OULU 2019
C 720

ACTA UNIVERSITATIS OULUENSIS

Kalle Lähetkangas

SPECIAL APPLICATIONS AND SPECTRUM SHARING WITH LSA

UNIVERSITY OF OULU GRADUATE SCHOOL;
UNIVERSITY OF OULU,
FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

ACTA UNIVERSITATIS OULUENSIS
C Technica 720

KALLE LÄHETKANGAS

SPECIAL APPLICATIONS AND SPECTRUM SHARING WITH LSA

Academic dissertation to be presented with the assent of the Doctoral Training Committee of Information Technology and Electrical Engineering of the University of Oulu for public defence in the Saalasti Hall, Linnanmaa, on 28 November 2019, at 12 noon

UNIVERSITY OF OULU, OULU 2019

Acta Univ. Oul. C 720, 2019

Supervised by
Docent Harri Saarnisaari

Reviewed by
Professor Jon M. Peha
Professor Marcello L. R. Campos

Opponent
Professor Mikko Valkama

ISBN 978-952-62-2393-3 (Paperback)
ISBN 978-952-62-2394-0 (PDF)

ISSN 0355-3213 (Printed)
ISSN 1796-2226 (Online)

Cover Design
Raimo Ahonen

JUVENES PRINT
TAMPERE 2019

Lähetkangas, Kalle, Special applications and spectrum sharing with LSA.
University of Oulu Graduate School; University of Oulu, Faculty of Information Technology and Electrical Engineering
Acta Univ. Oul. C 720, 2019
University of Oulu, P.O. Box 8000, FI-90014 University of Oulu, Finland

Abstract

The commercial long-term evolution (LTE) networks of today offer fast and regionally wide access to the Internet and to the commercial applications and services at a reasonable price. At the same time, public safety (PS) users are still communicating with old-fashioned, second-generation voice and data services. Recently, the commercial LTE networks have been standardized to offer capabilities to mission-critical users. However, the commercial networks do not yet fully support the coverage requirements of the PS users. Moreover, the commercial infrastructure might be out of order in critical scenarios where PS actors are needed. Thus, the PS users require, for example, rapidly deployed LTE networks to support their own communication. This thesis studies the PS use of commercial operators' LTE networks and rapidly deployed closed LTE networks. The key tasks are to find out how to connect users seamlessly together between the different networks as well as finding out how the frequency planning is implemented. This thesis provides practical design solutions to guarantee network interoperability by connecting the networks as well as radio spectrum utilization solutions by licensed shared access (LSA). While the concept of LSA has been well developed, it has not been thoroughly investigated from the point of view of the PS actors, who have special requirements and should benefit from the concept.

Herein, the alternatives for spectrum sharing between PS and commercial systems are discussed. Moreover, the thesis develops a specific LSA spectrum sharing system for the PS actors deploying their own network in scenarios where the commercial networks are insufficient. The solution is a robust LSA-based spectrum sharing mechanism. Note that PS actors also need to be able to utilize the spectrum when the LSA system is not available and when the commercial system has failed. Thus, this thesis proceeds on developing sensing methods for complementing LSA, where the sensing methods guarantee spectrum information for a rapidly deployed PS network. It is shown how PS actors can utilize available spectrum with a secondary spectrum licence. This is a good alternative to reserving the spectrum completely. The work assembles missing pieces of existing methods to ensure the functionality of the commercial and of the supporting rapidly deployed networks, both in terms of spectrum usage and application services.

Keywords: collaborative sensing, dynamic spectrum sharing, energy detection

Lähetkangas, Kalle, Erityisapplikaatiot ja spektrin jakaminen LSA:lla.
Oulun yliopiston tutkijakoulu; Oulun yliopisto, Tieto- ja sähkötekniikan tiedekunta
Acta Univ. Oul. C 720, 2019
Oulun yliopisto, PL 8000, 90014 Oulun yliopisto

Tiivistelmä

Kaupalliset long-term evolution (LTE) -verkot tarjoavat nopean, edullisen ja alueellisesti kattavan pääsyn Internettiin sekä laajaan valikoimaan sovelluksia. Samaan aikaan turvallisuustoimijat (public safety (PS) -toimijat) käyttävät vanhanaikaisia äänen sekä vaatimattoman datayhteyden tarjoavia verkkoja. LTE-verkot ovat kuitenkin äskettäin standardoitu tarjoamaan valmiudet myös toimintokriittiseen kommunikointiin. Toisaalta, kaupalliset LTE-verkot eivät vielä tarjoa esimerkiksi tarvittavaa alueellista kattavuutta PS-käyttäjille. Lisäksi, kaupalliset verkot saattavat olla epäkunnossa kriittisissä tilanteissa. Tämän vuoksi PS-toimijat tarvitsevat omia nopeasti pystytettäviä LTE-verkkoja tukemaan nykyaikaista viestintäänsä. Opinnäytetyössä tutkitaan näiden nopeasti pystytettävien LTE-verkkojen käyttöä kaupallisten LTE-verkkojen kanssa. Keskeiset tehtävät ovat eri verkkojen PS-toimijoiden saumaton yhdistäminen sekä verkkojen taajuusjaon toteuttaminen.

Tämä opinnäytetyö tarjoaa käytännön ratkaisuja verkkojen yhteentoimivuuden takaamiseksi ja radiotaajuuksien jakoratkaisuja lisensoidun jaetun käyttöoikeuden licensed shared access (LSA) -metodin avulla. Vaikka LSA:n käsite on jo pitkälle kehitetty, sitä ei ole tutkittu perusteellisesti PS-toimijoiden näkökulmasta ottaen huomioon heidän erityisvaatimuksensa. Tässä työssä syvennytään näiltä osin LSA järjestelmään yhtenä vaihtoehtona taajuuksien saamiseksi nopeasti pystytettäville verkoille. Lisäksi työssä kehitetään robusti LSA-pohjainen taajuuksien jakamisjärjestelmä nopeasti pystytettäville verkoille tilanteissa, joissa kaupalliset verkot ovat riittämättömät. Huomaa, että PS-toimijoiden on pystyttävä hyödyntämään taajuuksia myös silloin, kun LSA-järjestelmän kaikki osat eivät ole käytettävissä ja kun kaupallinen LTE järjestelmä on alhaalla. Tätä varten opinnäytetyössä kehitetään LSA:ta täydentävä havainnointimenetelmä, jolla taataan taajuustiedot vapaista taajuuksista nopeasti pystytettäville verkoille, sekä näytetään, miten PS-toimijat voivat hyödyntää LSA:ta toissijaisen taajuuslisenssin avulla. Tämä on hyvä vaihtoehto radiospektrin varaamiseksi kokonaan. Työ kokoaa puuttuvia osia olemassa oleviin menetelmiin, jotta voidaan varmistaa kaupallisten verkkojen toimivuus PS-käyttäjille yhdessä niitä tukevien nopeasti pystytettävien verkkojen kanssa taajuuksien käytön ja sovelluspalvelujen osalta.

Asiasanat: dynaaminen spektrinjako, energiahavainnointi, yhteistyöllinen sensorointi

To my family

Acknowledgements

I would like to express my gratitude to my supervisor, Adjunct Professor Harri Saarnisaari, for his valuable support and guidance. In addition, I would like to extend my gratitude to Dr. Harri Posti for all his ideas, inspiration and support. I wish to thank the pre-examiners of the thesis, Professor Jon M. Peha and Professor Marcello L. R. de Campos, for their valuable suggestions and encouraging comments regarding the thesis. I also extend my gratitude to Professor Ari Pouttu, Professor Behnaam Aazhang, Professor Jari Iinatti, Adjunct Professor Marian Codreanu, Professor Markku Juntti, Professor Matti Latva-Aho, Associate Professor Mehdi Bennis, and Professor Premanandana Rajatheva. I would also like to thank my follow-up group, the chairman Adjunct Professor Pekka Pirinen and Assistant Professor Hirley Alves, for the assistance they provided.

Thank you very much Abdul Moiz, Antti Arvola, Dr. Anna Pantelidou, Brett Kaufman, Dr. Carlos Morais de Lima, Jaakko Leinonen, Jani Saloranta, Jari Marjakangas, Jari Moilanen, Dr. Joonas Kokkoniemi, Dr. Juha Petäjäjärvi, Adjunct Professor Madhusanka Liyanage, Dr. Manosha Kapuruhamy, Adjunct Professor Marja Matinmikko-Blue, Markku Jokinen, Marko Mäkeläinen, Dr. Markus Leinonen, Muhammad Arif, Dr. Nuwan Ferdinand, Olli Liinamaa, Dr. Pedro Juliano Nardelli, Dr. Petri Luoto, Dr. Qiang Xue, Lic. Sc. Risto Vuohtoniemi, Dr. Tuomo Hänninen, Dr. Ville Niemelä and Lic. Sc. Visa Tapio.

The work for this dissertation was conducted at the Centre for Wireless Communications at the University of Oulu during the time period of 2015 to 2019. The work was done in CORE++ and CORNET projects, and I would like to acknowledge all the project partners at Airbus Defence and Space, Anite, Bittium, Business Finland, Centria University of Applied Sciences, Elisa, Fairspectrum, Finnish Communications Regulatory Authority, Finnish Defence Forces, Keysight Technologies, Nokia, PehuTec, Turku University of Applied Sciences and VTT. Special thanks go to Ari Hulkkonen. Furthermore, I would like to thank all the administrative staff members at CWC. This research has been financially supported by Academy of Finland 6Genesis Flagship (grant 318927). I want to express my gratitude to the Tauno Tönning Foundation, HPY:n Tutkimussäätiö, and Riitta ja Jorma J. Takasen säätiö for the financial support for this work.

I would also like to thank my parents, sisters and parents-in-law for all the love and support throughout my life. Foremost, my warmest acknowledgements go to my children and to the love of my life, my wife Maija.

Oulu, August 15th, 2019 Kalle Juhani Lähetkangas

List of abbreviations

Acronyms:

2G	Second wireless generation
AF	Application function
APN	Access point name
ARP	Allocation retention priority
ASA	Authorized shared access
CS	Commercial system
dB	decibel
dBm	decibels relative to one milliwatt
dOMS	Distributed operations and management system
e.g.	For example
EPC	Evolved packet core
EPS	Evolved packet system
ESC	Environmental sensing capability
GCSE_LTE	Group communications system enablers for LTE
i.e.	That is to say
IMT	International mobile telecommunications
Inc	Incumbent
IP	Internet protocol
IPsec	IP security architecture
LSA	Licensed shared access
LTE	Long-term evolution
MCPTT	Mission critical push to talk service
OAM	Operations, administration and management
PCC	Policy and charging control
PCRF	Policy and charging rules function
ProSe	Proximity services
PS	Public Safety
RP1	First research problem
RP2	Second research problem
RP3	Third research problem

RP4	Fourth research problem
RP5	Fifth research problem
QCI	Quality of service class identifiers
QoS	Quality of service
SAS	Spectrum access system
SNR	Signal-to-noise ratio
TETRA	Terrestrial trunked radio
VLAN	Virtual local area network
VPLS	Virtual private local area network service
VPN	Virtual private network
WLAN	Wireless local area network

Symbols:

$a(\cdot)$	Antenna height gain
α	Exponent for fading
$b(\cdot)$	Antenna height gain
B_r	Receiver bandwidth in Hz
d	Distance between receiver and transmitter in km
$D(\cdot)$	Decibel threshold values for random draws of log-normal shadowing
d_{f}	Radius likely free of transmitters, given no detection
d_{t}	Radius including a detected LTE transmitter with a high probability
$\mathrm{erf}^{-1}(\cdot)$	Gauss error function
f	Centre frequency in MHz
$G(\cdot)$	Gaussian distribution
γ	Sum energy threshold
$\Gamma_{\mathrm{up}}^{-1}(\cdot,\cdot)$	Inverse upper incomplete gamma function
G_r	Receive antenna gain, (including feeder loss and antenna directivity loss) in dB
G_t	Transmit antenna gain (including feeder loss and antenna directivity loss) in dB
H_b	Antenna height of the higher antenna in a transceiver pair in m
H_m	Antenna height of the lower antenna in a transceiver pair in m
$\log_{10}(\cdot)$	Base 10 logarithm
$\max\{\cdot,\cdot\}$	Maximum of the inputs
$\min\{\cdot,\cdot\}$	Minimum of the inputs

$L_{\text{hata}}^{\text{open}}(\cdot,\cdot,\cdot,\cdot)$	Propagation loss of the Extended Hata model in an open rural setting in dB
$L_{\text{m}}^{\text{open}}(\cdot,\cdot,\cdot,\cdot)$	Median propagation loss of the Extended Hata model in an open rural setting in dB
$L_{\text{m}}^{\text{urban}}(\cdot,\cdot,\cdot,\cdot)$	Median propagation loss of the Extended Hata model in urban setting in dB
N	Number of samples in energy detection
NF	Noise figure in dB
N_{dBm}	Nominal thermal noise power in dBm
p	Parameter for probability
P_D	Probability of detection
P_{FA}	Probability of false detection
p_r	Received power in dBm
p_t	Transmission power in dBm
r_n	Received signal
$Q_{\chi_N^2}(\cdot)$	Right-tail probability function of a chi-squared random variable for N samples
ρ	Parameter quantifying noise power uncertainty
s_n	Transmitted signal
σ^2	Thermal noise power in Watts
σ_{dBm}^2	Thermal noise power in dBm
σ_{hata}	Standard deviation of the slow fading distribution
σ_n^2	Nominal noise power in Watts
σ_s^2	Received signal noise power in Watts
T_{check}	Time interval between connectivity check requests
T_{empty}	Time to empty the spectrum by an access point
$T(\cdot)$	Value drawn from a fading distribution
T_i	Predetermined time before which the incumbent is required to send its spectrum reservation
$T_{timeout}$	Time interval with no messages before considering a timeout
w_n	White Gaussian noise

List of original publications

A list of original publications, which are referred to in the text by their Roman numerals (I–III):

I Lähetkangas K, Saarnisaari H and Hulkkonen A (2016) Licensed Shared Access System Possibilities for Public Safety, in Mobile Information Systems, vol. 2016, Article ID 4313527, pp. 1-12. URI: https://doi.org/10.1155/2016/4313527

II Lähetkangas K, Posti H, Saarnisaari H and Hulkkonen A. (2019) Sensing LTE Base Stations with Energy Detectors for Public Safety, submitted in IEEE Transactions on Cognitive Communications and Networking.

III Höyhtyä M, Lähetkangas K, Suomalainen J, Hoppari M, Kujanpää K, Trung K, Kippola T, Heikkilä M, Posti H, Mäki J, Savunen T, Hulkkonen A and Kokkinen H (2018) Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control, in IEEE Access, vol. 6, pp. 73572-73582. URI: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8550640

Contents

1 Introduction

Today's commercial long-term evolution (LTE) networks offer fast and regionally wide access to the Internet and to the commercial applications and services that are constantly developing. Moreover, the 3rd Generation Partnership Project is currently standardizing the next generation of wireless technologies beyond LTE [1]. At the same time, the public safety (PS) actors are still utilizing the second wireless generation (2G) type of legacy systems, such as terrestrial trunked radio (TETRA) [2, 3], to guarantee voice and short data service communications.

The advances in commercial networks have made them an attractive option for the PS actors who also want to benefit from the efficient technologies. The LTE equipment can provide higher data rates than TETRA, in addition to voice services. The higher data rates can, in turn, help the work of PS actors, for example, by providing a faster data base connectivity and video streaming possibilities. Moreover, the commercial LTE equipment is relatively inexpensive, and the infrastructure is readily available. Thus, the commercial operators can also offer their services to the PS actors, such as border control, police, first responders and military, whose effective communication capabilities are vital for society. In principle, the PS actors could already utilize existing commercial networks and do not need to build a countrywide LTE network for themselves.

In some countries, there are already commercial operators that solely offer LTE services to industrial and PS actors [4]. However, while the commercial mobile operators can offer LTE services to PS actors, the coverage, reliability, quality and security requirements of the PS actors are high. This makes it hard for the commercial LTE operators to have a profitable business model from the PS communications. It is also a political decision how the PS actors communicate. While commercial networks have advantages over the traditional closed PS networks, such as TETRA, the PS actors do not completely rely on communication over the commercial networks.

First, the full functionality of the community infrastructure might not be available in the PS operations due to electrical breaks or infrastructure damages. Second, there might be a need for critical communication in locations that are not fully supported by the commercial network. These are the areas where the necessity of a high data speed mobile network is generally low and where the PS actors would require the networks

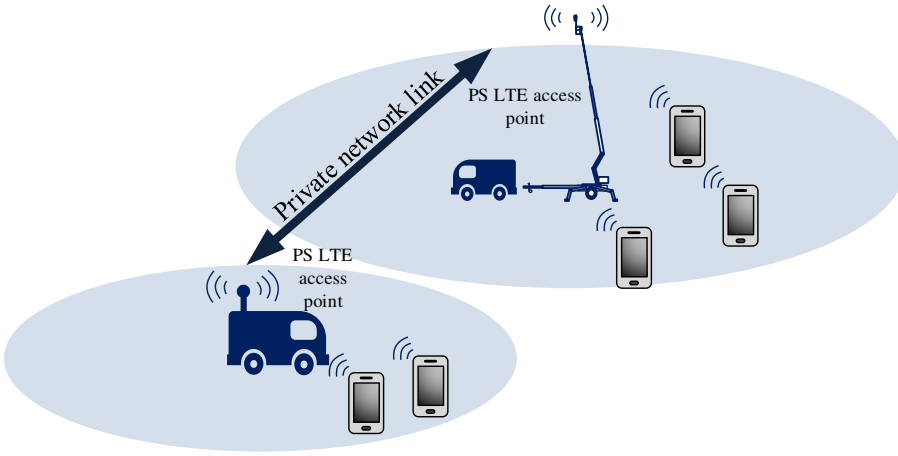

Fig. 1. The LSA system for a mobile operator as an LSA licensee.

maybe only once. In these areas, it is not financially beneficial to build high data speed networks.

A solution that supports the commercial LTE networks in these situations and locations is a local, rapidly deployable LTE network. It can be carried with the PS actors to the point of action (see Fig. 1). The rapidly deployed network can then offer interconnected hot spots for the PS actors in scenarios where the PS actors would not have a commercial LTE network coverage for their user equipment.

Moreover, the PS actors have full control over their services in this rapidly deployed network. The rapidly deployed network is described in more detail later in Section 1.5. The framework of this thesis is using these rapidly deployed networks together with the commercial networks, which is depicted in the next section. In this way, the PS actors can utilize the applications offered by a commercial LTE network, and still do not need a static countrywide network.

