Dissertação de Mestrado

Inatel
Instituto Nacional de Telecomunicações

Acesso Dinâmico ao Espectro Habilitado por Base de Dados e Internet das Coisas

ELIVANDER JUDAS TADEU PEREIRA

DEZEMBRO / 2020

ACESSO DINÂMICO AO ESPECTRO HABILITADO POR BASE DE DADOS E INTERNET DAS COISAS

ELIVANDER JUDAS TADEU PEREIRA

Dissertação apresentada ao Instituto Nacional de Telecomunicações, como parte dos requisitos para obtenção do Título de Mestre em Telecomunicações.

ORIENTADOR: Prof. Dr. Dayan Adionel Guimarães.

Santa Rita do Sapucaí
2020

Pereira, Elivander Judas Tadeu
P414a
Acesso Dinâmico ao Espectro Habilitado por Base de Dados e Internet das Coisas. / Elivander Judas Tadeu Pereira. – Santa Rita do Sapucaí, 2020.
86p.

Orientador: Prof. Dr. Dayan Adionel Guimarães.
Dissertação de Mestrado em Telecomunicações – Instituto Nacional de Telecomunicações – INATEL.
Inclui bibliografia e anexo.

1. Sensoriamento Espectral 2. Rádio Cognitivo 3. Redes IoT 4. Base de Dados 5. Alocação do Espectro 6. Mestrado em Telecomunicações. I. Guimarães, Dayan Adionel. II. Instituto Nacional de Telecomunicações – INATEL. III. Título.

CDU 621.39

Ficha Catalográfica elaborada pelo Bibliotecário da Instituição
CRB6-2718 – Paulo Eduardo de Almeida

FOLHA DE APROVAÇÃO

Dissertação defendida e aprovada em _____/_____/_____, pela comissão julgadora:

Prof. Dr. Dayan Adionel Guimarães
INATEL

Dr. Edielson Prevato Frigieri
ASML NETHERLANDS B. V.

Prof. Dr. Antônio Marcos Alberti
INATEL

Coordenador do Curso de Mestrado
Prof. Dr. José Marcos Câmara Brito

I still have a long way to go, but
I'm already so far from where I
used to be, and I'm proud of that!

Autor desconhecido

Aos meus pais,
Sr. Joaquim e Sra. Francisca.

Agradecimentos

Agradeço inicialmente a minha família que sempre foi minha força motriz. Meus pais, Joaquim A. Pereira e Francisca D. Pereira, meus irmãos Josimar D. Pereira e Leiliane A. Pereira, e minha sobrinha, Sabrina A. Pereira.

Agradeço a todos que confiaram em mim e me concederam uma forma de trabalho em Santa Rita do Sapucaí, o qual permitiu que me manter durante meus estudos. Em especial, Vinicius Fraga Correa, que me deu muitas oportunidades durante meu estágio na graduação, e Gesuel Beraldo Silva e família, que me acolheram e apoiaram durante todo esse tempo em seu restaurante. Um agradecimento aos inúmeros amigos, entre colegas e clientes, que fiz nos vários outros locais onde muito me orgulho de ter trabalhado.

Ao meu Orientador, Professor Dr. Dayan Adionel Guimarães, pelos ensinamentos, apoio e pelo amadurecimento que tive durante o mestrado. Agradeço ao Professor Dr. Arismar Cerqueira Sodré Junior pela motivação que me fez ingressar no mestrado. Aos Professores Dr. Luciano Leonel Mendes, Dr. Samuel Baraldi Mafra, Dr. Antônio Marcos Alberti, Dr. Rausley A. A de Souza pelos conhecimentos adquiridos ao longo do curso. Aos Professores Geraldo Gil Ramundo Gomes, Joao Bosco Assis Leite, Evandro Luiz Brandão Gomes, Vinícius A. Montgomery de Miranda, Daniel A. Nunes, Carlos Alberto Ynoguti, André Luís da Rocha Abbade, Edson Josias Cruz Gimenez, Egidio Raimundo Neto, Estevan Marcelo Lopes, Renzo Paranaiba Mesquita, dentre outros que cultivei grande amizade desde o curso da graduação.

Gostaria de agradecer a muitos outros amigos que fiz na faculdade e fora dela, com cada um pude adquirir um novo conhecimento e trocar experiências. Me lembro de todos neste momento, contudo, nomear um a um seria muito extenso. Aos que estiveram comigo, me apoiaram e me deram forças, o meu muito obrigado!

Elivander J. T. Pereira

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

5G	Quinta geração
AMQP	*Advanced Message Queuing Protocol*
Anatel	Agência Nacional de Telecomunicações
AWGN	Ruído aditivo Gaussiano branco (Additive White Gaussian Noise)
BF	Falsificação de *beacons* (*beacons falsification*)
CBRS	Serviço de rádio banda larga do cidadão (*citizens broadband radio service*)
CCC	Canal de controle cognitivo (*cognitive control channel*)
CR	Rádio cognitivo (*cognitive radio*)
CREW	*cognitive radio experimentation world*
CSMA/CA	Acesso múltiplo por verificação de portadora com prevenção de colisão (*carrier sense multiple access with collision avoidance*)
CSS	Sensoriamento espectral cooperativo (*cooperative spectrum sensing*)
DAG	Grafo acíclico dirigido (*directed acyclic graph*)
DAP	Protocolo de acesso à base de dados (*database access protocol*)
DLT	Tecnologia de registro distribuído (*distributed ledger technology*)
DoS	Negação de serviço (*denial of service*)
DSA	Acesso dinâmico ao espectro (*dynamic spectrum access*)
EESS	Serviço satélite de exploração terrestre (*Earth exploration satellite service*)
ESC	Capacidade de sensoriamento do ambiente (*environmental sensing capability*)
FC	Centro de fusão (*fusion center*)
FCC	Comissão federal de comunicações (*Federal Communications Commission*)
FPCA	Algoritmo de continuação de ponto fixo (*fixed point continuation algorithm*)
FSBaaS	*full-spectrum blockchain as a service*
GAA	Acesso geral autorizado (*general authorized access*)
GLDB	Base de dados de geolocalização (*geolocation database*)
GLRT	Teste de máxima verossimilhança generalizado (*generalized likelihood ratio test*)
HAGL	Altura da antena acima do nível do solo (*height above ground level*)
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos (*Institute of Elec-*

	trical and Electronic Engineers)
IETF	Internet Engineering Task Force
IoT	Internet das coisas (Internet of things)
ISM	Industrial, científica e médica (*industrial, scientific and medical*)
ITU	União Internacional de Telecomunicações (*International Telecommunication Union*)
KNN	K-ésimo vizinho mais próximo (*k-nearest neighbor*)
LTE	*long term evolution*
MAC	Controle de acesso ao meio (*media access control*)
MLME	Entidade de gerenciamento da camada MAC (*MAC layer management entity*)
MQTT	*Message Queuing Telemetry Transport*
n.	Número
Ofcom	Escritório de comunicações (*Office of Communications*)
p.	Página
PAL	Licenças de acesso prioritário (*priority access licenses*)
PAWS	Protocolo para acessar espaço em branco (*protocol to access white-space*)
PMSE	*programme making and special events*
PoS	Prova de participação (*proof of stake*)
PoW	Prova de trabalho (*proof of work*)
PSD	Densidade espectral de potência (*power spectral density*)
PU	Usuário primário (*primary user*)
PUE	Emulação do usuário primário (*primary user emulation*)
QoS	Qualidade de serviço (*Quality of Service*)
RAS	Serviço de rádio astronomia (*radio astronomy service*)
RF	Radiofrequência
SAS	Sistema de acesso ao espectro (*spectrum access system*)
SBW	Pequena janela de *backoff* (*small backoff window*)
SDR	Rádio definido por software (*software defined radio*)
SIG	*Special Interest Group*
SM	*spectrum manager*
SoC	*system-on-a-chip*
Spass	*spectrum sensing as a service*
SQDDP	*Sensor Query and Data Dissemination Protocol*
SRS	Serviço de pesquisa espacial (*space research service*)
SSDF	Falsificação dos dados de sensoriamento espectral (*spectrum sensing data falsification*)
SSIoT	Internet das coisas com sensoriamento espectral (*spectrum sensing Internet of things*)
SSL	*Secure Sockets Layer*
SU	Usuário secundário (*secondary user*)
SULI	Dedução da localização baseada na utilização do espectro (*spectrum utilization-based location inferring*)
TDMA	Acesso múltiplo por divisão de tempo (*time division multiple access*)
TLS	*Transport Layer Security*

TV	Televisão
TVWS	Espaço em branco na banda de TV (*TV white-spaces*)
WPAN	*wireless personal area network*
WSD	Dispositivo de espaço em branco (*white space device*)
WSDB	Base de dados de espaço em branco (*white space database*)

Lista de Símbolos

d	Distância entre transmissor e receptor
f	Frequência
γ	Limiar de decisão
G_R	Ganho da antena do receptor
G_T	Ganho da antena do transmissor
$\mathcal{H}_0$	Hipótese correspondente à ausência de sinal do UP
$\mathcal{H}_1$	Hipótese correspondente à presença de sinal do UP
h_R	Altura da antena do receptor
h_T	Altura da antena do transmissor
K	Menor número de decisões em favor de $\mathcal{H}_1$ na regra K-out-of-M
λ	Comprimento de onda
M	Número total de rádios cognitivos
P_{d}	Probabilidade de detecção
P_{fa}	Probabilidade de falso alarme
π	Número Pi
%	Por cento
P_R	Potência recebida
P_T	Potência transmitida

Resumo

Pereira, E.J.T. Acesso dinâmico ao espectro habilitado por base de dados e internet das coisas [dissertação de mestrado]. Santa Rita do Sapucaí: Instituto Nacional de Telecomunicações; 2020.

Com o crescimento no número de dispositivos sem fio, a escassez de espectro se tornou um problema. Diante deste problema, muitos órgãos reguladores pelo mundo começaram a estudar novas formas de aumentar a eficiência espectral das bandas de rádio-frequência. Dentre as alternativas encontram-se o acesso dinâmico ao espectro viabilizado por base de dados e também o uso de técnicas de acesso oportunista através de sensoriamento espectral. No entanto, é conhecido que esses modelos individualmente podem não levar à máxima eficiência possível, ou ainda, podem não assegurar a devida segurança aos usuários primários. Buscando resolver esses problemas, este trabalho traz um estudo com a idealização uma infraestrutura de sensoriamento espectral baseada em redes IoT, que associada com uma base de dados, provê todas as ferramentas necessárias para gerência do espectro, habilitação de redes secundárias oportunistas, garantia da segurança dos usuários, maior precisão e confiabilidade sobre a ocupação do espectro, além de um mercado de espectro entre os usuários baseado em contrato inteligente. Nesta concepção, a abordagem mais conservadora com uso de base de dados funciona em conjunto com a infraestrutura proposta para rede de sensoriamento, buscando manter-se atualizada com a mais precisa informação da ocupação do espectro em tempo real.

***Palavras-Chave*:** Sensoriamento espectral, rádio cognitivo, redes IoT, base de dados, alocação do espectro.

Abstract

Pereira, E.J.T. Dynamic spectrum access enabled by database and internet of things [master's thesis]. Santa Rita do Sapucaí: National Institute of Telecommunications; 2020.

With the growth in the number of wireless devices, spectrum scarcity has become an issue. Faced with this problem, many regulatory agencies around the world studied new ways to increase the spectral efficiency of radio frequency bands. Among the alternatives, the dynamic spectrum access is made possible by a database and also the use of opportunistic access techniques through spectrum sensing. However, it is known that these individual models may not lead to the maximum possible efficiency, or even, they may not ensure proper safety for primary users. Aiming to solve these problems, this work brings a study with the idealization of a spectrum sensing infrastructure based on IoT networks, which associated with a database, provides all the necessary tools for spectrum management, enabling opportunistic secondary networks, ensuring users security, greater accuracy and reliability on spectrum usage, as well as a spectrum market among users based on a smart contract. In this conception, the most conservative approach using a database works in conjunction with the proposed infrastructure for the sensing network, intending to keep up to date with the most accurate information on spectrum occupation in real-time.

***Keyords*:** Spectrum sensing, cognitive radio, IoT networks, database, spectrum allocation.

Capítulo 1

Introdução

A falta de bandas livres no espectro de radiofrequência (RF) é um conhecido obstáculo para a implantação de sistemas de comunicação e para o desenvolvimento de novos. Essa escassez de espectro se deve, principalmente, ao modelo de alocação de espectro predominantemente adotado pelas agências reguladoras, a alocação fixa. Neste modelo, o usuário titular ou usuário primário (*primary user*, PU) recebe uma licença de uso exclusivo para uma faixa de frequências que depende do serviço prestado. Outra política adotada é a alocação não-licenciada, como por exemplo, a banda industrial, científica e médica (*industrial, scientific and medical*, ISM). Nestas bandas, os usuários não necessitam fazer a aquisição de licenças com as agências reguladoras, o que resulta em alta eficiência no uso do espectro, contudo, diferentemente dos canais licenciados, diversos usuários competem entre si para se comunicar, levando à interferência mútua dos múltiplos sistemas de comunicação. A alocação fixa do espectro protege a qualidade de serviços oferecida aos usuários, mas leva a uma má utilização espectral.

Apesar da divisão e alocação de espectro ser uma atribuição das agências reguladoras, parte do governo local de cada país, um padrão mundial costuma ser seguido. Isso é feito segundo o Artigo 5 da regulamentação de rádio da União Internacional de Telecomunicações (*International Telecommunication Union*, ITU). A ITU provê referência para cada autoridade reguladora desenvolver seu plano nacional de alocação de frequências baseando-se em 3 macro-regiões globais, estas regiões são demonstradas na Figura 1.1. Nesta divisão, a região 1 compreende o continente africano, o europeu e o norte asiático (em especial, a maioria dos países membros da antiga União Soviética e a Mongólia); a região 2 estende-se ao continente americano; por último, a região 3 compreende a Oceania e os demais países asiáticos não inclusos na região 1. A referência dada pela ITU facilita a inter-operacionalidade entre sistemas de diversos países, facilita para fabricantes, agências reguladoras e usuários.

A demanda por faixas de espectro deve se agravar com a implantação massiva de dispositivos de Internet das coisas (*Internet of things*, IoT) e chegada da quinta geração (5G) das redes de comunicações móveis [2, 3]. É previsto um crescimento sem precedentes no número de conexões, taxas de dados e serviços nessas redes. Uma solução promissora para aliviar esse problema é a política de alocação dinâmica, idealizada com o surgimento do conceito de rádio cognitivo (*cognitive radio*, CR) [4]. O CR é

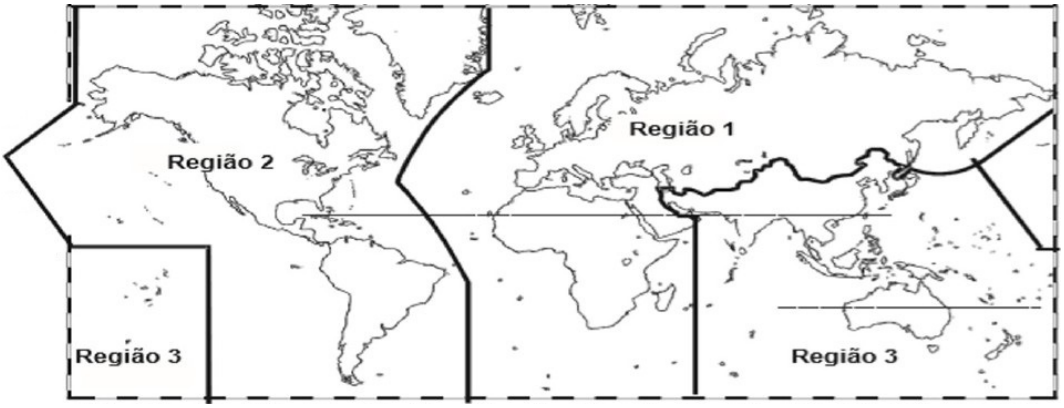


Figura 1.1: *Divisão das regiões da ITU para alocação de espectro [1].*

baseado na tecnologia de rádio definido por software (*software defined radio*, SDR), rádios de *hardware* versátil, capazes de mudar seus parâmetros de operação via *software* sem necessidade de alterações físicas. Esta solução é reconhecida como candidata a ser um dos principais facilitadores do 5G e de redes relacionadas [3].

A ideia de acesso dinâmico ao espectro viabilizada pelo CR tem ganhado bastante força, onde um usuário secundário (*secondary user*, SU), pertencente a uma rede não licenciada, utiliza bandas licenciadas na ausência do PU detentor desta licença, sob a condição de não causar interferência (ou em alguns casos, causar abaixo de um dado limiar) na comunicação do PU quando o mesmo retorna a transmitir. Partindo de uma iniciativa da comissão federal de comunicações (*Federal Communications Commission*, FCC), autoridade reguladora nos Estados Unidos, e seguido mais tarde por órgãos de outros países, o acesso dinâmico ao espectro (*dynamic spectrum access*, DSA) começou a ser visto como a solução para a baixa utilização espectral de bandas destinadas a alguns serviços, por exemplo a banda de televisão (TV). Além disso, o DSA visa permitir a conexão de regiões carentes de comunicações, como áreas rurais. Em [5], cerca de 28% dos canais na banda de TV foram identificados como vagos, mesmo em locais densamente habitados, este número chega a cerca de 60% em regiões menos habitadas nas áreas urbanas. O CR pode viabilizar o acesso dinâmico ao espectro baseando-se em três paradigmas [6]:

Interweave – consiste no uso oportunista do espectro, isto é, de forma intercalada, onde o SU de forma alguma pode transmitir ao mesmo tempo e na mesma frequência que o PU. Para isso, o CR deve ter plena ciência do ambiente de rádio, para utilizar as frequências livres ao longo do tempo e alternar entre elas, dessa forma, sem causar qualquer interferência ao PU.

Underlay – baseia no uso concorrente do espectro, tanto o PU quanto o SU podem transmitir simultaneamente na mesma frequência. O requisito deste paradigma é que a interferência causada pelo SU ao PU esteja sempre abaixo de um limiar aceitável pela rede primária.

Overlay – muito similar ao paradigma *underlay*, pode ser interpretado como o uso concorrente do espectro acrescido de mitigação de interferência, isto é, ambos os usuários da rede podem transmitir ao mesmo tempo, mas os SUs devem atuar de forma a cancelar a interferência que causarem às transmissões do PU. Podem, por

exemplo, atuar como nós repetidores para as mensagens do PU da rede.

Para que o rádio cognitivo possa operar sob um dos paradigmas acima citados, ele deve gozar de pleno conhecimento sobre o ambiente de rádio e/ou das características do PU. Dentre estas visões, os órgãos reguladores preferiram o uso oportunista. Este tipo de acesso é possível devido ao fato de que nem todas as faixas de frequência alocadas estão em uso constante pela rede primária em toda a área de cobertura mas, para isso, a ciência do ambiente de rádio se torna imprescindível.

O processo de ciência do ambiente de rádio é feito através de três abordagens. No primeiro caso, os SUs adquirem conhecimento sobre bandas de espectro desocupadas ao acessar um banco de dados de ocupação de espectro, onde encontram-se armazenados dados dos canais disponíveis. Este banco de dados é comumente referido como base de dados de geolocalização (*geolocation database*, GLDB) [7] ou base de dados de espaço em branco (*white space database*, WSDB) [8], sendo este último o termo mais adotado pelo Instituto de Engenheiros Eletricistas e Eletrônicos (*Institute of Electrical and Electronic Engineers*, IEEE) [9], pela FCC nos Estados Unidos, e pelo escritório de comunicações (*Office of Communications*, Ofcom) no Reino Unido [10,11]. A segunda abordagem que tem permitido o DSA é o uso da técnica de sensoriamento espectral [12, 13], utilizada pelo CR para detectar bandas de frequências vagas que serão acessadas pelos SUs. Por fim, é possível se combinar as fontes de informação, base de dados e sensoriamento espectral, numa última abordagem híbrida, em busca de melhores resultados.

O padrão IEEE 802.22 [9] é um exemplo no qual se aplica uma combinação das duas abordagens. Ele regulamenta como as informações de sensoriamento espectral, proveniente dos CR, bem como o mapa de disponibilidade de canais obtidos da WSDB, serão combinados para a tomada de decisão na entidade responsável existente no dispositivo mestre da rede, o chamado *spectrum manager* (SM).

Não importa a abordagem seguida, uma vez que o direito de licença do espectro ainda pertence ao PU, sempre que este retornar sua transmissão, o SU deve estar preparado para deixar aquele canal sem causar quaisquer interferência ao PU. Neste caso, o SU deve interromper sua transmissão e procurar por outra faixa de frequência livre.

1.1 Contextualização

Como citado anteriormente, a ciência do ambiente de rádio pode se dar de duas formas. Uma delas, através do sensoriamento espectral, que consiste em constantemente monitorar o espectro e usar de algoritmos de detecção para tentar encontrar canais fora de uso nas bandas de frequência em que o rádio deseja operar. Outra, é consultar o estado de ocupação do ambiente de rádio para a posição geográfica do rádio em uma base de dados.

O sensoriamento espectral feito individualmente por cada SU é pouco eficaz, com a tomada de decisões não confiáveis em relação à ocupação de uma determinada banda. Isso se deve principalmente ao desvanecimento por múltiplos percursos, sombreamento e o problema do terminal oculto. O sensoriamento espectral cooperativo (*cooperative spectrum sensing*, CSS) vem para solucionar este problema, fornecendo

decisões mais confiáveis ao explorar a diversidade espacial criada por vários SUs localizados em diferentes posições geográficas [12, 13]. Da mesma forma, a WSDB não é capaz de fornecer dados tão confiáveis sobre a ocupação do espectro. A principal razão para colocar em dúvidas a eficiência desta técnica são os modelos de predição de cobertura utilizados para modelar e obter essas informações [14], além da taxa com que as informações alimentam esses bancos de dados. A combinação do CSS com WSDB, similar ao previsto no padrão IEEE 802.22, é capaz de aprimorar o desempenho dos sistemas com maior precisão nos dados de ocupação de espectro. No entanto, essa combinação também pode sofrer com informações do banco de dados possivelmente desatualizadas e aumentar tanto a complexidade quanto o consumo de energia do terminal do SU, isso devido ao *hardware* dedicado à tarefa de sensoriamento espectral. Outro ponto negativo é que ainda não há aproveitamento dos dados colhidos ao longo do tempo através do sensoriamento espectral. Dentre as duas abordagens separadas, o modelo centralizado em base de dados de geolocalização teve muitos avanços com os órgãos reguladores dada a maior facilidade de implementação e maior controle sobre os dispositivos cognitivos, enquanto os modelos de sensoriamento espectral concentraram esforços no desenvolvimento de estatísticas de teste cada vez mais robustas e precisas.

Neste trabalho, em vez de apenas combinar as informações de ocupação de espectro provenientes do CSS e da WSDB, é proposto uma estrutura para DSA baseado em uma WSDB aprimorada, com alta confidencialidade, integridade, disponibilidade e autenticidade. Esta base de dados é alimentada pelas informações oriundas do sensoriamento espectral, valendo-se de uma rede de sensores de espectro não pertencentes à rede de SUs. As principais características desta rede são uma alta densidade de nós sensores e capacidade de rápida obtenção dos dados, afim de que o mapa de ocupação de canais tenha grande fidelidade espacial e possa fornecer informações em tempo real. As informações de ocupação espectral vindas da WSDB são utilizadas para dar suporte na tomada de decisão sobre o uso do espectro. A ideia é explorar a densidade e extensão geográfica de redes de dispositivos IoT, utilizando dessas redes como infraestrutura de suporte para realizar a tarefa de sensoriamento espectral, assim, retirando a necessidade de *hardwares* mais sofisticados da rede secundária. Alguns dispositivos IoT, com capacidade de estabelecer com precisão sua posição geográfica, são equipados com um módulo de sensoriamento espectral, transformando-os em dispositivos de Internet das coisas com sensoriamento espectral (*spectrum sensing Internet of things*, SSIoT). Posto isto, combinando as informações temporais e de predição de cobertura existentes na base de dados com as medições em tempo real obtidas pela rede SSIoT, espera-se melhorar a precisão dos dados e garantir novas oportunidades. Esses dados combinados são utilizados em seguida para realimentar a base de dados, de forma a mantê-la atualizada em tempo real, para que possa ser consultada com informações de máxima confiabilidade por redes secundárias ou pela própria rede IoT. Um grande facilitador para estrutura proposta é a tecnologia de registro distribuído (*distributed ledger technology*, DLT), que possibilita também a criação de um mercado direto de espectro, fim a fim entre os interessados, e a implementação do plano de controle da solução.

1.2 Contribuições e Estrutura do Trabalho

Dentre as contribuições deste trabalho, encontram-se:

- Revisão de necessidades e falhas dos modelos convencionais de compartilhamento de espectro.
- Concepção de uma nova infraestrutura de sensoriamento espectral baseada em redes de dispositivos IoT.
- Apresentação de oportunidades de uso de DLT para aumentar segurança do compartilhamento de espectro.
- Conceito de mercado secundário de alocação de espectro baseado em contrato inteligente para um cenário de alocação dinâmica do espectro.
- Prova de conceito para uso da tecnologia do modo adaptativo de saltos em frequência (*adaptative frequency hopping*, AFH) do protocolo Bluetooth para sensoriamento espectral, dando viabilidade dos módulos de sensoriamento idealizados para a rede de dispositivos IoT, com baixo custo e baixo consumo energético.
- Modelo de arquitetura para guiar a construção prática de uma base de dados para gerência do espectro.

