band," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2019, pp. 1495–1503.
- [22] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 193–205, Jun. 2019.
- [23] J.-M. Park, J. H. Reed, A. Beex, T. C. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing," *Proc. IEEE*, vol. 102, no. 3, pp. 270–281, Mar. 2014.
- [24] N. Zhang, W. Sun, W. Lou, Y. T. Hou, and W. Trappe, "ROSTER: Radio context attestation in cognitive radio network," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2018, pp. 1–9.
- [25] R. Zhang, N. Wang, N. Zhang, Z. Yan, W. Lou, and Y. T. Hou, "PriRoster: Privacy-preserving radio context attestation in cognitive radio networks," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DySPAN)*, 2019, pp. 1–10.
- [26] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "ALDO: An anomaly detection framework for dynamic spectrum access networks," in *Proc. IEEE INFOCOM*, 2009, pp. 675–683.
- [27] Q. Feng, Y. Zhang, C. Li, Z. Dou, and J. Wang, "Anomaly detection of spectrum in wireless communication via deep auto-encoders," *J. Supercomput.*, vol. 73, no. 7, pp. 3161–3178, 2017.
- [28] Z. Li, Z. Xiao, B. Wang, B. Y. Zhao, and H. Zheng, "Scaling deep learning models for spectrum anomaly detection," in *Proc. 20th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2019, pp. 291–300.
- [29] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Mimo-based jamming resilient communication in wireless networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2014, pp. 2697–2706.
- [30] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342–1363, 3rd Quart., 2015.
- [31] F. Adelantado and C. Verikoukis, "A non-parametric statistical approach for malicious users detection in cognitive wireless ad-hoc networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2011, pp. 1–5.
- [32] F. Penna, Y. Sun, L. Dolecek, and D. Cabric, "Detecting and counteracting statistical attacks in cooperative spectrum sensing," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1806–1822, Apr. 2012.
- [33] P. Kaligineedi, M. Khabbazi, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2008, pp. 3406–3410.
- [34] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2008, pp. 1876–1884.
- [35] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2009, pp. 1–5.
- [36] T. Zhang, R. Safavi-Naini, and Z. Li, "ReDiSen: Reputation-based secure cooperative sensing in distributed cognitive radio networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2013, pp. 2601–2605.
- [37] O. Fatemeh, A. Farhadi, R. Chandra, and C. A. Gunter, "Using classification to protect the integrity of spectrum measurements in white space networks," in *Proc. NDSS*, 2011.
- [38] Z. Luo, S. Zhao, Z. Lu, J. Xu, and Y. E. Sagduyu, "When attackers meet AI: Learning-empowered attacks in cooperative spectrum sensing," 2019. [Online]. Available: arXiv:1905.01430.
- [39] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proc. 1st IEEE Workshop Netw. Technol. Softw. Defined Radio Netw.*, 2006, pp. 110–119.
- [40] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Phys. Commun.*, vol. 4, no. 1, pp. 40–62, 2011.
- [41] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proc. IEEE*, vol. 100, no. 12, pp. 3172–3186, Dec. 2012.
- [42] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Commun.*, vol. 19, no. 6, pp. 106–112, Dec. 2012.
- [43] *Requirements for Commercial Operation in the U.S. 3550–3700 MHz Citizens Broadband Radio Service Band, Version V2.0.0*, document WINNF-15-S-0112, Wireless Innovation Forum, Reston, VA, USA, Feb. 2017.
- [44] M. Grissa, B. Hamdaoui, and A. A. Yavuz, "Location privacy in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1726–1760, 3rd Quart., 2017.