1.1 Framework

The framework for this thesis is depicted in Fig. 2, which shows an example setup of a rapidly deployable PS network concept together with a commercial LTE network. This type of rapidly deployed network can be built, for example, with towable lifts or crane cars equipped with the necessary equipment. The thesis concentrates on design solutions

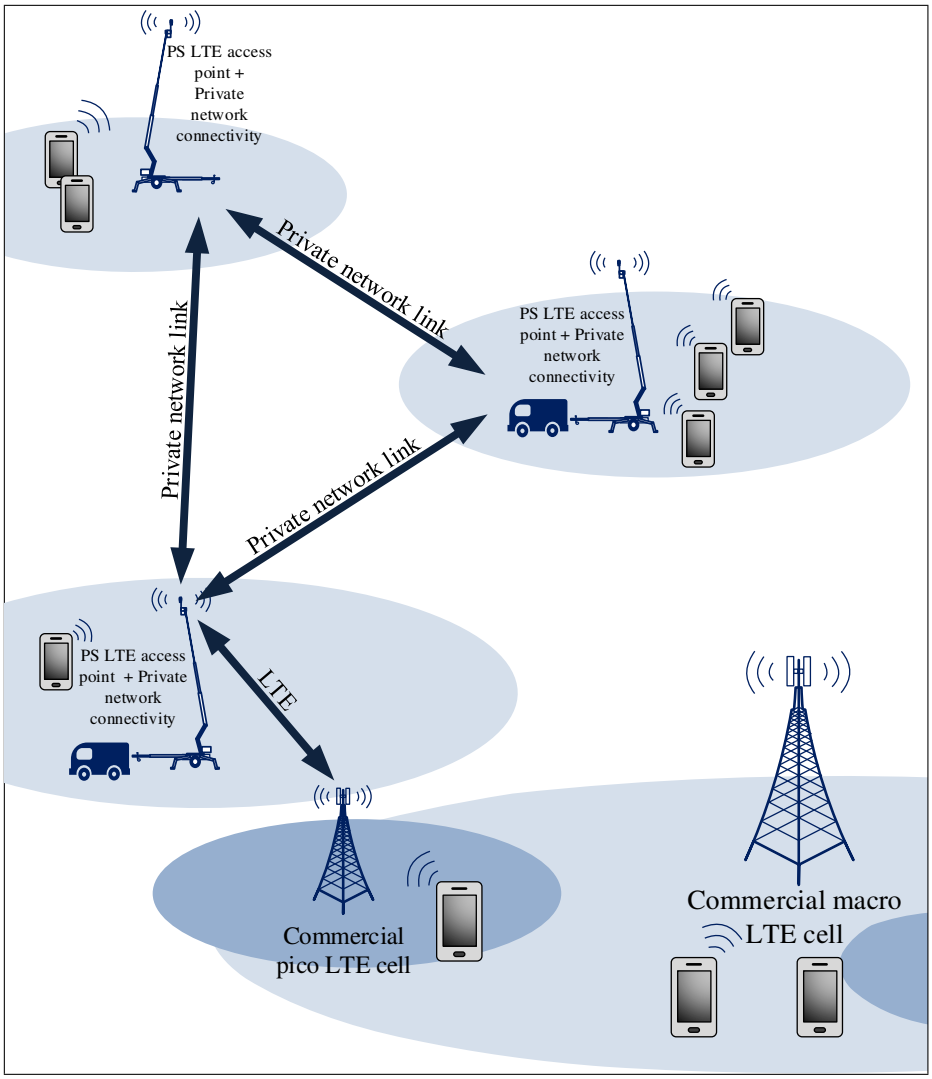

Fig. 2. A rapidly deployable LTE network concept for PS actors in conjunction with a commercial network.

to connect the commercial LTE networks together with rapidly deployed networks, as well as on the related radio spectrum utilization solutions.

More specifically, the deployable networks require radio spectrum. The spectrum may be solely owned by the PS users, but that is an inefficient way of using scarce radio spectrum, since locally, most of the time, the majority of the PS spectrum is unused. As another option, the spectrum can be shared. The PS users could utilize the unused spectrum, when it is available. At other times, the PS can borrow spectrum from the commercial LTE networks, which might be using the spectrum to speed up their transmissions, e.g., with carrier aggregation [5].

One spectrum sharing mechanism is licensed shared access (LSA) [6, 7], and that is the topic of this thesis. It is a centralized, repository- based spectrum sharing method for two distinct systems. LSA with other spectrum sharing methods is further reviewed in Section 1.2. The architecture of the LSA concept has been described in [8].

In LSA, the primary spectrum user can, for example, be another mobile network operator, or TV, radio, or other live streaming programme maker. The programme-making services require spectrum for broadcasting, news gathering with cameras or theatrical productions, which are defined in [9, 10]. The LSA enables the spectrum licensing and sharing to be operator-specific between the different stakeholders and incumbents.

An LSA system for PS actors must also operate in certain problematic situations. One such situation is a connection loss, which denies access to the central spectrum repository. Moreover, the information in the repository might not be valid. This could occur, e.g., in a crisis situation when the primary spectrum users, such as commercial networks, are down. For these types of scenarios, the spectrum must be guaranteed for the PS network. Moreover, the PS network should interfere with the commercial networks as little as possible. It follows that the LSA sharing arrangements must be robust, and the necessary spectrum sharing rules for more specific critical scenarios are required.

This thesis focuses on the above-mentioned LSA spectrum sharing solutions, and includes the use of sensors to complement LSA information. The robust LSA solution for PS actors is presented in more detail on a component level in Chapter 4, and the proposed sensing methods are presented in Chapter 5.

Fig. 3 depicts the framework for the sensing distances of LTE base stations. In the figure, there are two pictures of two different scenarios. Namely, a scenario for using a radio head to detect a macro base station and a scenario for using a radio head to detect

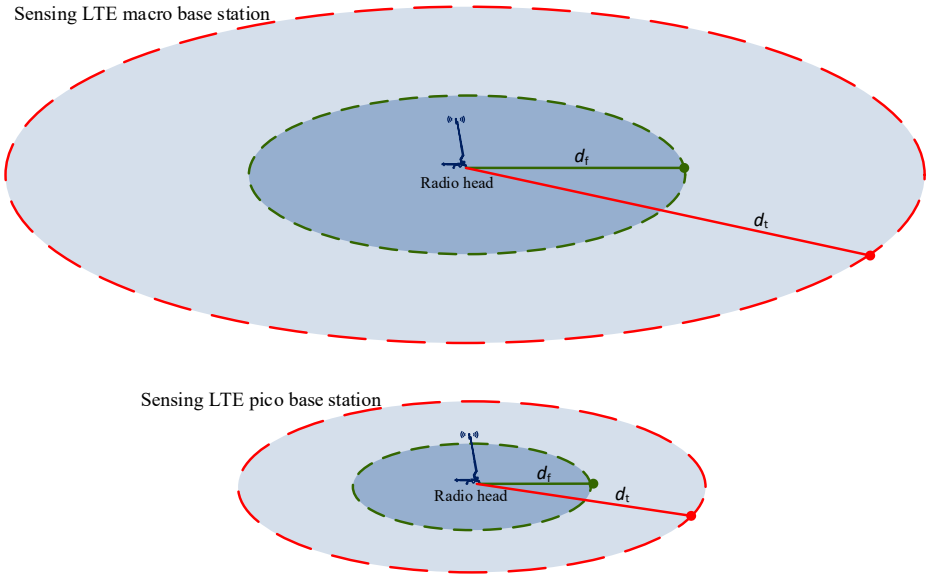

Fig. 3. The sensing framework for pico and macro base stations with a radio head. The radiuses for detecting the pico base station are shorter than for the macro base station. This is because the transmit power of a pico base station is lower.

a pico base station. Distance d_t is the distance within which the detected base station is with a high probability. If the base station is further than this distance, the detections will happen very rarely. Moreover, the radius d_f is likely free of base stations, given that there is no detection. The detection probability from this distance d_f is very high. In the figure, a macro base station is detected further away than a pico base station that uses less transmit power.

The following sections give the background to the thesis. These sections and their connections to the topics of the thesis can be seen in Fig. 4. Furthermore, Fig. 4 shows the considered communication and spectrum sharing aspects in each chapter.

In Section 1.2, an overview of *spectrum sharing* methods is given. The overview concentrates on the recent database-based spectrum sharing methods, where the database is offered via an Internet connection. In Section 1.3, an introduction to *spectrum sensing* is given. Sensing is used in this thesis in addition to database-based sharing methods in order to enable robust spectrum sharing. Furthermore, in this section, the *energy detection* performance is formulated. This is the detection model that is assumed in the upcoming sensing performance simulations. In Section 1.4, the state-of-the-art methods that enable *LTE networks for public safety communications* are described.

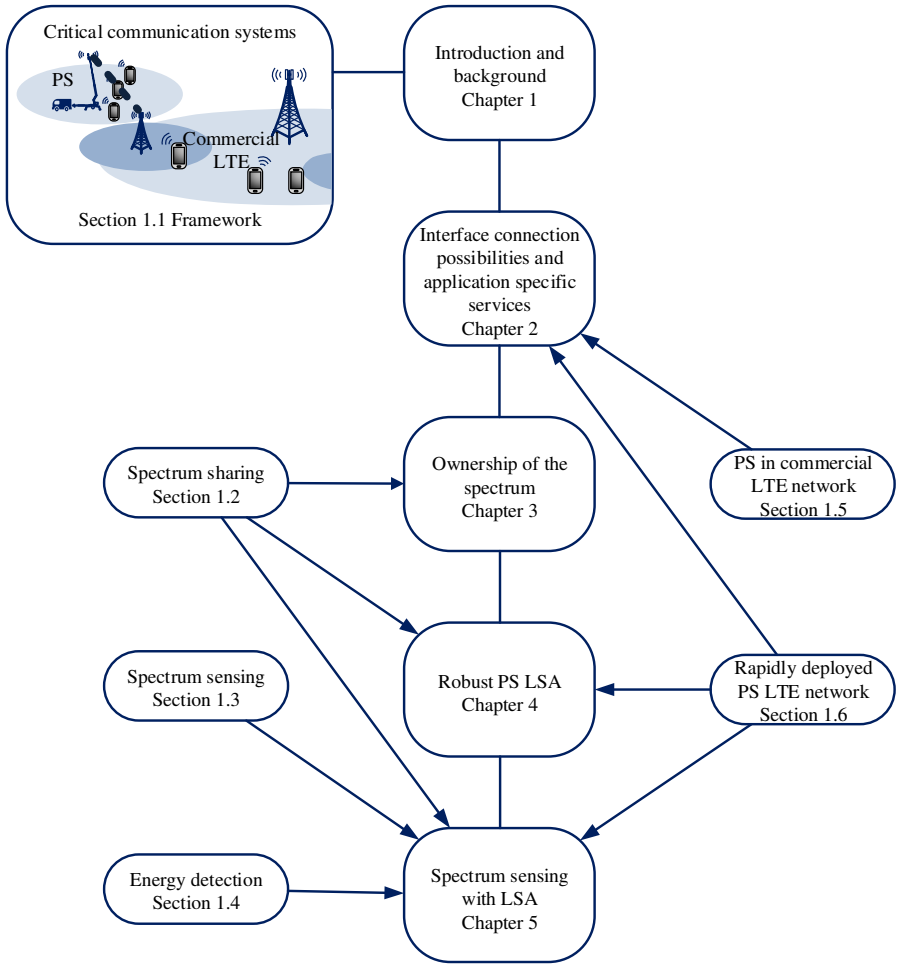

Fig. 4. A diagram of the critical PS communication topics in this thesis.

More specifically, an overview is given of the current standards enabling the PS use in the LTE networks. This includes the standardized group communication enablers, proximity services, push to talk services and standardization that supports the isolated operation of LTE base stations. Finally, in Section 1.5, the *rapidly deployable PS network* is described.

1.2 Spectrum sharing methods

The wireless operators should prepare for high growth in mobile data over the next decade [11, 12]. This growth is putting pressure on governmental spectrum users, which rarely utilize their spectrum, to free up their frequencies for commercial use. In the United States, 500 MHz of the spectrum from federal and non-federal applications is going to be freed completely or by spectrum sharing for commercial mobile radio systems by the year 2020 [13]. This may also be the direction in Europe, where the standardization is gradually changing in the direction of shared spectrum [14, 15, 16].

The radio spectrum can be shared administratively, in a market-based manner and by enabling it technically [17, 18]. First, the administrative method is where the different types of users are given their own spectrum. This is the traditional method, where the spectrum sharing is managed by communications regulatory authorities that define the required standards and methods used in different frequency bands, as in [19]. Second, market-based sharing is where the governments sell licenses to users for utilizing certain frequency bands in certain applications, such as mobile communications. Third, technically-enabled spectrum sharing covers the different technical methods that can be used to share the spectrum [20]. The technical methods include time sharing, frequency sharing, spatial sharing, and signal separation techniques such as ultra-wideband and spread spectrum. Additionally, the technical methods include overlaying methods where the spectrum can be dynamically shared in all the dimensions.

The main interest in the United States for dynamic spectrum sharing is the spectrum access system (SAS) [13, 21, 22]. The SAS concept is a three-tiered spectrum sharing system for the 3.5 GHz band. The tiers are primary access, secondary access, and general authorized access. These three tiers have been selected because it has been noticed that the spectrum is currently efficiently utilized in the auctioned mobile operator bands and in the Wi-Fi bands under general authorization. One of the goals of the SAS system is efficient spectrum utilization.

More specifically in the SAS concept, the primary access users are military radars and fixed satellite service systems in federal systems. They are further divided into informing and non-informing primary access users. The non-informing primary users are sensed by environmental sensing capability (ESC) to guarantee their operation. Note that while the primary access users have guaranteed resources for their use, they do not use their spectrum nation-wide and constantly. The secondary access users have the second highest priority, for example, because of payments or because of the public interest. The secondary spectrum licences are granted in three year periods. The secondary users can, for example, be mobile operators. With a licence, they obtain additional and interference-free spectrum for certain geographical areas with high commercial data traffic, given that the primary access users are silent. The additional spectrum can be utilized by offering carrier aggregation, as demonstrated in [23]. The secondary users have interference protection from other secondary and from general authorized access users. The general authorized access users are given the spectrum opportunistically within designated geographic areas. This spectrum is free of charge, but it is not guaranteed to be free of interference from other spectrum users.

1.2.1 Licensed shared access

For spectrum sharing, the LSA concept [6, 24, 25, 7, 26, 8] has also gained interest. It also originated from the market demand for new spectrum resources. The standardization of the general LSA regulatory framework started in response to the mandate of the European Commission [27], which ordered the standardization towards flexible spectrum use between incumbents and secondary spectrum users without interoperability and connectivity. The LSA concept is based on a system concept of Authorized Shared Access (ASA) [28], which is a spectrum sharing method for the international mobile telecommunications (IMT) spectrum [29]. While the LSA concept is a similar method to ASA, it is not restricted to any specific spectrum band. However, it is initially planned for the 2.3 GHz band.

The LSA/ASA concept has two access tiers, namely the primary incumbent and the secondary LSA licensee. The LSA/ASA method is a repository-based method where the spectrum usage of primary users is stored in data-bases. This information is then used to guarantee the primary users' interference-free transmission.

The LSA has been mentioned as an option for sharing the spectrum with PS actors in [30, 31]. The complete series of LSA standards [7, 25, 8, 26] are very flexible for

different agreements between the primary and secondary spectrum users. They enable the industry to already apply LSA technologies. Moreover, the LTE is specifying support for LSA [32, 33, 34]. Therefore, the LTE operators can agree on their own spectrum utilization between the possible secondary users with standard methods. The LSA spectrum resource availability information is agreeable and the synchronizing for the information can be made robust. This flexibility is well suited for PS actors who might need to reserve their right for spectrum in specific situations, such as emergencies. Additionally, in homeland defence situations where the military would be a secondary spectrum user in peace-time, the LSA systems would require a role change between the primary and secondary users as discussed in [35]. The key components of the LSA system are depicted in Fig. 5.

The LSA licensee obtains an LSA licence that allows them to use the spectrum that is not used by the incumbent. The key stakeholders, elements, and related dynamics and interactions in the LSA work flow have been described in [36, 37]. The use of the LSA framework in a mobile broadband operator network with a system reference information has been provided in [8]. To enable the LSA concept, the national regulatory authority for telecommunications, the mobile operator, and the incumbent (also known as primary spectrum user) first negotiate the sharing framework. This contains the policies and rules for the shared spectrum use, e.g., the frequency band, and the technical and operational conditions for spectrum sharing [6]. The policy data in Fig. 5 is input about the usage conditions of the LSA band [36].

The LSA licensee, here a mobile network operator, obtains the available spectrum information from the incumbent via an LSA repository according to the sharing policies. The LSA controller computes spectrum availability in the spatial, frequency and time domains. More specifically, the LSA controller computes exclusion, protection and restriction zones that are geographical areas within which LSA licensees are not allowed to have active radio transmitters, areas within which incumbent receivers will not be subject to harmful interference and areas within which LSA licensees are allowed to operate radio transmitters with restrictions, respectively [26].

Then, the mobile operator as an LSA licensee uses an operations, administration and management (OAM) system to manage the licensed spectrum use based on the LSA controller information [38, 8, 32]. It sends the control messages to the base stations that change their frequencies accordingly.

The fall-back measures of the current LSA standard are given as informative examples in [7]. The measures are as follows. If there is suddenly no valid spectrum

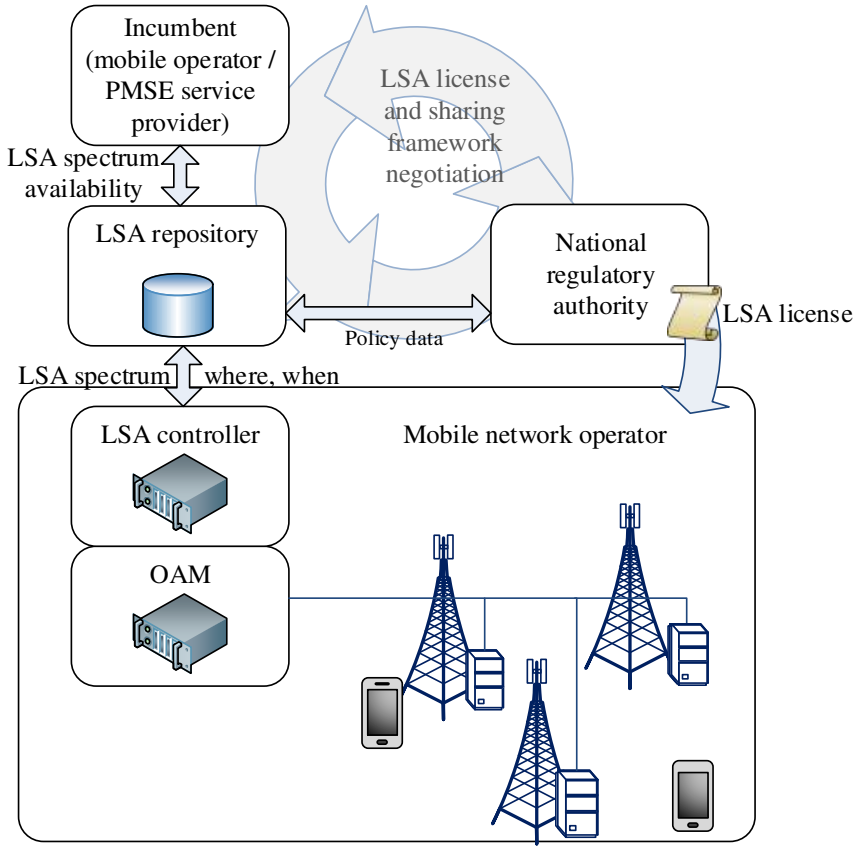

Fig. 5. The LSA system for a mobile operator as an LSA licensee.

information, the LSA licensee can either continue to use the licensed spectrum, fall-back to use spectrum according to some predetermined plan, or stop the spectrum use completely. These measures can happen either instantly, successively, or after the agreed time in the case of a detected connection loss. The used fall-back measures need to be agreed more specifically together with other sharing conditions in the sharing framework negotiations between the incumbent and the LSA licensee.

In this thesis, an LSA solution for PS actors is presented on a system level in Chapter 4. Moreover, in there it is described how to use the LSA method in a robust manner when the connection to the central repository is unreliable.

1.3 Spectrum sensing

The sensing is generally used to detect vacant spectrum bands, signals, their power levels and changes in the spectrum usage. Spectrum sensing has been extensively studied for wireless communications and it is the element that enables cognitive radio systems and software-defined radios to function in varying environments. For this, the International Telecommunication Union has given recommendations for spectrum sensing methods and for analyzing the sensed results in [39] and [40]. They recommend methods for detecting weak signals and separate co-frequency signals. Moreover, they recommended locating techniques such as the angle of arrival [41], the time difference of arrival [42], the frequency difference of arrival [43, 44], the power difference of arrival [45], the gain ratio of arrival [46] and identification-aided locating.

A survey for sensing in [47] examines the spectrum sensing challenges and goes through selected sensing algorithms for cognitive radios. The challenges are related to hardware requirements, to hidden node problems, to the sensing duration and to the speed of the detection. The algorithms include, among others, energy detector [48, 49, 50], waveform based [51], signal correlation [50, 48], cyclostationary [50, 52, 53], and radio identification [54] -based sensing methods.

Moreover, the work in [55] provides an extensive overview on real spectrum occupancy measurements. They concentrate on interference mapping methods for analyzing the spectrum occupancy. In this thesis, the focus is on the spatial dimension among the dimensions of frequency, space, time and power. The additional dimensions are directional information [56] and polarization [57].

The spatial dimension is an important aspect in central repository spectrum sharing methods such as SAS, described in the previous section. Therein, the environmental sensing capability (ESC) is used to detect non-informing military radars in the 3.5 GHz band from moving ships in the coastal areas. For protecting the location of the incumbent, the ESC is allowed to use only minimum radar characteristics to detect only a coarse location of the incumbent radar [58]. Moreover, the ESC sensors must report the measurements with quantized signal levels. Additionally, the ESC will not use highly directional antennas or store and transmit any time series data to enable angle or time difference of arrival methods. The sensing for ESC can be done with collaborative sensing.