O restante desta dissertação está organizado da seguinte forma: o Capítulo 2 traz uma revisão do cenário atual para compartilhamento de espectro, com grande enfoque em regulamentações já difundidas mundialmente; no Capítulo 3 são revisados trabalhos científicos correlatos que fundamentam ou contribuem para esta proposta; a arquitetura de rede IoT para sensoriamento espectral, tecnologias viabilizadores, oportunidades e desafios para sua construção englobam o Capítulo 4; por fim, o Capítulo 5 traz as conclusões e oportunidades existentes para trabalhos futuros. Esta dissertação também contempla no Apêndice I as pesquisas sobre uso do AFH para sensoriamento espectral e no Apêndice II o desenho de arquitetura para a base de dados de gerência de espectro para o compartilhamento dinâmico integrado com a infraestrutura proposta. Como resultado das pesquisas deste trabalho, foram publicados os seguintes artigos:

- D.A. GUIMARÃES, E.J.T. PEREIRA, A.M. ALBERTI e J.V.B. MOREIRA. Design Guidelines for Database-Driven Internet of Things-Enabled Dynamic Spectrum Access. Ad Hoc Networks (submetido).
- E.J.T. PEREIRA, D.A. GUIMARÃES e C.S. FONSECA. Sensoriamento Espectral via Modo Adaptativo de Saltos em Frequência do Padrão Bluetooth. *Simpósio Brasileiro de Telecomunicações, SBrT 2020*, Florianópolis, SC, Novembro 2020.

Capítulo 2

Métodos, Padrões e Regulamentações Existentes para DSA

PARA a compreensão do acesso dinâmico ao espectro, no contexto deste trabalho, é necessário fazer uma revisão das regulamentações das agências governamentais e dos padrões estabelecidos por entidades da área. As seções a seguir irão detalhar estes tópicos.

Os dois países que foram pioneiros e melhor regulamentaram seus serviços de telecomunicações para o DSA foram os Estados Unidos e o Reino Unido. Por este motivo, as regulamentações revisadas neste trabalho serão as estabelecidas pela FCC e Ofcom nestes países, respectivamente.

Dentre as padronizações, aquelas que merecem maior enfoque são os padrões IEEE 802.22, IEEE 1900.4 e o protocolo para acessar espaço em branco (*protocol to access white-space* , PAWS), dado a correlação com o presente trabalho. No entanto, vale ressaltar a existência de outros padrões para DSA, concebidos para operar nas frequências livres da faixa de TV, são eles: IEEE 802.11af (Super Wi-Fi ou White-Fi); IEEE 802.15.4m (*Wireless Personal Area Networks*) e IEEE 802.19.1 (*Wireless Coexistence*).

A partir da política de alocação fixa do espectro, não é uma tarefa trivial regulamentar o compartilhamento dessas bandas. O usuário primário tem garantido uma licença de uso exclusivo da faixa. Ao introduzir o compartilhamento do espectro, a entidade reguladora muda o caráter dessa licença de uso exclusivo para uma licença de garantia de operação livre de interferência. O uso da banda deixa então de ser exclusivo para ser prioritário e protegido.

Partindo de uma inciativa da FCC nos Estados Unidos, o DSA começou a ser estudado e regulamentado para o uso oportunista por redes secundárias. De forma a assegurar a proteção do PU, as principais regulamentações focaram nos métodos por onde os SUs obtém conhecimento sobre o ambiente de rádio.

Dentre as faixas de frequência que possuem grande potencial para políticas de acesso compartilhado ao espectro encontram-se os espaço em branco na banda de TV (*TV white-spaces* , TVWS). Além das faixas destinadas para radiodifusão televisiva, é conhecido que existem bandas utilizadas para a comunicação fixa por satélite muito

mal aproveitadas, que tem levado à abertura para o acesso dinâmico em frequências dentro das bandas S (2 a 4 GHz) e C (4 a 8 GHz) em alguns países [15]. Nos Estados Unidos, o serviço de rádio banda larga do cidadão (*citizens broadband radio service*, CBRS) é uma regulamentação de DSA para serviços operando na banda de 3.5 GHz, uma porção de espectro reservada para o Governo Federal dos EUA para evitar interferência nos sistemas de radares navais, estações de comunicação via satélite terrestres e nas comunicações de aeronaves [16]. Além disso, houve a liberação por completo da faixa de 6 GHz. Nesta última regulamentação, a FCC autorizou no início de 2020, o uso não licenciado de 1200 MHz entre 5.925 e 7.125 GHz [17].

2.1 Base de Dados de Espaço em Branco (WSDB)

A WSDB é uma das abordagens utilizadas para dar suporte ao processo de DSA. Essa base de dados pode armazenar vários tipos de informações, sendo a mais importante delas uma lista de ocupação do espectro baseada em geolocalização. Essa técnica é a mais bem detalhada pela autoridades reguladoras e já faz parte de padrões como o IEEE 802.22 [9], o IEEE 802.11af [18] e o PAWS [19]. Em 2014, a FCC designou dez administradores de banco de dados que seriam responsáveis por manter o serviço no país, dentre os quais, quatro deles estão atualmente certificados e a prestar o serviço: Spectrum Bridge; Iconectiv; Keybridge Global; e LS telcom [10]. Como nota, as empresas RadioSoft e Google também foram administradores de banco de dados aprovados e em operação, mas a RadioSoft foi adquirida pela LS telcom em 2014 e seus serviços foram unificados, o Google por sua vez encerrou seu projeto de TVWS em 2018 para priorizar um novo projeto direcionado ao CBRS.

A base de dados deve trabalhar fazendo uso de informações do terreno e modelos de propagação para definir as zonas de exclusão para os usuários secundários. Os dados do relevo são necessários para os cálculos de obstruções nos percursos. Dentre os modelos de propagação utilizados, pode-se usar modelos tão simples quanto o de propagação no espaço livre (*free space*) ou o modelo Egli.

Com base no modelo de propagação no espaço livre é possível estimar a potência de recepção através da Equação 2.1. Na equação, P_R é a potência recebida, P_T é a potência transmitida, G_T o ganho da antena do transmissor, G_R o ganho da antena do receptor, d é a distância entre os dispositivos e λ o comprimento de onda.

$$P_R = G_T G_R \left(\frac{\lambda}{4\pi d}\right)^2 P_T \tag{2.1}$$

O modelo de Egli possui maior precisão por considerar outras variáveis no cálculo, porém é um modelo para ser utilizado em frequências de até 900 MHz. A Equação 2.2 permite calcular a potência recebida através deste modelo. As variáveis adicionadas são h_T e h_R, as alturas das antenas do transmissor e receptor, respectivamente. f na equação denota a frequência de operação.

$$P_R = G_T G_R \left(\frac{h_T h_R}{d^2}\right)^2 \left(\frac{40}{f}\right)^2 P_T. \tag{2.2}$$

Contudo, os dois modelos acima ainda não são os mais indicados para o uso nas bases de dados de geolocalização. Três modelos mais precisos e utilizados são: (i) o modelo Longley-Rice, (ii) o modelo baseado em curvas-F e (iii) o modelo Okumura [20]. Estes modelos aumentam a precisão da estimação de interferência. A geometria do relevo e uma série de novas variáveis são incluídas no processo para obter estes resultados. Nos Estados Unidos a abordagem recomendada pela FCC e utilizada pelos administradores de bases de dados são as curvas-F de propagação [20, 21]. No Japão, o administrador NICT optou pelo modelo Okumura para uso no seu projeto de WSDB.

Dentre os principais pontos a serem destacados deste modelo de compartilhamento, destacam-se: (i) o método utilizado pela comunicação entre os dispositivos secundários e a base de dados; (ii) o papel de cada personagem no processo (PU, SU e WSDB); e (iii) os parâmetros devem ser informados no processo por parte dos usuários.

A interface do PAWS é um exemplo de como um dispositivo secundário pode acessar a WSDB. Isso é feito através do estilo de "requisição-resposta" presente no protocolo *Hypertext Transfer Protocol* (HTTP). De forma resumida, este procedimento é ilustrado na Figura 2.1 [22]. O dispositivo secundário utiliza da interface do PAWS em um processo de inicialização e registro com o sistema de gerência da base de dados. Quando o dispositivo secundário (neste caso o mestre da rede) recebe a resposta de registro, ele efetua em seguida a solicitação pelo estado do espectro para a sua geolocalização, informada no processo anterior. Através da interface do PAWS são checadas as credenciais dos dispositivos, emitindo-se uma requisição para o algoritmo de alocação de canais pelo estado do espectro logo após a validação das credenciais feita pela base de dados. Este algoritmo consulta os dados existentes na base de dados, processa e responde através da interface o estado do espectro para aquela determinada localização. O dispositivo secundário mestre requisita através da interface a alocação para o uso de um canal específico dentre aqueles que foi informado estarem livres. O algoritmo de alocação responde a requisição para o canal solicitado. Uma vez recebida a resposta pelo dispositivo secundário mestre, uma notificação é emitida e a partir do recebimento da confirmação que o processo foi concluído, o mesmo está apto a habilitar os dispositivos escravos e fazer suas transmissões.

Cada personagem desempenha um papel neste modelo de regulamentação. O PU fornece dados à respeito de sua operação para que a base de dados possa definir as zonas de exclusão visando proteger os seus direitos de licença. Contudo, as informações na base dados tem caráter estático e os operadores primários podem adotar comportamentos egoístas, ou simplesmente por não ter uma motivação, não atualizar os dados na WSDB para informar oportunidades espectrais. Uma das vantagens no modelo que será apresentado mais a frente nesta dissertação, que vislumbra um mercado secundário de espectro, é o incentivo ao detentor da licença em alocar ela quando o canal estiver fora de uso, uma vez que o mercado através de contratos inteligentes pode ser vantajoso. O papel do SU mestre é coordenar a rede secundária com base na interação com a WSDB e habilitar a transmissão dos rádios escravos. No início do processo, apenas o dispositivo mestre possui comunicação com a base de dados e é capaz de efetuar o registro para descobrir as oportunidades espectrais. A WSDB desempenha o papel principal para assegurar a proteção dos usuários protegidos (PU) e viabilizar o compartilhamento para os dispositivos de redes secundárias.

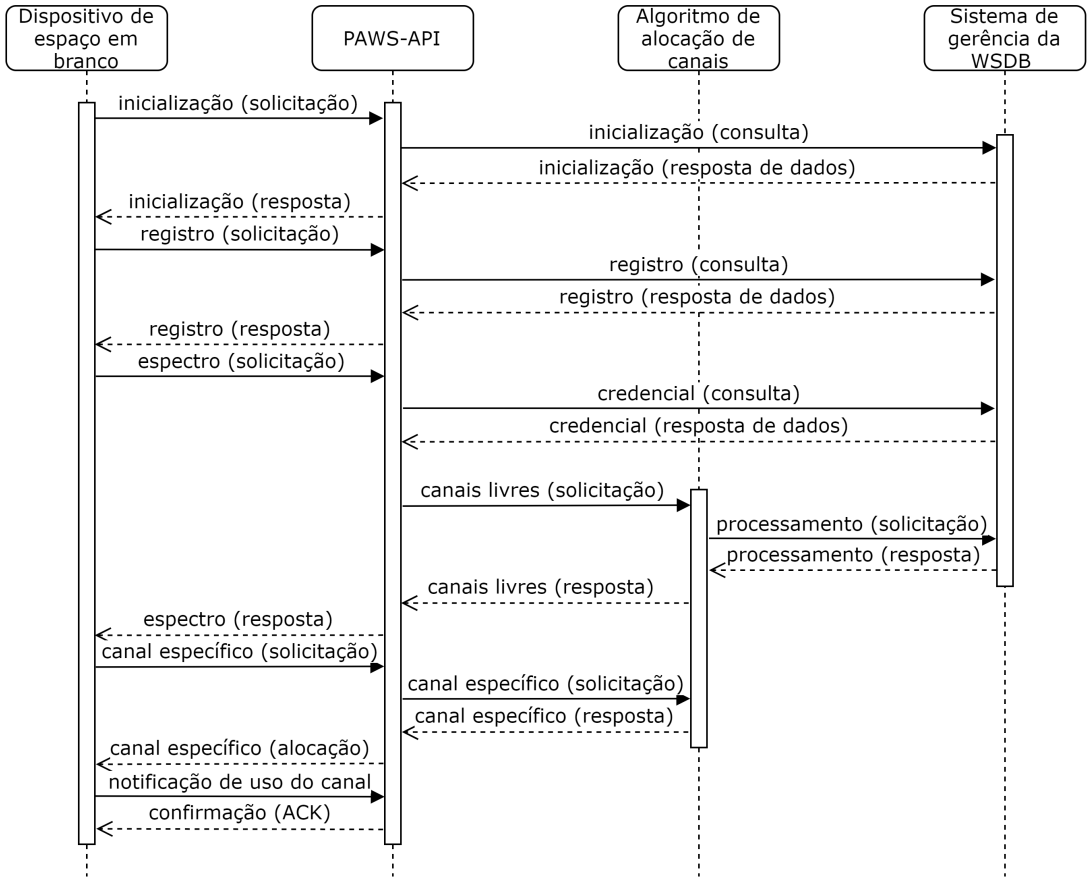
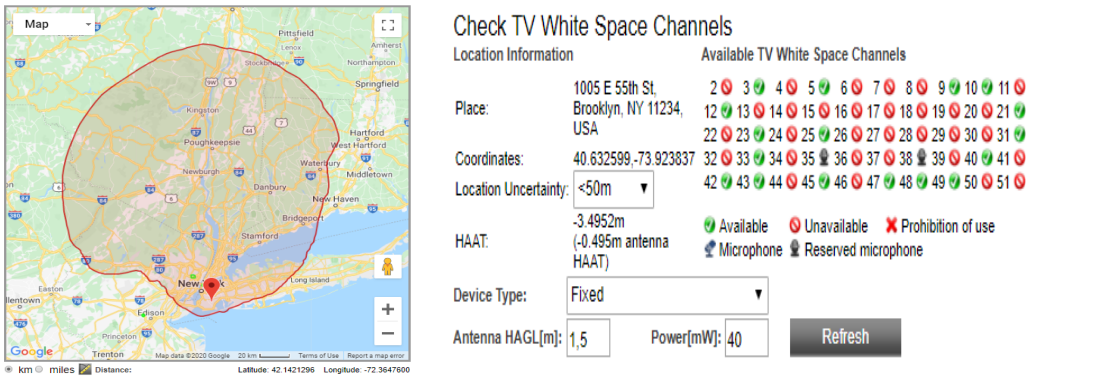


Figura 2.1: *Compartilhamento de espectro assistido por base de dados utilizando o PAWS. Adaptado de [22].*

Os parâmetros necessários para o funcionamento da WSDB variam conforme a regulamentação de cada órgão. Por parte do usuário primário, os parâmetros a serem informados incluem os dados necessários para a estimação de cobertura e informações de registro da rede na base de dados. O dispositivo mestre da rede secundária precisa prover a geolocalização da sua rede, dados que identifiquem o operador da rede, identificação dos dispositivos (em geral, código de homologação do órgão regulador e números do fabricante como *serial number* e *part number*), além dos seus parâmetros de operação, que incluem especificação de emissão em canais adjacentes, potência e a altura da antena acima do nível do solo (*height above ground level*, HAGL). Ao responder uma requisição, a WSDB também informa os parâmetros permitidos, os quais devem ser respeitados pelos SUs.

A abordagem de compartilhamento de espectro assistida pela WSDB apresenta duas principais desvantagens. Uma delas é sua confiabilidade, que depende da precisão do modelo de predição de cobertura utilizado; a outra é não a garantir atualização em tempo real para as informações sobre o uso do espectro. Os modelos de predição de cobertura adotados podem não refletir a ocupação do espectro em certos locais [14,23]. A Figura 2.2 demonstra a interface de usuário e como são apresentados os dados na WSDB do administrador LS Telcom [24]. É mostrado na Figura 2.2a a zona de exclusão para o canal 27 em específico, em nenhuma localização dentro da zona vermelha



(a) *Zona de exclusão para o canal 27.* (b) *Disponibilidade de canais no Brooklyn, Nova Iorque.*

Figura 2.2: *Interface da base de dados do administrador LS Telcom.*

este canal está livre para uso. Essa zona de exclusão é definida baseada no cálculo da cobertura do sinal do PU, e um raio maior assegura que o sinal dos SUs não sejam interferentes para os rádios primários. Na Figura 2.2b, pode se ver parâmetros informados ao serviço e a resposta do estado todos os canais para aquela determinada localização, neste caso, para um ponto no bairro do Brooklyn em Nova Iorque.

Outro ponto importante a se destacar no compartilhamento em TVWS baseado nessa abordagem é que trata-se de um método muito conservador. O uso da WSDB cria zonas muito mais extensas do que o necessário para a proteção dos PUs, fato que demonstra que este tipo de regulação não otimiza a eficiência do uso do espectro ao máximo. Além disso, não há diferenciação no uso interno (*indoor*) ou externo (*outdoor*). O perfil de uso interno, com menores potências de transmissão, com alta atenuação por obstáculos como paredes, não pode ser equiparado à sistemas de comunicação externos, de maior potência e com transmissão no espaço livre.

2.2 Sensoriamento Espectral

Diferente de acessar uma base de dados para obter conhecimento dos PUs e das oportunidades, o sensoriamento espectral faz isso utilizando do processamento digital de sinais amostrados. O sensoriamento espectral pode ser feito de forma individual, onde cada CR coleta amostras do sinal, efetua o processamento, decide pela presença ou não do PU e faz sua transmissão quando considerar o canal livre. O ponto negativo deste modelo é a sua precisão e a susceptibilidade ao chamado problema do terminal oculto, onde por não ter visão do PU, o CR pode ser levado a tomar uma decisão errada. No CSS, vários CRs distribuídos espacialmente colhem amostras, podendo tomar uma decisão local primeiro ou encaminhar diretamente as amostras para um centro de fusão (*fusion center*, FC), fazendo uso de um canal de controle e técnicas de acesso múltiplo por divisão de tempo (*time division multiple access*, TDMA). Estes métodos de envio são chamados de fusão de decisões (*hard decision*), o envio das decisões locais tomadas em cada rádio, e fusão de dados (*soft decision*), o envio das amostras colhidas. O método de fusão de dados performa melhor, no entanto, consome mais recursos de transmissão no canal de controle e processamento no FC. No caso da fusão de decisões, o FC utiliza de um algoritmo baseado nas regras OU, E ou K-em-

M (*OR, AND ou K-out-of-M*) para tomar a decisão global a respeito do espectro e em seguida reportá-la aos CRs através do canal de controle. O sensoriamento espectral tem como princípio um teste de hipóteses binário, onde a hipótese $\mathcal{H}_0$ representa a ausência de sinal primário e a hipótese $\mathcal{H}_1$ indica que o PU está transmitindo. No caso da fusão de dados, uma estatística de teste é criada com o processamento do sinal recebido e analisado pelos CR, no FC é feita a decisão em favor de uma hipótese de acordo com um limiar γ. Algumas estatísticas de teste comuns são: detector de energia, filtro casado, detecção de cicloestacionariedade e detecção por autovalores [12, 13].

Dentre os desafios envolvidos no sensoriamento espectral, a técnica utilizada é um dos pontos críticos. O desempenho do método é fortemente afetado de acordo com a técnica utilizada. Contudo, certos requisitos necessários podem limitar o uso de determinadas estatísticas com desempenho superior. Por exemplo, algumas estatísticas, como filtro casado, apresentam alto desempenho mas requerem conhecimento prévio das características de transmissão do PU, de fato, esta condição é dificilmente atendida na prática. Quando determinados parâmetros não são conhecidos, duas opções podem ser adotadas, aferir uma distribuição normalmente não-informativa, como a distribuição Gama, para os parâmetros ou estimá-los através de dados obtidos por observações. Um teste popular nesta abordagem é o teste de máxima verossimilhança generalizado (*generalized likelihood ratio test*, GLRT).

Para medir o desempenho da técnica de sensoriamento espectral são utilizadas duas métricas. Uma delas é a probabilidade de detecção (P_d) do sinal, que é definida como sendo a probabilidade de se decidir em favor da hipótese $\mathcal{H}_1$ sob a presença de sinal da rede primária, $P_\mathrm{d} = \Pr\{\text{decisão} = \mathcal{H}_1|\mathcal{H}_1\}$. A outra é a probabilidade de falso alarme (P_fa), que defini-se como a probabilidade de se decidir em favor da hipótese $\mathcal{H}_1$ na ausência do PU, isto é, interpretar que o canal está em uso por causa do ruído, $P_\mathrm{fa} = \Pr\{\text{decisão} = \mathcal{H}_1|\mathcal{H}_0\}$. Para que o sensoriamento espectral tenha um bom desempenho, a P_d deve ser maximizada a fim de que não sejam causadas interferências na rede primária, ao mesmo tempo, é desejado que a P_fa seja minimizada para que não se desperdice as oportunidades espectrais, garantindo assim a máxima vazão. Como exemplo, o padrão IEEE 802.22 estabelece como requisitos uma P_fa máxima de 0.1, uma P_d mínima de 0.9 e uma sensibilidade -116 dBm para sinais de televisão digital [25].

A utilização comercial de sensoriamento espectral não seguiu todo o potencial que a tecnologia oferece. A relação entre vantagens e desvantagens, quando ponderada para redes específicas, pode não se mostrar lucrativa. O processo de sensoriamento espectral, por necessitar de uma varredura constante de faixas de frequência, demanda um maior consumo energético. Quando isso é aplicado em dispositivos limitados em energia, como *smartphones*, move-se em direção contrária a um de seus pilares da evolução tecnológica que é a autonomia de bateria. O *hardware* necessário para realizar esta tarefa possui maior complexidade, sendo assim, acrescenta um custo extra ao dispositivo. Para a viabilidade comercial de uma tecnologia, redução de custos e aumento da escalabilidade do produto são fundamentais [26]. Em contrapartida, esta tecnologia dota a sua rede com importantes capacidades. O sensoriamento espectral permite a obtenção dos dados em tempo real (ou o mais próximo possível desta condição), permite o CR conhecer o estado ambiente de rádio no exato momento em que for necessário trans-

mitir. Além disso, os dados obtidos por sensoriamento espectral são mais precisos para caracterizar o ambiente de rádio na região onde se encontra a rede secundária. Modelos de predição de cobertura e a criação de zonas de exclusão no entorno do PU diminuem as possibilidades de uso do espectro em termos geográficos. Além disso, há a possibilidade de utilizar os dados de sensoriamento espectral para auditar a operação de SU devidamente registrados ou fazer a detecção de usuários ilegais em operação.

A utilização do sensoriamento espectral pode não ser lucrativa para todo tipo de dispositivo ou rede de dispositivos. No entanto, a sua inserção no contexto de uma rede distribuída e dedicada para a tarefa, capaz de prover os dados colhidos ao maior número de usuários é uma proposta voltada a otimizar a relação custo-benefício do sensoriamento espectral, tornando-o uma tecnologia altamente viável e lucrativa nesse cenário.

No sensoriamento espectral também existem desvantagens quanto à segurança do processo. Ataques podem ser feitos à rede secundária visando obter vantagens na operação ou até a negação do serviço. Neste caso, ocorrem riscos tanto para as redes secundárias no processo de DSA quanto ao PU de receber interferência de um SU malicioso. Detalhes sobre aspectos de segurança das duas abordagens serão dados na Seção 4.4.

2.3 WSDB Combinada com Sensoriamento Espectral

Para melhorar a confiabilidade das duas abordagens anteriores, o sensoriamento espectral pode ser utilizado para auxiliar a WSDB, formando uma solução híbrida. Nesse caso, a WSDB é explorada a fim de ter informações prévias dos canais a sensorear e ajudar a evitar o problema do terminal oculto. O sensoriamento espectral por sua vez age para detectar sinais protegidos que podem não estar registrados na base de dados, por exemplo, microfones sem fio. Vale ressaltar que no Reino Unido, o Ofcom não permite que dispositivos operem com base apenas na abordagem de sensoriamento espectral, ou seja, obrigatoriamente eles devem estar em conformidade com a WSDB. Um dos argumentos do Ofcom para isso é que o sensoriamento espectral pode não funcionar corretamente em alguns canais dependendo do serviço prestado, que são os serviço de rádio astronomia (*radio astronomy service*, RAS), serviço satélite de exploração terrestre (*Earth exploration satellite service*, EESS) e serviço de pesquisa espacial (*space research service*, SRS) [11, 27].

Na abordagem híbrida, o papel de ambos os métodos pode variar muito. Por exemplo, é possível utilizar os dados existentes na base de dados diretamente na rede cognitiva no processo de sensoriamento, sendo estes dados então, utilizados para dar conhecimento prévio do ambiente de rádio. Isso permite otimizar o processo de sensoriamento e utilizar taxas de amostragem abaixo da taxa de Nyquist, o que reduz a complexidade computacional e o tempo gasto para realizar a tarefa em função do menor volume de dados gerados, mas sem comprometer o desempenho do sensoriamento espectral. Tal abordagem pode ser vista mais comumente em trabalhos científicos [14, 28–30].