- [45] M. Altamimi, M. B. Weiss, and M. McHenry, "Enforcement and spectrum sharing: Case studies of federal-commercial sharing," in *Proc. 41st Res. Conf. Commun. Inf. Internet Policy (TPRC)*, Mar. 2013.
- [46] *Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS)—Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification, Version V1.0.1*, document WINNF-TS-00, Wireless Innovation Forum, Reston, VA, USA, Dec. 2016.
- [47] E. Bertino and R. Sandhu, "Database security—Concepts, approaches, and challenges," *IEEE Trans. Dependable Secure Comput.*, vol. 2, no. 1, pp. 2–19, Jan.–Mar. 2005.
- [48] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. J. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DYSPAN)*, 2014, pp. 236–247.
- [49] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2013, pp. 2751–2759.
- [50] M. Clark and K. Psounis, "Can the privacy of primary networks in shared spectrum be protected?" in *Proc. IEEE INFOCOM 35th Annu. Conf. Comput. Commun.*, 2016, pp. 1–9.
- [51] L. Zhang, C. Fang, Y. Li, H. Zhu, and M. Dong, "Optimal strategies for defending location inference attack in database-driven CRNs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2015, pp. 7640–7645.
- [52] L. Wang, D. Zhang, D. Yang, B. Y. Lim, and X. Ma, "Differential location privacy for sparse mobile crowdsensing," in *Proc. IEEE 16th Int. Conf. Data Min. (ICDM)*, 2016, pp. 1257–1262.
- [53] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proc. IEEE Symp. Security Privacy (SP)*, 2008, pp. 111–125.
- [54] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.
- [55] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *Proc. 31st Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Minneapolis, MN, USA, Jun. 2011, pp. 383–392.
- [56] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.
- [57] W. Sun *et al.*, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in *Proc. 8th ACM SIGSAC Symp. Inf. Comput. Commun. Security*, Hangzhou, China, May 2013, pp. 71–82.
- [58] B. Wang, W. Song, W. Lou, and Y. T. Hou, "Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Hong Kong, China, Apr. 2015, pp. 2092–2100.
- [59] V. Costan and S. Devadas, "Intel SGX explained," *IACR Cryptol. ePrint Arch.*, vol. 2016, no. 86, pp. 1–118, 2016.
- [60] F. Schuster *et al.*, "VC3: Trustworthy data analytics in the cloud using SGX," in *Proc. IEEE Symp. Security Privacy*, 2015, pp. 38–54.
- [61] T. Hunt, Z. Zhu, Y. Xu, S. Peter, and E. Witchel, "Ryoan: A distributed sandbox for untrusted computation on secret data," *ACM Trans. Comput. Syst.*, vol. 35, no. 4, pp. 1–32, 2018.
- [62] W. Sun, R. Zhang, W. Lou, and Y. T. Hou, "REARGUARD: Secure keyword search using trusted hardware," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2018, pp. 801–809.
- [63] O. Weisse, V. Bertacco, and T. Austin, "Regaining lost cycles with hotcalls: A fast interface for SGX secure enclaves," *ACM SIGARCH Comput. Archit. News*, vol. 45, no. 2, pp. 81–93, 2017.
- [64] J. Winter, "Trusted computing building blocks for embedded linux-based arm trustzone platforms," in *Proc. 3rd ACM Workshop Scalable Trusted Comput.*, 2008, pp. 21–30.
- [65] A. Seshadri, A. Perrig, L. Van Doorn, and P. Khosla, "SWATT: Software-based attestation for embedded devices," in *Proc. IEEE Symp. Security Privacy*, 2004, pp. 272–282.
- [66] N. Asokan *et al.*, "SEDA: Scalable embedded device attestation," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Security*, 2015, pp. 964–975.
- [67] M. Ambrosin, M. Conti, A. Ibrahim, G. Neven, A.-R. Sadeghi, and M. Schunter, "SANA: Secure and scalable aggregate network attestation," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 731–742.