Collaborative sensing has been surveyed in [59, 60, 61]. Furthermore, multiple sensors can be used to mitigate the effect of shadowing and fading by sharing their

information [62, 63, 64]. More specific ESC system and algorithm development is ongoing [65, 66, 67, 68]. In this context, the spectrum monitoring pilot program [69] intends to offer available spectrum monitoring data to the whole community. Furthermore, [70] has proposed a nationwide centralized radio frequency inventory to support dynamic spectrum access.

A centralized frequency inventory is also a part of the LSA spectrum sharing system. However, sensing is not necessarily required in LSA, as the incumbent informs its spectrum use. Nevertheless, sensing has been suggested for better overall spectrum utilization in [71, 72]. In these works, sensing is used to fill a radio environment map for coordination with multiple possible LSA licensees. In [71], LSA licensees and incumbent users are considered to have sensing capabilities, and the functionality between licensed users is modelled from the viewpoint of hidden Markov models [73] and clustering. In [72], a sensor network for spectrum information is proposed together with resource allocation algorithms for the licensees. In this thesis, when sensing is considered, a single LSA licensee uses available sensors for spectrum information when the centralized repository systems might not be available. Moreover, the sensors are used for verifying the repository information when the repositories are available. Collaborative sensing methods probabilistically increase the detection probability. Herein, the proposed sensing method takes a spatial perspective to obtain spectrum information. It can obtain a higher detection probability by simply considering smaller spatial areas that are reliably detected by a single detector.

1.3.1 Energy detection model

This subsection explains energy detectors used in this thesis for sensing purposes. Energy detectors are studied to find out their performance for the circumstances where they are sufficient in rapidly deployed PS network scenarios. The application is to find out the available frequencies for the PS networks which do not necessarily require the most efficient sensing methods possible. Other reasons to utilize energy detection are its simplicity and its ability to detect multiple types of primary users, such as LTE base stations, wireless cameras and microphones.

The transmitted signal s_n is assumed to be a zero mean, white, and wide sense stationary Gaussian random process with variance σ_s^2 as in [74]. The noise w_n is white Gaussian noise with variance σ^2. Let $r_n, n = 0, 1, \ldots, N-1$, be the received energy of

signal samples. The energy detection problem is to distinguish between two hypotheses

$$\begin{aligned} H_0 &: r_n = w_n && n = 0,1,\ldots,N-1 \\ H_1 &: r_n = s_n + w_n && n = 0,1,\ldots,N-1, \end{aligned} \tag{1}$$

where hypothesis H_1 denotes a signal present and H_0 denotes signal not present. An energy detector decides the result by calculating the sum energy received and by comparing it with a detection threshold γ. It is decided H_1 if the sum of energy samples $\sum_{n=0}^{N-1} r_n^2 > \gamma$ and H_0 otherwise.

The performance of an energy detector is well known [48]. The probability of false detection is

$$P_{FA} = Q_{\chi_N^2}\Big(\frac{\gamma}{\sigma^2}\Big), \tag{2}$$

where γ is the detection threshold and the $Q_{\chi_N^2}(\cdot)$ is the right-tail probability function of a chi-squared random variable for N samples [48]. The probability of detection is

$$P_D = Q_{\chi_N^2}\Big(\frac{\gamma/\sigma^2}{\sigma_s^2/\sigma^2+1}\Big), \tag{3}$$

where σ_s^2/σ^2 is the signal-to-noise ratio (SNR).

An alternative expression [75] for probability of false detection (2) is obtained by using upper incomplete gamma function $\Gamma_{\text{up}}(\cdot,\cdot)$ [76] as

$$P_{FA} = \Gamma_{\text{up}}(\frac{N}{2}, \frac{\gamma/\sigma^2}{2}) = \frac{\Gamma(\frac{N}{2}, \frac{\gamma/\sigma^2}{2})}{\Gamma(\frac{N}{2})} = \frac{1}{\Gamma(N/2)} \int_{\frac{\gamma/\sigma^2}{2}}^{\infty} t^{\frac{N}{2}-1} e^{-t} dt, \tag{4}$$

where $\Gamma(\cdot)$ is the Gamma function. To obtain value for a specific threshold γ, the equation (4) can be inverted by using Newton's root finding method [77].

1.4 Public safety communications in commercial LTE networks

Traditionally, PS networks and commercial networks have been separate. However, the technological innovations of commercial networks have been noted in the PS area, which wants to benefit from the modern networks, their affordable prices, and their over-the-top services [78, 79].

On the other hand, the PS actors have special requirements for the commercial LTE networks and the supported applications. Thus, PS associations have joined in

the standardization of LTE networks to fulfil their mission critical LTE requirements [80, 81, 82, 83, 84]. The mission critical LTE standards belong to the LTE standards. They will enable the critical PS communication in areas with LTE networks and with stand-alone equipment.

In this thesis, mission critical LTE is considered as a part of the communication solution for PS actors. The requirements and the standardization work to satisfy the mission critical LTE requirements are as follows.

The PS requires LTE devices to support isolated operation for PS actors without the connection to the backbone network. In non-isolated operation of an LTE network, a central evolved packet core (EPC) authorizes the subscribers to the LTE network, manages the mobility and quality of service (QoS) of the users and provides data gateways for them [85]. To support PS requirements and use cases [86], isolated operation has been specified in [87]. In this standard, the connection to a centralized EPC is not necessarily needed. For this, the LTE base stations can operate in a nomadic stand-alone mode and the connected base stations can be used to support PS communication[1]. The communication between PS actors can be guaranteed, for example, with mission critical push to talk service (MCPTT) [88]. This service makes use of group communications system enablers for LTE (GCSE_LTE) [89, 90], which enables the communication without a connection to the central EPC. This can be done in practice with distributed service applications. The communication is controlled by third party group communication service application server(s), where the PS actors register themselves.

The GCSE_LTE allows the PS actors to be grouped and to communicate flexibly with different groups. The GCSE_LTE is based on Evolved Packet System (EPS) bearer services [91] and multimedia broadcast multicast bearer services [92], and it enables the PS actors to share multimedia content, to have group calls, and to have multi-agency communication in a harmonized manner. Moreover, the users can be included in multiple groups. Then, the data flows and multimedia streams can be distributed simultaneously to several groups. The group communication service application servers can, for example, be used to integrate communication between LTE and TETRA networks.

Additionally, critical users require device-to-device connectivity between user equipment in the proximity. The proximity services (ProSe) [93] have been standardized

[1]This operation can be guaranteed in practice by having a light EPC type of solution next to the base stations, which do not satisfy the most recent LTE standards. This light EPC should itself have the necessary functionalities for connecting the users to the mobile network.

for LTE networks and equipment. The ProSe communication can happen directly between the user equipment without any base station. Additionally, the discovery and the communication between the devices can happen via an LTE base station and via wireless local area network (WLAN). Moreover, the users themselves can use ProSe to share LTE connectivity to the nearby devices. More specific use cases are given in [94]. The ProSe standard also supports roaming between multiple operators. This operation can be obtained in practice by using the universal Internet protocol (IP) -based applications. Because IP-based applications of the PS actors can be utilized via unknown WLAN and roaming connections, the ProSe is specially designed with strong end-to-end requirements of confidentiality, integrity and authenticity [95].

Note that the PS actors also require a higher service priority for their data and video applications than the commercial users. The QoS with compatibility and security requirements for mission critical data and for mission critical videos are specified in [83] and [84], respectively. The QoS for LTE is controlled by the policy and charging control (PCC) [96, 97, 98]. The PCC enables centralized session control for all the subscribers. The QoS control can be applied on a per service data flow basis. For example, the PS actors can use non-critical civil applications with the same priority as the commercial users.

To enable the service data flow QoS control in practice, the PCC includes a policy and charging rules function (PCRF) [98]. This function controls the pricing and the dynamical service decisions for the different flows. If required, the PCRF can be adjusted dynamically for different flows with the application function (AF). Then, when allowed in roaming situations, the dynamic QoS control takes place through the visitor PCR. Moreover, the dynamic QoS control is specified to be done via a broadband policy control framework, when the application services for PS actors work over WLAN [99].

The PCRF has multiple sources of information to be able to control the flow policies. Namely, the PCRF extracts flow-based information and service requirements from the AF. Additionally, the PCRF obtains the information about user identities and service profiles, available service capabilities, different data flows, different bearer events and the congestion status of the network. With these information sources, the PCRF can decide the enforced policies for different users and flows. More specifically, the PCRF decides values for the maximum authorized and guaranteed data rates, the quality of service class identifiers (QCI), and the allocation retention priority (ARP) numbers. [98]

The decisions by PCRF are applied by the policy and charging enforcement function [98], which enforces the predefined rules. The decisions are also sent to the traffic

steering support function, which ensures the policy enforcement in the IP-based services. The decisions can be enforced as follows.

If multimedia priority service is initiated, the PCRF generates corresponding PCC and QoS rules with ARP and QCI parameters for the prioritized service for the users of the multimedia priority service. The EPS bearer QCI numbers are used for scheduling the radio resources for the most critical applications. Then, if there is network congestion, the ARP numbers are used to ensure the service for critical communication [98]. An ARP request defines the relative priority of a resource request at a given congestion level. It is used to determine, for example, whether the bearer with the guaranteed data rate can be accepted or not. Furthermore, if the network becomes too congested, the low-priority users with the largest ARP priority numbers can pre-emptively lose their assigned resources. Moreover, the access class barring [100] can be used to increase the delay of non-critical users to access the network, so that higher priority users obtain access to services faster.

Note that while the upcoming commercial LTE and 5G networks are standardized for PS applications, the PS actors also require broad coverage. If there is no commercial network available, the PS actors can either use device-to-device connectivity or deploy their own rapidly deployed network. This thesis develops the spectrum sharing methods between commercial and rapidly deployed networks.

1.5 Rapidly deployable public safety network

The rapidly deployable network is depicted with an example setup in Fig. 6, where the PS actors have their private, closed LTE network. This network enables the connection between its mobile users and provides a connection to an external commercial network, such as the Internet. The commercial networks can be connected to this system, e.g., with multi-radio access technologies such as a multi-operator 3G/4G/LTE router. The antenna of the router can be lifted high above the ground level and have a high antenna gain for broad coverage.

This kind of network can be rapidly built, for example, with towable lifts or crane cars equipped with the necessary equipment. The network is scalable, i.e., the number of LTE access points and routers can vary. The size of the network will be scaled according to the operational needs of the PS users.

There exists an underlying backhaul network for connectivity between the base stations of PS. This network handles the route discoveries and offers data transfer and

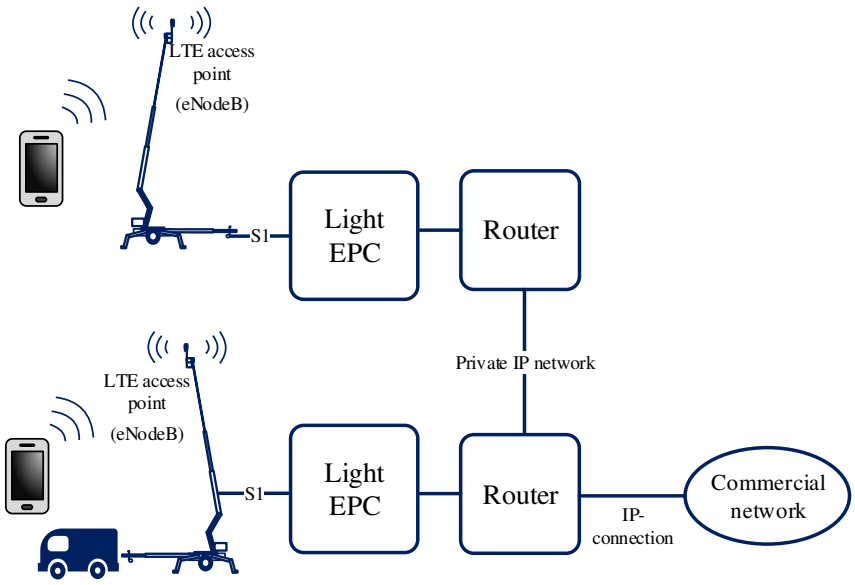

Fig. 6. Distributed rapidly deployable LTE network for PS actors.

LTE voice services for the user equipment of the PS actors. Moreover, the backhaul network offers backbone connectivity to other available commercial networks and to the user equipment therein.

The backhaul for the LTE network can be built with routers that form a private IP network. An example solution to build the backhaul rapidly is by using tactical routers [101] with radio heads. In addition to wired links, these routers also support radio link connections. They can also automatically reroute any given data from the source to the destination via alternative routes, given that the primary route fails. Every LTE access point is connected to the private IP network via a light EPC solution, (such as lite-EPC [101]) and a router. A light EPC solution provides an LTE access point and its users to the network and emulates the EPC functionalities of an LTE network. The LTE access points are connected with an S1 interface to the light EPC solution.

1.6 Research problems

This thesis researches how the PS actors can obtain connectivity and similar capabilities in rapidly deployed networks as in commercial networks, and how PS actors can obtain radio spectrum for their communications at their rapidly deployed networks. These questions are approached by dividing them into smaller research problems.

The first research problem (RP1) is to study the possibilities to connect the rapidly deployable PS network concept together with a commercial LTE network. The beneficial applications offered by the commercial networks should also be available in the rapidly deployable network. Furthermore, the users in different networks should be interconnected.

The second research problem (RP2) is to assess the options of PS actors to utilize spectrum sharing for their deployed networks. For this, spectrum sharing ideas based on the LSA concept are investigated between the PS network and commercial radio systems. While the concept of LSA has been well developed, it has not been thoroughly investigated from the PS actors' point of view, who have special requirements for robustness and spectrum availability.

The third research problem (RP3) is to design an LSA framework to be utilized in a rapidly deployable PS network that ensures the necessary application-specific services for the PS operations. These database-based services are generally offered via the commercial network connections, but the commercial network might be unreliable or unavailable. Thus, there is a need for a robust PS network with a robust spectrum sharing method of finding the spectrum for the PS network.

The fourth research problem (RP4) is to study a backup system for the LSA framework in the means of sensing the available spectrum and the incumbents. This problem originates from the need to study how to utilize the already available sensors in practice and not from developing a more efficient sensing algorithm. This problem includes defining and determining the distances, from which an energy detector can detect incumbent LTE base stations as shown in Fig. 3.

The fifth and final research problem (RP5) is to find out how the sensor information from multiple sensors can be used collaboratively with LSA as a backup spectrum information system.

1.7 Contributions and outline of the thesis

Chapter 2 discusses the RP1 and gives alternatives for interface connection possibilities between a rapidly deployed PS network and commercial networks. Chapter 2 is based on the journal III. Similar services and applications must be guaranteed in both networks, and this requires a common connection point. The contribution of this chapter is in giving alternatives for the architecture combining commercial LTE networks and rapidly deployable PS networks. Furthermore, this chapter provides requirements and proposals for the application-specific services to support similar services and mobility between both networks. Also, the security aspects of commercial LTE equipment are considered in this chapter.

Chapter 3 discusses the RP2 and gives alternatives for spectrum sharing between PS and commercial systems. Its contribution is to study the available spectrum sharing options from the PS actors' viewpoint. Chapter 3 is based on the journal I.

Chapter 4 designs an LSA framework for RP3. In this chapter, a more specific system is planned for the PS actors, where they are an LSA licensee for the LSA spectrum resources of the commercial systems. Chapter 4 is based on the journal I. While the LSA technologies are well investigated, these methods have not been developed for the robust PS application needs. The chapter also further develops the LSA framework to support decentralized operation. The contribution of this chapter is the design of a highly robust LSA system to be implemented with current commercial technology and equipment. By robust, it is meant that the proposed system is resilient to connection breaks in the LSA system that may happen in real life due to electric breaks or other issues, i.e., in cases where the PS services are often needed. Importantly, if the PS actors utilize LSA spectrum resources, they require the sharing process to be robust against connection problems. However, the fall-back measures for the LSA system are generally presented only on a high level [7]. Therefore, the LSA system is proposed to include more information in verifying the spectrum information validity.

The proposed method is validated via simulations. The simulations are further used to study the main system design parameters and for giving guidelines to select them properly. The proposed time information for valid spectrum information has subsequently been included and further developed in the LSA design specifications in [26].

Chapter 5 further develops the LSA system of the previous chapter to include spectrum sensors to answer the RP4. Chapter 5 is based on the journal II. The

contribution of this chapter is to define and determine the distances from which an energy detector can detect LTE base stations with different transmit power in the Extended Hata attenuation model [102] with noise uncertainty [103].

As another contribution, this chapter describes a solution to RP5 on how the detector information can be used in practice together with an LSA system in a rapidly deployed PS network. More specifically, a decision method for using sensing results is proposed for ensuring the availability of spectrum for PS networks. The proposed method can be used, firstly, to validate the spectrum information requested from the LSA repository or, secondly, to obtain spectrum information when there is no valid LSA information. Note that comparable collaborative sensing methods that can be used for complementing a centralized LSA system have not been suggested before.

Chapter 6 concludes the thesis and provides some uncovered open problems.

1.8 Authors contributions

This thesis is based on one published journal paper I with a conference version [104], and one submitted journal paper II with a conference version [105]. Moreover, parts are taken from a journal paper III, where the author is the writer of the rapidly deployable network parts describing live trials and collaboration trials between the commercial 5G network and the rapidly deployable PS networks.

The proposed resource allocation method in this thesis builds on previous LSA work in [106, 107]. The LSA system presented in this thesis has been demonstrated in the projects CORE++ [24] and CORNET [108], where the author was working and taking part in project demonstrations. The rapidly deployable network concept has been collaboratively trialled with commercial networks [109]. The tests have been conducted during public safety operations so that the personnel have used more than 20 end user equipments that can access both rapidly deployed and commercial networks. The solution has ensured operational safety and priority communications in commercial networks. Moreover, after publishing I, its proposed time information for valid spectrum information has subsequently been included and further developed in the LSA design specifications in [26].

2 Interface connection possibilities with commercial networks and application-specific services for public safety

In this chapter, it is assumed that the necessary commercial services are available with and without the full functionality of the commercial networks. While the commercial networks are designed to support PS applications, the PS actors might still need a rapidly deployed PS network to guarantee their own communication. The applications should be able to collaborate between rapidly deployed PS networks and commercial networks. Therefore, there should be interconnection between the PS actors utilizing the different networks.

In this chapter, possible network and application solutions are considered for enabling the PS communication and data traffic. The chapter provides solutions to the RP1 and is based on the journal III. The four first sections describe interface connection possibilities between the PS network and the commercial networks. As an example, both networks can be connected via the public Internet. Another option is to connect the PS actors only via the network switches and routers of the commercial operator without a connection to the public Internet. Moreover, it is possible to utilize a common commercial EPC network and its services.

Then, the last section describes the possible PS communication applications and new applications that can be enabled with higher data rates. Moreover, the last section discusses the application-specific requirements and concludes with security issues that PS wireless communication experts must consider when utilizing commercial LTE networks.

2.1 Common services on the Internet

The overall PS communication system can offer its application servers and data bases for its users over the Internet. The connection can be secured, for example, with a virtual private network (VPN) [110]. The application servers and data bases can be hidden services in a closed PS network, and alternatively offered in any other private or public

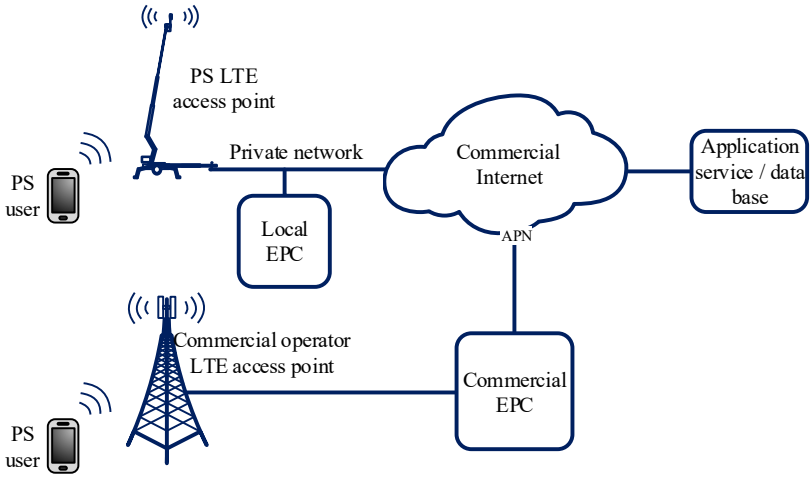

Fig. 7. An application service given to all the PS actors via the commercial Internet access.

networks. These applications can then be reachable from any network having an Internet connection. Fig. 7 plots an example scenario where the application service is accessible publicly from the Internet. The benefit of this solution is that it is straightforward for connecting multiple PS actors also with different Internet service providers. Moreover, the PS actors can access the Internet in multiple ways, among which at least one has to be functional. Normally, the PS actors can obtain wireless Internet with single or multi-radio access technologies. Technology examples are long-range Wi-Fi, WiMAX, or multi-operator 3G/4G/LTE routers. To obtain a long range, this type of router can be combined with a high gain directional narrow beam antenna that is lifted high above the ground level. Then, if there are multiple networks available, the PS actors can select the best quality network. This kind of setup gives network access in areas where the normal LTE mobile phones do not have coverage. For even remoter environments, the PS actors can utilize satellite broadband connections.