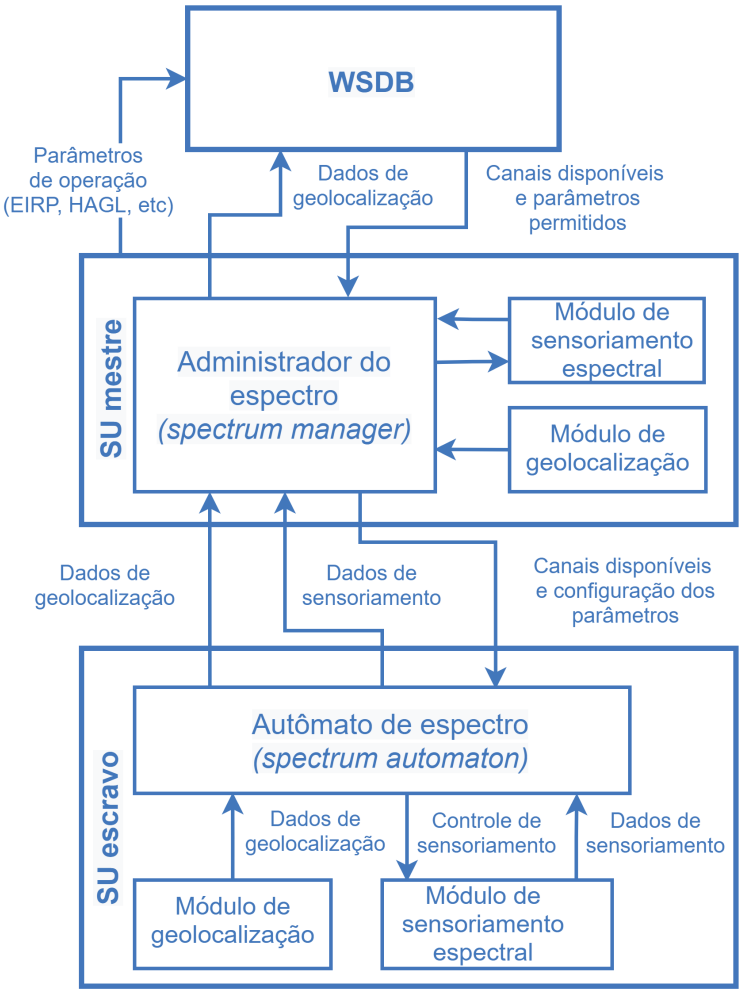


Figura 2.3: *Modelo de arquitetura híbrida no padrão IEEE 802.22 com sensoriamento espectral e WSDB.*

Outra opção que pode ser abordada é utilizar as informações de ambas as fontes e, através de políticas aplicadas em entidades da camada controle de acesso ao meio (*media access control*, MAC), ponderar o peso de cada fonte para a tomada de decisão. A Figura 2.3 ilustra o conceito de um modelo híbrido genérico seguindo o padrão IEEE 802.22. Uma entidade muito importante nesta arquitetura é o *spectrum manager*, que faz parte da entidade de gerenciamento da camada MAC (*MAC layer management entity*, MLME). Seu principal papel, neste contexto, é reunir os dados de sensoriamento espectral dos CRs e as informações de ocupação do espectro da WSDB, posteriormente aplicar políticas estabelecidas para decidir sobre a disponibilidade do espectro e reportar sua decisão aos CRs, de forma a habilitar todos os dispositivos secundários escravos conectados à rede. Essas políticas incluem a aplicação dos requisitos de proteção dos usuários titulares estabelecidos pelos órgãos reguladores e a classificação dos canais de acordo com 6 grupos (não permitido, operacional, backup, candidato, protegido e não classificado). O SM controla os parâmetros de operação e gerencia o acesso aos recursos espectrais para toda a célula [31, 32].

Além destas alternativas, a WSDB pode ser utilizada como infraestrutura para o

sensoriamento espectral, neste ponto, a base de dados atua como nó central recebendo as informações, processando e retornando o resultado para os CR. Um exemplo pode ser o uso de uma base de dados local centralizando os dados de sensoriamento [33]. Nesta dissertação, o enfoque será dado a um modelo similar, onde uma base de dados global é mantida com informações obtidas por sensoriamento e da WSDB convencional. A base de dados traz como vantagem ao sistema a capacidade de compartilhamento de informações, como as de sensoriamento, entre redes secundárias, além de permitir maior gerência do espectro.

A principal vantagem dessa abordagem é o uso de informações de espaço em branco tanto espaciais quanto temporais [15]. No entanto, embora melhore o cenário do DSA, vale ressaltar que os terminais de SU, que podem ser simples como nós sensores ou sofisticados como *smartphones*, ainda precisam estar equipados com *hardware* dedicado para a tarefa de sensoriamento espectral. Os dados do sensoriamento espectral são utilizados apenas na combinação com as informações da base de dados no processo de tomada de decisão, toda essa informação é perdida após este processo e eles não podem ser acessados por outros dispositivos.

2.4 Regulamentações: FCC e Ofcom

O processo de regulamentação DSA nos Estados Unidos foi pioneiro no mundo, iniciando-se os estudos ainda em 2004. Em 2006, a FCC definia os primeiros critérios de operação compartilhada na banda de TV e que seriam aperfeiçoados nos anos seguintes. Este processo foi bem longo e serviu de base para o Ofcom regulamentar de forma similar no Reino Unido, divergindo no entanto em alguns pontos.

Os dispositivos dos SUs são comumente referidos por estas agências como dispositivos de espaço em branco (*white space device*s, WSDs). Os WSDs são classificados de forma diferente de acordo com cada agência reguladora. A FCC opta por classificar estes dispositivos em quatro grupos com base no caráter de operação do dispositivo, já o Ofcom adota uma classificação de apenas duas classes baseadas na função exercida pelo dispositivo.

Para entender as quatro classes estabelecidas nos Estados Unidos, precisa-se entender o critério adotado pelo órgão regulador. Como a FCC regulamentou o serviço de TVWS baseado em base de dados e sensoriamento, o primeiro ponto que a agência adotou para fazer essa divisão foi o caráter de mobilidade do equipamento, que é um quesito muito importante quando se trabalha com base de dados. No caso do sensoriamento espectral foi criada uma classe à parte. As quatro classes para WSDs são: (i) fixo, (ii) móvel modo I, (iii) móvel modo II e (iv) baseado apenas em sensoriamento. Os dispositivos fixos são equipamentos que uma vez instalados não terão sua posição alterada e que possuem a capacidade de conexão com a WSDB, capazes de se registrar e habilitar a operação dos demais dispositivos da rede secundária, são portanto, os dispositivos mestres já citados no decorrer deste trabalho. Os dispositivos móveis, que alterarão sua geolocalização com o tempo, podem ser de modo I ou modo II. O modo I é uma classificação para o que já se definiu como dispositivo escravo, que não possui capacidade de conexão com a WSDB e é integralmente dependente do equipamento mestre para ser ativo e entrar em operação. O modo II pode ser descrito como

um dispositivo mestre que pode ter sua posição alterada com o tempo. Os dispositivos baseados apenas em sensoriamento são aqueles que não possuem qualquer forma de acesso à WSDB, seu funcionamento é habilitado pela detecção ou não do sinal do PU através de sensoriamento espectral [31].

O Ofcom por sua vez estabeleceu uma classificação dos WSD baseada na função que o dispositivo exerce na rede. Sendo assim, a divisão foi feita apenas entre o dispositivo mestre e o escravo. Os dispositivos baseados apenas em sensoriamento espectral foram excluídos do cenário regulatório e a WSDB desempenha o principal papel no compartilhamento do espectro. Para o órgão, a característica de estar conectado ou não com a base de dados foi o fator mais importante ao estabelecer a diferenciação entre os tipos de dispositivos.

Tabela 2.1: *Requisitos de operação para as classes de WSD segundo a FCC.*

	Fixo	Móvel modo I	Móvel modo II	Apenas sensoriamento
Máxima potência transmitida (potência isotrópica irradiada efetiva (*effective isotropic radiated power* , EIRP))	4 W; não permitido em canais adjacentes a usuários protegidos	100 mW; 40 mW em canais adjacentes a usuários protegidos	100 mW; 40 mW em canais adjacentes a usuários protegidos	50 mW
Limite de densidade espectral de potência (*power spectral density*, PSD) na banda do canal em uso (100 kHz)	12.6 dBm; não permitido em canal adjacente aos UPs	2.6 dBm; -1.4 dBm em canal adjacente aos UPs	2.6 dBm; -1.4 dBm em canal adjacente aos UPs	-0.4 dBm
Limite de PSD na banda dos canais adjacentes (100 kHz)	-42.8 dBm	-52.8 dBm; -56.8 dBm em canal adjacente aos UPs	-52.8 dBm; -56.8 dBm em canal adjacente aos UPs	-55.8 dBm
Canais permitidos	2, 5-36, 38-51	21-36, 38-51	21-36, 38-51	21-36, 38-51
Faixas de frequências permitidas (MHz)	54-60, 76-88, 174-216, 470-608, 614-698	512-608, 614-698	512-608, 614-698	512-608, 614-698
Método de descoberta de canal disponível	WSDB	WSDB	Obtido através de um dispositivo fixo ou modo I	Sensoriamento do espectro
Taxa de checagem da disponibilidade de canal	1 vez ao dia	1 vez ao dia ou após deslocar-se 100 m	1 vez por minuto	1 vez por minuto
Precisão dos dados de geolocalização	< 50 m	< 50 m, atualização a cada minuto	N/A	N/A
Sensibilidade de sensoriamento	N/A	N/A	N/A	TV digital: -114 dBm (6 MHz) TV analógica: -114 dBm (100 kHz) Microfones sem fio: -107 dBm (200 kHz)
Distância mínima de separação para microfones sem fio	1 km	400 m	400 m	N/A

Para cada classe de dispositivos, foram definidos os respectivos requisitos e parâmetros de operação. Dentre os mais importantes que variam conforme cada classe, estão: a máxima EIRP, o limite de PSD na banda e nos canais adjacentes, precisão dos métodos de geolocalização e de sensoriamento.

A EIRP para dispositivos fixos pode ser de até 4 W, dispositivos móveis podem transmitir tipicamente até 100 mW quando não estiverem operando em canal adjacente a um usuário protegido, neste caso, o limite é reduzido para 40 mW, os dispositivos baseados apenas em sensoriamento podem transmitir uma EIRP de até 50 mW.

Dispositivos fixos possuem regras mais rígidas para operação, por exemplo, não são autorizados a transmitir em canais adjacentes a usuários protegidos devido à sua maior potência de transmissão. Nos canais que estiverem operando, a PSD máxima por cada 100 kHz de banda deve ser de 12.6 dBm, já nos canais vizinhos, não deve ultrapassar -42.8 dBm. Dispositivos móveis possuem uma variação nestes valores caso o canal que estejam a utilizar seja adjacente ao canal de um usuário protegido. A Tabela 2.1 resume os principais requisitos para as diferentes classes de WSDs [31].

No Reino Unido, os canais de TV digital são divididos em bandas de 8 MHz em vez dos 6 MHz como é feito nos Estados Unidos. A faixa de canais definida para o DSA estende-se do canal 21 ao canal 60 (470 à 790 MHz), exceto pelo canal 38 que é reservado para dispositivos auxiliares de produção de conteúdo, como microfones sem fio. No que diz respeito à máxima EIRP permitida para os WSDs, o valor irá variar de acordo com cada canal, mas o maior valor permitido é de 4 W para ambas as classes de dispositivos [34].

Na Tabela 2.2 são demonstradas as principais diferenças entre as funções desempenhadas pela base de dados nas regulamentações dos dois órgãos, as informações que a WSDB deve prover aos WSD, o tempo padrão de validade dos dados, a precisão de geolocalização e os canais reservados para os WSD. Dentre estas diferenças destacam-se a precisão de geolocalização, que no Reino Unido foi flexibilizada para 100 m, e os dados que a WSDB deve fornecer ao dispositivo mestre que se conectar à ela.

No Reino Unido, o Ofcom adotou uma política ligeiramente diferente para definir a disponibilidade de canais, em vez de basear-se em modelos de predição de cobertura como na abordagem feita pela FCC, a disponibilidade de canal é obtida a partir do histórico de dados coletados das transmissões de radiodifusão ao longo de todos os anos [31].

Dentre os padrões que estão em conformidade com estas regulamentações, o PAWS desenvolvido pelo Internet Engineering Task Force (IETF) é um protocolo que estabelece a interface de comunicação entre a WSDB e os WSDs, enquanto isso, o IEEE 802.22 inclui todo o detalhamento e requisitos de arquitetura em camada física para os rádios. Dentre os pontos que o PAWS abrange estão: (i) descoberta da base de dados, (ii) inicialização, (iii) registro dos dispositivos, (iv) consulta do espectro livre, (v) notificação do uso do espectro e (vi) validação dos dispositivos [31]. O padrão IEEE 802.22 estende-se às especificações de camada física e de MAC, como o tipo e ordem de modulação, os códigos corretores de erro, a estrutura e o tempo de quadro, as entidades de controle como o já citado SM, dentre outras.

Tabela 2.2: *Comparativo regulamentações da FCC e Ofcom para WSDB.*

	FCC	Ofcom
Dados que a WSDB deve fornecer à rede secundária	Canais de TV disponíveis.	1 - Frequências de início e fim das bandas disponíveis; 2 - Níveis máximos de potência; 3 - Duração da validade dos dados; 4 - Número máximo de canais de TV contíguos; 5 - Número máximos de canais de TV em que os SUs podem transmitir; 6 - Área geográfica onde os parâmetros de operação são válidos; 7 - Níveis máximos de potência para operação multi-canal.
Duração da validade dos dados (padrão)	1 h	2 h
Precisão mínima dos dados de geolocalização	50 m	100 m
Canais reservados para SUs	1	0

2.5 Sumário

Esta seção busca trazer um resumo para o fácil entendimento dos pontos abordados ao longo deste capítulo. Os demais capítulos também seguirão esta didática, com seções sumário, para melhor compreensão do leitor.

Tabela 2.3: *Comparativo dos métodos para conhecimento do ambiente de rádio.*

Abordagem	Vantagens	Desvantagens
Base de dados (WSDB)	Menor custo e facilidade de implantação, centralização e maior controle.	Baixa taxa de atualização dos dados, modelos de predição imprecisos e zonas de proteção muito extensas.
Sensoriamento espectral	Informação em tempo real, fidelidade espacial e independência das redes.	*Hardware* mais caro e complexo, consumo energético e restrição da informação localmente.
Base de dados (WSDB) + Sensoriamento espectral	Redução da complexidade de sensoriamento, maior precisão dos dados ou redundância de fontes de informação.	*Hardware* mais caro e complexo, consumo energético e má definição do papel de cada tecnologia.

A Tabela 2.3 traz um comparativo de vantagens e desvantagens no que compete aos métodos para se obter ciência do ambiente de rádio abordadas nas Seções 2.1, 2.2 e 2.3. O uso de uma WSDB para habilitar o DSA proporciona como vantagens um menor custo de implantação, uma vez que centraliza toda a solução em uma base de dados controlada por um administrador aprovado, e também maior controle em função do registro das redes na própria base de dados. Por outro lado, os dados presentes na WSDB costumam ser quase estáticos e modelados de forma imprecisa, além de estenderem demasiadamente as zonas de proteção. No que diz respeito ao uso exclusivo de sensoriamento espectral, as vantagens estão na taxa de atualização dos dados em tempo real, uma fidelidade espacial maior e no fato das redes serem independentes e não precisarem de registro. As desvantagens da técnica no entanto são grandes, a necessidade

de um *hardware* mais caro e complexo, gasto energético extra para realização da tarefa de sensoriamento e o caráter individualista das redes que impede o compartilhamento das informações colhidas. O uso combinado de sensoriamento espectral e de uma WSDB pode ser feito de várias formas, algumas bem definidas e padronizadas, outras ainda em estudo que serão vistas na revisão da literatura no Capítulo 3. De acordo como foi feita essa associação das técnicas, pode se usar dados da WSDB para fornecer informação prévia e reduzir a complexidade do sensoriamento espectral com menores taxas de amostragem, alternativamente pode-se aumentar a precisão dos dados ou tê-los como fontes redundantes. Apesar de poder se beneficiar das duas fontes, ainda é necessário o *hardware* mais caro e complexo, além do gasto energético extra, mas uma das principais desvantagens é a falta de padrão com definição de um papel claro para cada fonte de dados.

Dentre as regulamentações definidas por agências governamentais e revisadas na Seção 2.4, pode ser visto um perfil mais liberal, como a regulamentação da FCC, e de perfil mais conservador, como a do Ofcom. Por outro lado, os requisitos podem ser mais ou menos restritivos para o processo de DSA, sendo os definidos pela agência dos Estados Unidos mais restritivos que os definidos pela agência do Reino Unido. Além disso, as regulamentações podem ser feitas seguindo o caráter de mobilidade dos equipamentos (fixo/móvel) ou seguindo o papel exercido pelo dispositivo na rede (mestre/escravo). Os parâmetros, apresentados na Seção 2.4, servem de referência para os requisitos ao qual a proposta deste trabalho deva ser submetida para a aprovação por agência reguladora.

Capítulo 3

Trabalhos relacionados para compartilhamento de espectro

ESTE capítulo tem por objetivo fazer uma revisão de trabalhos existentes no meio acadêmico que fundamentaram e auxiliaram na elaboração do modelo de arquitetura para DSA proposta nesta dissertação. Para melhor compreensão, o capítulo será estruturado em duas seções. A primeira, detalhando abordagens e/ou técnicas que fundamentaram e contribuíram para a concepção do uso integrado de base da dados com sensoriamento espectral, bem como o uso de sensoriamento em redes IoT cognitivas. A outra seção, abordará os trabalhos que exploram alternativas e possibilidades para o DSA ao se empregar DLTs na criação das bases de dados, bem como soluções de serviços que podem ser implementadas com elas.

3.1 Sensoriamento e WSDB para DSA

Um modelo de construção de base de dados para TVWS através de sensoriamento espectral é apresentado em [20], com a proposta de um algoritmo para estimação de dados incompletos. Os autores iniciam com a discussão sobre os atuais métodos de estimação de interferência utilizando modelos de propagação de canal e traz como alternativa o método via sensoriamento espectral. Resultados de simulação são utilizados para comparar algoritmos que estimam medições faltantes espacialmente. Este artigo demonstra a possibilidade de valer-se do poder de computação na base de dados para obter boa precisão na base de dados baseada em sensoriamento, preenchendo lacunas espaciais de medições através de algoritmos de estimação.

Em [35], Aslam et al. explora a coexistência entre redes 5G e redes secundárias cognitivas de IoT. Propondo para isso, uma estrutura de quadro de transmissão para DSA, onde mecanismos são designados para coletar informações das transmissões da rede IoT e classificar as oportunidades espectrais com base nesta realimentação durante um tempo de quadro (atual). Com estas informações de sensoriamento espectral e da qualidade de serviço (*Quality of Service*, QoS), determinados canais serão priorizados para alocação no tempo de quadro subsequente. Na divisão apresentada pelo autor, redes 5G operam no caráter primário, enquanto a rede IoT encontra-se em caráter secundário. Na proposta a ser apresentada nesta dissertação, o usuário primário será

representado por algum sistema detentor da licença de uso do espectro, por exemplo, sistemas de radiodifusão, comunicação satélite e sistemas de radar, e a rede IoT atuará com o sensoriamento espectral para viabilizar o compartilhamento de espectro e coexistência para outros sistemas de comunicação em caráter secundário, podendo a rede IoT estar inclusa, mas não limitada apenas à ela. Na análise feita pelo autor, simulações demonstraram que esta combinação foi capaz de melhorar o uso do espectro e a taxa de transferência de dados, ao mesmo tempo que melhora a QoS e a vazão da rede. Tal abordagem pode ser explorada de forma diferente no contexto desta proposta, cuja finalidade é manter um mapa de disponibilidade de canal atualizado em uma base de dados, a adição de um sistema de realimentação com reporte do estado do canal pode ser uma solução para implantação de QoS neste cenário.

Em [36] é feita uma revisão de modelos para DSA, assim como foi apresentado nas seções anteriores do presente capítulo. A partir dos conceitos de regulação existentes, é proposto um esquema de compartilhamento de espectro voltado para redes 5G de longo alcance (5G-Range). Neste trabalho, o estudo tem por base as regulamentações do CBRS. Também são apresentadas propostas para níveis de classificação (*tiers*) dos usuários para acesso ao espectro e uma estrutura de decisão a respeito do uso do espectro, o qual é baseada na combinação entre sensoriamento espectral e bases de dados para DSA, como a WSDB. Os objetivos por trás desta dissertação vem de encontro a proposta do trabalho, porém estendendo o cenário de aplicação sem definir o tipo de rede secundária a operar, propondo mecanismos para coexistência coordenada de diferentes tipos de rede e um modelo de alocação com possibilidade de trocas ou compras entre usuários detentores de licença sub-utilizada e usuários interessados em adquiri-las.

Paisana et al. exploraram em [15] o estado-da-arte para o DSA e seu uso em bandas de radar. As bandas L, S e C são grandes candidatas a serem exploradas para uso compartilhado por redes secundárias. Métodos de sensoriamento espectral são propostos para detectar os pulsos utilizados pelos sistemas de radar, enquanto o estudo como um todo propõe um sistema de compartilhamento conjunto com uma base de dados de geolocalização. Os autores demonstraram que as informações providas pela base de dados pode ajudar significativamente no processo de sensoriamento espectral dos pulsos de radar quando dados sobre a forma de onda, período dos pulsos e outros são disponibilizados. Nesta proposta, o sensoriamento pode ser facilitado pela base de dados, porém, a base de dados desempenha um papel mais crucial, atuando como um centro viabilizador do DSA além da rede de CRs que estão atuando no sensoriamento espectral. Neste trabalho foi demonstrada a viabilidade das técnicas de sensoriamento para as bandas de radar e de como elas podem ser inseridas também no contexto de DSA.

Uma infraestrutura para sensoriamento é utilizada para criação de zonas de exclusão conjunta com WSDB em [37]. Os autores utilizaram uma plataforma de testes aberta situada na Liubliana (capital da Eslovênia) chamada Log-a-Tec, que faz parte do projeto europeu *cognitive radio experimentation world* (CREW) [38]. Os dados coletados são disponibilizados através de uma interface de usuário online e para os SUs através do protocolo PAWS. A infraestrutura de testes foi utilizados para a detecção de sinais de dispositivos auxiliares para produção de conteúdo, os chama-

dos *programme making and special events* (PMSE), como microfones sem fio, criando uma base de dados com zonas de exclusão em torno do local onde o sinal foi detectado. Geograficamente foi feita uma divisão baseada em *pixels*, de acordo com os limiares, a partir da localização do sinal primário são definidos os *co-pixels*, em zonas mais afastadas os *pixels* adjacentes, e fora da zona de exclusão encontram-se os *pixels* não afetados. Diferente deste trabalho, a proposta apresentada nesta dissertação figura o uso conservador dos dados de geolocalização auxiliado pelo processo de sensoriamento espectral, além de conceber o uso de base de dados distribuídas no processo. Porém, a arquitetura de infraestrutura utilizada por [37] no processo de sensoriamento pode ser usada para ilustrar e levantar requisitos existentes para a implantação da rede IoT proposta.

A abordagem vista em [33] propõe o armazenamento das informações obtidas através de sensoriamento espectral e a replica de dados provenientes da base de dados do órgão regulador. Essa abordagem é pensada visando garantir a proteção dos usuários licenciados e, ao mesmo tempo, auxiliar a rede secundária. Replicar os dados da WSDB em uma base de dados local que atua como *cache*, pertencente à rede secundária, faz com que o tráfego de dados de controle para redes externas sejam minimizados. Esses dados armazenados localmente podem ser uma cópia, ou de uma parcela de interesse, dos dados disponíveis na base de dados de espaço em branco do órgão regulador. Além disso, esta base local serve para auxiliar na tarefa de sensoriamento espectral, agindo como armazenamento de forma similar a FC. Os autores avaliaram o desempenho dessa abordagem híbrida através de simulações, demonstrando ter atingindo melhores resultados com menos dispositivos de sensoriamento espectral quando os dois métodos foram combinados. Na proposta desta dissertação, a base de dados não é endereçada localmente a uma rede secundária visto que se tem a visão de uma base acessível a várias redes secundárias, desta forma, o sensoriamento contribui para a formação da base de dados, mas ela está disponível em um nível global para que possa habilitar múltiplas redes, bem como coordenar as trocas entre PUs e SUs.

Vários trabalhos estudaram técnicas que possibilitassem menor complexidade para a tarefa de sensoriamento espectral, utilizando de taxas de amostragem inferiores à taxa de Nyquist. Para isso é feito o uso da WSDB para obtenção de dados prévios dos PUs. O papel da WSDB nestes estudos é atuar como método auxiliar para a tarefa de sensoriamento. Isso foi feito em [14, 28–30]. Em [14], adota-se a estratégia de armazenar localmente o algoritmo de geolocalização existente na base do regulador localmente na rede secundária, de forma similar ao que é proposto em [33]. Simulações são apresentadas posteriormente para ilustrar os ganhos da abordagem híbrida proposta. A combinação abordada em [29] adota um processo para a descoberta dos buracos espectrais otimizado através do uso conjunto sensoriamento espectral e informações recebidas da WSDB. Também são apresentadas simulações numéricas com resultados de ganho de eficiência espectral e redução da complexidade de sensoriamento. Essas abordagens também são adotadas em [28] e [30] com algoritmos diferentes para a otimização do processo de sensoriamento, no entanto, os resultados destes dois últimos foram baseados em experimentos práticos com medições de campo. Vale ressaltar que nestes estudos citados, o uso conjunto da base de dados serviu para redução da complexidade do sensoriamento e otimizar o desempenho utilizando técnicas de amostragem abaixo da taxa de Nyquist.