- [68] F. Brasser, U. Müller, A. Dmitrienko, K. Kostiaainen, S. Capkun, and A.-R. Sadeghi, "Software grand exposure: SGX cache attacks are practical," in *Proc. 11th USENIX Workshop Offensive Technol. (WOOT)*, 2017, p. 11.
- [69] J. Van Bulck *et al.*, "Foreshadow: Extracting the keys to the intel SGX kingdom with transient out-of-order execution," in *Proc. 27th USENIX Security Symp. (USENIX Security)*, 2018, pp. 991–1008.
- [70] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.
- [71] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.
- [72] *Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS)—SAS Interface Technical Specification, Version V1.3.2*, document WINNF-TS-0096, Wireless Innovation Forum, Reston, VA, USA, Mar. 2020.
- [73] D. Palmer, *FCC Eyes Blockchain to Better Manage Scarce Wireless Spectrums*, 2019, CoinDesk, New York, NY, USA.
- [74] S. Rjöllä, "Analysis of blockchain use cases in the citizens broadband radio service spectrum sharing concept," in *Proc. Int. Conf. Cogn. Radio Oriented Wireless Netw.*, 2017, pp. 128–139.
- [75] T. Ariyaratna, P. Harankahadeniya, S. Isthikar, N. Pathirana, H. D. Bandara, and A. Madanayake, "Dynamic spectrum access via smart contracts on blockchain," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2019, pp. 1–6.
- [76] H. Zhang, S. Leng, and H. Chai, "A blockchain enhanced dynamic spectrum sharing model based on proof-of-strategy," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1–6.
- [77] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin, 2008. Accessed: Mar. 16, 2021. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [78] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Zug, Switzerland, Ethereum, Yellow Paper, 2014.
- [79] K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financ. Cryptogr. Data Security*, 2016, pp. 106–125.
- [80] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Security*, 2015, pp. 112–125.
- [81] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: Scaling blockchain via full sharding," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2018, pp. 931–948.
- [82] R. Cheng *et al.*, "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts," in *Proc. IEEE Eur. Symp. Security Privacy (EuroS&P)*, 2019, pp. 185–200.
- [83] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts," in *Proc. 27th USENIX Security Symp.*, 2018, pp. 1353–1370.
- [84] M. Bowman, A. Miele, M. Steiner, and B. Vavala, "Private data objects: An overview," 2018. [Online]. Available: [arXiv:1807.05686](https://arxiv.org/abs/1807.05686).
- [85] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, "Privacyguard: Enforcing private data usage control with blockchain and attested off-chain contract execution," in *Proc. Eur. Symp. Res. Comput. Security*, 2020, pp. 610–629.
- [86] K. Wüst, S. Matetic, S. Egli, K. Kostiaainen, and S. Capkun, "ACE: Asynchronous and concurrent execution of complex smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2020, pp. 587–600.
- [87] M. Strasser, B. Danev, and S. Čapkun, "Detection of reactive jamming in sensor networks," *ACM Trans. Sens. Netw.*, vol. 7, no. 2, pp. 1–29, 2010.
- [88] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, 2nd Quart., 2011.
- [89] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" in *Proc. 4th ACM Conf. Wireless Netw. Security*, 2011, pp. 47–52.
- [90] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming resilient communication using MIMO interference cancellation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1486–1499, Jul. 2016.
- [91] H. Zhu, C. Fang, Y. Liu, C. Chen, M. Li, and X. S. Shen, "You can jam but you cannot hide: Defending against jamming attacks for geo-location database driven spectrum sharing," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2723–2737, Oct. 2016.
- [92] K. A. 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.