In operations where the commercially-available mobile network is limited,[2] the PS actors can use locally-available commercial public or private networks for connecting to the Internet. The connections can be obtained, for example, with wired local networks.

[2]Examples are rural areas and blind spots in the city behind strongly attenuating walls.

In this scenario, the PS actors can use an authorized relay to connect to the network.[3] This relay can then offer the necessary Internet port for the end users of PS actors behind it and to a rapidly deployed LTE network. Note that to enable sufficient setup speed and coverage, the authorized relays need to be configured beforehand to the required locations.

2.2 Common commercial network switches and routers

The commercial networks can offer the backbone of the commercial networks for PS use. There are multiple ways for PS actors to utilize the common commercial network switches and routers and any of the connected networks can offer the required applications. The applications are then accessible to critical users via routing.

Fig. 8 plots an example scenario, where the application service is accessible by routing all the critical data to the same PS network. In this example, all the PS actors' data traffic can be routed to the network address of the PS command centre. Then, the PS actors can utilize services offered by the command centre. In this figure, the rapidly deployed PS LTE access point is connected to the commercial network with an interface device, which is a secure traffic relay. It serves as the point between the local loop and the commercial operators' wiring. The PS actors can have multiple interface devices connected to the commercial IP networks. The devices can be connected to each other with methods like a virtual local area network (VLAN) [111] or a virtual private local area network service (VPLS) [112]. After that, the PS users can communicate using their desired method. For example, multiple PS networks can be interconnected via these methods while the connection appears to be a local area network for the users. Note that these interface setups can be dynamically set up with software-defined switches or pre-defined permanent installations. For rapid deployment, the interface devices can have the necessary means to connect to the installations, for example with specifically-designed automatic radio links.

In addition, the data of the PS actors using commercial LTE networks can be routed to the same VLAN or a communication group by setting access point name (APN) rules correspondingly [91]. First, the PS actors specify a known APN for critical communications to their user equipment application. This APN is then authenticated by the mobility management entity of the commercial network. Finally, the critical

[3]The relay can, for example, be a personal computer with two network cards. One network card is connected to the rapidly deployed PS network and the other card is configured for obtaining the Internet connection.

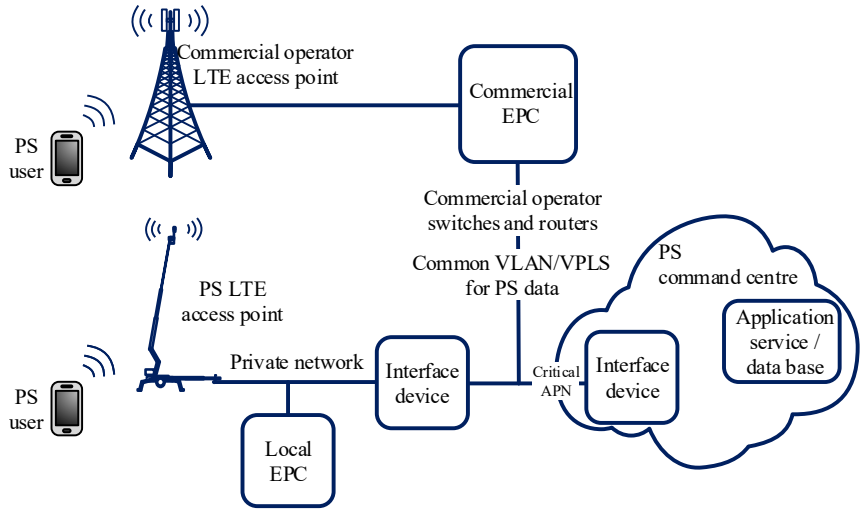

Fig. 8. The PS command centre gives application service access for PS actors at commercial networks and for PS actors at a closed PS network.

data of the PS actors is routed to the corresponding APN by the network. The critical application services can then be offered behind the critical APN. This includes data bases and, for example, filtered Internet access. Note that the LTE has been specified for a multiple packet data network support as described in clause 5.10. at [91]. Thus, not all the commercial traffic has to go via the PS command centre. Instead, the non-critical data can be routed elsewhere.

Note that in Fig. 8, the user equipment under the PS LTE access point can also be connected to the PS command centre by using commercial LTE networks. In this scenario, the interface device would be a commercial LTE router specifically designed to be connected to the commercial LTE network.

Another way for PS actors to utilize a common network is to have a commercial network slice as a backbone connection. More specifically, a part of the radio access networks can be virtually sliced to critical communications with software-defined networking [113] and network functions virtualization [114]. This slice can include LTE base stations that are predefined for PS use. Note that this type of network slice can also be permanent or could be configured for PS use only where and when required.

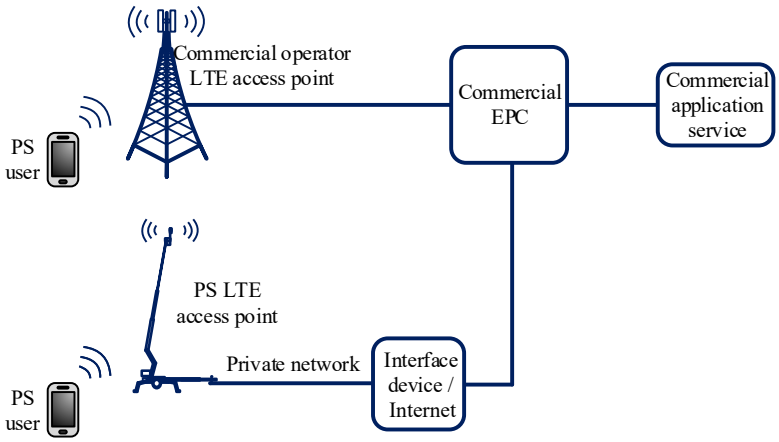

Fig. 9. An application service access given for PS actors via a common commercial EPC.

2.3 Common commercial evolved packet core network

The commercial services can be offered via a commercial EPC for the PS actors as in Fig. 9. In this setup, the commercial network configures the PS base stations to its EPC. Likewise, the PS actors configure their base stations to use the commercial EPC. The main benefits of this scenario are the latest commercial application services and the interoperability with older mobile systems. Moreover, the interconnection between the PS actors at the commercial and at the PS networks is offered by the commercial EPC.

The PS base stations can be connected to the EPC via a VPN using an Internet connection or via physical network layer configurations. Thereafter, if there is no connection, the PS base stations can utilize a local EPC solution, which can support the services that the PS actors have noticed to be beneficial.

Note that the PS network operator could also act as a mobile virtual network operator inside the commercial LTE networks [115]. Furthermore, the PS operator can operate a full commercial EPC service itself. With this setup, the PS actors obtain more control over the network they use. For example, the PS operator would own and control the subscriber information, the home location registers, the data bases, the base station configurations, and the access point names. Then, the PS operators can have roaming

agreements with all the different commercial operator networks, to enable the widest possible coverage for PS actors with the available commercial networks.

With roaming, the PS actors can also allow selected commercial users to use their deployed base stations. This can be critical in some operational scenarios, where the commercial network is down, and the commercial users do not have a connection to the outside world. For example, if commercial users are allowed to use the PS base stations, emergency calls could be enabled. These calls can then be routed to the emergency response centre or to an equivalent service that is enabled in the field. Additionally, the commercial mobile users under the area can be located if their mobile phones attach to the deployed base stations. Note that the PS actors can still obtain higher priority to use the network from the commercial core with methods discussed in Section 1.4.

For a common EPC, the PS actors must establish a core network connection. To do this, the PS actors can connect to the core network via a VPN using an Internet connection or via dedicated network ports of the commercial networks. If there is no connection, the PS actors can still utilize a local EPC solution to offer the necessary services. Note that all the necessary services can also be developed into the local EPC solution.

2.4 Combination of common connection points

Note that the PS actors can also utilize all the above options based on their availability. This way, the PS actors obtain redundancy and compatibility for their operational needs and situations. Fig. 10 plots an example of this. In this scenario, the PS actors that utilize the PS network and commercial networks make use of the commercial EPC service when it is available. When it is not available, they utilize their own EPC solutions and PS networks and the commercial routers. In this scenario, all the application services can be utilized by all the users in different parts of the networks.

2.5 Application-specific services and security

In this section, requirements and proposals are given for the application-specific services to support full mobility and access to the commercial and to the PS networks. More specifically, the section goes through the user applications, the network applications and the commercial LTE network security for PS-specific scenarios. Note that the

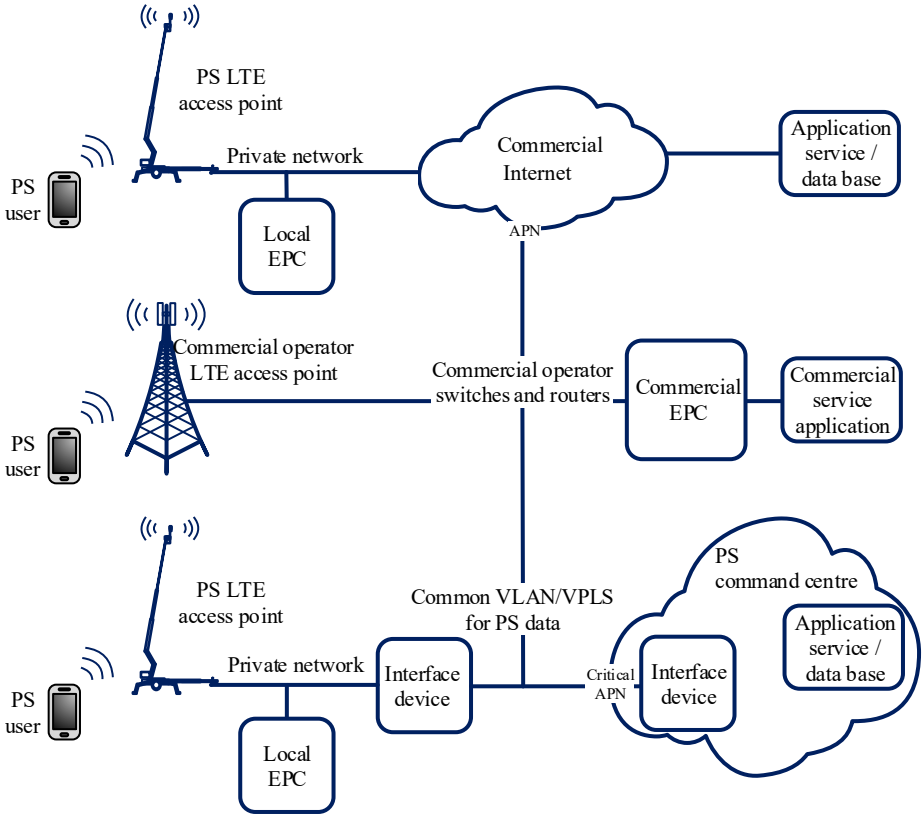

Fig. 10. Utilizing all the common connection points together.

applications should work consistently for the PS actors regardless of the availability of the commercial networks.

The PS actors need interconnection and require a similar operation of the applications and services in every network. Thus, both the rapidly deployed and the commercial PS network must support all the necessary applications. This section discusses the issues that need to be considered before PS actors can use commercial networks and their beneficial applications.

2.5.1 User applications

This subsection gives some examples of the possible PS applications and use cases where the LTE services can be used [116]. After the review of application possibilities, general requirements and possible solutions are given for the PS applications to securely use services with commercial networks.

The applications for PS actors include the basic individual and group communication applications for voice, text, multimedia and data sharing. As a special requirement, the PS actors should have communication applications for interconnecting the LTE user equipment with the services they currently use, such as TETRA [88].

Additionally, the commercial communication networks can be used for situational awareness [117]. More specifically, the PS actors can have additional applications for utilizing the available real time sensors, temperature cameras and commercial cameras for surveying, for automatic recognition and for alarming. Moreover, the PS actors in the field can use location-specific services together with LTE networks to obtain the data from the sensors and the cameras in their vicinity. Also, PS actors can benefit from various map tools and from knowing the location of the other PS actors. The security measures for these applications must be considered individually per each application.

As another application, the remote high data rate connections can enable leveraging expertise from remote locations. This can enable telemedicine and, for example, forensic capabilities or other special analysis from the field and to the field [118]. The LTE connection enables a remote connection to the multitude cloud services, personal computers, robots with special tasks, drones, and data bases. For example, the PS actors might use data bases to acquire information about the people they are going to meet or the places they are going into.

In simplicity, the LTE and the commercial services offer a high number of beneficial applications for PS actors. All these applications require secure, authenticated, and

encrypted connections between the users and services. Next, multiple requirements are presented for PS end user applications to be able to connect to PS services with commercial and rapidly deployed networks.

First, for routing the critical data towards the PS network, the critical PS applications should be able to request a specific APN connection from the commercial networks [91]. This enables the routing of the critical data to a known PS network via the commercial networks.

Second, the application service should be encrypted. If the service application does not by default encrypt the transmission, additional services such as VPN [110] should be used. Thus, the commercial user equipment should have a VPN client type of service. Moreover, VPN client service can be offered to the users at the rapidly deployed PS networks in a network interface device between the public and private networks.

Third, some specific application services can be hidden via onion [119] or garlic [120] routing. This is particularly useful when the locations of PS actors are confidential. This type of routing makes it harder to find out the content, service location and end user location by commercial network operators or anyone listening to the traffic. The services can be hidden either in the PS or in the commercial network. To access the hidden service, the client can utilize a mobile application for onion routing. Another option is for the interface device of the PS network to have an onion routing client. Note that this routing method still requires end-to-end encryption.

Fourth, to support the multitude of evolving applications, the PS actors require an application sharing method. This can be implemented centrally in commercial networks and with peer-to-peer or as a distributed service inside the rapidly deployed PS networks. If PS actors use commercial applications, they need to be trusted and properly secured. For example, the application sharing service should allow only the sharing of verified applications that are properly inspected. The inspection should verify that the security and privacy requirements for the PS use cases are fulfilled. For highly secure scenarios, trusted open source applications compiled from the inspected source codes can be a possible solution.

In rapidly deployed networks, the PS actors can utilize commercial applications and data bases with a mediator pattern and a proxy-based application approach [121]. The mediator or the proxy server can, for example, act as a single user to the commercial service, but distribute the access or relevant data to all the PS actors inside the rapidly deployed network. This approach can make it easier to handle special situations such as connection breaks inside the PS networks. For example, the mediator program can work

stationary at the edge of the commercial network and keep the most recent information utilizing the commercial networks. After experiencing a connection break, the PS actors inside the rapidly deployed networks only need to connect to the mediator, and not to the commercial network service. This type of solution can reduce connections to the central service, given that the topology of the rapidly deployed PS network might be changing.

Moreover, all the necessary service applications, such as voice or data sharing services, can be made to work distributed. This brings robustness to the network. More specifically, multiple copies of interconnected service applications can run in commercial and in rapidly deployed PS networks and exchange data. Then, the individual PS end users do not necessarily need direct connections to a central commercial service application, but can connect to the nearest distributed application service.

2.5.2 Network applications for public safety communication via commercial networks

In this subsection, requirements are given for network applications that enable the PS network operators to offer commercial LTE network connections via rapidly deployed networks. These applications include information service applications and practical applications for guaranteeing connectivity and security. Furthermore, requirements are given to a network interface device between a rapidly deployed network and a commercial network.

The PS network operator requires real-time information on the service levels and availability of the commercial radio access network [122]. The operator has to know where and how the PS actors can have a commercial connection with the existing network. Then, if the commercial systems are available at the scene of action, the PS actors can connect to them with their commercial user equipment. Otherwise, a rapidly deployed PS network is required.

For the PS end user, it should be irrelevant whether they communicate using a commercial or a rapidly deployed network. The PS actors require the communication to work. They want to take care of their work without fighting with their communication equipment. Therefore, if the rapidly deployed network is carried with the operators to the point of action, there is a need for an application that decides whether the rapidly deployed LTE base station should be turned on or not.

Thus, the PS network operators need to have a network monitoring application that, for example, includes a map of the available commercial LTE base stations and

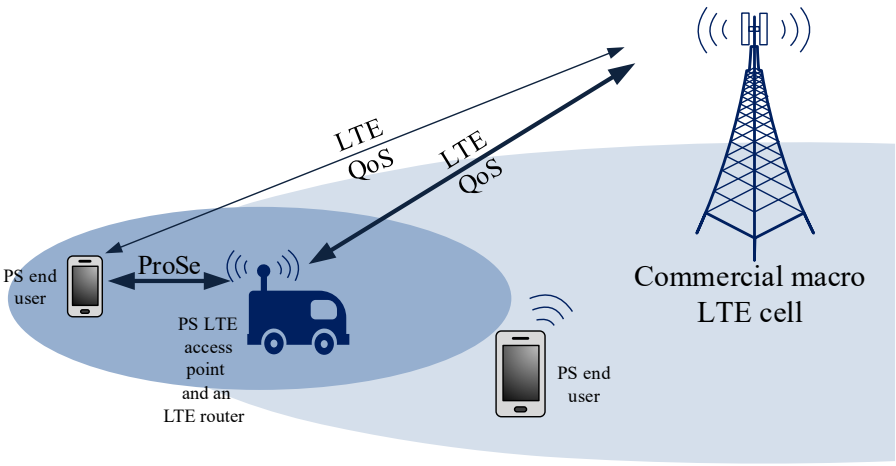

Fig. 11. A rapidly deployed LTE base station has automatically started, as the QoS of the commercial network is too small.

their status, together with the QoS monitoring application. This application can then be combined with an automatic decision method deciding the operating status of the rapidly deployed network.

An example situation, when the rapidly deployed network is turned up and running, is shown in Fig. 11. The decision method can work, for example, as follows. Before the PS LTE base station offers full LTE service, the rapidly deployed network equipment can be connected via an LTE router to the end user with a ProSe type [93] of solution and vice versa. Moreover, the rapidly deployed network equipment can be connected to the commercial network with an LTE connection. Then, the end user mobile can offer QoS information to the rapidly deployed network via a ProSe connection and via the commercial LTE network. This information can then indicate whether to turn the full LTE base station on or not.

Note that the rapidly deployed LTE base station requires spectrum. Initially, if spectrum is available, the rapidly deployed LTE base station could use it, for example, with LSA [6, 7]. If there is no available spectrum, it should be obtained with other means, such as with flexible spectrum use by the commercial operators.

Furthermore, an application is needed for controlling the possible network slices [114]. Moreover, if there are no commercial LTE networks available, the PS users in some longer-term operations require knowing beforehand the connection points that are planned for attaching rapidly deployed networks. As an example, the PS operator could have a program listing other types of available Internet and network connection points,

e.g., the network exchange points and the actual router cabinets to connect to. There can also be other types of pre-planned connection points, such as specifically-designed radio link connection points.

Note that the PS actors might require an interface device that acts as a mediator between the PS actors inside the commercial networks and inside the PS network. This device would then relay commercial network services to the PS actors. For this it can, e.g., satisfy the proximity service standards for network relays described in [93]. Moreover, the interface device could act as a network access server [123] and route the service requests from the commercial network to the corresponding services inside the PS network.

The interface device should be able to offer a secure connection between the PS users, e.g., by offering a VPN [110] type of encryption service. To hide the rapidly deployed network and the PS users, the interface device can also act as an onion router [119]. Moreover, the interface can have the necessary means for preventing malicious actions. Naturally, when a rapidly deployed PS network uses commercial networks, they must include a firewall to filter and monitor the packets coming in and out from their network.