Em janeiro de 2020, a FCC aprovou regras para o uso comercial por completo para DSA na banda de radar de 3,5 GHz, chamado de CBRS [39]. Nesta regulamentação, os usuários são divididos em três níveis, (i) os usuários protegidos, que são os de maior prioridade, são serviços federais (sistemas de radares navais e serviços fixos de satélite) que não podem receber nenhuma interferência de quaisquer outros usuários; (ii) as licenças de acesso prioritários (*priority access licenses*s, PALs), que são licenças renováveis de 10 anos para acesso a canais de 10 MHz. Os usuários do nível PAL não estão protegidos contra interferências causadas pelos usuários protegidos, mas recebem proteção contra interferências causadas pelos usuários de nível inferior; e (iii) o acesso geral autorizado (*general authorized access*, GAA) é um usuário que não possui licença, o qual pode servir para os mais diversos tipos de terminais, como dispositivos sem fio fixos, dispositivos *long term evolution* (LTE) privados e IoT. Os usuários que possuem classificação do tipo GAA não tem nenhuma proteção contra interferências causadas por usuários protegidos ou usuários de licença PAL. Os usuários que tiverem adquirido licenças PAL podem ceder o direito da licença quando não utilizada em local, canal ou tempo, por meio do administrador de um sistema de acesso ao espectro (*spectrum access system*, SAS), através de recursos já previstos para mercado de licenças no CBRS. Um recurso criado pela FCC para garantir a integridade de operação dos usuários protegidos é denominado capacidade de sensoriamento do ambiente (*environmental sensing capability*, ESC), uma tarefa realizada por sensores de espectro especificamente designados para detectar sinais dos radares navais. Uma rede ESC se comunica com as bases de dados dos SASs, de forma a negar o acesso ao espectro de qualquer dispositivo PAL ou GAA caso um sinal de radar seja detectado pela rede ESC. Uma vez que essa rede de sensores de espectro é projetada para ser usada exclusivamente para detecção dos sinais de usuários protegidos, como radares navais e estações fixas de satélites, não é necessário que todo o território seja atendido por uma rede ESC, mais especificamente, apenas regiões costeiras e as próximas a estações de satélite [40].

Como a abordagem do CBRS apresenta algumas semelhanças com a estrutura proposta, destaca-se que a principal diferença é que a rede ESC é uma rede sensoriamento de propósito específico, implantada em uma área restrita e controlada por um administrador aprovado pela FCC. Já a rede SSIoT tem como ideia usar um módulo de detecção de espectro acoplado a qualquer tipo de dispositivo IoT de uso genérico, que pode ser implantado em redes com abrangência a todo o território de um país. Além disso, o recurso de troca de espectro presente no CBRS é feita entre as partes interessadas, o usuário PAL que arrendará a licença e o usuário que pagará por ela, normalmente por intermédio de alguma interface do administrador SAS. Na estrutura aqui proposta, este recurso é viabilizado por contratos inteligentes executados em uma base de dados baseada em DLT, com a segurança atribuída ao contrato inteligente e necessidade de intermédio do administrador.

Outra regulamentação para abertura de espectro pioneira por parte da FCC foi a abertura de toda a faixa de 6 GHz (5.925 - 7.125 GHz) [17]. Porém o uso destes 1200 MHz de largura de faixa não foi condicionado ao uso compartilhado licenciado e sim para uso não licenciado. Essa banda foi pensada para ser disponibilizada para uso de redes como a nova geração de sistemas WiFi, redes 5G NR-U e outros. Por outro lado, muitos países ainda não obtiveram êxito em adequar suas regulamentações

e sua alocação de espectro para as necessidades atuais e futuras. A abordagem que será discutida no Capítulo 4 traz conceitos para um modelo integrado e abrangente que pode ser utilizado e viabilizar o cenário principalmente em países que possuem visão mais conservativa a respeito da alocação de espectro.

3.2 Tecnologia de registro distribuído e possibilidades

Em [41–43], a tecnologia Blockchain foi idealizada e aplicada ao contexto do DSA. O principal papel dessa tecnologia é fornecer um ambiente descentralizado para troca e processamento de informações, como um banco de dados, permitir a computação baseada em contratos inteligentes, armazenamento e processamento de informações de detecção de espectro e registro de transações de maneira permanente e à prova de violação. As abordagens em [41–43] são exploradas na sequência.

Em [41], Weiss et al. analisaram e classificaram quatro categorias de compartilhamento de espectro, baseadas seja no caráter primário ou secundário, seja no caráter cooperativo ou não-cooperativo. O compartilhamento primário é descrito como a situação onde todos os usuários possuem direitos iguais sobre a faixa de espectro similar ao uso não licenciado, enquanto isso, o secundário apresenta características hierárquicas, maior prioridade ou direito, como os cenários regulatórios citados anteriormente neste capítulo. Quando se trata das diferenças entre o caráter cooperativo e não-cooperativo, a diferença se dá nas interações entre os usuários. No cenário cooperativo é possível que os usuários interajam fazendo transações de espectro, enquanto no não-cooperativo o uso é não coordenado e oportunista. Segundo os autores, informações sobre usuários que permitam identificar os equipamentos de rádio ou dispositivos sensoriamento espectral podem ser armazenadas dinamicamente em uma Blockchain, no entanto, a principal função da Blockchain é registrar as transações de um mercado de espectro.

Os autores de [42] descrevem um modelo de negócios para o DSA chamado de *full-spectrum blockchain as a service* (FSBaaS). Duas Blockchains diferentes são empregadas: (i) uma centralizada, chamada Blockchain Lite; e (ii) o Hyperledger Fabric [44], um projeto colaborativo iniciado pela Linux Foundation de DLT descentralizado. O acesso às duas Blockchains é implementado por meio de uma API RESTful unificada, que é um tipo de estilo de arquitetura de *software* para serviços Web, como HTTP. A solução centralizada se aplica a clientes e usuários que não se importam com uma autoridade que monitora os registros de novos blocos, ao mesmo tempo, a opção descentralizada está focada nos usuários que desejam fazer transações de maneira independente. A idéia de usar duas Blockchains é aproveitar os cenários oferecidos pelas abordagens centralizada e descentralizada. As duas Blockchains compartilham de um gerente de negócios da rede e de um executor de contratos inteligentes. O gerente de negócios da rede de analisa e gerencia todo o ecossistema de negócios, enquanto o executor de contratos inteligentes é responsável pela execução lógica das soluções da rede. Os usuários não mantêm um nó de Blockchain por si mesmos, em vez disso, confiam nos hospedeiros dos nós de Blockchain aos quais se conectam. Isso ilustra uma decisão importante dentro de um projeto de DSA baseado em Blockchain, quais são os nós que validam os registros e onde eles serão executados.

Em [43], é apresentada uma solução de compartilhamento de espectro dinâmico por meio de contratos inteligentes sobre a Blockchain Ethereum. Os autores desenvolveram um novo ativo digital para o mercado de espectro chamado *Spectral Token*. Este *token* é usado para validar e rastrear o uso de bandas de frequência licenciadas. A solução reforça o acesso sequencial ao espectro pelos SUs, a fim de evitar interferências. O *token* evita colisões e garante que os PUs receberão um pagamento pelo espectro alugado. A plataforma permite que os usuários se apropriem das faixas de frequência pagando à autoridade, por exemplo, agências reguladoras como a FCC. Cada banda de frequência é codificada como um *token* e um PU pode alugá-la para um SU. O PU pode anunciar a oportunidade de concessão, assim como o SU pode procurar bandas de frequência gratuitas. Depois de definido o inicio, o local, o período e uma taxa de acesso, uma certa faixa de frequência pode ser negociada através da plataforma. Os autores desenvolveram uma solução de prova de conceito nas bandas ISM de 2.4 e 5 GHz. A análise de desempenho mostrou que o sistema possui características de vazão e latência adequadas para atender casos de uso no CBRS, IEEE 802.22 ou pequenas células como um serviço. Essa prova de conceito serve de referência para demonstrar que é viável adotar Blockchain nesse tipo de solução.

Em [45, 46], os autores também exploraram o uso da Blockchain Ethereum em uma proposta intitulada *spectrum sensing as a service* (Spass). Nele o sensoriamento espectral é oferecido como um serviço monetizado através de contratos inteligentes do Ethereum. De forma complementar, os autores propõe um algoritmo para detecção de participantes maliciosos provendo falsas informações de sensoriamento, com sua inclusão numa lista negra e exclusão de contratos futuros.

3.3 Sumário

Neste capítulo, dois grupos de estudos foram revisados para fundamentar a arquitetura proposta, o primeiro propõe soluções para DSA envolvendo sensoriamento espectral e/ou o uso de base de dados; o outro, a aplicação de DLTs em soluções de DSA.

Dentro do primeiro cenário, alguns trabalhos trazem uma abordagem visando a combinação das técnicas de sensoriamento e base de dados, onde o enfoque é a redução do custo da tarefa de sensoriamento (menor amostragem por exemplo) com informações prévias obtidas da WSDB. Isso pode ser visto em [14, 28–30]. Outros trabalhos estudam a formação da base de dados por meio de sensoriamento espectral, seja externamente (em rede) [20,37] ou localmente (na estação base) [33]. O uso de sensoriamento com redes IoT ou sua viabilidade em outras frequências, como a banda de radar, pode ser visto em [35] e [15], respectivamente. Por fim, há regulamentações [17,39,40] ou revisões do cenário regulatório para DSA [36].

Na bibliografia sobre o uso de DLTs para DSA, [41] detalha as opções e oportunidades neste cenário; [42] testa a implementação de Blockchains; [43] introduz a possibilidade de um ativo digital para transações de espectro; e [45, 46] detalha o uso de contratos inteligentes e sensoriamento espectral como um serviço.

Capítulo 4

Acesso dinâmico ao espectro habilitado por base de dados e internet das coisas

NESTE capítulo, será detalhado o modelo de arquitetura proposto como solução para DSA baseado em redes IoT. Dentre as concepções a serem apresentadas, também encontra-se a relação entre as redes primária, secundária e IoT e eventuais protocolos que podem utilizados. Outras características importantes ao conceito são as relações entre a gerência e o armazenamento da base de dados, concebidos separadamente e que podem ser construídos com diferentes tecnologias. Algumas soluções que podem ser empregadas na sua concepção, dentre elas o uso de DLTs, também serão detalhadas. Diferentes cenários e combinações surgem para serem levados em conta em trabalhos futuros na construção prática do modelo. A segurança como um todo é detalhada na última seção do capítulo, onde a base de dados e as tecnologias escolhidas para sua construção desempenham um papel crucial, mas por se tratar de uma abordagem híbrida com sensoriamento espectral, características da tecnologia são atribuídas para aumentar a confiabilidade do modelo de rede proposto.

4.1 Visão global

O módulo de sensoriamento espectral envia as informações de uso do espectro para o dispositivo IoT em que está conectado. Caso o dispositivo IoT não possa definir sua própria geolocalização, esta capacidade pode ser delegada ao *hardware* do módulo de sensoriamento. Se o sensor IoT já possuir a capacidade de obter suas coordenadas, uma versão mais simples do módulo de sensoriamento espectral sem essa capacidade pode ser utilizada. Após os dados de sensoriamento serem enviados pela interface de comunicação para o dispositivo IoT, a camada principal de aplicação da *firmware* do sensor deve estar apta a receber estes dados, encapsular e encaminhá-los para o *gateway*, que é responsável por enviar o pacote até a WSDB.

Nem todos os dispositivos da rede IoT precisam estar equipados com um módulo de sensoriamento espectral, apenas o número suficiente para que a densidade dos dados atinja a confiabilidade e os requisitos estipulados. O módulo de sensoriamento espec-

tral deve possuir sua própria antena (principalmente devido à largura de banda e à sua frequência de operação), enquanto no caso sensores IoT sem fio, os mesmos também podem possuir antenas com características que vão diferir significativamente.

As principais entidades e seus relacionamentos na arquitetura proposta para o acesso dinâmico ao espectro habilitada por redes IoT são ilustradas na Figura 4.1. Neste cenário, considera-se as redes primária, IoT e secundária estarem posicionadas em uma mesma região de forma a possuírem áreas de cobertura total ou parcialmente sobrepostas.

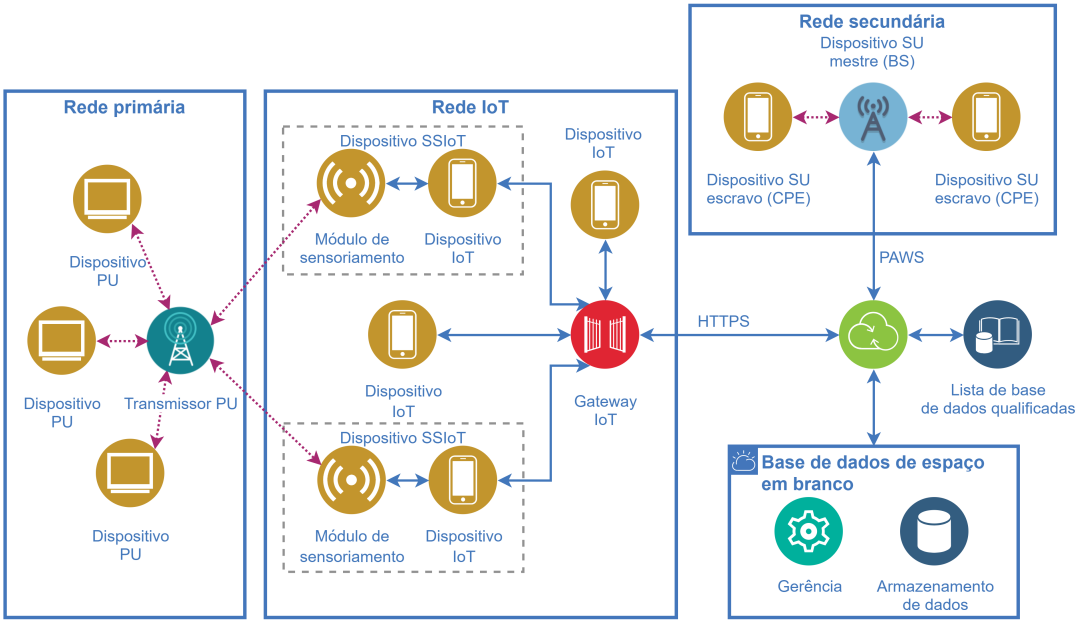


Figura 4.1: *Arquitetura proposta para rede SSIoT, suas entidades e relacionamentos.*

Uma das principais características dessa estrutura é que a tarefa de detecção de espectro é transferida dos SUs para os dispositivos SSIoT que faz parte de uma rede IoT de suporte, reduzindo desta forma a complexidade dos equipamentos dos SUs. Os dispositivos SSIoT são formados pela conexão de um dispositivo IoT comum a um sensor de espectro, através de uma interface de comunicação padrão, com ou sem fio, como UART, I^2C ou SPI [47], como é melhor detalhado na Figura 4.2. Os dispositivos SSIoT efetuam o sensoriamento espectral nas potenciais frequências para DSA, para isso o mesmos devem ter uma ampla distribuição espacial e cobrir posições dentro da cobertura de transmissão do PU. Os dados colhidos são enviados via rede até uma WSDB, que irá utilizar esta informação para atualizar o mapa de disponibilidade de canais. Uma rede secundária a fim de transmitir conecta-se à WSDB e requisita acessar o espectro. Licenças temporárias e trocas podem ser feitas através da base de dados utilizando-se de contratos inteligentes diretamente entre os PUs e os SUs, ou ainda sem participação do PU e baseando-se apenas no mapa de disponibilidade de canais. Este é o processo detalhado na Figura 4.1.

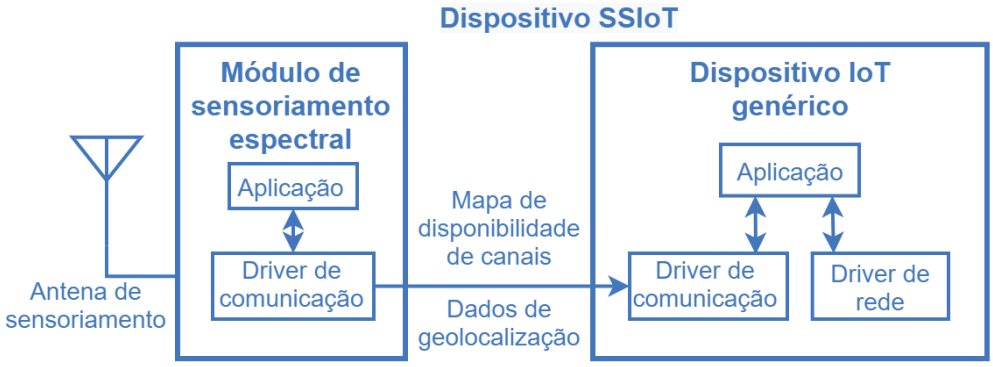


Figura 4.2: *Concepção de um dispositivo SSIoT.*

Como as características de RF podem variar muito em função de uma ou mais frequências alvo do DSA, diferentes módulos podem ser concebidos no desenho de uma rede SSIoT. Alguns podem vir equipados com antenas e perfil de sensibilidade para as bandas de TV, enquanto outros podem ser desenvolvidos para o sensoriamento segundo requisitos das bandas de satélite. Essa característica permite uma heterogeneidade dos módulos sensores ao longo da rede SSIoT.

A carga de processamento computacional do sensoriamento espectral é atribuído apenas ao *hardware* do módulo de sensoriamento, isto é, na prática toda a tarefa de sensoriamento é realizada e processada pelo *hardware* do módulo. A partir disso, os dados gerados são transmitidos para o dispositivo IoT cuja responsabilidade é exclusivamente encapsular a informação e enviá-la pela rede à WSDB. Neste ponto, a comunicação com o *gateway* segue padrões fora do escopo do projeto, uma vez que os dispositivos podem estar conectados por diferentes protocolos. O único acréscimo de complexidade computacional ao *hardware* do dispositivo IoT deve ser uma tarefa de suporte, capaz de distinguir as informações coletadas pelo módulo de sensoriamento acoplado das informações para o qual o dispositivo foi projetado, separar e endereçá-las de acordo com seu destino.

O endereçamento direto das informações de sensoriamento espectral nos dispositivos IoT para a WSDB é um caso ideal para que a latência do processo seja mínima, porém existe a possibilidade de uma interface de aplicação ser executada diretamente no serviço de base de dados da rede IoT para fazer a separação dos dados que pertencem à rede e redirecionar os dados de sensoriamento para a WSDB. Isso faz com que possa ser menor o impacto na *firmware* do dispositivo ao qual será acoplado o módulo de sensoriamento, mas ao mesmo tempo, aumenta a latência do processo devido ao redirecionamento dos dados.

A alta densidade de nós da rede IoT é capaz de fornecer dados para a criação de zonas de exclusão com muita precisão utilizando os dados de sensoriamento espectral fornecidos pelos dispositivos SSIoT comparado às tradicionais zonas de exclusão baseadas na perda por propagação, como a considerada em [37].

Os dados de ocupação do espectro coletados por esta rede IoT especial são armazenados na WSDB e ficam disponíveis para serem acessados por redes secundárias interessadas no acesso dinâmico ao espectro. O acesso às faixas livres é feito por meio de um monitoramento constante do WSDB, que pode ser facilmente realizado durante

a comunicação de controle entre os SUs e suas estações base. Qualquer dispositivo secundário, equipado ou não com a capacidade de sensoriamento espectral, pode acessar as informações espaciais-temporais sobre a disponibilidade do canal.

É importante ressaltar que as informações de sensoriamento espectral neste contexto serão utilizadas apenas para a atualização da WSDB, viabilizando um DSA preciso para os terminais da rede secundária. Em outras palavras, o DSA da rede secundária será feito apenas com base na disponibilidade do espectro obtida da WSDB, o que significa que os dispositivos secundários não precisam estar equipados com nenhum *hardware* que forneça a capacidade de sensoriamento espectral. Os dispositivos SSIoT também podem ser usados para monitorar o espectro utilizado pela própria rede IoT do qual fazem parte, visando ajudar seus nós a acessar bandas menos lotadas ou livres de forte interferência.

Dentro do contexto da WSDB, torna-se importante destacar a divisão entre as funções de gerência e armazenamento da base de dados. Tanto o plano de gerência quanto o de armazenamento podem ser implementados com soluções convencionais de banco de dados ou DLTs, ou ainda, cada um adotar sua própria solução. O armazenamento da base de dados se refere à parte responsável por guardar as informações de sensoriamento espectral recebidas da rede SSIoT, os dados de geolocalização, parâmetros de operação e registro dos dispositivos envolvidos no DSA. Quando citado a parte de gerência da WSDB, refere-se ao conjunto de entidades aos quais são atribuídas a estimação das zonas de exclusão com base nas informações de sensoriamento espectral e geolocalização, alocação de canais para SUs, rescisão do uso de canais por SUs, trocas de licenças de uso do espectro entre os usuários, ferramentas de controle para órgãos governamentais aplicarem políticas reguladoras sobre o DSA, dentre outras.

4.1.1 Planejamento da distribuição dos dispositivos SSIoT

Como citado, nem todos os dispositivos da rede IoT necessitam estar equipados com o módulo de sensoriamento espectral. A escalabilidade dos dispositivos dotados da capacidade de sensoriamento, dentro da rede IoT como um todo, deve-se basear no quão capaz é a distribuição destes dispositivos de fornecer, com precisão e abrangência, o mapa de ocupação de espectro.

O alcance e sensibilidade dos dispositivos devem ser considerados na hora de dimensionar a densidade de sensores de espectro na rede IoT. Para exemplificar o cenário de distribuição dos dispositivos, considere uma região circular, como a área de sensibilidade e detecção de um módulo de sensoriamento espectral dotado de uma antena omnidirecional, ilustrado pela Figura 4.3. As regiões em tom avermelhado indicam sobreposição das áreas onde sensores de espectro adjacentes são capazes de aferir a ocupação do espectro. Reduzir as áreas de sobreposição serve para otimizar a eficiência da rede, diminuindo a necessidade de mais módulos sensores de espectro e minimizando o tráfego para a base de dados. Algumas regiões podem ficar fora da região de sensibilidade dos sensores de espectro, isso é representado pela área em amarelo na figura. Para a maior fidelidade dos dados na WSDB, o ideal é que as regiões sem informação, ou de informação de baixa confiabilidade, sejam reduzidas ao máximo.

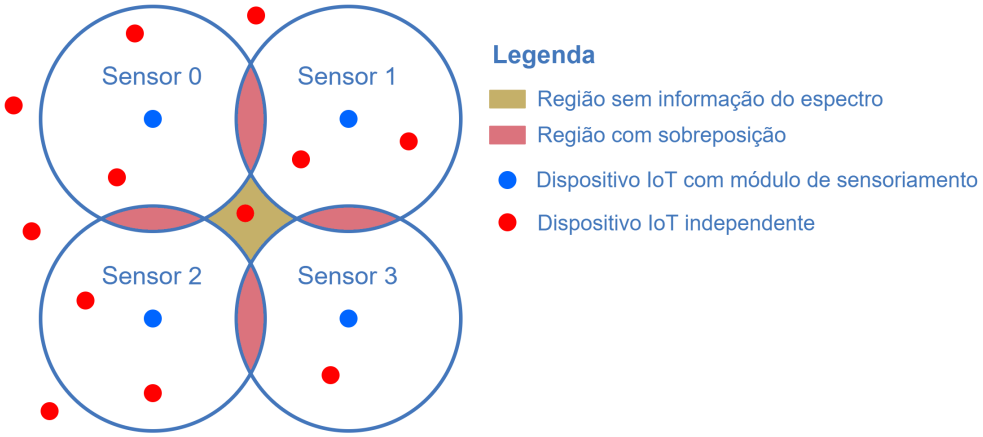


Figura 4.3: *Distribuição espacial e sobreposição dos módulos sensores de espectro.*

Na composição do mapa de ocupação de espectro, cada região pode ser tratada como um *pixel*. Na Figura 4.3 são ilustradas as regiões correspondentes a quatro dispositivos IoT que receberam módulos sensores de espectro, nomeados: Sensor 0, 1, 2 e 3. Conforme visto em [20], um mapa de ocupação de espectro pode ser completo, mesmo que haja regiões sem informação, através de algoritmos de estimação. Um algoritmo de estimação, baseado em inteligência artificial, pode ser capaz de preencher o mapa de ocupação de espectro baseando-se nas informações dos sensores que atuam como *pixels* no entorno da região. O desafio passa a ser a redução desta área à menor região onde um algoritmo de estimação performe bons resultados, assim, minimizando também a região de sobreposição dos módulos sensores de espectro.