- [93] Y. Hou and M. Li, "Enforcing spectrum access rules in cognitive radio networks through cooperative jamming," in *Proc. Int. Conf. Wireless Algorithms Syst. Appl.*, 2013, pp. 440–453.
- [94] *CBRS Communications Security Technical Specification, Version V1.2.0*, document: WINNF-15-S-0065, Wireless Innovation Forum, Reston, VA, USA, Jun. 2020.
- [95] R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: Current state and future challenges," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 32–39, Nov. 2011.
- [96] P. Kaligineedi, M. Khabbazi, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Trans. Wireless Commun.*, vol. 9, no. 8, pp. 2488–2497, Aug. 2010.
- [97] R. Chen, J.-M. Park, Y. T. Hou, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008.
- [98] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Pattern based anomalous user detection in cognitive radio networks," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2015, pp. 5605–5609.
- [99] Y. Shi, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, Z. Lu, and J. H. Li, "Adversarial deep learning for cognitive radio security: Jamming attack and defense strategies," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2018, pp. 1–6.
- [100] Y. Shi, T. Erpek, Y. E. Sagduyu, and J. H. Li, "Spectrum data poisoning with adversarial deep learning," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2018, pp. 407–412.
- [101] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014. [Online]. Available: arXiv:1412.6572.
- [102] C. Szegedy *et al.*, "Intriguing properties of neural networks," 2013. [Online]. Available: arXiv:1312.6199.
- [103] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," 2017. [Online]. Available: arXiv:1706.06083.
- [104] R. Feinman, R. R. Curtin, S. Shintre, and A. B. Gardner, "Detecting adversarial samples from artifacts," 2017. [Online]. Available: arXiv:1703.00410.
- [105] N. Carlini and D. Wagner, "Adversarial examples are not easily detected: Bypassing ten detection methods," in *Proc. 10th ACM Workshop Artif. Intell. Security*, 2017, pp. 3–14.
- [106] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, "Distillation as a defense to adversarial perturbations against deep neural networks," in *Proc. IEEE Symp. Security Privacy (SP)*, 2016, pp. 582–597.
- [107] N. Carlini and D. Wagner, "Defensive distillation is not robust to adversarial examples," 2016. [Online]. Available: arXiv:1607.04311.
- [108] F. Tramèr, A. Kurakin, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel, "Ensemble adversarial training: Attacks and defenses," 2017. [Online]. Available: arXiv:1705.07204.
- [109] T. Miyato, S.-I. Maeda, M. Koyama, and S. Ishii, "Virtual adversarial training: A regularization method for supervised and semi-supervised learning," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 8, pp. 1979–1993, Aug. 2019.
- [110] *CBRS Operational Security, Version V1.0.0*, document WINNF-15-S-0065, Wireless Innovation Forum, Reston, VA, USA, Jul. 2017.
- [111] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Trans. Antennas Propag.*, vol. 34, no. 3, pp. 276–280, Mar. 1986.
- [112] R. Roy and T. Kailath, "ESPRIT-estimation of signal parameters via rotational invariance techniques," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 37, no. 7, pp. 984–995, Jul. 1989.
- [113] *CBRS Communications Security Technical Specification, Version V1.0.0*, document WINNF-15-S-0065, Wireless Innovation Forum, Reston, VA, USA, Aug. 2016.
- [114] *WebTrust Principles and Criteria for Certification Authorities*, WebTrust, 2000. [Online]. Available: [https://cabforum.org/wp-content/uploads/WTBR2\\_2.pdf](https://cabforum.org/wp-content/uploads/WTBR2_2.pdf)
- [115] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol version 1.2," Internet Eng. Task Force, Fremont, CA, USA, RFC 5246, 2008.
- [116] *Operations for Citizens Broadband Radio Service (CBRS); GAA Spectrum Coordination: Approach 1, Version V1.0.0*, document WINNF-TR-2003, Wireless Innovation Forum, Reston, VA, USA, May 2019.
- [117] *Operations for Citizens Broadband Radio Service (CBRS); GAA Spectrum Coordination: Approach 2, Version V1.0.0*, document WINNF-TR-2004, Wireless Innovation Forum, Reston, VA, USA, May 2019.
- [118] *Operations for Citizens Broadband Radio Service (CBRS); GAA Spectrum Coordination: Approach 3, Version V1.0.0*, document WINNF-TR-2005, Wireless Innovation Forum, Reston, VA, USA, May 2019.
- [119] C. Tarver *et al.*, "Enabling a 'use-or-share' framework for PAL–GAA sharing in CBRS networks via reinforcement learning," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 3, pp. 716–729, Sep. 2019.
- [120] DARPA. *Spectrum Collaboration Challenge (SC2)*. Accessed: Mar. 16, 2021. [Online]. Available: <https://www.darpa.mil/news-events/spectrum-collaboration-challenge>
- [121] C. Bowyer, D. Greene, T. Ward, M. Menendez, J. Shea, and T. Wong, "Reinforcement learning for mixed cooperative/competitive dynamic spectrum access," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DySPAN)*, 2019, pp. 1–6.
- [122] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 270–282.
- [123] S. Ellis, A. Juels, and S. Nazerov, *Chainlink: A Decentralized Oracle Network*, Chainlink, Grand Cayman, Cayman Islands, 2017.
- [124] Y. Li *et al.*, "A survey on truth discovery," *ACM SIGKDD Explor. Newsl.*, vol. 17, no. 2, pp. 1–16, 2016.
- [125] *OFR: Electronic Code of Federal Regulations, Title 47: Telecommunication, Part 96—Citizens Broadband Radio Service*, Office Federal Register (OFR) Govt. Publ. Office, Washington, DC, USA, 2016.
- [126] C. E. Caicedo and M. B. Weiss, "The viability of spectrum trading markets," in *Proc. IEEE Symp. New Front. Dyn. Spectr. (DySPAN)*, 2010, pp. 1–10.