Additional central network services for PS actors to consider are, e.g., domain name system servers [124] and certificate authorities. The communication system becomes more resilient by having the central network functionalities.

2.5.3 Commercial LTE network security

The PS actors must consider security issues before utilizing the commercial LTE networks. In this subsection, some of the security issues are presented. The commercial LTE networks have been standardized to have high security. The security measures are available and all of them need to be used. These include the use of the latest secure verification methods between the users and the network, an air interface protecting with the latest ciphering mechanisms, and IP security architecture (IPsec) [125] for the traffic from the base stations. Moreover, the user applications should always communicate with cryptographic communication protocols.

The enabling of available network security measures has been optional for the commercial LTE network operators. Thus, they are not always used in the commercial LTE networks, where network speed and simple set ups are more important. For example, all the base stations might be allowed to connect to the EPC functionalities

simply given that they know the IP addresses of the EPC functionalities. A reason behind this is that the internal network, behind what the end users see, has been considered as a private network also physically. This is because the base stations and other network components have traditionally been behind locked doors where others have no access. However, the current indoor base stations are closer to the end users and can even be touched by the end users, if desired.

Therefore, when using commercial services, the PS actors need to verify the use of the security measures. For example, the control messages must be secured with IPsec [125]. If they are not, it is easy to sniff subscriber identities from commercial indoor base stations with basic multiport repeaters. Moreover, standard security procedures such as changing the default passwords to all the network equipment need to be enforced. Additionally, the data at the base stations could be encrypted.

Moreover, commonly used backdoors [126] in LTE base stations and other utilized commercial network equipment should be considered. The LTE network equipment manufacturers use these types of backdoors, for example, to base station maintenance at the factory. These backdoors can possibly be used to copy the base station information, which in turn can be used in a malicious manner. This includes, for example, faking a PS LTE base station or reconfiguring the commercial base station to be less secure. These manufacturer backdoor mechanisms and their existence should be acknowledged by the PS network operator. If required, the backdoors could be made accessible only by combining key information from the manufacturer with key information originating from the PS network administrator. This requires direct collaboration with the manufacturer.

Also note that the current commercial systems are designed for high efficiency and with backward compatibility to less secure systems. Thus, if security is required, the networks and user equipment should be up to date for not allowing this. Otherwise, it is possible to set up false base stations, where the user equipment of the PS actors can try to connect [127, 128]. This type of attack could, for example, be used to listen to the PS data traffic.

Moreover, the international mobile subscriber identity code is sent without ciphering over the air during the first attachment procedures and when an identity request is sent by a base station [91]. This code can be listened to over the air and be collected by anybody. Note that these attachments happen relatively rarely, because temporary identity codes are used after the first successful network attachment. However, the original code can still be listened to over a long period of time, for example, next to the workplaces of PS users, to obtain the identity codes of people that turn on their new cell phones.

In certain PS operations, when the locations of PS actors are highly confidential, the PS actors should not use commercial LTE networks as they usually work. This is because if precautions have not been taken, the commercial network operators (or a malicious person with a false base station) can possibly access the location and the subscriber information of the PS actors. Instead, the PS actors need to follow secure practices defined by the communication security experts. Moreover, if required, the LTE network can be further designed to hide the PS actors. The communication can, for example, occur via specifically designed protocols for hiding the location of PS end users and their communication. To do this, similar practices as in [120, 119] can be used.

If the commercial LTE equipment is needed in higher security situations, closed PS LTE networks could be preferred against commercial networks. However, the ease of jamming, listening and data collecting possibilities over the air must also be acknowledged with closed LTE networks. In general, the PS use cases of commercial networks need to assume that these networks can be easily surveyed and attacked maliciously.

2.6 Summary

This chapter concentrated on the possible network and application solutions for enabling the collaboration between the PS and the commercial networks.

Interface connection possibilities were given to connect users from one network to another, namely using the Internet, commercial network switches and routers and common commercial EPC network services. Moreover, possible PS applications and requirements were listed for the application-specific services to support full mobility and access to the commercial and to the PS networks. The PS network should support all the beneficial commercial applications for them to work consistently, regardless of the availability of the commercial networks. Therefore, the support also needs to be included in the PS network.

Moreover, this chapter presented the security issues that must be considered by PS actors before utilizing the commercial LTE networks and PS networks. The commercial networks need to use all the available security measures [129], e.g., commercial networks should always use the latest secure verification methods between the users and the network, protect the air interface with the latest ciphering mechanisms, and use IP security architecture (IPsec) [125] for the traffic from the base stations. While the secure

mechanisms are available, their actual use should also be verified. Moreover, the user applications should communicate with cryptographic communication protocols.

3 Public safety spectrum sharing possibilities with licensed shared access

Spectrum sharing alternatives between a PS and a commercial system (CS) are discussed in this chapter. The chapter provides solutions to the RP2 and is based on the journal publication I.

Some countries will still have dedicated spectrum for critical communications, but the trend in Europe has been to auction spectrum for commercial operators, as it is financially beneficial. As the commercial networks develop, it is becoming more likely that spectrum sharing will occur between critical and commercial operators in the future [130].

The truth is that the PS actors might not always use their full spectrum and it might remain available most of the time, at least locally. Examples are with police patrolling, where just a small voice service part of the spectrum needs to be reserved, and with military users that often, in peace time, need a large part of the spectrum only in exercises and in special exercise areas. Naturally, in the case of increased threat, they need it in situations like patrolling in the cities. The temporally and spatially-unused spectrum could be used for other purposes, assuming it will be released immediately back to the PS actors when needed. For example, utilization for non-used PS spectrum improves the capacity of the CS users and their transmissions, e.g., to ease rush hour data traffic; naturally this is of interest in areas that have high mobile traffic and not in isolated areas.

In addition, the PS actors may also need complementary or additional resources for their events, and thus it would be beneficial for them to get spectrum from CSs. For example, when the situation a large fire in a city, the demands of the PS actors will grow dramatically, especially if they would like to use new services like video, connections to databases to collect information about the area, and social media to alert people. In that case, the PS actors require their full spectrum and possibly even more. With spectrum sharing, the additional spectrum can be obtained if it is currently or locally unused by the commercial devices that are silent or elsewhere. For example, LSA is proposed for obtaining spectrum for rapidly deployed networks in [31].

The target spectrum bands considered are any bands that can be exploited by the PS actors, such as the bands of mobile operators and wireless camera and microphone systems. In [131], the possible frequencies are further discussed. As is natural, the

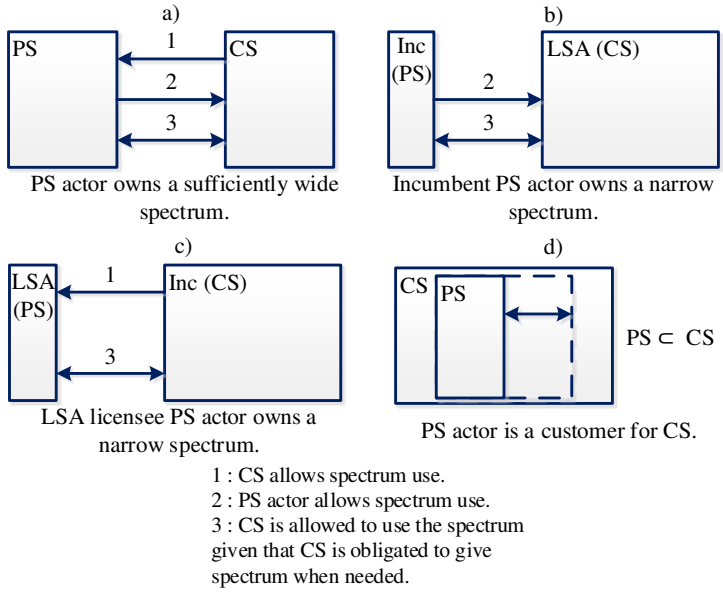

Fig. 12. There are multiple options for spectrum sharing. *Inc* is used as an abbreviation for the incumbent of the system. a) The PS actors own sufficient amount of spectrum to support all of their requirements. b) The incumbent PS actor has only the critical amount of spectrum and the CS operator has a wide spectrum. c) The PS actor is an LSA licensee of the incumbent CS operator. After the overview, this thesis concentrates more specifically on this setting where CS providers allow spectrum use to PS actors. d) The incumbent is a roaming user at the CS network.

PS actors are interested in the lower frequencies for backhaul coverage. The higher frequencies can be used in the hot spots. The exact frequencies vary, because on the European level, while the importance of harmonized allocations for public protection and disaster relief applications are widely recognized, the spectrum use is still not currently happening in a harmonized way [132, 133].

To enable spectrum sharing, the CS operators must collaborate with the PS network and equipment providers. The collaboration can be enabled with a political decision. Alternatively, the commercial operators can have monetary incentives to offer tailored and complete solutions for PS together with the rapidly deployable network equipment providers.

Fig. 12 plots different options for spectrum sharing in the means of owned spectral resources. The different options for allowing the other entity to use the spectrum are depicted with arrows. Table 1 briefly goes through the advantages and disadvantages

of different system approaches. All the approaches can be grouped as follows. First, the sharing framework is designed so that the CS operators are the LSA licensees. This way, the incumbent is always allowed to use the spectrum and the CS operators obtain additional spectrum. Second, the CS operator is incumbent, and complementary spectrum is given to the LSA licensee, such as a PS network. The third option is that all the users are using the CS network. Note that these ideas can also be used in parallel in different situations and areas.

The current state of affairs is that the PS and CS operators have their own spectrum and they do not cooperate. Therefore, to obtain functionalities similar to those of the CS users, the PS operators require an amount of spectrum equal to that of the CS operator. The first step in this setting is cooperation, as illustrated in Fig. 12 a). Naturally, sharing rules must be agreed, i.e., either one or both allow their spectrum to be used by the other one. The following sections go through the other options above for spectrum sharing in more detail for LSA systems.

3.1 Public safety system is the incumbent

This section considers options where the PS actor is the incumbent in an LSA system, e.g., as in Fig. 12 a) and b). In these options, a part of the PS spectrum has been released for CS operators under the requirement that they must allow the incumbent, i.e., the PS actors, to use that spectrum when and where needed. Obviously, this requires a political decision, but it is listed here as an opportunity. It is discussed in the United States that the CS operators and other spectrum users can share the spectrum as secondary users [13]. Moreover, in the United States, a wide bandwidth of spectrum will be released from governmental users to CSs in the upcoming years. Note that the majority of spectrum can still be used by the PS actors during critical operations.

By being the incumbent, the PS actor has all the control to support its critical and non-critical applications with a predictable quality. In this scenario, the PS actor can build its network infrastructure and the management system for organizing its network and services. However, the PS actor might not build a nationwide network for itself. Moreover, the PS actor might not use its spectrum all the time. This leads to free spectrum, which can be utilized by other applications. A possibility is to co-operate with the CS operators. The additional spectrum could be used as a complementary resource by the CS operators to unload its data traffic. There are multiple possibilities for co-operation:

Table 1. An overview of spectrum sharing system possibilities for special applications.

The PS actors own a relatively wide spectrum. See Fig. 1-a).	CS operator own the majority of the spectrum. See Fig. 1-b) and 1-c).	The PS actors utilize the CS network. CS operators have a complete system. See Fig. 1-d).
1. The incumbent PS actor allows CS operators to use all its spectrum. – In some areas, where the incumbent does not usually have activity, allowing is more or less naturally permanent. – In cities, the incumbent activity can be more frequent and allowing happens on a faster time scale. 2. The incumbent PS actor allows CS operators to use its free spectrum. – The incumbent system might not need the entire spectrum. Therefore, the remaining spectrum can be allowed to CS operators.	1. CS operators give the available spectrum to the PS actors (Fig. 1-c). 2. CS operators have the obligation to give enough spectrum to the other system using the spectrum during critical operations (Figs. 1-b and 1-c). 3. CS operators have the responsibility to give all the resources, including physical equipment, to PS actors during critical operations. Note: Some spectrum can be given for CS operators by the other system but, as a trade-off, they can be demanded to give their spectrum to the other system if needed.	1. All of the spectrum users, PS system and CS users can be roaming users of the CS network. 2. The PS actors can rent/obtain the CS network for their own use.
Pros: + The incumbent has all the control for spectrum utilization. + The incumbent has a predictable quality for its applications. + CS operators obtain additional spectrum. - No guaranteed additional resources for CS operators	Pros: + The LSA licensee obtains additional resources for its applications.	Pros: + The PS actors obtain instant coverage. + The CSs are constantly developed to satisfy the customers.
Cons: - CS users' need for devices that work using the spectrum of the incumbent.	Cons: - If CS operators are obligated to give spectrum to the other user, they cannot have guaranteed resources for themselves.	Cons: - The PS actors do not have complete control over the CS network. - The system needs a priority protocol if the incumbent users are PS actors. - There is no coverage or support for all the applications at every location. The PS actors still need their own service in the areas where the CS network cannot support it. - Security aspects

First, the PS actors can allow the CS operator to use the spectrum at predetermined times and areas. This is applicable when the possible PS spectrum usage is known in advance. This is the case, e.g., when the PS actors have scheduled their operations. In these cases, the PS actors can have the spectrum for the reserved time and area, even if they are not using it. With this method, the spectrum is free at given times and the individual PS actors do not need to worry about the CS operator transmitting at the same time. This is applicable, for example, in some of the military training scenarios and in border protection, as the military is mostly using their spectrum in known areas during peace time.

As a second option, the PS actors can allow the CS operators to use the spectrum at all the times when the spectrum is free. This option needs a rapid method for the spectrum reservation. The PS actor should preferably notify the LSA repository a few moments before the transmission, so that the spectrum can be guaranteed to be free for the PS network.[4] Another possibility is for the PS actors to notify the LSA repository when the transmission begins. In this setting, the PS actors should accept possible interference from the LSA licensee at the beginning of its transmission. Moreover, in the scenarios above, the fall-back measures to handle connection breaks for guaranteeing the possible incumbent transmission should be expeditious.

Third, the PS actors can allow the CS operators to use the spectrum at the locations where the spectrum is not currently needed by the PS actors. This option can be accomplished by tracking the PS actors and by reserving the necessary spectrum for them at their locations. This is applicable, for example, with the first responder units, whose locating is also important from the operational perspective.

Fourth, depending on the applications, the PS actors might not always need all of their frequencies. The PS actors can allow the CS operator to use the remaining free frequencies. Furthermore, the spectrum band can be divided into multiple smaller bands that can be used by the CS operator according to the need of the PS actors.

Moreover, any combination of the above is also possible. In these systems, however, the spectrum is a complementary resource for the CS operator when the PS actors are silent. To start building the system, the agreements between the incumbent PS actors and commercial LSA licensees can first be allowed in smaller areas. Then, if the CS

[4]The evacuation time of a time division LTE base station can be around 50 seconds, when it uses an LSA setup and a graceful shutdown period of 35 seconds for lowering the transmission power gradually to zero [106]. Additionally, frequency change of a frequency division duplex LTE base station takes around 26 seconds [109].

operator develops their applications in such a way that they do not cause intolerable interference to the PS operations, the agreements are easy to expand to wider areas.

The amount of additional spectrum obtained by the CS network depends on the activity of the PS network. If the PS actors are silent most of the time, the CS operators obtain the spectrum most of the time. The major benefit for the PS actors of owning the spectrum is the control. It is possible for the PS actors to freely use the spectrum for their own applications. In addition, it is always possible to decline the spectrum use of the CS network or other spectrum users.

However, the resources owned by the PS actors might still not be enough to support all the PS operations. Moreover, the PS actors might not want to reserve a wide spectrum for their applications. Therefore, it may be beneficial for the PS actors to also obtain additional resources and services from the CS network when needed.

3.2 Commercial system is the incumbent

This section gives options for a scenario where the CS operator is the incumbent in an LSA system as shown in Fig. 12 c). The CS operator has a wide spectrum and is giving spectrum resources to the PS actor, which only has a small portion of spectrum reserved, e.g., for voice communication.[5] There are multiple possibilities for cooperation, which can all be implemented in parallel depending on the PS actors' needs.

First, the resources can be shared with an LSA system. When the incumbent user comes to the area, PS actors will retreat, or change their frequency. This suits the case when the PS actors are mostly using the spectrum in the areas where the CS users or other incumbent users remain silent. This is applicable if the PS actors use spectrum mainly for non-critical applications, such as training, and have the authority to reserve the spectrum completely for itself during critical operations. This is the use case, for example, in military and border control applications, where they would require spectrum for their communication during peace time. These PS actors can agree on multiple LSA agreements with multiple incumbents to obtain multiple spectrum bands. Then they are able to legally utilize the band that is available. Moreover, PS actors being the LSA licensees provides security, i.e., the PS actors do not necessarily need to inform their location to the LSA repository, and the PS actors are not tracked for spectrum information. Another example of resource sharing like this is a high speed mobile network for the PS actors in sparsely populated training areas. These kinds of high

[5]This thesis will concentrate on this scenario when developing an LSA system for the PS network.

speed networks can also offer a backup mobile infrastructure, for example, in disaster areas and in rescue operations during electrical shortages when a commercial network of the CS is down.

Second, the CS operator can be obligated to give spectrum to the PS actors in areas that are not covered by the CS network. Thus, the PS actors can obtain spectrum for their own use, i.e., for training and for emergency use. This option is applicable in the long term only if the CS operator is not building its network in these areas, e.g., if these areas do not offer financial benefit. Otherwise, there is no long-term guarantee of interference free spectrum for the PS network.

Third, the CS operator has the obligation to give required spectrum to the PS actors during critical operations. In this scenario, the PS actors can have the rights of the incumbent during critical operation. This is a viable option when the PS actors are mainly minor users of the spectrum and critical operations rarely happen. The CS operator can build its network using a wide spectrum. Then, the spectrum is released when the PS actors come to the area and need it. This option would require a backdoor for PS actors to be installed in CS network equipment. For example, by using this type of feature, the PS actors could reserve spectrum or switch off related CS base stations with alarm signals or via central controller. In some use cases, the spectrum can also be reserved by the basis of the emergency calls, which usually happen via CS base stations and near the locations of the required PS needs.

3.3 Public safety system utilizes commercial network

One additional option in the above scenarios is the following. As shown in Fig. 12, the PS actors can be the users of the CS network. These types of radio access network sharing solutions between commercial networks and PS actors are currently considered all over the world [134, 130]. The entire spectrum is owned by the CS operator and it is responsible for building the network.

When the PS actors use the CS network, they should obtain the highest priority for their critical applications. The benefit of being a user in commercial networks is the instant coverage of the CS network in densely built areas. Another benefit is that the CS operators develop their spectrum usage to meet the current requirements better, because they are competing for users. However, the PS actors do not have full control over the network, which always reduces the security. Moreover, there are security aspects for the PS actors, and the CS network should be built robustly.

Then, a backup system for the most critical applications and communication is still needed for the PS actors to not be dependent on CS networks. This backup system should then have the possibility of using the commercial spectrum in critical scenarios. The details should be agreed with the CS.

In practice, the PS actors would have their own PS LTE base stations as a backup communication method, for example, in their vehicles. The backhaul to the working commercial networks could, for example, be formed with high gain dedicated links and with a multi-operator LTE router. Then, the PS actors should have the permission to utilize the spectrum of the commercial network for their hot spots. Note that the spectrum use of the PS backup network should preferably not interfere with the commercial networks. Thus, if there is a commercial network connection, the spectrum sharing should be centrally managed.

One additional solution to not interfere with commercial users is to offer a roaming service with a lower priority also for the commercial users via the rapidly deployed PS base stations. Then, if the commercial users hear the PS base station, they could connect to the commercial network also via it. The PS base station could, for example, offer minimum quality connections and enable emergency calls for the commercial users.

Then, if the PS actors have no connection to the commercial networks, the commercial networks are not working properly. If this is the scenario, the spectrum use should be allowed for standalone use for the PS users.