4.2 Características específicas

A aplicação principal em execução no dispositivo SSIoT recebe informações do sensor de espectro, encapsula e as encaminha para o *gateway* usando o protocolo de comunicação específico do seu *driver* de rede, por exemplo o IEEE 802.15.4, Ethernet ou LoRa. O *gateway* de uma rede IoT pode ser um nó especializado que serve par publicar qualquer tipo de dado na Internet. O protocolo mais popular utilizado nos dispositivos IoT para essa função é o chamado *Message Queuing Telemetry Transport* (MQTT). Como este é um protocolo desenvolvido para dispositivos com recursos limitados, ele possui limitações em relação à segurança, por exemplo, nenhuma criptografia dos dados [48]. Como mostrado em [37] e [48], a segurança na conexão entre a rede IoT e a WSDB pode ser feita, por exemplo, com o chamado *Secure Sockets Layer* (SSL) ou com seu certificado sucessor, o *Transport Layer Security* (TLS), usando uma autenticação via *Hypertext Transfer Protocol Secure* (HTTPS) [37], dessa forma mantendo a rede segura contra ataques maliciosos. Nesse caso, existem autoridades de certificação, públicas e confiáveis, que emitem os certificados assinados digitalmente que são utilizados pelo SSL/TLS para autenticar os clientes. Eles também podem ser usados para permitir que apenas quem é certificado acesse uma determinada informação. Em [48], estes tipo de mecanismo foi empregado para a segurança em um sistema de controle de acesso. Maiores detalhes à respeito da segurança da rede serão abordados à frente na Seção 4.4.

A viabilidade dos protocolos pode ser avaliada considerando o MQTT, o HTTPS e outros, como o CoAP e o *Advanced Message Queuing Protocol* (AMQP). Comparações de características destes protocolos e funcionalidades podem ser vistas em [49, 50]. Partindo do ponto de vista de segurança, pode-se avaliar, por exemplo, o MQTT como o menos seguro, enquanto o HTTPS e o AMQP são os protocolos com maior segurança. Contundo, é necessário o desenvolvimento e avaliação deste módulo para julgar os mesmos frente ao *hardware* dos dispositivos.

As comunicações entre o dispositivo IoT e o *gateway* ou entre o *gateway* e a WSDB encontram-se fora do escopo desta proposta. A principal razão por isso é que já se pressupõe a existência de uma conexão utilizada pelos dispositivos IoT para transmitir os dados colhidos para serviços em nuvem, seja conexão sem fio ou cabeada. O que se propõe é o uso de protocolos, que podem dar maior segurança no processo como o uso do HTTPS, mas demais protocolos de camada física encontram-se fora do escopo.

Antes de se conectar à base de dados, caso exista mais de um administrador provendo o serviço de WSDB, a estação base da rede secundária (mostrada na Figura 4.1) pode buscar uma lista de base de dados qualificadas e escolher a mais apropriada, de acordo com a área geográfica atendida e a própria localização dos SUs. O conceito de bases de dados qualificadas já está em uso, por exemplo, no Reino Unido [51] e pode ser igualmente aplicado ao modelo proposto para facilitar que a rede secundária encontre a WSDB ideal em um cenário onde o serviço pode ser provido por vários administradores, estejam eles atuando concorrentemente na mesma área ou não.

Ao conectar-se a uma WSDB, a estação base da rede secundária deve fazer seu próprio registro, informando a existência da sua rede. Uma vez aceito o registro, a estação base também fornece os dados dos dispositivos escravos conectados à ela. Segundo as regulamentações da FCC, durante o registro, a estação base deve informar o número identificador da FCC, o fabricante, o número de série do equipamento, a HAGL e detalhes sobre o proprietário ou a pessoa responsável do dispositivo, como nome, endereço, e-mail e número de telefone. A estação base deve repetir este processo sempre que alterar qualquer parâmetro operacional ou quando um dispositivo alterar sua localização em um determinado valor (por exemplo, ao mover-se 100 metros de onde estava durante o registro anterior). Esse processo e todas as tarefas relacionadas são feitas por camadas de alto nível na estação base, por exemplo, no SM se for considerado o padrão IEEE 802.22. Após o registro, a estação base solicita à WSDB a disponibilidade de espectro para sua posição, recebendo os dados atualizados de ocupação do espectro, que posteriormente permitirão que os terminais escravos sejam habilitados e transmitam nos canais disponíveis, de acordo com os parâmetros estabelecidos.

Uma entidade que pode ser adicionada à arquitetura mostrada na Figura 4.1 para estender os cenários de uso é um agregador na rede IoT. Sua principal função seria combinar dados de diferentes fontes e ajudar na segurança da rede, removendo protocolos mais complexos dos dispositivos IoT de recursos limitados. Um *smartphone* pode ser usado para exemplificar esse papel, quando conectado a relógios inteligentes ou outros dispositivos portáteis que coletam dados do usuário, como informações de sensores cardíacos, o *smartphone* atua como um agregador de dados, removendo a complexidade dos sensores, tornando-se o responsável pela segurança dos dados e pelo

envio de todas as informações para o *gateway* que os encaminhará para os servidores em nuvem; observe que, quando o agregador é usado, ele pode assumir a função do próprio *gateway*. No modelo prático do sistema de segurança de controle de acesso proposto em [48], um agregador foi implementado com um Raspberry Pi 3, enquanto o nó IoT foi implementado com um ESP32-DevKitC.

A frequência de atualização da WSDB pode depender de como a tarefa de detecção de espectro é implementada, por exemplo, essa taxa pode ser definida pela periodicidade na qual um dispositivo SSIoT reporta as informações de sensoriamento, ou ainda coletar os dados do espectro quando se fizer necessário utilizando do chamado *Sensor Query and Data Dissemination Protocol* (SQDDP). De certa forma, a primeira abordagem consome mais energia, mas tende a manter a WSDB sempre atualizada, a segunda pode ter uma melhor eficiência energética, mas pode causar uma latência intolerável ao processo de atualização da WSDB. A taxa de atualização também pode ser associada à frequência com que a rede secundária acessa a WSDB, que pode acontecer uma vez ao dia para dispositivos fixos, de acordo com as regras da FCC, mas pode ser ainda da ordem de segundos para dispositivos móveis [8].

O SQDDP é um protocolo de aplicação proposto para redes de sensores, descrito em [52] como um protocolo que fornece aos usuários interface para emitir consultas e responder às consultas em sensores. Essas consultas em geral não são endereçadas a nós específicos, mas podem ser endereçadas a grupos (*clusters*) em locais especificados. Essa abordagem pode ser útil para coletar informações de ocupação de espectro em tempo real, sob demanda, diretamente dos dispositivos SSIoT, permitindo a leitura e o processamento simultâneo dessas informações de maneira semelhante ao sensoriamento espectral cooperativo. A entidade de gerenciamento, parte da estrutura do banco de dados, usa um algoritmo para combinar as informações de geolocalização (o qual são baseadas nos registros das redes primárias) e os dados previamente armazenados com as novas informações de sensoriamento recebidas para se atualizar e aumentar a precisão das zonas de exclusão. Esse recurso é mostrado na Figura 4.4.

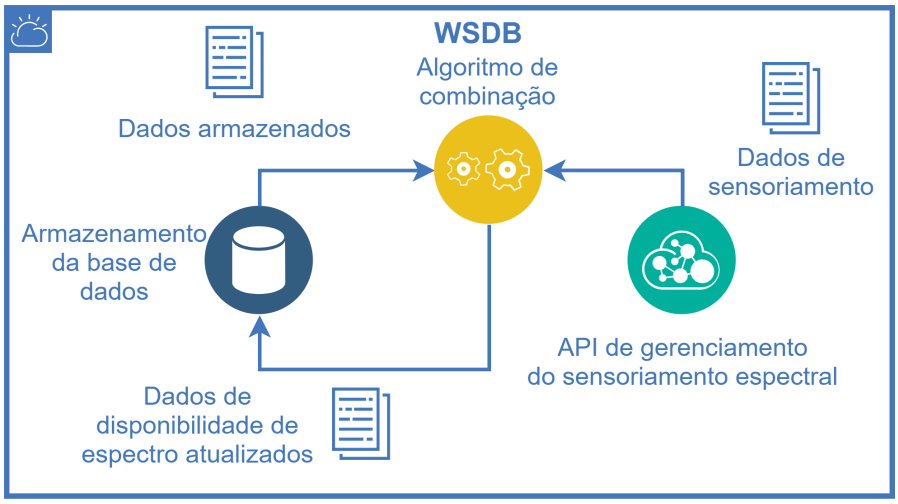


Figura 4.4: *Interação entre dados existentes de diferentes fontes no algorítimo de atualização da WSDB.*

Os dados armazenados na WSDB mostrados na Figura 4.4 incluem: dados estáticos dos PUs tal como são utilizados e disponibilizados pela base de dados do regulador, histórico de sensoriamento espectral, dados dos SUs, registro das trocas de licença de espectro e o mapa atual de disponibilidade de canais. Este mapa de disponibilidade de canais que será atualizado em função do tempo na WSDB, o mesmo depende de todas as variáveis citadas anteriormente e também dos registros de troca e transações de espectro que podem ocorrer via contratos inteligentes entre PUs e SUs.

É necessário enfatizar que a latência do processo, isto é, o atraso desde a realização do sensoriamento e o momento em que essas informações são disponibilizadas na WSDB, depende da topologia adotada pela rede IoT e de como é feita a agregação dos dados. Os dados de sensoriamento podem ser transmitidos apenas aos dispositivos mais próximos ou podem ser transmitidos para todos os dispositivos da rede até chegar ao *gateway*, o que afeta claramente a latência das informações fornecidas dentro da rede IoT. Após isso, ainda deve-se considerar o atraso do *gateway* até a base de dados, atraso de processamento e o atraso até a resposta chegar ao dispositivo secundário. De acordo com [8], nas regras do Ofcom, uma WSDB deve responder a uma consulta dentro de 10 segundos. Esse tempo inclui a solicitação aos dispositivos SSIoT, o processo de sensoriamento, recepção de informações do sensoriamento, processamento do mapa de canais e zonas de exclusão e resposta aos dispositivos secundários. No entanto, essa resposta pode se fazer necessária dentro de um prazo menor no caso de dispositivos móveis.

Para o processo de atualização da WSDB, a rede SSIoT pode fornecer os dados de sensoriamento de forma periódica ou sob requisição, por exemplo, através de uma chamada com o protocolo SQDDP. Estes dados da rede como um todo podem então, serem utilizados pelo algorítimo de combinação na gerência da base de dados. Outra opção, que se aplica melhor para o perfil de dispositivos internos (*indoor*) é requisitar a informação em tempo real à rede SSIoT. Isso pode ser feito com a divisão da rede em *clusters* e endereçando a requisição para aquele no qual sua posição geográfica está inserida (podendo estender-se aos adjacentes).

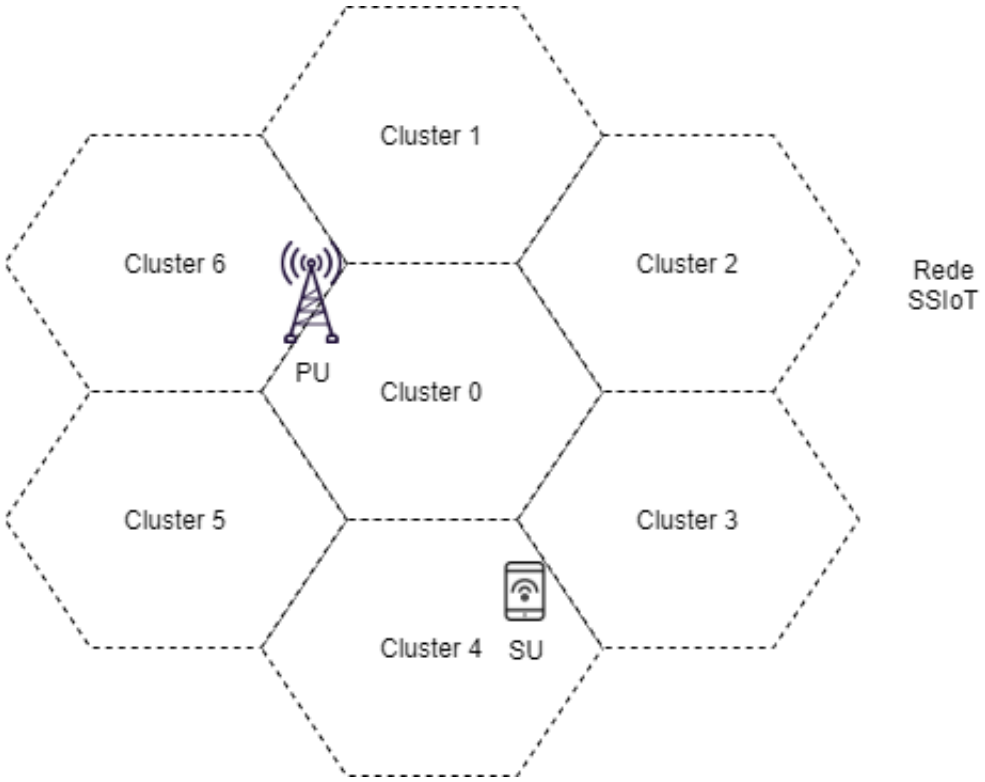


Figura 4.5: *Subdivisão da rede e sensoriamento em tempo real baseado em clusters.*

A Figura 4.5 ilustra o cenário onde a rede SSIoT é dividida em 7 *clusters*. Um PU encontra-se localizado entre o *cluster* 0 e o *cluster* 6, no *cluster* 4 encontra-se um SU. Na atualização da base de dados, as informações de sensoriamento são colhidas em toda a rede. Porém, o SU pode ser um dispositivo interno, que dentro dos seus parâmetros, é viável operar na zona de exclusão sem causar interferências. Nesse caso, o SQDDP pode ser usado para colher dados no *cluster* 4 onde ele se localiza, ou ainda, estendendo-se aos mais próximos, neste caso, os *clusters* 0 e 3. Uma política de disponibilidade de canal mais branda, menos conservadora, pode ser adotada nesse processo para estes dispositivos de uso interno. Ressaltando, que a rede secundária não possui interface direta para a rede SSIoT, tudo isso é feito por intermédio da WSDB, que pode, inclusive, tarifar o uso de espectro segundo as ferramentas da sua parte de gerência.

4.3 Tecnologias viabilizadoras

A tecnologia de registros distribuídos (*distributed ledger technology*, DLT) tem ganhado cada vez mais notoriedade graças às suas capacidades e benefícios. Seu princípio básico é ser um banco de dados distribuído entre vários dispositivos conectados, os nós da rede. Diferentemente de um banco de dados tradicional, onde a informação é armazenada em um ponto único, em uma rede baseada em DLT a informação está presente em todos os nós da rede.

Redes convencionais baseiam-se em topologias centralizadas ou descentralizadas. A Figura 4.6, baseada em [53], ilustra diferentes topologias de rede. Em um rede cen-

tralizada, toda informação é armazenada em um único nó, responsável pela integridade da rede, já a descentralizada, múltiplos nós serão responsáveis pela integridade da rede, servindo aos usuários conectados neles, onde no caso de uma falha, nem toda a rede é comprometida. Uma rede distribuída no entanto, todos os nós estão conectados e compartilham dos mesmos dados, neste caso, a rede não é afetada mesmo que perca algum nó.

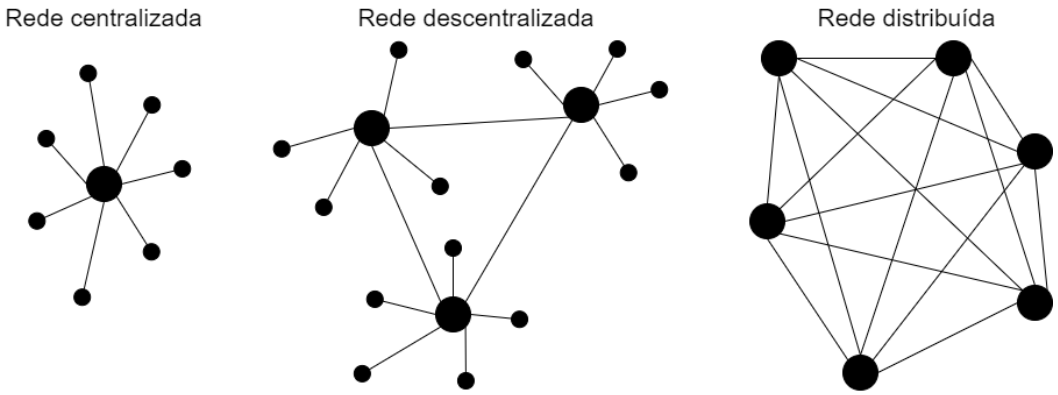


Figura 4.6: *Topologia de redes centralizadas, descentralizadas e distribuídas. Alternativa à figura de [51].*

Existem vários tipos de DLT: a Blockchain, o grafo acíclico dirigido (*directed acyclic graph*, DAG), o hashgraph, o holochain e o radix [54]. Nesta dissertação, aquelas exploradas e que serão detalhadas para DSA são a Blockchain e o DAG. Algumas implementações destas DLTs também serão abordadas, como o Ethereum e o Tangle (IOTA).

Uma Blockchain pode ser pública ou privada. Blockchain pública é aquela onde os usuários são anônimos, a rede é aberta à entrada de qualquer novo membro. Neste tipo de rede todos os nós possuem os mesmos poderes e todos podem auditar a rede. Neste tipo de rede é indispensável a existência de uma criptomoeda. Como não existe coordenação entre os nós, alterações e registros na rede são lentos por necessitarem de um consenso. Por outro lado, uma Blockchain privada não é aberta à participação de qualquer novo membro, os usuários não são anônimos e precisam de obter permissão para integrar a rede. Este tipo de rede pode não precisar de uma criptomoeda, uma vez que já existe coordenação entre os membros. Isto também faz com que este tipo de rede seja mais rápida para receber mudanças e novos registros. Ainda nas Blockchains privadas, uma ou mais entidades podem exercer controle sobre a rede, o que as faz muito viável para cenários corporativos ou que um membro regulador seja necessário.

Diferente das redes centralizadas, onde o nó central é uma autoridade com confiança por parte dos demais nós, em uma Blockchain existe o problema da confiança entre os nós. Para um registro se propagar na rede é necessário que haja um consenso entre os nós, isso é feito através do chamado "algoritmo de consenso". Dentre os algoritmos mais comuns para esta tarefa estão a prova de trabalho (*proof of work*, PoW) e a prova de participação (*proof of stake*, PoS) [55].

O algoritmo PoW faz com que os membros tenham que gastar tempo e energia realizando uma tarefa para poderem registrar um bloco na Blockchain. Da necessidade

de realizar a tarefa surge o nome prova de trabalho. No caso do Bitcoin por exemplo, a PoW consiste na solução de uma *função hash* (SHA-256). Parte da segurança que uma Blockchain oferece vem justamente da complexidade da realização da PoW para um usuário malicioso. O problema por parte deste método é a maior complexidade computacional e gasto energético que ele apresenta.

A outra alternativa, o algoritmo de consenso PoS, em vez de realizar uma tarefa o nó deve possuir uma carteira com uma determinada quantidade de moeda. Um sorteio aleatório define o criador do próximo bloco na cadeia, onde existe uma chance maior de ser sorteado conforme maior quantidade de recurso existir na carteira. Pra participar de uma transação uma determinada quantidade da moeda é colocada como garantia, uma quantidade é recebida no sucesso do processo, mas pode também haver penalização e perder caso tente alterar o bloco. Como a PoS não depende de capacidade de processamento para resolução de uma tarefa, esta abordagem possui menor complexidade e maior eficiência energética. Um exemplo de Blockchain tradicional que utilizava PoW mas implementou a PoS é o Ethereum (2.0).

Comparando os dois algoritmos de consenso, tanto a PoW quanto a PoS garantem segurança da rede. Numa rede que utiliza PoW os ativos são gerados com base na criação dos blocos, já em uma rede baseada em PoS todo o montante de ativos são gerados na criação da própria Blockchain. Desta forma, no primeiro caso, um atacante precisa garantir a maior parcela do poder de processamento da rede, já no segundo, o mesmo deve deter a maior parcela dos ativos da rede [54].

Na Blockchain, é formada uma cadeia linear onde cada bloco carrega consigo o *hash* do bloco anterior. As transações são colocadas dentro de blocos que devem ser validados, uma vez que o bloco é validado ele é adicionado à cadeia e o seu *hash* será colocado no bloco seguinte [55]. Outra classe de DLT é o grafo acíclico dirigido e um exemplo que tem potencial para o cenário de DSA é o Tangle. Neste DAG, antes de ter uma transação validada pela rede, um usuário deve validar duas transações anteriores. Dessa forma, no DAG aquele que gera transações também valida outras, assumindo os dois papeis neste tipo de DLT. Isso elimina a figura dos mineradores existentes na Blockchain, que são nós responsáveis pela PoW, consequentemente, também elimina a necessidade das taxas pagas aos mesmos.

Existem alguns aspectos que precisam ser abordados para a implantação de uma WSDB baseada em Blockchain: (i) é necessário decidir o tipo de mecanismo de consenso a ser usado para validar as transações; (ii) o custo das transações deve ser levado em consideração, uma vez que uma transação, por exemplo, fazendo ou recebendo um pagamento pelo aluguel de uma faixa de espectro, tem dois tipos de custos a serem observados: o custo da Blockchain, que está relacionado à moeda a ser usado como o método de pagamento e o custo energético, que está associado à energia utilizada no consenso da transação; (iii) a escolha entre design de Blockchain público versus privado: um Blockchain público ou aberto é uma rede no qual qualquer pessoa pode ingressar, com permissões completas de participação (leitura e gravação). Por outro lado, uma Blockchain privada tem restrições sobre quem pode participar da rede; e (iv) o uso de uma Blockchain centralizada versus descentralizada: uma Blockchain centralizada possui uma autoridade central que mantém todos os registros da Blockchain, enquanto uma Blockchain descentralizada tem seus dados distribuídos pela rede, sem

um nó central para coordenar sua operação.

Implementar uma solução de WSDB com bancos de dados convencionais requer uma infraestrutura complexa, que ofereça segurança, disponibilidade, redundância e um número adequado de nós para manipular os dados da rede, além de uma solução para tornar os dados armazenados imutáveis. Atingir esses requisitos é caro e propenso a um processo de desenvolvimento demorado. Uma alternativa é alugar algum serviço de nuvem que já possua bancos de dados distribuídos tradicionais ou implementações de DLT, dependendo da tecnologia para construção da WSDB escolhida. Essa opção reduz o tempo de desenvolvimento, uma vez que a responsabilidade sobre a infraestrutura é do proprietário da nuvem, no entanto, essa opção ainda é cara e exige o conhecimento da nuvem que está sendo usada.

Se a opção for por soluções públicas baseadas em DLT, a infraestrutura necessária será compartilhada entre os participantes, baseado em nuvem também se aplica, mas também existe o caso da computação distribuída em servidores locais ou em pequenos *data centers*. Nos dois casos, para a DLT, existe o custo adicional associado à disseminação de informações (por exemplo, a ocupação do espectro e as transações relacionadas no contexto do DSA) para todos os nós da rede que participam armazenando os registros dos dados. Espera-se dos nós participantes das DLTs a capacidade de se associarem e manterem a rede ativa, ajudando no estabelecimento de um consenso e no armazenamento de dados. Essa capacidade é compartilhada entre os nós da rede, pois se houver um nó inativo, as propriedades da rede serão preservadas, eliminando a necessidade de infraestrutura dispendiosa. Por exemplo, uma WSDB descentralizada pode ser implementada por um conjunto de entidades que participam de um mercado de espectro, dividindo os custos de infraestrutura. Nesse caso, cada participante cobre seus próprios custos ao executar um nó da DLT, contribuindo para a resiliência da solução final e para a imutabilidade no armazenamento e processamento de informações.

Uma característica comum entre DLTs existentes, como por exemplo o Bitcoin [56], Ethereum [57] e IOTA [58], é o uso de algum tipo de moeda virtual para as transações. A primeira Blockchain, criada por Satoshi Nakamoto, utiliza como moeda o Bitcoin, a Blockchain Ethereum utiliza o Ether e a moeda da IOTA é o Miota. Para realizar qualquer transação na rede Ethereum (por exemplo, efetuar ou receber um pagamento ou trocar dados), é necessário ter uma carteira com a respectiva moeda. Portanto, o requisito de ter uma carteira com moedas para realizar uma transação é um aspecto relevante, uma vez que evita comportamentos maliciosos. Assim, um operador mal-intencionado precisa obter uma carteira com alguma moeda antes de tentar alguma ação, aumentando o trabalho a ser realizado para executar alguma transação fraudulenta. Na IOTA existe a possibilidade de realizar transações de valor zero, no entanto, para concluir uma transação, os clientes precisam validar duas anteriores, executando uma prova de trabalho, neste caso os usuários maliciosos também são desmotivados pelo trabalho extra que devem fazer. Esses e muitos outros aspectos precisam ser colocados em consideração na escolha de uma DLT (ou uma combinação de tecnologias) para a estrutura DSA, especialmente, se um mercado de troca e locação com pagamentos pelo uso do espectro for implantado.

Com o Ethereum existe a possibilidade de implementar contratos inteligentes para

monetizar o sensoriamento espectral, trocas e locações de licenças para criar um novo tipo de mercado de espectro, conforme explicado em [46] e [59]. Contratos inteligentes são *scripts* autônomos que concluem as transações entre as partes somente quando seus requisitos são atendidos. Eles podem ser utilizados para controlar o processo de alocação de espectro entre a WSDB e os dispositivos secundários interessados e, ao mesmo tempo, os contratos inteligentes podem ser usados para recompensar a rede IoT que fornece as informações de sensoriamento. O contrato também pode ser usado para cobrar taxas de SUs e pagar PUs, criando assim um novo modelo de negócios do mercado do espectro, onde o PU, ciente da ociosidade do espectro do qual é dono da licença, o PU pode locá-lo para um SU recebendo por isso. O principal benefício do uso de contratos inteligentes é que, uma vez publicados, eles são imutáveis e serão executados exatamente como foram programados, sem exceções, essa característica pode ser usada para garantir a integridade das operações de compartilhamento de espectro, uma vez que sempre se comportará conforme o esperado. Este tipo de abordagem torna-se mais atrativo para a concepção da gerência da WSDB.