**Shanghao Shi** (Graduate Student Member, IEEE) received the B.S. degree from the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China, in 2019. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Virginia Tech, Blacksburg, VA, USA, supervised by Prof. W. Lou. His research interests lie in wireless security and IoT security.



**Yang Xiao** (Graduate Student Member, IEEE) received the B.S. degree from the School of Electrical and Information Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2014, and the M.S. degree from the Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI, USA, in 2017. He is currently pursuing the Ph.D. degree with the Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA, USA, supervised by Prof. W. Lou.

His research interests lie in network security, blockchain, and IoT security.



**Wenjing Lou** (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Florida in 2003.

She is currently the W. C. English Endowed Professor of Computer Science with Virginia Tech, Blacksburg, VA, USA. Her research interests cover many topics in the cybersecurity field, with her current research interest focusing on wireless network security, trustworthy AI, blockchain, and security and privacy problems in the Internet-of-Things systems.

Prof. Lou received the Virginia Tech Alumni Award for Research Excellence in 2018, the INFOCOM Test-of-Time Paper Award in 2020. She is a Highly Cited Researcher by the Web of Science Group. She was the TPC Chair for IEEE INFOCOM 2019 and ACM WiSec 2020. She was the Steering Committee Chair for IEEE CNS Conference from 2013 to 2020. She is currently a Steering Committee Member of IEEE INFOCOM and IEEE TRANSACTIONS ON MOBILE COMPUTING. She served as a Program Director at the U.S. National Science Foundation from 2014 to 2017.



**Chonggang Wang** (Fellow, IEEE) received the Ph.D. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2002.

He is a Principal Engineer with InterDigital Communications, Inc., Princeton, NJ, USA. He has over 20 years of experience in the field of communications, networking, and computing, including research, development and standardization of wireless systems, Internet of Things, quantum Internet, and Internet protocols. He currently leads a technical team with the Customer Project and Partners

Department, InterDigital's Research and Innovation Wireless Lab. In this role he and his team focus on research, innovation, and standardization of blockchain technology and its applications for future communications and computing systems (e.g., 5G/6G, decentralized machine learning, and federated learning). He and his team actively engage in collaborations with leading universities/institutions and industry to explore future networking and networked systems. He participates industry standardization activities with IETF, ETSI, 3GPP, oneM2M, and IEEE. He holds more than 100 U.S. granted patents. His research interests also include blockchain technologies and applications, 5G/6G systems, quantum Internet, edge computing, and intelligent IoT.

Dr. Wang is the Founding Editor-in-Chief of IEEE INTERNET OF THINGS JOURNAL. He is currently the Editor-in-Chief of IEEE NETWORK—The Magazine of Global Internetworking. He is a Fellow of the IEEE for his contributions to IoT enabling technologies.



**Xu Li** received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2009.

He is a Senior Staff Engineer with InterDigital Communications Inc., Princeton, NJ, USA. He has published technical papers on mainstream international journals and conferences, such as IEEE INFOCOM, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He has more than 70 U.S. approved/pending patent

applications. His research interests include 3GPP wireless systems, Internet of Things, blockchain technology, and data semantics. His current major activities include wireless system standardization (such as 3GPP, oneM2M, IETF, and W3C).

Dr. Li has been on the Technical Program Committee of major technical conferences, such as IEEE Globecom, IEEE ICC, and IEEE WCNC.



**Y. Thomas Hou** (Fellow, IEEE) received the Ph.D. degree from Tandon School of Engineering, New York University in 1998.

He is currently a Bradley Distinguished Professor of Electrical and Computer Engineering with Virginia Tech, Blacksburg, VA, USA, which he joined in 2002. He has published over 300 papers in IEEE/ACM journals and conferences. He holds five U.S. patents. He authored/coauthored two graduate textbooks, such as *Applied Optimization Methods for Wireless Networks* (Cambridge University Press,

2014) and *Cognitive Radio Communications and Networks: Principles and Practices* (Academic Press/Elsevier, 2009). His current research focuses on developing innovative solutions to complex science and engineering problems arising from wireless and mobile networks. He is also interested in wireless security.

Dr. Hou's papers were recognized by eight best paper awards from IEEE and ACM. He was named an IEEE Fellow for contributions to modeling and optimization of wireless networks. He was/is on the editorial boards of a number of IEEE and ACM transactions and journals. He was Steering Committee Chair of IEEE INFOCOM conference and was a member of the IEEE Communications Society Board of Governors. He was also a Distinguished Lecturer of the IEEE Communications Society.



**Jeffrey H. Reed** (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of California, Davis, in 1987.

He is the Willis G. Worcester Professor of Electrical and Computer Engineering with the Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA, USA. He is the Founding Director of Wireless @Virginia Tech, one of the largest wireless research groups in the United States, and the previous Interim Director and currently a CTO for the Commonwealth Cyber

Initiative for the State of Virginia. In 2010, he founded the Ted and Karyn Hume Center for National Security and Technology and served as its Interim Director. His current areas of expertise are in software-defined radios, AI-enabled 5G wireless, wireless security/information assurance, interference analysis, and vehicular communications.