3.4 Summary

Spectrum sharing alternatives between a PS and a commercial system were discussed in this chapter, since it may be possibile to find more spectrum for both users in the future. While there are multiple choices for PS actors to utilize spectrum sharing, it is also a political decision about how the spectrum will be shared. Therefore, PS actors should be ready for every scenario. If PS actors own the spectrum, they can rent out the free spectrum to CS operators via an SAS/LSA system. Another option for providing high quality performance for PS actors is the following. Only a small portion of the spectrum is reserved for voice service to PS actors. CS networks are allowed to utilize the remaining spectrum with the condition that the CS operator is obligated to release spectrum to PS actors when needed for critical applications. For this, the chapter gave multiple options to automatically reserve CS resources for PS use. In addition, the PS actors can be roaming users at the CS network. Furthermore, PS actors can be LSA

licensees of the incumbent CS network. Note that all these options can also work in parallel. Herein, the CS network is utilized by PS actors when it is available. When the CS network is not available, PS actors can utilize their own rapidly-built network as a licensee or as an incumbent. The advantages and disadvantages of the various approaches were presented in Table 1.

The rest of the thesis considers solutions to guarantee system robustness for the PS actors when they have an LSA licence for available spectrum resources. Note that the use case, when the PS actors would be the incumbent users, does not necessarily require robustness from the PS actors' point of view. There, if the sharing system was not working, the commercial LSA licensee would simply not use the spectrum.

4 Robustness for public safety in spectrum sharing with licensed shared access

In this chapter, a more specific spectrum sharing system is planned for the PS actors when they have an LSA licence for the LSA spectrum resources. More specifically, the RP3 is answered by designing an LSA framework to be utilized in a rapidly deployable PS network. The chapter is based on the journal publication I.

The reason to use a secondary licence to obtain the spectrum for rapidly deployed PS networks is the following. The PS actors are assumed to use commercial network services for their communication as discussed in Section 3.3. Thus, the rapidly deployed PS networks should not interfere with the commercial networks. Then, the secondary spectrum licence is used in applications where commercial networks are not available, i.e., there is spectrum available. In this scenario, having the LSA licence enables the PS actors to utilize all the currently available spectrum shared with LSA without interfering with the commercial networks that might be serving other PS users.

Moreover, it can be assumed that the PS actors always have the available spectrum resources for their rapidly deployed networks for critical missions. In critical scenarios, the spectrum can be guaranteed, e.g., by temporarily changing the role to incumbent, as discussed in [35]. Another option is that the regulatory authorities allow the PS actors to have temporal transmissions with sufficient power on the commercial radio channels that are either i. sensed to have the least congestion, or ii. in the use of the locally unavailable commercial network that serves the PS users. However, the backup spectrum-use method has to be agreed to beforehand.

Nevertheless, importantly, if the PS actors utilize LSA spectrum resources, the PS actors require the sharing process to be robust against connection problems. Note that the connection to the central repository systems may be unavailable in locations where the backup networks are needed. The commercial network might not even exist in these locations. In this chapter, a robust LSA system is proposed. By robust, it is meant that the method is resilient to all kinds of connection breaks in the LSA system that may also exist in real life due to electric breaks or fibre cuts.

In the following sections, the proposed LSA system model and its functionalities are first described. This enables building the proposed system with the currently available commercial equipment. Then, the functionality of the system is validated via simulations.

More specifically, a simulation setup and numerical results for the spectrum reservation method and for the possible connection failures are presented. The simulation results are further used to study the main system design parameters and to select them properly. The results give insight to the system behaviour.

4.1 System model

This section presents a system model of an LSA system for the PS actors and the key functionalities of the system components to overcome connection breaks. The PS actors act as an LSA licensee for accessible LSA spectrum resources. Here, the network of Section 1.5 obtains spectrum with LSA as shown in Fig. 13. Note that the sharing framework negotiation also includes the rules on how to allow the spectrum for the public safety operator in critical situations. In our scenarios the private IP backhaul network is considered to be rapidly deployed, highly robust and self-configuring.

Note that this figure is different from the normal LSA system in Fig. 5. Herein, a rapidly deployed network of a PS operator is using licensed spectrum in a distributed fashion without any OAM. In other words, the PS base stations together share the available frequencies obtained from the LSA repository. Moreover, there is no central LSA controller. The functionality of it is distributed into the rapidly deployed network.

In Fig. 14, it is shown more precisely how to combine the LSA system together with a rapidly deployable LTE network. The PS actors have their own rapidly deployed LTE base stations with a private IP network as a backhaul for the data. Here, every LTE access point is connected to a light EPC solution that also works as a distributed LSA controller. Thus, no single device is solely responsible for the spectrum allocations.

Moreover, an LSA server is introduced to the system. Any LSA controller can work as the LSA server and then act as a mediator between the LSA repository and the other LSA controllers. By using a mediator, the PS network can be separated from the IP network, which provides security. Moreover, the LSA server is a single device of the PS network that needs the connection to the LSA repository. The LSA server reports only the necessary network information from the LSA licensee network to the LSA repository.

The system works as follows. The incumbent reserves the resources by connecting the LSA repository with an incumbent manager. Then, the repository sends the notification of the spectrum reservation to the LSA server. After the LSA server obtains spectrum reservation information, it forwards the information to the LSA controllers of

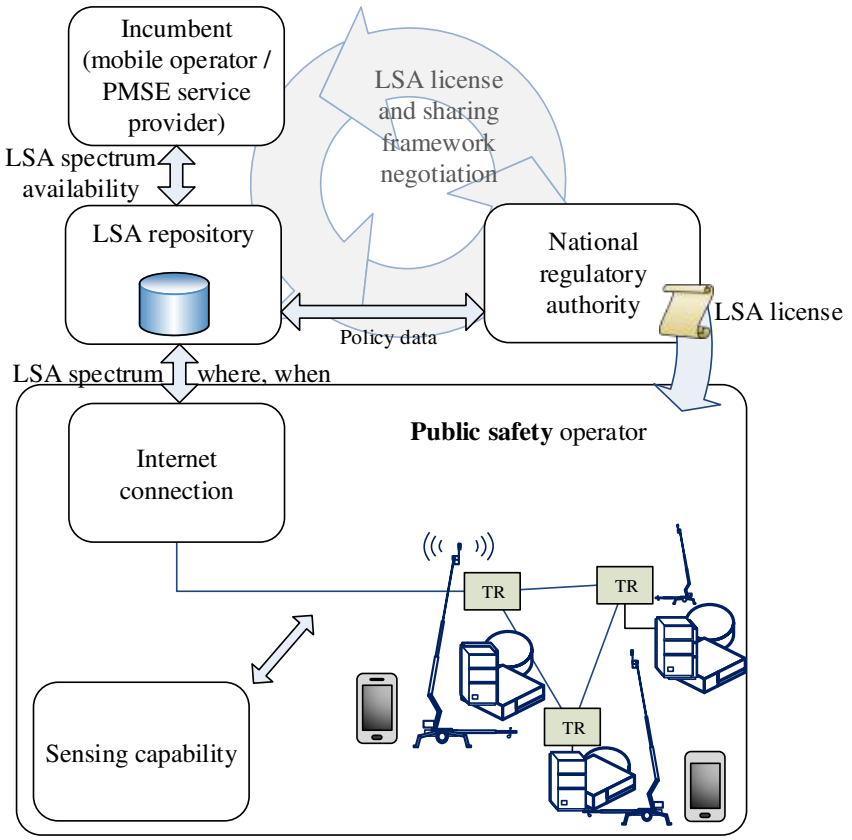

Fig. 13. The specific LSA system for a PS operator as an LSA licensee using a rapidly deployed network. The TR in this figure is a router for forming a closed PS network. Note that the sensing capability is discussed in the next chapter.

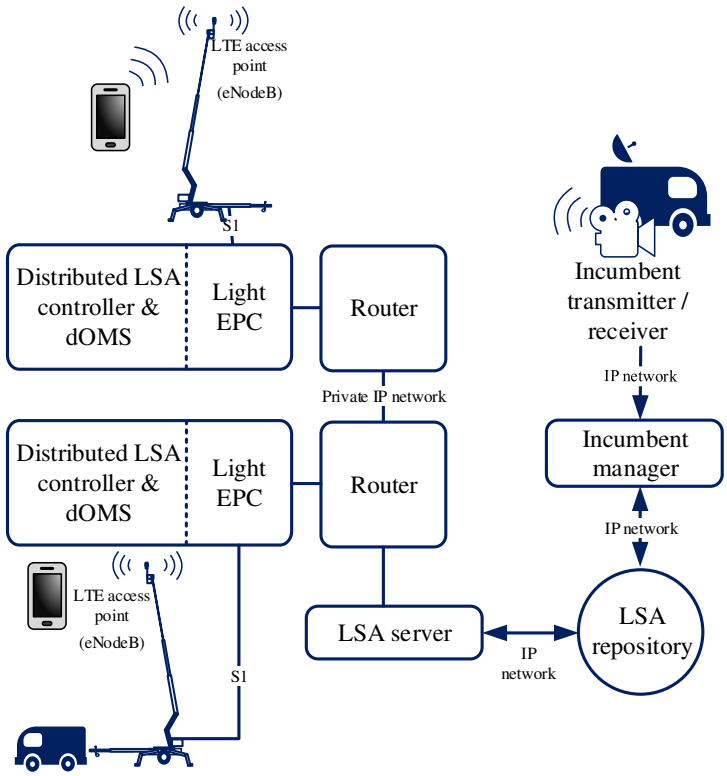

Fig. 14. Two LTE access points in an LSA licensee network.

affected base stations. Finally, the LSA controllers compute the protection criteria of the incumbent and control the spectrum usage of the base stations.

Naturally, the spectrum sharing rules for PS actors must be robust against connection breaks. Thus, in this thesis, it is proposed that the incumbent user can only reserve the spectrum for a predetermined time before its transmission, contrary to the on-demand operation mode for LSA spectrum resource reservation [25]. Then, because the incumbent transmits only after the predetermined time, the currently known spectrum information is valid for the predetermined time, even if there are short connection breaks to the LSA repository. Additionally, connection checks are introduced to the system.

The following subsections go through the main functions of the main system components in more detail, as well as the differences of the system with the LSA specifications [7, 25, 8, 26].

4.1.1 Incumbent via incumbent manager

The incumbent is the primary spectrum user. The necessary spectrum resource availability information for spectrum sharing includes the zone type, geographical areas, frequency parameters, time and other radio restriction parameters that describe how the restrictions apply [26]. The incumbent informs their spectrum use to the LSA repository for the LSA system to calculate this information. Note that according to the specifications, the actual parameters sent by the incumbent can be sent flexibly with agreed methods and accuracies to the repository, e.g., to protect the confidentiality and information sensitivity requirements of the incumbent user [8].

In this work, it is assumed that the incumbent reservation message includes the "starting" and "ending" time of the incumbent's transmission, the reserved frequencies (centre frequencies and bandwidths), the location and the base station type. This information is enough to calculate the exclusion, protection, and restriction zones [26] around the incumbent. The incumbents are assumed to inform the repository of their spectrum access using an incumbent manager over the Internet.

It is also assumed that the incumbent manager allows the incumbent to reserve the spectrum only a predetermined time beforehand. More specifically, the incumbent has to send a reservation message via the incumbent manager to the LSA repository at least a predetermined time T_i before its transmission. Recall that this gives the LSA system time to recover from short connection breaks, as the most recent spectrum information is still valid for the predetermined time. This functionality can be enabled, for example, at the incumbent manager. [6]

4.1.2 LSA repository

The LSA repository keeps a data base of up-to-date information about incumbent spectrum reservations and about the conditions for utilizing the spectrum. The LSA repository forwards information about the incumbent and its planned use of LSA spectrum resources to the LSA server when new information becomes available. The LSA repository can also reply to a request for the incumbent information. This reply includes the information that is new to the requesting device. Compared with the LSA

[6] The requirement for a reservation a predetermined time before the incumbent transmission can also be voluntary in some of the systems. Then, if the incumbent does not reserve the spectrum on time, it is obligated to possibly tolerate interference from the LSA licensee for the predetermined time, given that there are connection breaks.

specifications, all the information sent from the repository also includes the time when it is sent: a timestamp.

Connection checks to the LSA repository happen via the connectivity check request procedure [26]. The devices, which check the connection, send connectivity check requests to the LSA repository. The LSA repository replies to the connectivity check request with a connectivity check response. If there is no response, the connection is broken.

4.1.3 LSA server

The LSA server is a mediator between the LSA controllers and LSA repository. It is briefly described in the LSA specifications and called a proxy LC in the architecture examples of [7]. The basic functionality of the LSA server is to act as a single LSA controller to the LSA repository and mediate information to the LSA controllers. This method hides the complexity and the identities of rapidly deployed networks.

Any distributed LSA controller can act as an LSA server, given that it has Internet access. After obtaining incumbent information from the LSA repository, the LSA server broadcasts this information to the distributed LSA controllers. The LSA server also saves incumbent information until the information expires. In the PS LSA system, the repository information can be updated online before even going to the mission.

The LSA server sends connectivity check requests to the LSA repository between time intervals of T_{check}. The connectivity check responses are then forwarded to the LSA controllers. The LSA server notices a connection break to the LSA repository if connectivity check response signals are not received within time $T_{timeout}$ from the connectivity check request. When this kind of a connection break occurs, the LSA server sends connectivity check failure signals to the distributed LSA controllers periodically between time intervals T_{check}. These signals provide information for the LSA controllers whether the connection break is external or internal.

The LSA server tries to reconnect to the LSA repository during a connection break. The LSA server requests up-to-date incumbent information from the LSA repository connecting to it. The LSA server can also answer a request for incumbent information and replies the information that is new to the requesting device.

4.1.4 Distributed LSA controller

The LSA controllers control the spectrum utilization of the LSA licensee PS network. The LSA licensee can utilize the spectrum according to the latest unexpired information without waiting. The main task for an LSA controller is to calculate the protection zone for the incumbent using incumbent information. They obtain the incumbent information from the LSA server when it becomes available.

In this work, an LSA controller requests up-to-date incumbent information from the LSA server when connecting to the PS network. All the LSA controllers save the received incumbent information until it expires. The calculation is done similarly at every LSA controller using the same algorithms as would be done in the centralized controllers.

4.1.5 Distributed operations and management system

In addition to what is defined in the LSA standards for LTE networks [8], Fig. 14 depicts a distributed operations and management system (dOMS). The dOMS are distributed per base stations, as it is a natural way for the PS base stations to be independent. The dOMS are responsible for sharing the spectrum between the other access points and include a command tool for controlling their own base stations. They also include the necessary congruent commission plans. More specifically, each of the individual dOMS send command messages to their own base station for the frequency allocations and power levels, which are collaboratively decided with other dOMS units. The dOMS can utilize the spectrum information from an LSA system or some other spectrum information source.

The spectrum sharing between base stations is done in dOMS that keep a list of base stations in the vicinity. To share the LSA spectrum resources, the dOMS can, for example, utilize signalling methods similar to co-primary spectrum sharing [135]. The difference with regard to [135] is that the spectrum sharing is done between a single PS operator, without the need to compete with other operators. The signalling messages are sent inside the closed PS network.

The dOMS has the task to clear the spectrum before the incumbent starts using the spectrum and when the spectrum reservation information becomes invalid due to a connection break. Recall that the sending times are included in all data originating from the LSA repository. The spectrum reservation information is valid for time T_i after a

successful connectivity check response signal or after any other data received from the LSA repository.

Fig. 15 shows how the reservation method works in a timeline. In the next section, this timeline is simulated for different failure models. Let T_{empty} be the time that it takes to empty the spectrum by the base station after a command from the dOMS. If no connectivity check response signal or other data arrives from the LSA repository, the LSA spectrum resources are freed after time $T_i - T_{empty}$ from the sending time of the last successful data from the LSA repository. The spectrum can be emptied immediately or gradually by using a graceful shutdown, which gradually lowers the power level of the base stations. The dOMS can also order its base station to utilize some available backup frequency. Alternatively, any other fall-back measure [7] can be used.

4.2 Simulation setup and numerical results

This section presents the simulation setup and results for the proposed LSA system reservation method. The simulations are used to validate the method setup in the case of connection breaks inside the IP network. It is assumed that the closed PS network is built reliably. This means that there is no connection break inside the PS network. The incumbent is also assumed to utilize the LSA spectrum resources only after a successful reservation. This is a conventional method for incumbents, such as programme making and special events services, which are required to inform their spectrum utilization to a national telecommunications regulator. The connection breaks in the LSA system occur in the IP network between the LSA repository and LSA controllers. It is assumed that the base stations of PS actors with the same frequency are at a long distance from each other. It is also assumed that the base stations, which are near each other, can utilize different frequencies.

The spectrum utilization and *valid spectrum knowledge* of the LSA licensee is used to measure the performance of the LSA system. The latter measure tells the ratio of time that the spectrum reservation information is valid with respect to the total simulation time. For example, when the value of it is 0.5, the spectrum reservation information is valid for 50% of the time. Recall that the LSA licensee utilizes the free spectrum only when the spectrum knowledge is valid. Therefore, the incumbent and the LSA licensee share the LSA resources perfectly only during this time. Therefore, the amount of valid spectrum knowledge reflects the LSA system performance. It also relates directly to

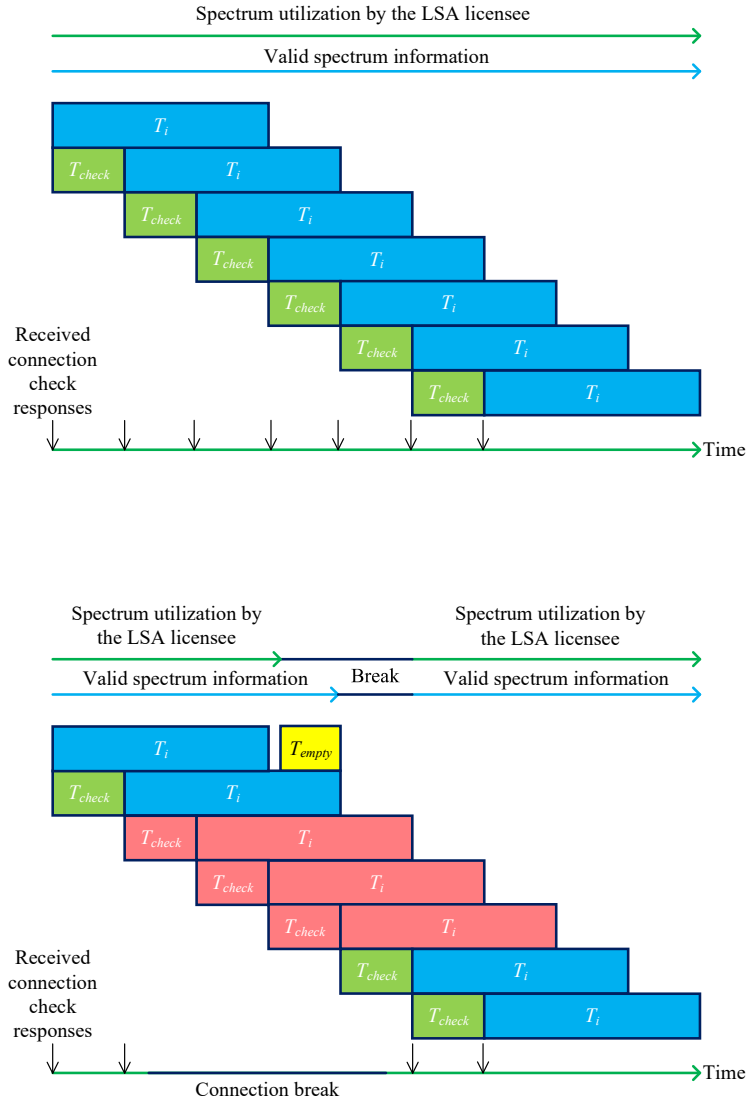

Fig. 15. A timeline of the received connectivity check responses by the LSA licensee, a connection break, the spectrum validity information and the spectrum utilization. Incumbents make their transmit announcements a time T_i before their transmission. The PS systems check the LSA repository every T_i time period. The time it takes to empty the spectrum is T_{empty}.

the reliability of the LSA system, as the spectrum can be utilized by the LSA licensee during connection breaks if the spectrum knowledge is valid.

The upcoming simulations show how the proposed LSA system design parameters, T_{check} and T_i, affect the performance in different network scenarios with different incumbent activity levels. Every scenario is simulated over 1000 iterations with different connection breaks and incumbents for average results.