Neste ponto, é importante ressaltar o papel da monetização e da cobrança de eventuais taxas no processo. O mercado secundário de espectro é idealizado com contratos inteligentes fim a fim, isto é, realizados diretamente entre PU e SU, com a base de dados fornecendo apenas a infraestrutura para realização do contrato. A licença de espectro é um ativo a ser negociado entre as partes com o pagamento de alguma moeda (ou criptomoeda) no processo. Tomando como exemplo o que é feito na Blockchain Ethereum, uma taxa é cobrada pela rede para a realização de transações, por exemplo, um contrato inteligente. No Ethereum, essa taxa é dada em *Gas*, uma fração muito pequena da moeda desta DLT (o Ether). A taxa é utilizada como recompensa há mineradores da rede. No contexto de DSA, essa taxa pode ser vista como uma forma de recompensar o administrador da rede IoT que realiza a tarefa de sensoriamento espectral e disponibiliza estas informações para a base de dados. Assim sendo, a adoção de módulos de sensoriamento espectral pelo administrador de uma rede IoT pode ser incentivada economicamente com taxas oriundas da realização de contratos inteligentes na plataforma da WSDB.

A solução da fundação IOTA é outro tipo de DLT chamada *Tangle*, que é um espécie de DAG [60, 61]. A motivação para a solução da IOTA vem de duas desvantagens das soluções baseadas em Blockchain: o alto gasto de energia para executar uma rede e os custos de transação, que podem inviabilizar algumas aplicações. Diferentemente de uma Blockchain como o Ethereum, não existem mineradores ou taxas na *Tangle* da IOTA. Uma característica que dá vantagem ao DAG frente à Blockchain diz respeito quanto à escalabilidade da rede. A Blockchain possui problemas intrínsecos de gargalo conforme a rede cresce, limitados pela capacidade da rede de validar as transações e completar novos blocos. Devido ao princípio de validação do DAG, o mesmo não possui este problema de crescimento em escala, enquanto a Blockchain se torna mais lenta e menos produtiva à medida que cresce, ou seja, o tempo para realizar uma transação aumenta, a *Tangle* se torna mais escalável e mais rápido. A principal desvantagem em utilizar a *Tangle* da IOTA é que ele não suporta contratos inteligentes conforme mencionado em [62], no entanto, a IOTA criou um protocolo chamado Qubic (*Quorum-based Computations*) [63, 64], que propõe trazer esta funcionalidade dos contratos inteligentes para a *Tangle*. Caso isso concretize, este tipo de solução

torna-se um excelente candidato para WSDB em ensaio reais. Devido ao baixo custo energético das transações, a IOTA está sendo aplicado para monetizar dispositivos IoT, criando o que está sendo chamado de "mercado de dados das coisas" (*things data market*) [65,66]. O DSA com transações operadas com a *Tangle* poderia ser, portanto, uma forma de monetizar os dispositivos SSIoT na arquitetura proposta neste trabalho.

Para decidir em favor de uma DLT é necessário análise do cenário como um todo e de quais características devem possuir para atender aos requisitos. Em [67], um importante estudo é feito levantando os múltiplos cenários onde a Blockchain poderia ser empregado no CBRS. Entre os vários casos de uso citados pelo autor, o uso híbrido da Blockchain com bases de dados convencionais faz-se viável para interface entre administradores SAS (SAS-SAS), no sensoriamento espectral como um serviço (ESC-SAS), no mercado de espectro através dos administradores SAS (SU-SAS-PU)

4.4 Aspectos de segurança

Dentre as várias características a serem pensadas no projeto como motivação para se adotar uma tecnologia viabilizadora, a segurança, como um todo, é uma das mais importantes. Quando se trata da segurança neste contexto, ela pode se dar (i) nas transmissões dos usuários da rede; (ii) na confiabilidade, disponibilidade e integridade dos dados armazenados na WSDB e (iii) nas transações efetuadas através da base de dados.

Dentre as possibilidades de agressão à segurança das transmissões de uma rede pode-se citar a tentativa de interceptação da mensagem por nós maliciosos, o ataque através da geração de sinal interferente (*jamming*) ou a emulação do usuário primário (*primary user emulation*, PUE).

A segurança da informação numa base de dados como a WSDB alimentada por sensoriamento espectral, como a proposta neste trabalho, pode envolver tanto a confiabilidade da informação, uma vez que dispositivos maliciosos podem tentar produzir falsos dados a fim de serem recompensados indevidamente, quanto a segurança dos dados, contra leitura e registro indevido pelos dispositivos maliciosos ou violação à privacidade de ambos os usuários, primário e secundário.

Em um último cenário, ao se autenticar transações de espectro através de uma base de dados, fazendo a locação da licença de um PU para um SU através de um contrato na WSDB, é necessário prover mecanismos para que as transações não possam ser fraudadas.

Em [68], o autor fez uma ampla abordagem dos cenários e de ameaças à segurança envolvidas no compartilhamento de espectro. A Figura 4.7 reproduz um diagrama com a taxonomia das falhas e vulnerabilidades de segurança, alguns exemplos levantados pelo autor são citados para cada grupo. Também em [69] a segurança das redes cognitivas é abordada, as possibilidades de ataques e a taxonomia das vulnerabilidades. A vantagem da análise feita em [68] é que ela aborda de forma mais ampla os aspectos de segurança, seja para sensoriamento espectral, seja para base de dados. Em abordagens de compartilhamento do espectro por sensoriamento espectral, vulnerabilidades e ameaças podem ser levantadas para a camada física, para a camada MAC ou ainda

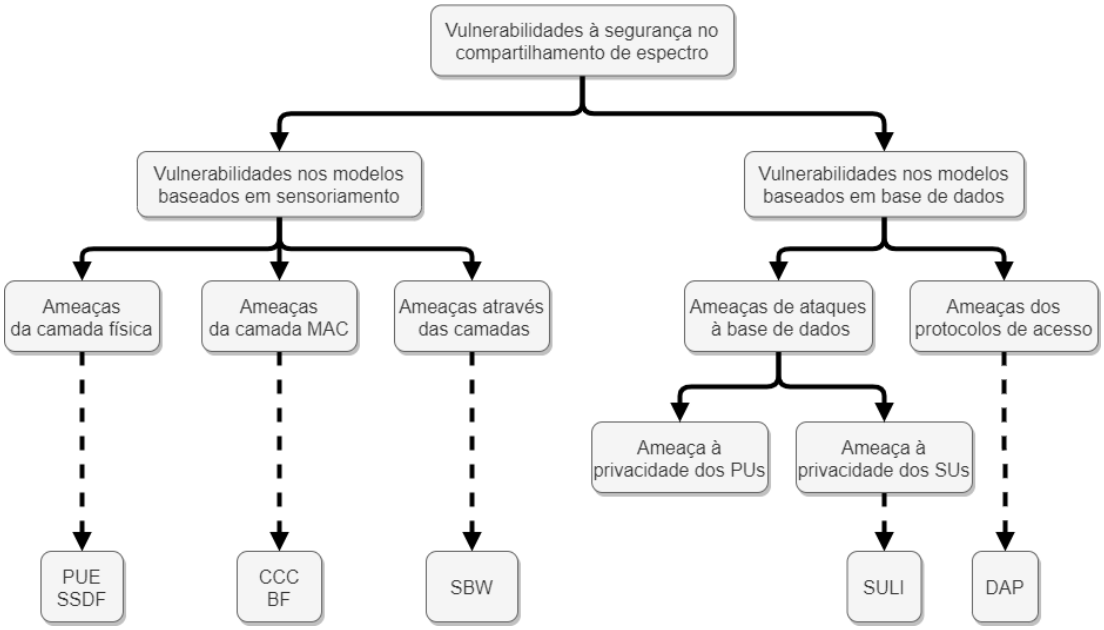


Figura 4.7: *Segurança e ameaças no contexto do compartilhamento de espectro.*

através de ambas as camadas. No que diz respeito ao compartilhamento do espectro possibilitado por base de dados, as ameaças podem englobar a base de dados em si, como a integridade e privacidade dos dados dos PUs e SUs, mas também falhas relacionadas aos protocolos de acesso à base.

Modelos de DSA baseados em sensoriamento espectral estão sujeitos à múltiplas falhas e ameaças de segurança, as quais serão analisadas segundo a taxonomia abordada por [68]:

- **Ameaças da camada física** são ameaças que impactam diretamente o processo de sensoriamento espectral, levando a um comprometimento do sistema em si. Dentre estas ameaças, levanta-se a PUE, onde o agressor emula a transmissão de um PU impossibilitando a rede secundária de transmitir devido a uma decisão errada a respeito do uso do espectro, e a falsificação dos dados de sensoriamento espectral (*spectrum sensing data falsification*, SSDF), onde os usuários mal intencionados enviam falsas medições de sensoriamento a fim de comprometer a tomada de decisão em uma rede com sensoriamento espectral cooperativo.
- **Ameaças da camada MAC** são ataques que podem impossibilitar as funções de controle da rede cognitiva. Este tipo de rede trabalha com canais fixos operando com alguma tecnologia de múltiplo acesso, como TDMA por exemplo, que possibilita a comunicação entre a estação base e os vários SUs. Um usuário mal intencionado pode atacar justamente o canal de controle cognitivo (*cognitive control channel*, CCC) a fim de desabilitar uma rede secundária ou fazer falsificação de *beacons* (*beacons falsification*, BF) utilizados para coordenar a transmissão dos SUs.
- **Ameaças através das camadas** são as formas de ataque que podem afetar mais de uma camada da rede. Em redes cognitivas que fazem uso da tecnologia acesso múltiplo por verificação de portadora com prevenção de colisão (*carrier sense*

multiple access with collision avoidance, CSMA/CA), após realizarem o sensoriamento, os CRs geram uma janela de tempo aleatória que devem esperar antes de transmitir, chamado de tempo de *backoff*. No caso de ocorrer uma colisão na transmissão, um tempo de *backoff* maior é gerado, o que pode crescer dobrando ou de forma exponencial. O dispositivo mal intencionado pode trabalhar gerando janelas de tempo muito pequenas e ganhando prioridade de transmissão frente a outros usuários, o que é chamado de ataque de pequena janela de *backoff* (*small backoff window*, SBW). Esse tipo de ataque pode ser feito combinado com SSDF e levando vantagem de vulnerabilidades entre múltiplas camadas.

Quando o DSA é viabilizado através de modelos de base de dados (WSDB por exemplo), uma série de riscos passam a envolver a segurança do sistema, incluindo a confiabilidade e integridade dos dados contra modificações não autorizadas, a disponibilidade da informação mediante ataques de negação de serviço (*denial of service*, DoS) e a privacidade contra vazamentos. Num primeiro cenário, pode-se analisar a segurança dos dados na WSDB como um todo, bem como a segurança da informação no processo de acesso à base de dados.

- **Ameaças à base de dados** envolvem principalmente a questão de privacidade, como são necessárias tanto informações dos PUs quanto dos SUs no registro, ambos os usuários correm o risco de exposição de dados. Como levantado por [68], as informações dos PUs possuem um certo grau de publicidade, uma vez que devem ser repassadas aos SUs para que os mesmos possam valer-se do compartilhamento do espectro. Contudo, se observar cenários como o CBRS, onde o usuário protegido da rede são serviços governamentais e que podem incluir questões de defesa nacional, a privacidade destes PUs se torna peça chave. Uma técnica de ataque que compromete a privacidade da localização do SU é estudada em [70], chamada de dedução da localização baseada na utilização do espectro (*spectrum utilization-based location inferring*, SULI), onde o usuário malicioso pode deduzir a localização de um SU através do seu uso do espectro. Além da privacidade dos dados, a disponibilidade pode ser comprometida caso ataques DoS sejam direcionados à base de dados e a confiabilidade dos dados pode ser duvidosa caso o provedor da informação seja uma rede que conte com dispositivos maliciosos, algo similar ao que ocorre com a falsificação das informações através de ataques PUE ou SSDF na abordagem de sensoriamento espectral.
- **Ameaças ao protocolo de acesso** são aquelas que podem ocorrer por meio de vulnerabilidades no protocolo de comunicação entre SUs e a WSDB. Os possíveis ataques ao protocolo de acesso à base de dados (*database access protocol*, DAP), levantados na concepção por exemplo do PAWS, são: dispositivos maliciosos camuflados como dispositivos registrados, ataques para modificar ou impedir consultas à base de dados, ataques para modificar ou impedir respostas da base de dados, dispositivos mal intencionados que atuem como uma base de dados provendo falsas respostas ou a falsificação das informações por meio de ataques do tipo *spoofing* [19, 71].

Dentre as vantagens que uma abordagem híbrida de sensoriamento espectral e base de dados tem a oferecer está o aumento da segurança geral no compartilhamento de

espectro. As falhas que podem ser exploradas por uma abordagem acabam sendo compensadas pela outra, tornando mais complicado o processo para o atacante. Pode-se citar por exemplo a PUE, no caso de uma rede cognitiva que detecte um rádio emulando o sinal do transmissor primário, o conhecimento prévio de que não existe nenhum PU transmitindo em dada localização possibilita que o sinal detectado pelo CR seja analisado como de um dispositivo malicioso. Por outro lado, redes de sensoriamento espectral podem ser utilizadas para fazer a detecção de usuários primários e disponibilizar dados que não requisitem expor informações da privacidade do PU quando se tratar de um usuário crítico (uma aplicação militar ou governamental sigilosa).

Em [72], um importante modelo de cooperação mútua entre a rede primária e os dispositivos secundários é abordada. Um tipo de ataque que pode ocorrer nas transmissões de uma rede é o chamado *eavesdropping* que pode atuar de forma a espionar as comunicações de uma rede, a fim de interceptar o conteúdo da mensagem transmitida (caso atue de forma passiva) ou até mesmo adulterar o conteúdo da mensagem (quando atua de forma ativa). Quando a rede primária carece de segurança, os SUs podem atuar de forma cooperativa, retransmitindo a mensagem na rede e ao mesmo tempo adicionando interferência contra o usuário malicioso (*jamming* cooperativo), chamado de *eavesdropper*. Como moeda de troca, a rede primária pode conceder o acesso ao espectro aos usuários secundários.

Para a infraestrutura das redes IoT esse tipo de abordagem auxiliando a rede primária pode não ser viável frente ao gasto energético ou à complexidade extra atribuída, contudo, pode ser vantajoso para as redes secundárias que estejam valendo-se do compartilhamento do espectro habilitado pela base de dados. Os SUs podem receber uma compensação ao atuarem auxiliando na segurança da rede primária. Essa compensação pode ser concebida através de ferramentas no sistema de gerência e troca de espectro da base de dados, onde a contribuição dada pela rede secundária pode servir como moeda por espectro para a rede primária.

Ainda no quesito de segurança das transmissões, quando se trata de bandas de interesse governamental, como o CBRS, os SUs são comunicados pela base de dados para cessar operação sempre que um dispositivo for transmitir, porém pode ser de interesse de um usuário mal intencionado interferir em sistemas de radares militares. Neste ponto, uma infraestrutura de sensoriamento operando em tempo real, como a SSIoT, pode ser útil para detectar o usuário malicioso e reportar aos agentes de segurança a geolocalização do mesmo, uma vez que a ampla distribuição de dispositivos permitiria estimar a posição com base nas potências recebidas em cada dispositivo.

O desempenho de técnicas de sensoriamento aliadas à base de dados para detecção de sinais de radar já foi estudado em trabalhos como [15]. Isso pode ser explorado para assegurar a confidencialidade do usuário protegido, uma vez que é possível fornecer à base de dados a zona de exclusão para os SUs que forem acessar o espectro, mas sem a necessidade de comprometer neste exemplo as coordenadas de um sistema federal de radar. Uma vez que a base de dados tradicional precisa destas coordenadas de um usuário protegido para que seja delimitada a zona de exclusão, essa informação crítica e sigilosa para este tipo de usuário pode ficar exposta à vulnerabilidades e ataques criminosos. O sensoriamento pode ser usado para modelar o mapa do ambiente de rádio sem a necessidade desta exposição do PU inerente do modelo de base de dados,

garantindo assim, maior privacidade e segurança.

Quando se trata da base de dados, uma série de pontos podem ser abordados. Quando se adota base de dados centralizada, existem riscos de segurança envolvidos relacionado à disponibilidade da informação. Um problema crítico que pode comprometer a disponibilidade dos dados é o chamado "ponto único de falha" quando se trada de uma arquitetura de DSA baseada em uma única base de dados. Para lidar com esse problema, um banco de dados distribuído é mais vantajoso. A realização dessa solução distribuída requer um sistema de suporte que implemente confidencialidade, integridade, disponibilidade e autenticidade. Logo, para construir uma base de dados que cumpra esses requisitos, pode se usar bancos de dados convencionais, como SQL, NoSQL ou ambos, podem ser explorados, ou uma solução baseada em DLT, ou ainda, uma hibridização deles.

Em um cenário de base de dados distribuído, uma outra falha pode acontecer, a chamada "falha bizantina" que ocorre quando dados inconsistentes estão presentes na base de dados. Como discutido em [73], algumas soluções de base de dados distribuídas como uma entidade para auditar os dados pode ser utilizado para solucionar o problema. Em outro caso, uma base de dados baseada em DLT já possui uma defesa natural contra o problema do "ponto único de falha" devido à característica descentralizada das DLTs e para fazer qualquer novo registro nesse banco de dados, é necessário que haja um consenso entre todos os participantes. O consenso também trata de uma questão importante em relação aos bancos de dados distribuídos: a impossibilidade de armazenar dados incoerentes ou entradas duplicadas (uma entrada duplicada em uma DLT significa uma despesa dupla), isso resulta na garantia de que todos os nós participantes da DLT possuem os mesmos dados. Desta forma, tecnologias DLT como a Blockchain também oferecem ferramentas de proteção contra "falhas bizantinas".

Bases de dados centralizadas também são vulneráveis a ataques DoS, cujo objetivo é interromper o funcionamento do sistema. Em uma rede centralizada o ataque deste tipo poderia levar desde a instabilidades quanto à suspensão dos serviços mantidos pela WSDB. Em redes DLT, como as informações são armazenadas nos nós distribuídos da Blockchain, a solução é capaz de se ajustar para lidar com os nós ausentes. Além disso, a vantagem da gravação imutável de informações torna os registros da Blockchain facilmente auditáveis. Qualquer organismo de regulamentação pode verificar as informações na Blockchain como uma fonte confiável, dependendo, é claro, da capacidade de confiança dos participantes que leem e escrevem na Blockchain. Certificados assinados digitalmente, criptografia pública e mecanismos de confiança podem ser adotados para autenticar e autorizar o acesso à esta WSDB.

Para soluções híbridas, onde a base de dados pode ser alimentada por sensoriamento, o uso de DLTs também pode melhorar a segurança desta rede, onde dispositivos maliciosos podem ter como objetivo fornecer dados incorretos de sensoriamento (SSDF), acessar ou modificar registros, ou ainda utilizar indevidamente o espectro. Como é possível utilizar dos mecanismos providos pela DLT para criar transações de arrendamento da licensa de espectro no cenário do DSA, esses dispositivos maliciosos podem ser incluídos em uma lista negra e impedidos de participar de futuros contratos para locação de espectro, desencorajando quaisquer comportamento malicioso ou egoísta por parte dos usuários.

As ameaças no entanto podem ocorrer na requisição à WSDB bem como na resposta que ela retorna à rede secundária. Para a comunicação com a base de dados, o PAWS [19] define o HTTPS como protocolo de comunicação, fazendo uso do TLS para a autenticação.

O arrendamento da licença de espectro, seja de caráter de uso exclusivo de um PU ou uma licença de caráter prioritário como a PAL descrita no CBRS, é um importante meio a ser explorado e que é viabilizado pelo uso de base de dados. De forma geral a base de dados permite que PUs, SUs, e usuários que apenas prestam serviço de sensoriamento interajam e façam trocas, seja em questão de remuneração ou de compensação. Por exemplo, um usuário secundário pode adquirir *tokens* para acesso ao espectro quando atuar contribuindo com a segurança da transmissão do PU, dispositivos de sensoriamento podem receber estes *tokens* ao prover informações para a base de dados e que forem confiáveis, como proposto em [46], ou outras formas de interação entre os atores presentes no DSA.

A atuação de usuários maliciosos neste contexto pode acontecer por exemplo, na tentativa de prover falsas informações de sensoriamento à base de dados, que pode ser contornado através de um sistema de lista negra na base de dados distribuída baseada em uma DLT. Tanto [46] quanto [72] trazem a concepção de mecanismos distintos de reputação para os dispositivos da rede. Se a base de dados do DSA for baseada em tecnologias distribuídas, a adulteração dos dados é improvável, uma vez que requer o consenso dos nós da rede.

Transações de alocação de licença efetuados através de contratos inteligentes incrementam ainda mais a segurança da operação, mesmo que as partes não tenham conhecimento ou confiança mútua, o contrato inteligente assegura que a transação só será completada quando os requisitos forem atendidos para ambas as partes, uma vez que isso ocorre, o contrato é registrado na DLT e se torna imutável. Em redes baseadas em DLTs como Blockchain ou Tangle, será necessário o uso de sua respectiva moeda, que desencoraja ainda mais comportamento mal intencionado nas operações.

Dessa forma, a segurança nos vários aspectos abordados para o DSA pode ser aprimorada ao se fazer uso das abordagens combinadas, sensoriamento espectral e base de dados de geolocalização, ganhando-se maior privacidade para usuários que necessitam de tratamento especial e cobrindo vulnerabilidades que podem ser exploradas quando as abordagens são empregadas de forma isolada. Além disso, o uso de novas tecnologias como base de dados distribuídas, baseadas em alguma DLT, além de mitigar falhas inerentes às bases de dados convencionais, também viabiliza maior segurança entre as interações dos vários atores envolvidos no processo de DSA, como a rede primária, a rede secundária e a rede de sensoriamento.

4.5 Sumário

Na Tabela 4.1 é apresentada uma relação com os principais elementos da proposta, seus papéis dentro da arquitetura introduzida neste capítulo, bem como os elementos diretamente relacionados, sejam os que fazem parte do elemento citado ou os agentes que com ele operam. Nesta tabela, ”rede”é utilizado para descrever a rede física, com

os equipamentos de comunicação, enquanto ”operador”descreve os responsáveis pela rede.

Tabela 4.1: *Síntese dos elementos, suas funções na arquitetura proposta e os elementos diretamente relacionados.*

Elemento	Papel	Elementos relacionados
Rede primárias	Manter um registro ativo na base de dados para oferta e alocação de espectro. Prover os dados dos transmissores para uso nos modelos de proteção.	Operador primários.
Rede secundárias	Realizar consultas periódicas à base de dados para realizar ou renovar o acesso ao espectro. Implementar os parâmetros estabelecidos para proteção dos usuários primários.	Operadores secundários, transmissores e dispositivos secundários.
Redes IoT	Fornecer dispersão espacial e infraestrutura de rede para implantação de módulos sensores de espectro.	Operadores IoT, dispositivos IoT, módulos sensores de espectro e *gateways*.
Bases de dados (WSDB)	Centralizar e manter o domínio da informação de espectro; agregar as funcionalidades de gerência do espectro, registro das redes secundárias e atribuição dos canais; fornecer as funcionalidades e infraestrutura para o mercado secundário de espectro.	Bancos de dados convencionais, DLTs e o PAWS.
PAWS	Interface de acesso ao espectro entre as redes secundárias e a WSDB	Redes secundárias e WSDB.
Bancos de dados convencionais	Permitir o armazenamento do mapa de canais para rápida resposta à rede secundária em cenários que não permitam altos atrasos associados às operações em DLTs.	WSDB
DLTs	Implementar segurança no processo de DSA e viabilizar o mercado secundário de espectro através de contratos inteligentes.	Contratos inteligentes. DLTs: Ethereum e IOTA.
Contratos inteligentes	Executar as transações de espectro diretamente entre os usuários, permitir a monetização destas transações e cobrança de taxas para manutenção do ecossistema.	Operadores primários e operadores secundários.
Tarifas sobre transações de espectro	Permitir arrecadação de recursos para o pagamento de incentivos à rede IoT pela realização da tarefa de sensoriamento espectral.	Operadores primários, secundários e IoT.
Núcleo (*core*) da WSDB	Permitir a gerência de todo o ecossistema, garantindo as interfaces para as redes conectadas efetuarem o registro e solicitarem acesso ao espectro. Além disso, fornecer a interface de comunicação para os operadores e a interface de controle para entes reguladores.	Redes secundárias, operadores primários, secundários, IoT e agência reguladora.

A nível de segurança da arquitetura, destacam-se três cenários levantados: (i) dos protocolos entre a rede IoT e a WSDB; (ii) da solução para o DSA; e (iii) da integridade da base de dados e confiabilidade das transações de espectro. Para segurança entre a rede IoT e a base de dados é sugerido o uso de protocolos que permitam encriptação dos dados e outras técnicas de proteção, uma alternativa menos segura é o MQTT, outras como o HTTPS e o AMQP oferecem mais proteção. Estes protocolos precisam ser testados em uma solução real para avaliar o desempenho e definir os melhores. No contexto geral do DSA, foi demostrado que a cooperação entre as técnicas de sensoriamento espectral e base de dados pode incrementar a segurança do processo. Uma

abordagem híbrida é capaz de mitigar ataques com informações prévias de transmissores e assegurar privacidade à usuários críticos. Por último, a integridade da base de dados pode garantida com o uso de DLTs, como o Blockchain, e transações de espectro realizadas por meio de contratos inteligentes são imutáveis uma vez publicado na rede.