The iterations for simulations are executed as follows. In every iteration for a set of parameters, the durations of the incumbent transmissions and connection breaks are drawn from Poisson distributions. The number of incumbent transmissions and connection breaks are drawn from normal distributions, where the negative values are set to zero. The starting times of incumbent user transmissions and connection breaks are uniformly distributed. The rationale for using these simplifying distributions is to obtain first-level insights into the proposed protocol behaviour when using different design parameters in different scenarios. The total simulated time is 12 hours, for which the connection breaks and incumbent transmissions are divided. The resolution scale is 1 second. The time to empty spectrum with an order from the dOMS, T_{empty}, is 30 seconds. The delay to transmit data from the LSA repository to the LSA controllers is three seconds when the connection is working.

The IP network connection breaks for different scenarios are modelled as follows. Three types of network connections are modelled. They are *reliable*, *medium* and *poor* and the parameters to simulate them are shown in Table 2. The last column, *Connection OK*, shows the quality of the connection, i.e., the ratio of time that the connection is working between the LSA repository and LSA controllers with respect to the total simulation time. These ratios are also a point of reference to *valid spectrum knowledge* in the currently available LSA systems. More specifically, in the current LSA systems, the spectrum is shared perfectly only when the connection is working. The rationale for simulating low connection reliabilities comes from the fact that the PS actors should remain functional when the commercial IP networks have serious connection problems.

Similarly, the incumbent activity is modelled for three types of incumbents. The incumbent types are *rare*, *occasional* and *active* and the parameters to simulate them are shown in Table 3. The last column, *spectrum utilization*, shows the ratio of time that the incumbent utilizes the spectrum with respect to the total simulation time.

In the next simulations, the LSA system performance is studied with respect to T_{check}. Recall that the value of T_{check} indicates the time between connectivity check

Table 2. The parameters for simulating the connection quality.

Connection quality	Mean # of connection breaks	Variance	Mean connection break duration	Connection OK
reliable	0	2	5 min	0.99
medium	7	2	20 min	0.73
poor	15	2	60 min	0.29

request signals that are sent to the LSA repository. In the figures, the markers are located at the average values for 1000 simulated iterations for the selected parameters.

In Fig. 16, the incumbent notifies 15 minutes before its transmission, i.e., $T_i = 15$ min. It can be observed from Fig. 16 that the spectrum knowledge for *reliable*, *medium* and *poor* Internet qualities are at least 99%, 73% and 29%, respectively. These are the corresponding percentages of times for the Internet connection working. Therefore, the spectrum can be utilized by the LSA licensee even during some of the connection breaks with the proposed reservation method. Moreover, it is seen from the figure that the spectrum knowledge curves are highly separated from each other for different qualities of Internet connections. This implies that the good quality of the Internet connection is important when the incumbent informs the LSA repository about its spectrum utilization on short notice.

It is also seen from Fig. 16 that the spectrum knowledge by the LSA licensee is higher when T_{check} is low, i.e., when the connection to the LSA repository is checked more often. This is because then it is more likely to get an answer from the repository for validating the connection. Therefore, with an unreliable Internet connection, the value of T_{check} should be as low as possible to have the most amount of valid spectrum knowledge. However, the figure also naturally shows that it is more important to have a good Internet connection than to make the value of T_{check} as low as possible. This makes the spectrum knowledge larger.

The simulation results of a scenario when the incumbent notifies about itself $T_i = 60$ min before its transmissions are in Fig. 17. When comparing this figure with Fig. 16, it is seen that the spectrum knowledge is overall better for every type of Internet quality

Table 3. The parameters for simulating the incumbent activity.

Incumbent activity	Mean # of transmissions	Variance	Mean transmission time	Spectrum utilization
rare	0	2	40 min	0.06
occasional	5	2	40 min	0.26
active	12	2	40 min	0.50

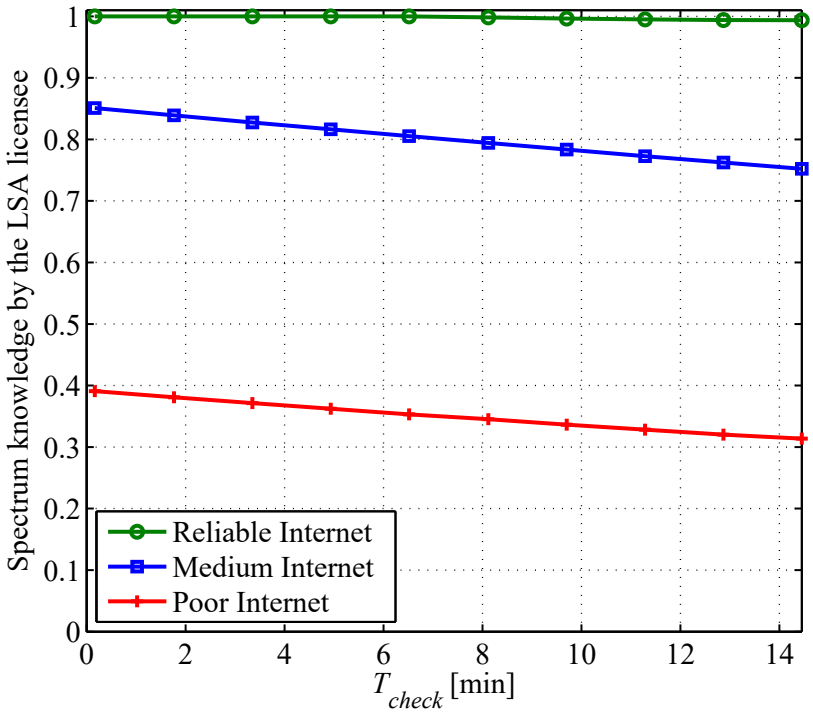

Fig. 16. The spectrum knowledge of the channel as a function of T_{check} while $T_i = 15$ min with different qualities of Internet connection. The incumbent is *rare*, i.e., utilizes the channel approximately 6% of the time.

for a greater value of T_i. It is also seen that setting T_i large is more important in terms of spectrum knowledge than to set T_{check} low. Moreover, we observe that the spectrum is known for over 50% of the time when the Internet quality is *poor*, i.e., when the Internet connection is working 29% of the time. Therefore, T_i should be large if the Internet quality is low. From Fig. 17, it is seen that the *medium* Internet quality is allowable in this setting, i.e., the spectrum can be utilized 100% of the time, when T_{check} is below 3 minutes. Therefore, given that the Internet connection to the PS network can be *medium*, the PS actors should utilize the frequencies of incumbents, which are able to report their frequencies reliably in advance. Moreover, if the Internet connection is *poor*, the PS actors require either additional methods for utilizing all the free spectrum or an incumbent that reports its spectrum utilization even earlier.

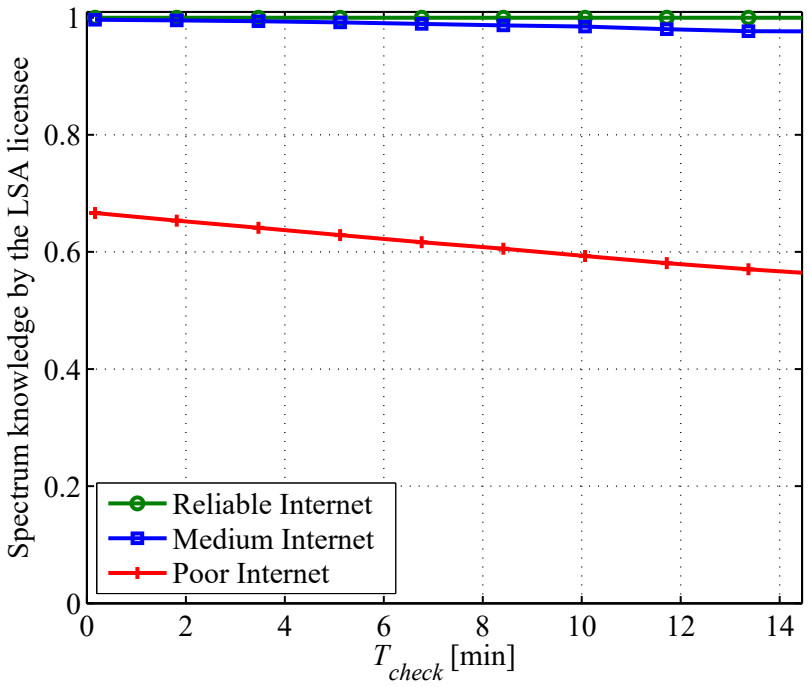

Fig. 17. The spectrum knowledge of the channel as a function of T_{check} while $T_i = 60$ min. The incumbent is *rare*.

In the next simulations, the LSA system performance is studied with respect to T_i with different types of incumbents and Internet qualities. Recall that the value of T_i indicates the predetermined time before which the incumbent is required to send its spectrum reservation to the LSA repository.

Fig. 18 plots simulated results for spectrum knowledge when the incumbent is *rare* and T_{check} is set to be 15 minutes. Fig. 18 shows a rise of the spectrum knowledge as a function of T_i. This implies that when the Internet quality is *poor*, the incumbent should reserve the spectrum as early as possible. This is applicable to incumbents that know their spectrum needs beforehand or rarely change their frequency allocations and have a static operation. An example of this kind of incumbent is an organizer of programme making and special events.

Fig. 19 shows how different activity levels of the incumbent affect the LSA system performance. The figure shows that the spectrum knowledge is higher when the incumbent is more active. This is because then the incumbent reserves the spectrum

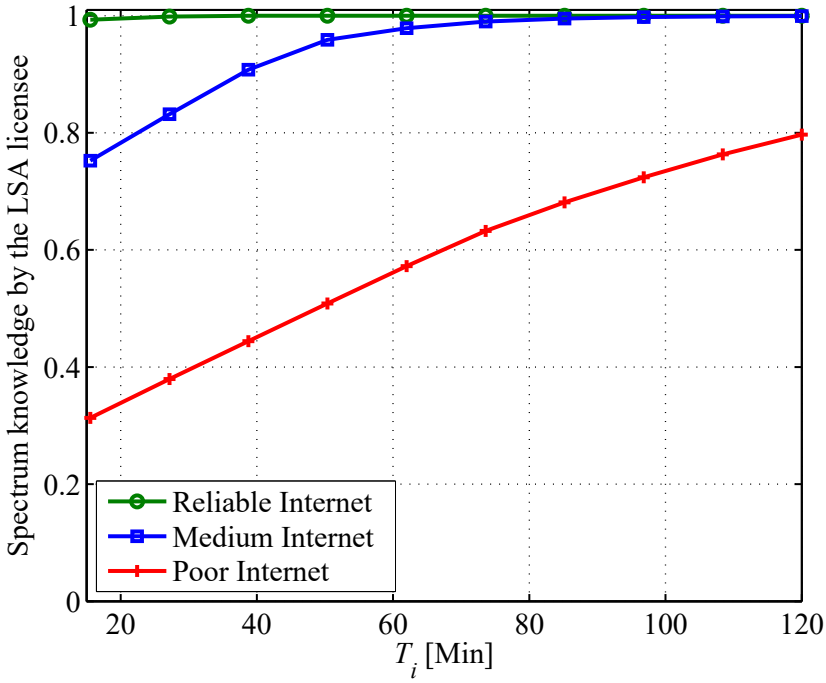

Fig. 18. The spectrum knowledge of the channel as a function of T_i while $T_{check} = 15$ min. The incumbent is *rare*.

more often, and the reservations include the spectrum knowledge. However, in practice, if the incumbent is very active, it might be hard for the incumbent applications to report the plans a predetermined time before utilizing the spectrum. Therefore, the PS actors with poor Internet connections should utilize different methods, such as sensing, to obtain the LSA resources with an active incumbent.

Fig. 20 plots the spectrum utilization of the LSA licensee. In this figure, the spectrum utilization by the LSA licensee has two measures. The first measure is the utilized spectrum resources divided by *all the resources*. The second measure is the utilized spectrum resources divided by the *available resources*, i.e., the LSA resources that are available at the times when the incumbent does not transmit. From the figure, it is seen that the LSA licensee can utilize the spectrum less often when the incumbent is more active, while the available spectrum for the LSA licensee is utilized relatively better. Therefore, as is natural, it is always preferable for the LSA licensee that the incumbent

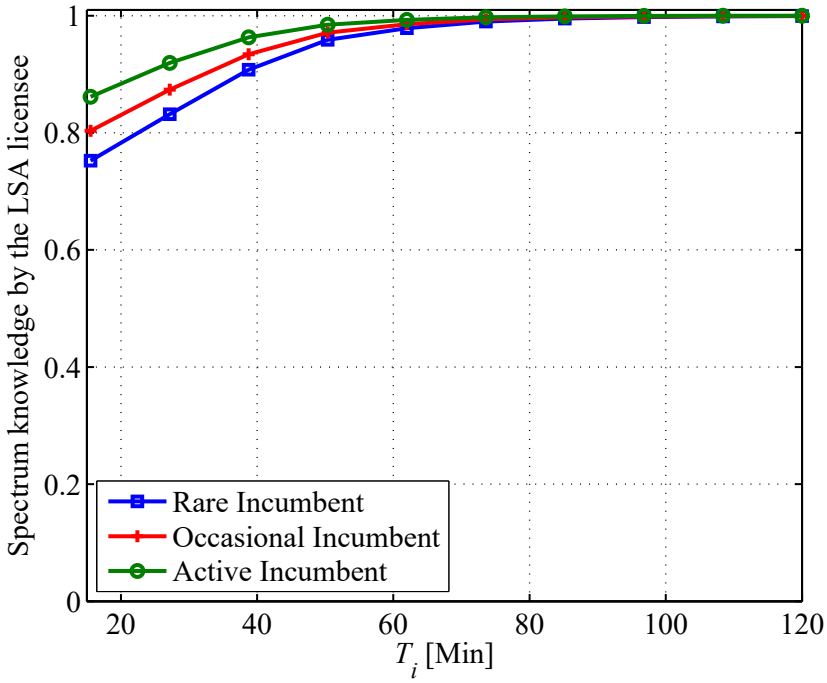

Fig. 19. The spectrum knowledge of the channel as a function of T_i while $T_{check} = 15$ min with different incumbent activity levels. The Internet connection is *medium*.

does not transmit. Moreover, the overall spectrum is utilized more effectively when there are more incumbents.

Fig. 21 shows the spectrum utilization of the complete LSA system. This is the utilization of the spectrum by either the LSA licensee or the incumbent. The figure plots the utilized spectrum resources divided by the total spectrum resources. It is seen that the spectrum utilization is in line with the spectrum knowledge by the LSA licensee shown in Fig. 19. The spectrum is utilized approximately 100% of the time when T_i is over 80 minutes. It is seen that the proposed LSA system with a *medium* Internet connection to the LSA licensee is fully applicable for sharing the spectrum with incumbents, such as mobile operators, if they reliably estimate their spectrum needs 80 minutes beforehand.

Fig. 22 plots the utilized spectrum resources divided by the total spectrum resources for different values of T_{check} with an *occasional* incumbent and a *medium* Internet. Note that the value of T_{check} affects only the spectrum utilization of the LSA licensee. It can be seen from the results in Fig. 22 that the LSA licensee receives more resources with

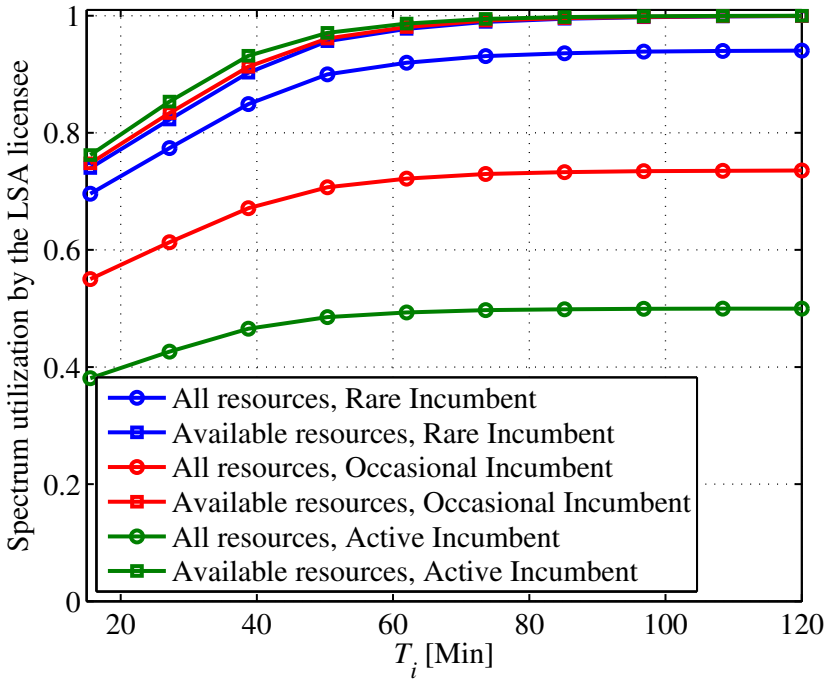

Fig. 20. LSA resource utilization by the LSA licensee as a function of T_i while $T_{check} = 15$ min. The Internet connection is *medium*.

smaller values of T_{check}. This is because the LSA licensee has a greater amount of valid spectrum information when it checks the connection more often. However, the amount of valid spectrum information does not grow significantly when T_{check} becomes smaller than 15 seconds. From the figure, it is also seen that the valid information does not vary significantly for different values of T_{check} if T_i is over 80 minutes. Therefore, the value of T_{check} can be set adaptively according to the value of T_i, i.e., according to the predetermined time before which the incumbent sends its spectrum reservation to the LSA repository.

The results in Figs. 16 - 22 show that the proposed LSA system can increase the spectrum knowledge for the LSA licensee in unreliable channel scenarios. The spectrum information can even be instant, even with connection breaks, given that the time parameters are adjusted properly. The key is to require that the incumbent reserve the channel a sufficient amount of time beforehand. However, if the incumbent requires the spectrum on short notice, the backhaul connection needs to be as reliable as possible for

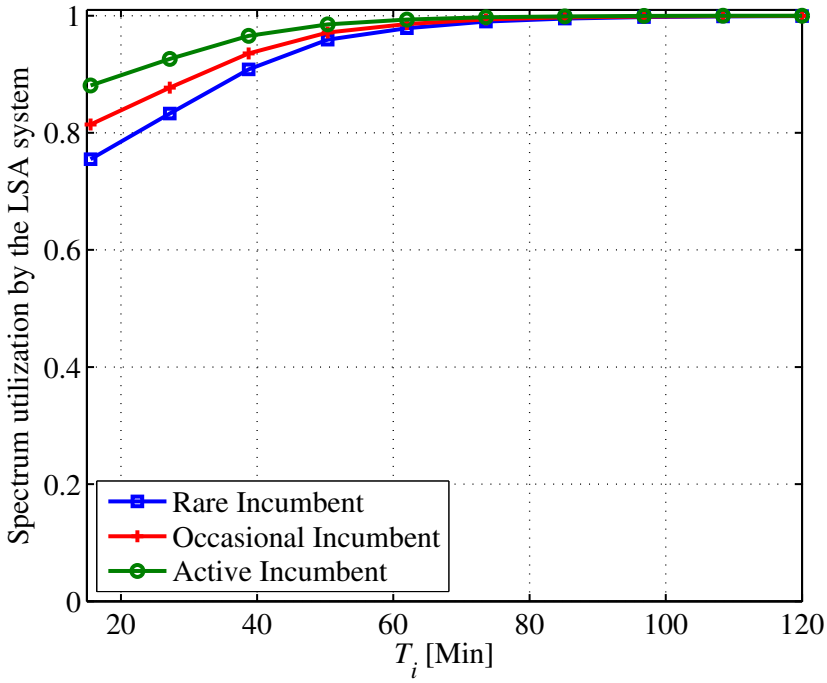

Fig. 21. LSA resource utilization by the LSA system as a function of T_i while $T_{check} = 15$ min. The Internet connection is *medium*.

the LSA system to be efficient. Moreover, the connection, if available, should then be checked as frequently as possible.