Capítulo 5

Conclusões e oportunidades futuras

Neste trabalho foi apresentada uma revisão das carências atuais no cenário de compartilhamento de espectro, seguido da proposta de uma nova arquitetura baseada em redes Internet das coisas (*Internet of things*, IoT) para sensoriamento espectral e um modelo de gerência de espectro integrado com esta arquitetura baseado em tecnologia de registro distribuído (*distributed ledger technology*, DLT).

A dispersão de dispositivos IoT pode ser um grande facilitador para que os dados de sensoriamento espectral, mantidos em uma base de dados, possam refletir com maior fidelidade a ocupação do espectro em determinadas localidades. Além disso, podem fornecer maior privacidade no compartilhamento de espectro, quando se tratar de usuários governamentais ou aplicações militares, como exemplo, os sistemas de radar no serviço de rádio banda larga do cidadão (*citizens broadband radio service*, CBRS). O uso DLTs por sua vez, traz diversos benefícios e funcionalidades ao cenário de gerência do espectro, viabilizando um modelo de alocação de bandas dinâmico mais eficiente que a alocação fixa, benéfico tanto aos detentores das licenças, aos usuários e aos órgãos de controle.

O caráter de integração e segurança da arquitetura proposta foi analisado com base nas deficiências existentes nos modelos convencionais de compartilhamento de espectro atuais. Dentre as vantagens do uso de DLTs, está a integridade, confiabilidade e imutabilidade dos registros, que são cruciais para aumentar a segurança e cobrir as falhas dos modelos em uso.

Um dos maiores os desafios existentes para a concepção da rede Internet das coisas com sensoriamento espectral (*spectrum sensing Internet of things*, SSIoT) é a criação de módulos de sensoriamento espectral de baixíssimo custo e com eficiência energética para serem acoplados à dispositivos IoT. Na pesquisa apresentada no Apêndice I foi investigado o uso de uma tecnologia de mitigação de interferência do protocolo Bluetooth como alternativa de baixo custo para realizar o sensoriamento espectral. A partir da prova de conceito criada abre-se oportunidade para desenvolvimento de protótipos funcionais para essa tarefa.

Um modelo para a construção da arquitetura proposta e integração com a base de dados de espectro é deixada no Apêndice II como caminho para investigação em trabalhos futuros. Aprimoramentos no conceito e avaliação prática do desempenho são campos a serem explorados.

Outra oportunidade é um estudo de caso para a monetização de espectro e da economia que é proposta entre os usuários pra alocação do espectro via contrato inteligente. Como serão pagas as trocas por espectro? Qual moeda? Moeda real ou uma criptomoeda atrelada à DLT? Estas questões são alguns dos desafios deixados. Ainda no que compete ao uso de DLTs, o tempo de transação neste tipo de rede é normalmente alto. Considerando que a base de dados deve habilitar a rede secundária em um espaço de tempo muito menor, algumas soluções da rede devem ser disponibilizadas ainda utilizando base de dados convencionais. É oportuno a investigação dos melhores métodos para o emprego de DLTs na arquitetura, mantendo a segurança nos contratos de espectro entre usuários, mas ao mesmo tempo, assegurando um baixo tempo de resposta na consulta pelo mapa de disponibilidade de espectro e permissão de acesso aos canais. O uso da arquitetura modular, tal qual apresentada no Apêndice II, pode contribuir para uma construção híbrida da solução que atinja estas metas.

Referências Bibliográficas

[1] ANATEL, "*Resolução Nº 716, de 31 de outubro de 2019*," Acesso em: 02/12/2020. [Online]. Disponível em: http://www.in.gov.br/web/dou/-/resolucao-n-716-de-31-de-outubro-de-2019-225245741.

[2] X. Hong, J. Wang, C. X. Wang, and J. Shi, "Cognitive radio in 5G: A perspective on energy-spectral efficiency trade-off," *IEEE Communications Magazine*, vol. 52, no. 7, pp. 46–53, 2014.

[3] L. Zhang, M. Xiao, G. Wu, M. Alam, Y.-C. Liang, and S. Li, "A survey of advanced techniques for spectrum sharing in 5g networks," *IEEE Wireless Communications*, vol. 24, no. 5, pp. 44–51, 2017.

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

[5] D. Corral-de-Witt, S. Ahmed, F. Awin, and J. L. Rojo-Álvarez, "An Accurate Probabilistic Model for TVWS Identification," *Applied Sciences*, vol. 9, no. 20, pp. 1–25, 2019.

[6] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, 2009.

[7] O. Holland, H. Bogucka, and A. Medeisis, *Opportunistic Spectrum Sharing and White Space Access: The Practical Reality*, 1st ed. New Jersey: John Wiley & Sons, Inc, 2015.

[8] H. Harada, "White space communication systems: An overview of regulation, standardization and trial," *IEICE Transactions on Communications*, vol. E97-B, no. 2, pp. 261–274, 2014.

[9] "IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 22: Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands," *IEEE Std 802.22-2011*, pp. 1–680, 2011.

[10] Federal Communications Commission *et al.*, "Amendment of part 15 of the commission's rules for unlicensed operations in the television bands, repurposed 600 MHz band, 600 MHz guard bands and duplex gap, and channel 37: Notice of proposed rulemaking," *FCC: Notice of Proposed Rulemaking, ET Docket No. 14*, vol. 144, 2014.

[11] Ofcom, "*A framework for spectrum sharing*," Jul. 2015, Acesso em: 02/12/2020. [Online]. Disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0032/

79385/spectrum-sharing-framework.pdf.

[12] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 4, no. 1, pp. 40–62, 2011.

[13] Y. Arjoune and N. Kaabouch, "A comprehensive survey on spectrum sensing in cognitive radio networks: Recent advances, new challenges, and future research directions," *Sensors*, vol. 19, no. 1, p. 126, 2019.

[14] Z. Qin, Y. Gao, and C. G. Parini, "Data-assisted low complexity compressive spectrum sensing on real-time signals under sub-nyquist rate," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1174–1185, 2016.

[15] F. Paisana, J. P. Miranda, N. Marchetti, and L. A. Dasilva, "Database-aided sensing for radar bands," *2014 IEEE International Symposium on Dynamic Spectrum Access Networks, DYSPAN 2014*, pp. 1–6, 2014.

[16] Federal Communications Commission *et al.*, "Amendment of part 15 of the commission's rules for unlicensed operations in the television bands, repurposed 600 MHz band, 600 MHz guard bands and duplex gap, and channel 37:," *FCC: Report and Order, No. 15*, vol. 99, 2015.

[17] F. C. Commission, "Fcc opens 6 GHz band to Wi-Fi and other unlicensed uses," *FCC: Report and Order and Further Notice of Proposed Rulemakin, No. 20*, vol. 51, 2020.

[18] "IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 5: Television white spaces (TVWS) operation," *IEEE Std 802.11af-2013 (Amendment to IEEE Std 802.11-2012, as amended by IEEE Std 802.11ae-2012, IEEE Std 802.11aa-2012, IEEE Std 802.11ad-2012, and IEEE Std 802.11ac-2013)*, pp. 1–198, 2014.

[19] L. Zhu, V. Chen, J. Malyar, S. Das, and P. McCann, "Protocol to Access White-Space (PAWS) Databases," *Internet Eng. Task Force, Fremont, CA, USA, RFC*, vol. 7545, 2015.

[20] M. Tang, Z. Zheng, G. Ding, and Z. Xue, "Efficient tv white space database construction via spectrum sensing and spatial inference," in *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*. IEEE, 2015, pp. 1–5.

[21] Federal Communications Commission, "*FM and TV Propagation Curves*," Acesso em: 02/12/2020. [Online]. Disponível em: https://www.fcc.gov/media/radio/fm-and-tv-propagation-curves.

[22] B. Somdyala, S. Rananga, L. Mfupe, M. Masonta, and F. Mekuria, "Spectrum regulation for future internet networks in developing economies," in *2017 IST-Africa Week Conference (IST-Africa)*. IEEE, 2017, pp. 1–12.

[23] Y. Luo, L. Gao, and J. Huang, *Economics of Database-Assisted Spectrum Sharing*, ser. Wireless Networks. Cham: Springer International Publishing, 2016. [Online]. Available: http://link.springer.com/10.1007/978-3-319-43231-1

[24] LS Telcom, "*Channel Availability*," Acesso em: 02/12/2020. [Online]. Disponível em: https://www.whitespaceforus.com/wsdb/wsdb_ui/Channel_Availability.html.

[25] S. J. Shellhammer *et al.*, "Spectrum sensing in ieee 802.22," *IAPR Wksp. Cognitive Info. Processing*, pp. 9–10, 2008.

[26] Y. Ma, X. Zhang, and Y. Gao, "Joint sub-nyquist spectrum sensing scheme with geolocation database over tv white space," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 3998–4007, 2017.

[27] Ofcom, "*The Wireless Telegraphy (White Space Devices) (Exemption) Regulations 2015*," Dec. 2015, Acesso em: 02/12/2020. [Online]. Disponível em: https://www.legislation.gov.uk/uksi/2015/2066/pdfs/uksi_20152066_en.pdf.

[28] X. Zhang, Y. Ma, H. Qi, Y. Gao, Z. Xie, Z. Xie, M. Zhang, X. Wang, G. Wei, and Z. Li, "Distributed compressive sensing augmented wideband spectrum sharing for cognitive IoT," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3234–3245, aug 2018.

[29] N. Wang, Y. Gao, and B. Evans, "Database-augmented spectrum sensing algorithm for cognitive radio," *IEEE International Conference on Communications*, vol. 2015-Septe, pp. 7468–7473, 2015.

[30] Y. Ma, X. Zhang, and Y. Gao, "An efficient joint sub-nyquist spectrum sensing scheme with geolocation database over tv white space," in *2017 IEEE International Conference on Communications (ICC)*. Paris: IEEE, 2017, pp. 1–6.

[31] S. W. Oh, Y. Ma, M.-H. Tao, and E. Peh, *TV white space: The first step towards better utilization of frequency spectrum*. John Wiley & Sons, 2016.

[32] C. R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE communications magazine*, vol. 47, no. 1, pp. 130—-138, 2009.

[33] H.-N. Tran, C. Sun, Y. D. Alemseged, and H. Harada, "A distributed sensing and caching database for cognitive radio systems," *IEICE transactions on communications*, vol. 95, no. 1, pp. 217–225, 2012.

[34] Ofcom, "Implementing TV White Spaces," p. 111, Fev. 2015, Acesso em: 02/12/2020. [Online]. Disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/68668/tvws-statement.pdf.

[35] S. Aslam, A. ul Haq, J. W. Jang, and K. G. Lee, "Unified channel management for cognitive radio sensor networks aided internet of things," *Sensors (Switzerland)*, vol. 18, no. 8, pp. 1–19, 2018.

[36] J. Vartiainen, M. Matinmikko-Blue, H. Karvonen, and L. Mendes, "Spectrum sharing and operator model for rural and remote area networks," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*. IEEE, 2019, pp. 53–57.

[37] R. Dionísio, J. Ribeiro, P. Marques, and J. Rodriguez, "Combination of a geolocation database access with infrastructure sensing in TV bands," *Eurasip Journal on Wireless Communications and Networking*, vol. 2014, no. 1, pp. 1–14, 2014.

[38] Cognitive Radio Experimentation World, "*Project Overview — CREW Project*," Acesso em: 02/12/2020. [Online]. Disponível em: http://www.crew-project.eu/index.html.

[39] Federal Communications Commission *et al.*, "Wireless Telecommunications Bureau and Office of Engineering and Technology approve four spectrum access system administrators for full scale commercial deployment in the 3.5 GHz band and emphasize licensee compliance obligations in the 3650-3700 MHz band under part 96," *FCC: Public Notice, GN Docket No. 15*, vol. 319, 2020.

[40] Federal Communications Commission, "*3.5 GHz Band Overview*," Abr. 2020, Acesso em: 02/12/2020. [Online]. Disponível em: https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview.

[41] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, "On the application of blockchains to spectrum management," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 193–205, June 2019.

[42] Y. Chen, J. Gu, S. Chen, S. Huang, and X. S. Wang, "A full-spectrum blockchain-as-a-service for business collaboration," in *2019 IEEE International Conference on Web Services (ICWS)*, July 2019, pp. 219–223.

[43] T. Ariyarathna, P. Harankahadeniya, S. Isthikar, N. Pathirana, H. M. N. D. Bandara, and A. Madanayake, "Dynamic spectrum access via smart contracts on blockchain," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2019, pp. 1–6.

[44] P. Yuan, X. Xiong, L. Lei, and K. Zheng, "Design and implementation on hyperledger-based emission trading system," *IEEE Access*, vol. 7, pp. 6109–6116, 2019.

[45] S. Bayhan, A. Zubow, and A. Wolisz, "Smart contracts for spectrum sensing as a service," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN 2018*. Institute of Electrical and Electronics Engineers Inc., jan 2019.

[46] ——, "Spass: Spectrum sensing as a service via smart contracts," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks, DySPAN 2018*. Institute of Electrical and Electronics Engineers Inc., jan 2019.

[47] F. Leens, "An introduction to I^2C and SPI protocols," *Instrumentation & Measurement Magazine, IEEE*, vol. 12, pp. 8–13, 03 2009.

[48] A. A. Wardana and R. S. Perdana, "Access control on internet of things based on publish/subscribe using authentication server and secure protocol," in *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*. IEEE, 2018, pp. 118–123.

[49] D. Mazzer, E. Frigieri, and L. Parreira, "Protocolos M2M para ambientes limitados no contexto do IoT: Uma comparaçao de abordagens," 2015, Inatel.Br.

[50] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," in *2017 IEEE international systems engineering symposium (ISSE)*. IEEE, 2017, pp. 1–7.

[51] Ofcom, "*Qualifying White Space Databases*," Acesso em: 02/12/2020. [Online].

Disponível em: https://tvws-databases.ofcom.org.uk/.

[52] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.

[53] P. Baran, "On distributed communications networks," *IEEE transactions on Communications Systems*, vol. 12, no. 1, pp. 1–9, 1964.

[54] "*Distributed Ledger Technology – DLT: A Raiz de Toda Revolução Tecnológica Atual*," Acesso em: 02/12/2020. [Online]. Disponível em: https://101blockchains.com/pt/distributed-ledger-technology-dlt-guia/.

[55] Y.-C. Liang, *Blockchain for Dynamic Spectrum Management*, jan 2020, pp. 121–146.

[56] S. Nakamoto, "*Bitcoin: A peer-to-peer electronic cash system*," 2009, Acesso em: 02/12/2020. [Online]. Disponível em: https://bitcoin.org/bitcoin.pdf.

[57] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, and M. Marchesi, "A massive analysis of Ethereum smart contracts empirical study and code metrics," *IEEE Access*, vol. 7, pp. 78 194–78 213, 2019.

[58] I. Korotkyi and S. Sachov, "Hardware accelerators for IOTA cryptocurrency," in *2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO)*, April 2019, pp. 832–837.

[59] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 32–39, mar 2018.

[60] S. Popov, "*The Tangle*," 2018, Acesso em: 02/12/2020. [Online]. Disponível em: https://www.iota.org/foundation/research-papers.

[61] W. F. Silvano and R. Marcelino, "IOTA Tangle: A cryptocurrency to communicate Internet-of-Things data," *Future Generation Computer Systems*, vol. 112, pp. 307–319, 2020.

[62] P. Holl, E. Scepankova, and F. Matthes, "Smart contract based API usage tracking on the Ethereum blockchain," *Software Engineering und Software Management 2018*, 2018.

[63] IOTA Foundation, "*The State of Qubic and the future of Smart Contracts on IOTA*," Acesso em: 02/12/2020. [Online]. Disponível em: https://blog.iota.org/the-state-of-qubic-63ffb097da3f.

[64] O. Lamtzidis, D. Pettas, and J. Gialelis, "A novel combination of distributed ledger technologies on internet of things: Use case on precision agriculture," *Applied System Innovation*, vol. 2, no. 3, p. 30, 2019.

[65] N. Živi, E. Kadušić, and K. Kadušić, "Directed acyclic graph as Tangle: an IoT alternative to blockchains," in *2019 27th Telecommunications Forum (TELFOR)*, 2019, pp. 1–3.

[66] P. Tzianos, G. Pipelidis, and N. Tsiamitros, "Hermes: An open and transparent marketplace for IoT sensor data over distributed ledgers," in *2019 IEEE Internati-*

onal Conference on Blockchain and Cryptocurrency (ICBC), 2019, pp. 167–170.

[67] S. Yrjölä, "Analysis of blockchain use cases in the citizens broadband radio service spectrum sharing concept," in *International Conference on Cognitive Radio Oriented Wireless Networks*. Springer, 2017, pp. 128–139.

[68] J.-M. Park, J. H. Reed, A. Beex, T. C. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing," *Proceedings of the IEEE*, vol. 102, no. 3, pp. 270–281, 2014.

[69] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proceedings of the IEEE*, vol. 100, no. 12, pp. 3172–3186, 2012.

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

[71] A. Mancuso, S. Probasco, and B. Patil, "Protocol to access white-space (paws) databases: Use cases and requirements. request for comments: 6953," 2013.

[72] F. Afghah, A. Shamsoshoara, L. Njilla, and C. Kamhoua, "A reputation-based stackelberg game model to enhance secrecy rate in spectrum leasing to selfish iot devices," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2018, pp. 312–317.

[73] R. Nithiavathy, "Data integrity and data dynamics with secure storage service in cloud," in *2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering*. IEEE, 2013, pp. 125–130.

[74] Bluetooth SIG, "*Bluetooth Special Interest Group - Bluetooth 5.2 Feature Overview*," Acesso em: 02/12/2020. [Online]. Disponível em: https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf.

[75] N. Instruments, "*Introduction to Bluetooth Device Testing*," Acesso em: 02/12/2020. [Online]. Disponível em: https://download.ni.com/evaluation/rf/intro_to_bluetooth_test.pdf.

[76] Nokia, "*Wibree forum merges with Bluetooth SIG*," Acesso em: 02/12/2020. [Online]. Disponível em: http://www.wibree.com/wp-content/uploads/Wibree_pressrelease_final_1206.pdf.

[77] R. . Schwarz, "*Bluetooth Adaptive Frequency Hopping on a R&S CMW*," Acesso em: 02/12/2020. [Online]. Disponível em: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1c108/1C108_0e_Bluetooth_BR_EDR_AFH.pdf.

[78] E. Systems, "*ESP32 Overview*," Acesso em: 02/12/2020. [Online]. Disponível em: https://www.espressif.com/en/products/socs/esp32/overview.

[79] ——, "*Standard Setup of Toolchain for Windows*," Acesso em: 02/12/2020. [Online]. Disponível em: https://docs.espressif.com/projects/esp-idf/en/latest/get-started/windows-setup.html#get-started-windows-tools-installer.

[80] F. RTOS, "*Free RTOS - Market leading RTOS (Real-time operating system) for microcontrollers*," Acesso em: 02/12/2020. [Online]. Disponível em: https:

//www.freertos.org/.

[81] Apache, "*Apache - mynewt-nimble*," Acesso em: 02/12/2020. [Online]. Disponível em: https://github.com/apache/mynewt-nimble.

Apêndice I

Sensoriamento Espectral via Modo AFH do Padrão Bluetooth

Uma das necessidades para a viabilização da arquitetura proposta no presente trabalho é a construção dos módulos de sensoriamento espectral de baixo custo e baixo consumo energético. Dentre as pesquisas desenvolvidas, uma prova de conceito para o uso do modo adaptativo de saltos em frequência (*adaptative frequency hopping*, AFH) presente no padrão Bluetooth para a detecção da ocupação espectral.

O protocolo Bluetooth desenvolvido pelo Bluetooth *Special Interest Group* (SIG) é um padrão de comunicação sem fio operando na banda industrial, científica e médica (*industrial, scientific and medical*, ISM) de 2.4 GHz. Sua última versão é a 5.2, apresentada em 6 de janeiro de 2020 [74]. Na geração do Bluetooth 5.0 houve a combinação de tecnologias de versões anteriores que caracterizavam dois modos distintos de operação do padrão, o Bluetooth 1.0/2.0, *basic rate* (BR)/*enhanced data rate* (EDR) e o Bluetooth 4.0 conhecido como Bluetooth *low energy* (BLE).

O Bluetooth BR (1.0) operava utilizando 79 canais de 1 MHz de largura de banda, transmitindo com modulação *Gaussian frequency-shift keying* (GFSK) e atingia taxas de transmissão da ordem de 1 Mbit/s. Na versão seguinte, o Bluetooth EDR (2.0), o protocolo continuou a utilizar da mesma divisão de canais, porém passou a adotar os esquemas de modulação do tipo *quaternary differential phase-shift keying* (QDPSK) e *differential 8-level phase-shift keying* (8DPSK), o que elevou a taxa de transmissão para a casa dos 3 Mbit/s [75].

O BLE inicialmente não foi um padrão desenvolvido pelo Bluetooth SIG, mas sim em paralelo nos laboratórios da Nokia sob o nome de Wibree. O padrão desenvolvido pela Nokia tinha como objetivo um baixíssimo consumo de energia, o que o tornaria adequado para sensores e dispositivos móveis limitados em energia. Posteriormente, o Bluetooth SIG incorporou o Wibree na especificação 4.0 do Bluetooth, dando origem ao BLE [76]. Nesta versão, a comunicação passou a ser feita através de 40 canais de 2 MHz de largura de banda e não mais os 79 canais de 1 MHz.

Desde à sua especificação 1.2, o Bluetooth adota a tecnologia AFH para combater a interferência oriunda de outros sistemas de comunicação, muito comum na banda de 2,4 GHz. Essa técnica utiliza um mapa reconfigurável de canais alocados ao processo

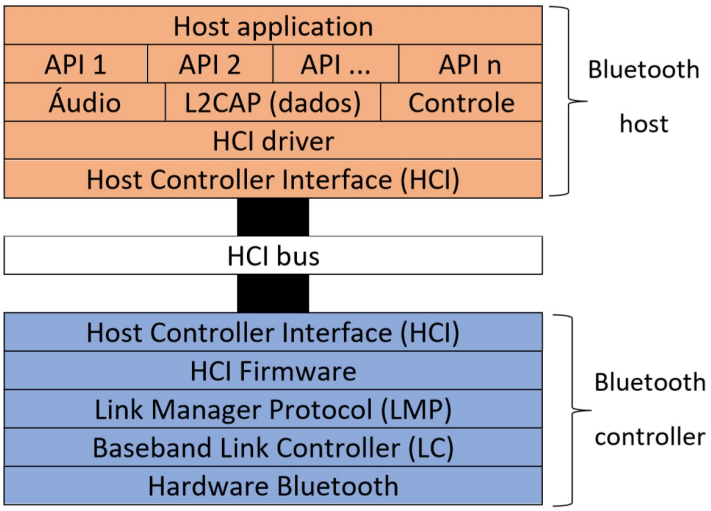


Figura I.1: *Camadas da arquitetura do protocolo Bluetooth.*

de espalhamento espectral por saltos em frequência (*frequency hopping spread spectrum*, FHSS) adotado na interface aérea do padrão. No FHSS, a frequência do canal de comunicação entre o dispositivo mestre e o dispositivo escravo é alterada de forma pseudo-aleatória. A sequência de saltos em frequência contém 2^{27} saltos que ocorrem 1600 vezes por segundo, resultando em um período de $23{,}3$ horas até que a sequência se repita. Durante a conexão Bluetooth, tanto o transmissor quanto o receptor conhecem o padrão pseudo-aleatório, que é calculado baseado na temporização (*clock*) do dispositivo mestre dentro da piconet [77].

Na comunicação Bluetooth, um mapa de canais mantido entre os dispositivos mestre e escravo. Canais livres de interferência são classificados como disponíveis, ou seja, canais que farão parte da sequência de saltos em frequência, neste caso atribuindo-os o bit 1. Caso seja detectada uma interferência suficientemente alta, estes canais são classificados como desabilitados, ou seja, os mesmos não farão parte da sequência de saltos, neste caso atribuindo-se o bit 0. As métricas utilizadas para atribuir essa classificação normalmente são: taxa de erro de bit (*bit error rate*, BER), taxa de erro de pacote (*packet error rate*, PER), indicador da potência do sinal recebido (*received signal strength indicator*, RSSI), razão sinal-ruído (*signal-noise ratio*, SNR) ou de alguma combinação destas métricas [77].

Considerando o uso do BLE, os 40 canais de comunicação são enumerados de 0 a 39, sendo que os canais de 0 a 36 são utilizados para a comunicação de dados enquanto os canais 37, 38 e 39 são canais reservados para controle da comunicação, recebendo o nome de *advertising channels*. Os canais de dados são enumerados de forma sequencial no espectro, enquanto os canais de controle são distribuídos de forma que o canal 37 seja o primeiro da banda, o canal 38 seja localizado entre o canal 10 e o canal 11, e por último o canal 39 localizado no final do espectro.

Na prática, o AFH é uma função do protocolo de gerenciamento de enlace protocolo de gerenciamento de enlace (*link manager protocol*, LMP) que é responsável por gerenciar a conexão entre os dispositivos e é parte da camada de controle (*Bluetooth controller*). Dados e funções pertencentes à funções desta camada inicialmente

não foram pensados para terem uso por camadas superiores e usados em quaisquer aplicações, uma vez que se referem à conexão entre os equipamentos. A camada de controle nem sempre é de código aberto, isso pode limitar como definir a métrica utilizada para classificar os canais. Além disso, nem toda pilha para a camada de hospedeiro (*Bluetooth Host*) possui funções definidas leitura do mapa AFH, quando for disponível, ela será parte da interface host-controlador (*host controller interface*, HCI), que é quem provê ferramentas para, se necessário, acessar dados da camada física. A Figura I.1 exemplifica a arquitetura Bluetooth.

I.1 Aplicação do AFH para sensoriamento espectral

Basicamente, o sensoriamento espectral através do modo AFH do padrão Bluetooth consiste em realizar, em um ambiente controlado, a leitura do mapa de canais dos saltos em frequência. Como ilustra a Figura I.2, dois dispositivos Bluetooth são mantidos conectados de forma cabeada de forma a manter a conexão livre de interferência externa. Ao enlace é adicionado um combinador ligado à uma antena responsável por receber o sinal que se deseja detectar e utiliza-lo como fonte interferente na comunicação Bluetooth.

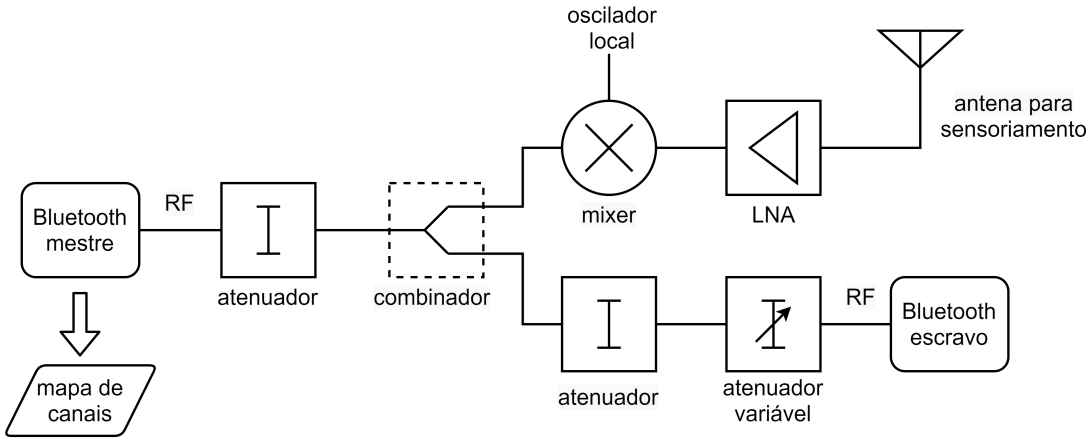


Figura I.2: *Configuração de hardware para sensoriamento via Bluetooth.*

O sinal sensoriado recebido pela antena é amplificado por um amplificador de baixo ruído (*low noise amplifier*, LNA) e tem sua frequência transladada para a faixa de frequências de operação dos transceptores Bluetooth (2.4 GHz), caso tal sinal esteja fora desta faixa. A translação é realizada pelo batimento (multiplicação) do sinal de saída do LNA pela portadora senoidal gerada pelo oscilador local. O sinal resultante do batimento é acoplado ao enlace Bluetooth por meio do combinador (*splitter* ou *combiner*). Atenuadores estão presentes no sistema para que o nível de potência da comunicação dos dispositivos Bluetooth seja colocado em um limiar próximo ao de classificação do canal como desabilitado, de forma que o menor sinal interferente recebido pela antena de sensoriamento seja capaz de alterar a classificação de um ou mais canais no mapa do AFH. A leitura do mapa é então feita através de uma função específica da HCI, permitindo interpretar os canais desabilitados como se a correspondente porção do espectro esteja em uso e os canais habilitados como faixas de

frequências ociosas.

O sensoriamento espectral através do AFH não permite utilizar vários dispositivos para uma fusão de dados no cenário cooperativo, uma vez que a consulta do mapa de canais no dispositivo mestre irá reportar um dado binário de canal livre ou ocupado. Entretanto, pode-se valer de vários módulos de sensoriamento como aquele ilustrado na Figura I.2, voltados para a implementação de um sensoriamento espectral cooperativo com fusão de decisões a fim de aumentar a precisão de detecção em relação ao sensoriamento não cooperativo. Como trata-se de um sistema de baixo custo comparado aos hardwares atualmente utilizados para sensoriamento espectral, almeja-se atingir as métricas de desempenho por meio da alta densidade e distribuição dos dispositivos em vez de alta qualidade individual no sensoriamento, o que se pode conseguir com o acoplamento de módulos de sensoriamento a dispositivos IoT. Esta medida visa prover um amplo sistema de sensoriamento espectral, com elevada resolução espacial e abrangência. Os resultados do sensoriamento podem então alimentar bases de dados de ocupação espectral, as quais podem ser consultadas pela rede secundária, eliminando a necessidade de se ter rádios cognitivos (*cognitive radio*s, CRs) equipados com a funcionalidade de sensoriamento.

I.2 Prova de conceito

Para realização da prova de conceito foram utilizados, como dispositivos Bluetooth, dois módulos *system-on-a-chip* (SoC) ESP32 produzidos pela empresa Espressif Systems [78]. Além destes, foi utilizado um equipamento de rádio definido por software Ettus USRP B210 como gerador de sinal interferente na comunicação entre os ESP32, bem como um computador para a leitura do mapa de canais do AFH. A Figura I.3 apresenta os principais dispositivos utilizados, bem como suas interconexões.

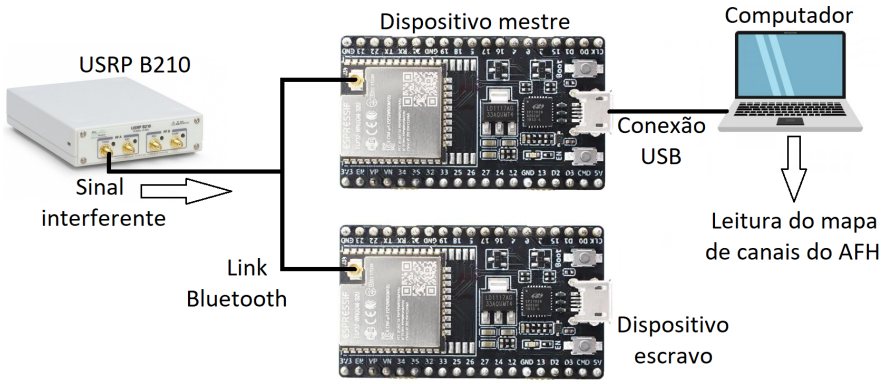


Figura I.3: *Montagem da prova de conceito do sistema de sensoriamento via AFH do padrão Bluetooth.*

O ESP32 é um microcontrolador de baixo custo com diversas funcionalidades já integradas, diversos pinos de entrada e saída analógica e digital, além de interfaces de conexão Bluetooth e WiFi. Suas várias versões podem ser encontradas no mercado pelo preço unitário de menos de 10 dólares americanos. A versão escolhida para este projeto foi o ESP32-WROOM-32U, que oferece conectores Hirose U.FL em vez de

antenas integradas, permitindo ligar os dois dispositivos de forma cabeada como prevê a Figura I.2. A Tabela I.1 lista algumas das especificações do ESP32-WROOM-32U.

Tabela I.1: *Algumas especificações do ESP32-WROOM-32U.*

Item	Especificação
Memória Flash SPI	4 MB
Cristal integrado	40 MHz
Antena	Conector U.FL
WiFi	802.11 b/g/n
Bluetooth	versão 4.2 compatível com BR/EDR e BLE
Sensibilidade de recepção (Bluetooth)	-97 dBm
Potência de transmissão (Bluetooth)	Controlável de -12 a $+9$ dBm
Tensão de alimentação	3.0 a 3.6 VDC
Corrente mínima	500 mA

Como a sensibilidade do ESP32 é elevada, a potência de transmissão foi configurada para seu valor mínimo de -12 dBm. Além disso, uma atenuação total de 30 dB foi inserida no enlace de comunicação para deixar os estados dos canais próximos do limiar de classificação, como desabilitados, e para evitar danos aos ESP32 que poderiam ser causados por elevada potência do sinal interferente gerado pela USRP B210.

Para a programação foram utilizadas as linguagens C/C++ com as ferramentas providas pelo fabricante, chamadas de *ESP IDF tools* [79]. O sistema operacional de tempo real (*real time operational system*, RTOS) embarcado foi o FreeRTOS [80] e a pilha (*stack*) do protocolo Bluetooth utilizada para camada de *host* foi o Apache NimBLE [81]. Apesar de as ferramentas de programação do ESP32 serem em grande parte de código aberto, a camada de controle do protocolo Bluetooth é de código fechado e proprietário do fabricante do chip, não sendo, portanto, passível de substituição ou alterações nesta parte do *firmware*.

A programação do código compilado em ambos dispositivos foi feita partindo de duas aplicações de exemplo existentes na biblioteca do NimBLE. Para o dispositivo mestre o código base utilizado foi o do exemplo *blecent* e para o escravo o código base foi o do exemplo *blephpr*. Como o FreeRTOS permite que se executem tarefas (*tasks*) simultâneas no microcontrolador, foi adicionada uma aplicação no código responsável pela manipulação dos dados lidos do mapa de canais e exibição serial dos mesmos na tela do computador. A arquitetura do código utilizado na programação do dispositivo mestre é exemplificada na Figura I.4.

Na pilha de *host* NimBLE para implementação do protocolo Bluetooth existe uma função da camada HCI que permite a leitura do mapa de canais do AFH. Esta função é utilizada através da tarefa responsável pela comunicação do dispositivo, a qual é baseada nos dois exemplos anteriormente citados. A mesma pode ser utilizada sob a sintaxe:

```
return=ble_hs_hci_read_chan_map(conn_handle, output),
```

cujos principais campos são assim descritos:

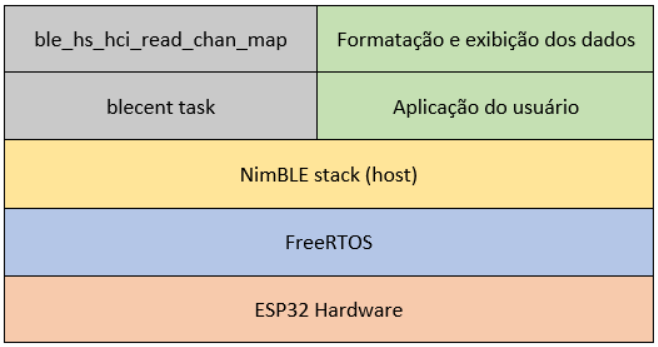


Figura I.4: *Arquitetura de código no dispositivo mestre utilizado nos testes.*

- `return`: é o comando de retorno da função. A função de leitura do mapa de canais é uma função do tipo `int`, cujo valor inteiro retornado indica o estado da requisição. Caso retorne zero, indica que a leitura do mapa de canais foi bem sucedida; caso contrário, a função foi negada ou não pôde ser executada por causa de algum erro, como por exemplo, nenhuma conexão ativa entre os dispositivos.
- `conn_handle`: informa de qual conexão se deseja fazer a leitura do mapa de canais, uma vez que pode haver mais de uma conexão ativa. Esta variável é do tipo `uint16_t`.
- `output`: é o parâmetro de saída da função que receberá o mapa de canais. Trata-se de um vetor de 5 posições do tipo `uint8_t`, ou seja, um vetor onde cada posição representa 8 bits e cada bit representa o respectivo canal. A primeira posição representa os canais de 0 a 7, e a segunda posição representa os canais de 8 a 15, e assim até o último bit da última posição, o qual representa o canal 39.

De forma a facilitar a leitura do mapa de canais na variável de saída durante o monitoramento via interface serial do computador, uma função com execução como segunda tarefa no sistema operacional foi criada para organizar os dados existentes em um vetor de 40 posições no qual o índice da posição coincide com o índice do canal a ser analisado. Para cada um dos 5 Bytes da variável de saída aplica-se uma máscara a fim de identificar se o bit de interesse é 1 ou 0, o que é feito para os 8 bits de cada um dos 5 bytes de forma que o retorno desta função indexe corretamente cada canal. Os canais 37, 38 e 39, como antes mencionado, são canais de controle da comunicação e, por isso, sempre constarão com o valor 0 no mapa de canais, uma vez que os mesmos não são participam do processo de AFH.

Durante os testes constatou-se que a forma como o AFH foi implementado no controlador do Bluetooth do ESP32 não gerava o mapa de canais da maneira esperada, em concordância com os canais afetados de forma controlada pela USRP. Por ser uma parte de código fechado do *firmware*, não foi possível concluir o método utilizado para classificação dos canais como ocupados. Os mesmos alteravam de forma muito rápida, não sendo possível obter dados confiáveis nas requisições feitas. Para contornar o problema criou-se um esquema de janela temporal, onde o mapa de canal final após um período era calculado através de um E-lógico entre todas as requisições feitas durante

aquele tempo. Dessa forma foi possível detectar sinais gerados pela USRP na banda de opeção do Bluetooth, os quais podiam ser visualizados através do *prompt* de comando do Windows. A Figura I.5 exemplifica, na linha superior, o caso a leitura dos canais sem a detecção de nenhuma interferência na banda. Na segunda linha, quatro canais no centro da banda foram desabilitados no mapa de canais do AFH por estarem sob interferência, neste caso um ruído de 8 MHz de banda foi adicionado ao enlace de comunicação.

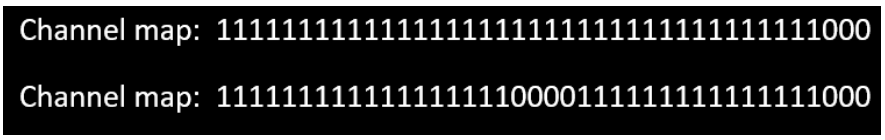


Figura I.5: *Exemplo de medições do mapa de canais do AFH.*

O sistema se mostrou capaz de detectar o sinal através da tecnologia AFH, contudo, espera-se que outros hardwares possam entregar leitura similar sem a necessidade da criação da janela temporal de leituras do mapa de canais, fato constatado em testes preliminares utilizando um *smartphone* Android como dispositivo mestre e o ESP32 como escravo. A partir desta prova de conceito inicial, abrem-se oportunidades para novos testes e amadurecimento da tecnologia visando módulos de sensoriamento espectral de baixíssimo custo e consumo energético. A técnica utilizada baseia-se na análise do impacto que um sinal interferente gera e não no processamento de amostras do sinal. Oportunidades para um aprimoramento da técnica ficam em aberto. Uma segunda etapa de prototipagem e avaliação da prova de conceito começou a ser desenvolvida utilizando-se do Raspberry Pi 3 e da pilha BlueZ do sistema operacional Linux, buscando resultados mais precisos e como previstos no AFH do padrão Bluetooth, sem a necessidade da criação de janelas temporais via *software* da aplicação. Outra opção existente não avaliada é migrar a implementação para o Bluetooth BR/EDR.

Apêndice II

Proposta de arquitetura para a base de dados

É uma tarefa complicada desenvolver as diretrizes para a construção de um banco de dados de espaço em branco para gerenciar o compartilhamento dinâmico do espectro entre usuários e reguladores. Esta seção apresentará uma visão de arquitetura para esta tarefa, porém, é necessário ressaltar que esta é apenas uma das soluções possíveis para construção de banco de dados. Além disso, o foco deste desenho de arquitetura é demonstrar os requisitos de interconexão entre os sistemas de sensoriamento, base de dados e gerência espectral, levantando os pontos cruciais para o desenvolvimento prático desta solução. A Figura II.1 ilustra por completo o projeto de arquitetura.

Algumas das entidades propostas para a integração do recurso de sensoriamento com o banco de dados: registro do dispositivo sensor, serviço de identidade do dispositivo sensor, gerenciador de sensor e API de gerenciamento. O registro do dispositivo sensor é o banco de dados que armazena registros da rede IoT de sensoriamento e seus dispositivos, este se faz necessário para que a base de dados de espaço em branco (*white space database*, WSDB) admita a infraestrutura de sensoriamento no sistema. O serviço de identidade do dispositivo sensor é responsável pela identificação específica dos dispositivos, com seus dados de localização, permitindo a WSDB enviar consultas para determinados *clusters* para realização de sensoriamento. Além disso, o gerenciador de sensor refere-se a todas as funções e ferramentas para se comunicar e controlar o dispositivo sensor. A API de gerenciamento do bloco de sensoriamento são recursos para processar os dados de detecção, tomar a decisão global acerca do espectro, responder às solicitações do núcleo da base de dados e fornecer meios para monetizar a rede de detecção. Neste desenho de arquitetura, a ligação azul é utilizada no diagrama para representar o tráfego de dados, como as informações de sensoriamento em tempo real (ou periódicos) encaminhados para o núcleo da base de dados, enquanto isso, a ligação amarela representa o fluxo de aplicação e controle, normalmente entre o núcleo e as entidades que atuarão no gerenciamento da rede.

A abordagem convencional, dentro da WSDB proposta nesta seção, tem os recursos de proteção por geolocalização com o recurso de locação de licenças de espectro conectados. Para este módulo, existem as seguintes entidades: diretório de registro do usuário primário (*primary user*, PU)/usuário secundário (*secondary user*,

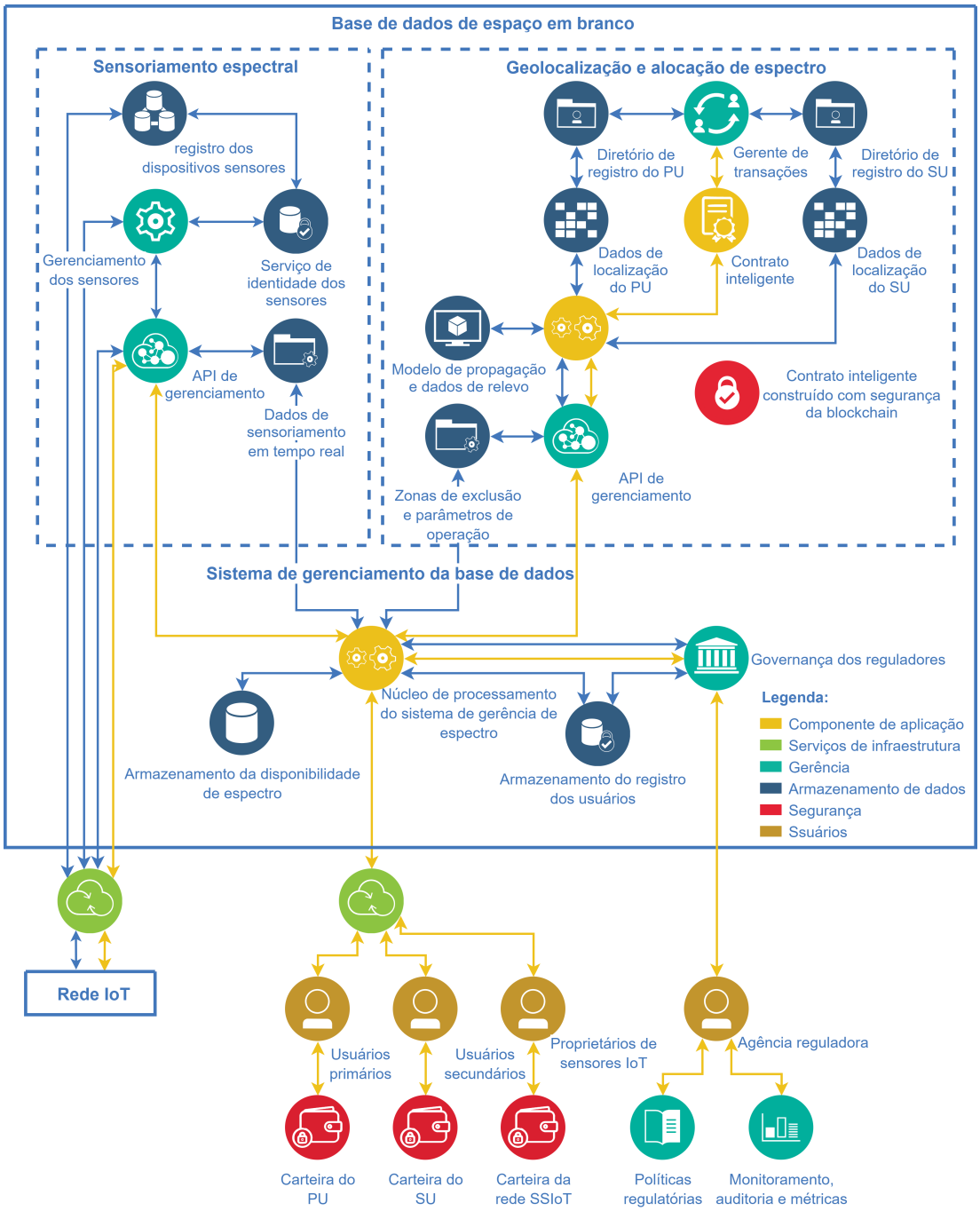


Figura II.1: *Desenho de arquitetura para base de dados de ocupação espectral integrada com a rede SSIoT.*

SU), gerenciador de transações, ferramenta de processamento de zonas de exclusão de geolocalização e API de gerenciamento. Outros itens representados são o modelo de propagação de canal e os dados de relevo, os dados do transmissor PU/SU e o contrato inteligente da Blockchain.

O diretório de registro do PU/SU refere-se aos diretórios onde são armazenadas as informações do registro e dos transmissores dos usuários do espectro. Os dados do transmissor PU/SU desses diretórios contêm as informações que serão usadas para calcular as zonas de proteção para os usuários. O modelo de propagação de canal e os dados do relevo referem-se às demais informações necessárias para calcular as zonas de proteção, por exemplo, os modelos de propagação Longley-Rice, curvas-F e Okumura. A ferramenta de processamento de zonas de exclusão de geolocalização é a capacidade de computação em nuvem, que calcula as zonas de proteção com base nos dados dos transmissores dos usuários, dados do relevo do terreno e registros de transações de contratos inteligentes. O gerenciador de transações é responsável por aplicar regras à locação de licenças do espectro de acordo com as políticas dos reguladores e viabilizar a troca do espectro através de contratos inteligentes da Blockchain. A API de gerenciamento pode parecer redundante neste bloco, mas aqui ela representa os recursos e funções para gerenciar esta parte específica do sistema, sendo responsável por fornecer a disponibilidade do espectro, os parâmetros operacionais permitidos e as zonas de proteção.

O motivo de cada sistema possuir sua própria API de gerenciamento são os diferentes requisitos existentes para cada um. Além disso, é possível que a construção destes dois sistemas seja feita separada e com tecnologias diferentes, por exemplo, usando bancos de dados convencionais, também empregando DLTs ou ainda soluções híbridas. Desta forma, cada um dos sistemas dentro da WSDB pode ter uma API de gerenciamento própria para se comunicar com o núcleo.

Outro ponto de extrema importância é a proteção dos usuários secundários, uma vez que no recurso de locação de licença os mesmos podem adquirir as licenças de espectro, eles devem receber proteção contra interferências de acordo com a licença que compraram. Dessa forma, para o cálculo das zonas de proteção, deve-se considerar os direitos adquiridos pelos SUs. Tendo em vista estas considerações, o presente estudo aborda as zonas de proteção por geolocalização e o recurso de locação de licença operando juntos. A projeção das zonas de exclusão é calculada utilizando de uma conexão com as ferramentas de contrato inteligente, utilizadas para validar os dados dos SUs que adquiriram licenças e assim serem tratados como um PU enquanto o contrato inteligente estiver em vigor.

O núcleo da base de dados é composto do armazenamento do registro de usuários do espectro e o armazenamento de dados do espectro. O diretório de registro do PU/SU mencionado anteriormente faz parte do armazenamento do registro de usuários do espectro, enquanto o armazenamento de dados do espectro contém a informação de utilização do espectro e a disponibilidade dos canais. Além disso, a entidade de gerenciamento e processamento de espectro é responsável pelas tarefas de computação, requisição às APIs de gerenciamento de fontes de dados, aplicação das políticas e regras dos reguladores para compartilhamento de espectro, permitir que os usuários acessem o espectro, monetizar os cenários de detecção/locação de licença e controlar

todo a WSDB. A governança de espectro dos órgãos reguladores representa as ferramentas e APIs que dão à autoridade reguladora o poder de gerenciar o sistema, que inclui funções para implementar regras, monitorar, auditar e métricas para analisar a eficácia da acesso dinâmico ao espectro (*dynamic spectrum access*, DSA).

Este conceito não se limita a um cenário de uma única banda, mas ele depende da banda de frequência dos dispositivos sensores de espectro e da faixa de frequência do modelo de propagação de canal utilizado. Por exemplo, módulos de sensores projetados para banda de televisão (TV) e o modelo Okumura funcionam para espaço em branco na banda de TV (*TV white-spaces* , TVWS). Se o alvo for a banda CBRS, novos requisitos e novas especificações de módulos de sensores de espectro e outros modelos de propagação são necessários. Essa capacidade torna a proposta versátil à mudanças nas políticas de alocação de espectro de acordo com o órgão regulador.