4.3 Summary

In this chapter, a specific LSA system was developed for robustness to overcome short-term connection breaks. In this system, the PS actors are the LSA licensee and the commercial system operator is the incumbent, which enables the PS actors to utilize the available spectrum resources. In this system, the incumbent, which is the primary spectrum user, reserves the spectrum a predetermined time beforehand and is not transmitting during this predetermined time. The LSA licensee, which is the secondary spectrum user, can utilize the spectrum according to its latest information without waiting. The reservation system was validated, and it was studied how to select suitable durations for the predetermined times and for time intervals between connection

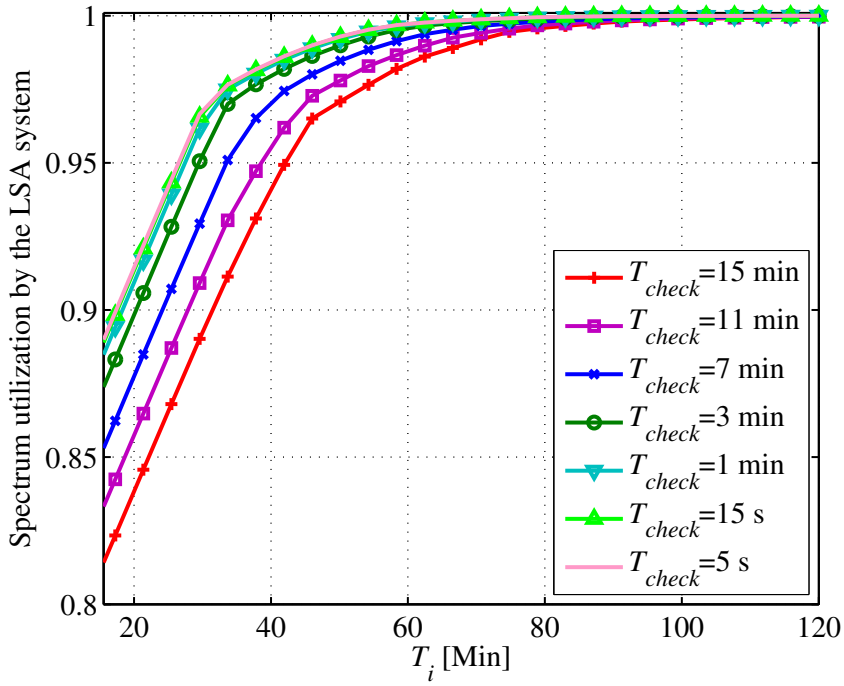

Fig. 22. LSA spectrum resource utilization as a function of T_i with an *occasional* incumbent. The Internet connection is *medium*.

checks. The time intervals between connection checks can be selected adaptively based on the network quality and on the time before which the incumbent sends its spectrum reservations. The simulations show that the proposed system can reduce the impact of possible connection breaks inside the LSA system. The values of the predetermined times must be agreed in the sharing framework negotiations where the mobile operator and the incumbent agree on all the specific policies and rules for the shared spectrum use. For example, the incumbent could be required to inform its spectrum use a day before the intended spectrum use. This would then guarantee the PS operators long enough time for most of their operations even without the constant connection to the spectrum repository.

However, this method is not sufficient alone for utilizing all the LSA spectrum resources during all connection breaks. There might be a long connection break and no possibility for an Internet connection. In addition, the incumbent might not always have an Internet connection but might still be allowed to utilize the spectrum. Therefore, if

the PS actors act as an LSA licensee and require available LSA spectrum resources, they need to develop other methods in order to guarantee their own error-free transmission and incumbent protection. This can be done with sensing.

5 Spectrum sensing for rapidly deployable network

In this chapter, sensing of primary, i.e. incumbent, LTE base stations are studied together with an LSA system. Chapter 5 answers the RP4 and RP5 and is based on the journal publication II. To answer the RP4, energy detectors, described in Section 1.3.1, are used in forming backup spectrum information for a rapidly deployed PS LTE network. Herein, energy detectors are first studied from the viewpoint of reliable detection distances. The detection distances are determined for incumbent LTE base stations with different transmit powers using the extended Hata attenuation model [102] while also considering noise uncertainty. The energy detection is considered, as it can also be used to detect other incumbent types, such as wireless cameras and microphones. The results show scenarios in a rural attenuation model where a single energy detector can be reliably used to detect incumbent base stations from far enough to guarantee the required separation for a similar secondary base station.

Then, to answer the RP5, methods are developed for using binary detection results in conjunction with an LSA system. The developed methods are specifically intended for incumbent protection and for finding available spectrum together with LSA. Also note that the sensor utilization methods developed are applicable to other sensing methods such as feature detectors for LTE synchronization signals. Herein, this chapter introduces a sensor manager application for PS actors to utilize the available sensors and communicate the gathered information to the PS network. The information provided by the sensor manager can then be utilized as a source for regional spectrum information at the location of the PS network.

5.1 System model and a description of the detection problem

The system is a part of a closed PS LTE network for which sensing provides additional and backup spectrum information. Fig. 23 presents the network components and their connections. The left side of the figure is the considered deployable network. It is used for communication in use cases when the commercial network might be unavailable or

is drastically limited. The LTE access points are assumed to use frequency division duplex.[7]

The PS actors require knowledge of the applicable spectrum in the area for their LTE base stations. The LSA repository offers available spectrum information for the LTE access points via an Internet Protocol (IP) network connection as discussed in Section 2.1. Compared with the earlier system model in Fig. 14, the deployable network is practically the same, except that now there are radio heads for sensing the channel. The sensing radio heads provide additional spectrum information and are controlled with a sensor manager application.

The distributed LSA controllers use the channel information from the repository and from the radio heads for controlling the used carrier frequency of the LTE access points. If the IP connection is unavailable and channel information is not valid, the channel is sensed with radio heads.

The secondary spectrum users require knowing the incumbent-free areas so that they can use the spectrum. In order to analyze incumbent-free areas, detection distances between a sensor and LTE access points in operative conditions must be defined. These distances depend on the specific sensing method, on transmitted signal type and power, on antenna heights and gains, on signal attenuation with or without shadowing and on random noise. The next subsections define the detection distances of frequency division duplex LTE base stations with an energy detector (see Section 1.3.1) using a rather realistic extended Hata attenuation model. This is all done in order to analyze incumbent-free areas.

5.1.1 Attenuation model

The considered attenuation model is the extended Hata model, recommended by the International Telecommunications Union for simulating outdoor-outdoor path loss calculations in the frequency range 30 MHz to 3000 MHz. This model is an empirical formulation developed from an extensive number of channel measurements. The extended Hata median attenuation includes the curvature of the earth. [102]

The extended Hata model has multiple subcases for different environments. The considered subcase is an open rural environment and frequencies considered are between

[7]The LTE base stations are also specified to use time division duplex [136, 137].These base stations send special subframes with pilot time slots [138]. Their detection is intended to be done with feature detectors and signal correlation methods [51] rather than energy detection.

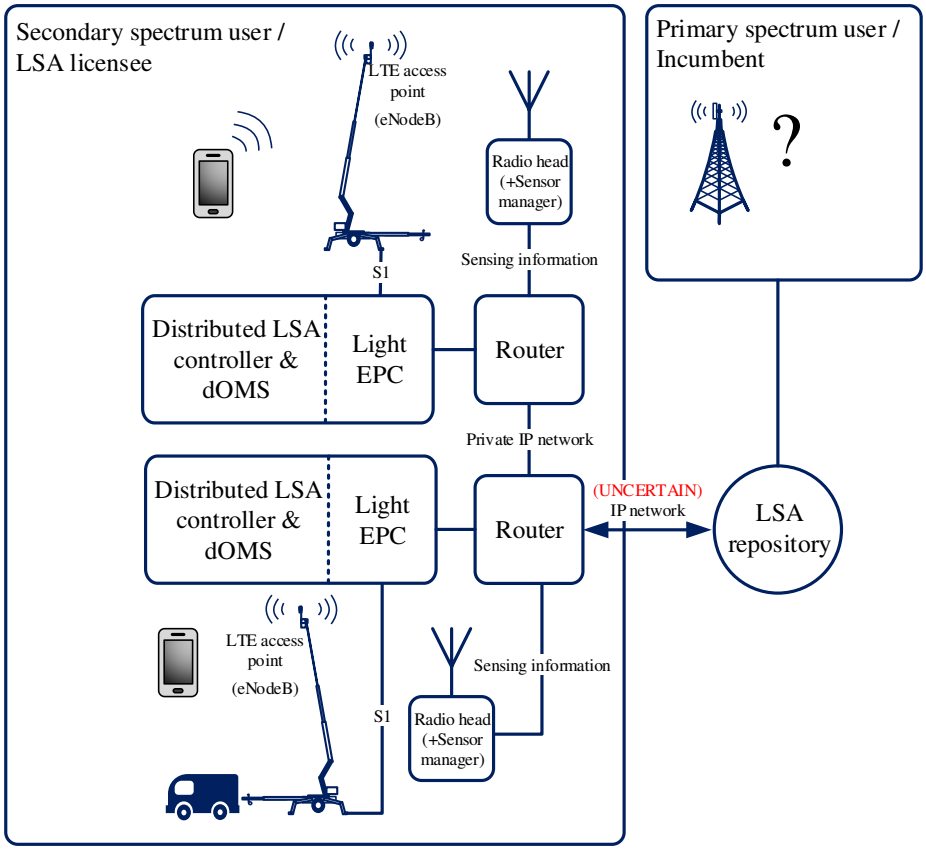

Fig. 23. LTE access points with radio heads for sensing in an LSA licensee network ([105] ©2018 Springer).

2000 MHz and 3000 MHz. Moreover, the distances are assumed to be between 0.1 km and 100 km, and both or at least one antenna is above roofs. This is the general use case, e.g., when using downlink LTE frequency band 7 between 2620 - 2690 MHz and a PS deployable LTE network. The propagation loss for the extended Hata model [102] is

$$L_{\text{hata}}^{\text{open}}(f,H_m,H_b,d) = L_{\text{m}}^{\text{open}}(f,H_m,H_b,d) + T(G(\sigma_{\text{hata}})), \tag{5}$$

where $T(G(\sigma_{\text{hata}}))$ is the slow fading distribution with a standard deviation of σ_{hata}. It gives the attenuation value in dB in the case of random obstacles in the environment. Loss $L_{\text{m}}^{\text{open}}(f,H_m,H_b,d)$ is the median propagation loss for the particular subcase in dB. The parameters for the propagation loss are the centre frequency f [MHz], the antenna height of the lower antenna H_m [m], the antenna height of the higher antenna H_b [m] and the distance between the receiver and the transmitter d [km]. The variable part of the slow fading distribution $T(G(\sigma_{\text{hata}}))$ in (5) is normally distributed in decibel values. The standard deviation for the normal distribution with respect to distance 0.1 km $\leq d$ is

$$\sigma_{\text{hata}} = \begin{cases} 12 \text{ dB}, & 0.1 \text{ km} \leq d \leq 0.2 \text{ km} \\ 12 + \frac{9-12}{0.6-0.2}(d-0.2) \text{ dB}, & 0.2 \text{ km} < d \leq 0.6 \text{ km} \\ 9 \text{ dB}, & 0.6 \text{ km} < d. \end{cases} \tag{6}$$

The median propagation loss for the open rural environment in dB is

$$\begin{aligned} L_{\text{m}}^{\text{open}}(f,H_m,H_b,d) &= L_{\text{m}}^{\text{urban}}(f,H_m,H_b,d) \\ &\quad - 4.78[\log_{10}(2000) + 18.33]\log_{10}(2000) - 40.94, \end{aligned} \tag{7}$$

while the median propagation loss for an urban environment in dB is

$$\begin{aligned} L_{\text{m}}^{\text{urban}}(f,H_m,H_b,d) &= 46.3 + 33.9\log_{10}(2000) \\ &\quad + 10\log_{10}(\frac{f}{2000}) - 13.82\log_{10}(\max\{30,H_b\}) + [44.9 \\ &\quad - 6.55\log_{10}(\max\{30,H_b\})]\log(d)^{\alpha} - a(H_m) - b(H_b), \end{aligned} \tag{8}$$

with $\alpha = 1$ for $d \leq 20$ km and

$$\begin{aligned} \alpha &= 1 + (0.14 + 1.87 \times 10^{-4} f + 1.07 \times 10^{-3} H_b) \\ &\quad \times (\log_{10}(\frac{d}{20}))^{0.8} \end{aligned} \tag{9}$$

otherwise. Moreover, the antenna height gains in dB are

$$\begin{aligned} a(H_m) &= (1.1\log_{10}(f) - 0.7)\min\{10, H_m\} \\ &\quad - (1.56\log_{10}(f) - 0.8) + \max\{0, 20\log_{10}(H_m/10)\} \end{aligned} \tag{10}$$

and

$$b(H_b) = min\{0, 20\log_{10}(\frac{H_b}{30})\}. \tag{11}$$

The received signal power at the sensor in dBm is

$$p_r = p_t + G_t + G_r - L_{\text{hata}}^{\text{open}}(f, H_m, H_b, d), \tag{12}$$

where p_t [dBm], G_t [dBi], G_r [dBi], and $L_{\text{hata}}^{\text{open}}(f, H_m, H_b, d)$ are the transmission power, the transmit antenna gain (including feeder loss and antenna directivity loss), the receive antenna gain and the propagation loss [dB], respectively.

5.1.2 The noise with noise uncertainty

The nominal thermal noise power at the receiver in dBm is

$$N_{\text{dBm}} = 10\log_{10}(1.38 \times 290 \times 10^{-20}) + 10\log_{10}(B_r) + \text{NF}, \tag{13}$$

where B_r [Hz] and NF [dB] are the receiver bandwidth and the noise figure, respectively. The noise uncertainty corresponds to the lack of knowledge of the exact noise power [103]. It has been estimated to have magnitude of 0.7 dB - 1 dB with 20 Kelvin thermal variation and with additional calibration errors [139]. The noise uncertainty is important to consider, because the amount of thermal noise can either increase or decrease the received signal power and thus increase, or decrease, the detection probability of an energy detector. This is especially true at a low SNR when using small detection thresholds. The noise uncertainty can therefore affect the detection distance.

The distributional thermal noise power with noise uncertainty seen at the receiver can be summarized to be in an interval [103]

$$\sigma^2 \in [\frac{1}{\rho}\sigma_n^2, \rho\sigma_n^2], \tag{14}$$

where σ_n^2 is the nominal noise power (13) in Watts and $\rho \geq 1$ is a parameter quantifying the noise uncertainty. The noise uncertainty is $x = 10\log_{10}(\rho)$ in dB scale, i.e., the thermal noise power in dBm can be summarized to be in an interval $\sigma^2_{\text{dBm}} \in [N_{\text{dBm}} - x, N_{\text{dBm}} + x]$.

5.1.3 Attenuation variability and detection distances

In this subsection, the definitions of the used detection distances with the extended Hata model are introduced. These distances are depicted in Fig. 3. Recall that a distance d_{t} denotes the radius within which the detected LTE transmitter is with a high probability. A detected active transmitter is most probably closer to the sensor than this maximum detection distance. Moreover, a distance d_{f} denotes the radius that is likely free of transmitters, given that there is no detection. This distance can be described as the maximum reliable detection distance. Note that the shadowing has a major effect on these distances.

Next, it is described how the shadowing affects the detection distances. Recall that the probability of detection depends on transmitted signal power, on signal attenuation and on random noise. The transmitted signal can be expected to attenuate in distance according to the extended Hata model. The amount of shadowing varies because there might be a line of sight connection to the transmitter, or there might be buildings and trees in front of the transmitter. Therefore, a detected active transmitter might be far from the sensor when there is a line of sight connection. Moreover, an undetected active transmitter can be close to the sensor when the signal experiences a deep fade.

In the extended Hata model, the amount of shadowing in decibels is randomly drawn from a normal distribution with a standard deviation (6). Therefore, the model can by change give unrealistically large or small values for shadowing. The effect of shadowing can be approximated to be within sensible limits by cutting the long tails of lognormal shadowing. This can be done as follows. Note that the variable part of shadowing $T(G(\sigma_{\text{hata}}))$ in (5) is normally distributed with a standard deviation of σ_{hata}. Thus, inverse of Gauss error function [76] $\text{erf}^{-1}(\cdot)$ can be multiplied with $\sigma_{\text{hata}}\sqrt{(2)}$ to obtain

$$D(p) = \pm\sigma_{\text{hata}}\sqrt{2}\text{erf}^{-1}(p), \tag{15}$$

which gives both constructive and destructive decibel tail values for a parameter p. More specifically, the random draws of shadowing in the extended Hata model $T(G(\sigma_{\text{hata}}))$ fall between $[-|D(p)|, |D(p)|]$ dB in part of p draws with $0 < p < 1$.

Distance d_{t} is defined to be the distance for which an active transmitter has a detection probability $P_D = 0.1$ when $-|D(p)|$ dB of constructive shadowing is present. Then, if there is a detection, the detected transmitter is considered to be within this distance from the sensor, i.e., closer to the sensor than this.[8]

In order to evaluate the worst case, i.e., maximum detection distance d_{t}, maximum noise uncertainty is considered, as it also increases the detection probability by increasing the detected power and therefore also the possible detection distance. To determine distance d_{t}, the value of $T(G(\sigma_{\text{hata}})) = -|D(p)|$ is substituted into propagation loss (5), which is then directly used in calculating the received signal power with (12). Then, with these modifications, distance d_{t} is the value of d for which the predefined probability of detection (3) holds when using received power (12) as signal strength and noise $\sigma^2 = \rho\sigma_n^2$ from (14).

Distance d_{f} is defined to be the distance for which an active transmitter has a detection probability $P_D = 0.99$ when $|D(p)|$ dB of destructive shadowing is present. Then, if there is no detection, this is the distance that is considered free of transmitters.

In order to evaluate the worst case, i.e., minimum detection distance d_{f}, minimum noise uncertainty is considered, as it also decreases the detection probability by decreasing the detected power and therefore also the detection distance. To determine distance d_{f}, the value of $T(G(\sigma_{\text{hata}})) = |D(p)|$ is substituted into propagation loss (5), which is then directly used in calculating the received signal power with (12). Then, with these modifications, distance d_{f} is the value of d for which the predefined probability of detection (3) holds when using received power (12) as signal strength and noise with minimum noise uncertainty $\frac{1}{\rho}\sigma_n^2$ from (14).

[8]The detection distance is defined this way and the probability, P_D, is set to 0.1, because now the value of p can be used alone as a single variable for limiting the effect of shadowing. Distance d_{t} could also very well be defined in other ways. An example is to consider the probability of detection with a mean propagation loss. However, this type of definition would not consider the shadowing, which is a real phenomenon that needs to be taken into account. Now, the detection probability P_D is less than 0.1 for a transmitter at a distance d_{t} in $\frac{p}{2} + 0.5$ of the possible shadowing channels.

5.2 Simulation setup and numerical results

In this section, the energy detection model and simulations in the extended Hata attenuation model are used to gain more insight into the energy detection distances in LTE networks. First, the energy detection model is studied under noise uncertainty. Then, simulations are used to determine the distances from which the energy detector can detect an incumbent spectrum user and the transmitter-free distances given that there is no detection. These distances are illustrated for LTE base stations that have different transmit powers and antenna heights.

The first aim for the simulations and numerical results is to gain more insight into the energy detection of LTE networks with noise uncertainty. The second aim is to validate the performance of energy detection for applicable scenarios for the closed PS LTE network system. If energy detectors are used, the resulting information can then be directly utilized together with an LSA system as shown in the subsequent section.

5.2.1 Energy detection performance under noise uncertainty simulations

Next, the energy detection performance is simulated with respect to SNR while considering the noise uncertainty. The number of energy samples per measurement, N, is 25 in this subsection, similar to the energy detection performance example in [48]. The effect that different N values have is examined in the following subsection. The detection performance of the energy detector is shown in Figs. 24, 25, and 26 for noise uncertainties 0.1 dB, 0.5 dB, and 1 dB, respectively.

In these figures, detection probabilities are shown for three different detection thresholds, γ, with respect to signal-to-noise ratio when noise uncertainty is also considered. The detection probabilities are seen as areas, as their exact values are unknown because of the noise uncertainty. The areas can overlap. Here, the upper limits of the areas in the figures are obtained from (3) with maximum noise uncertainty $\sigma^2 = \rho\sigma_n^2$. Moreover, the lower limits of the areas are obtained with minimum noise uncertainty $\sigma^2 = \frac{1}{\rho}\sigma_n^2$. The value of γ is bounded so that the maximum probability of false detection, P_{FA}, becomes either $10^{-3}, 10^{-2}$, or 10^{-1}.

Mathematically, the detection threshold γ is obtained from (2) by inverting it as follows

$$\gamma = 2\sigma^2\Gamma_{\text{up}}^{-1}(N/2, P_{FA}), \tag{16}$$

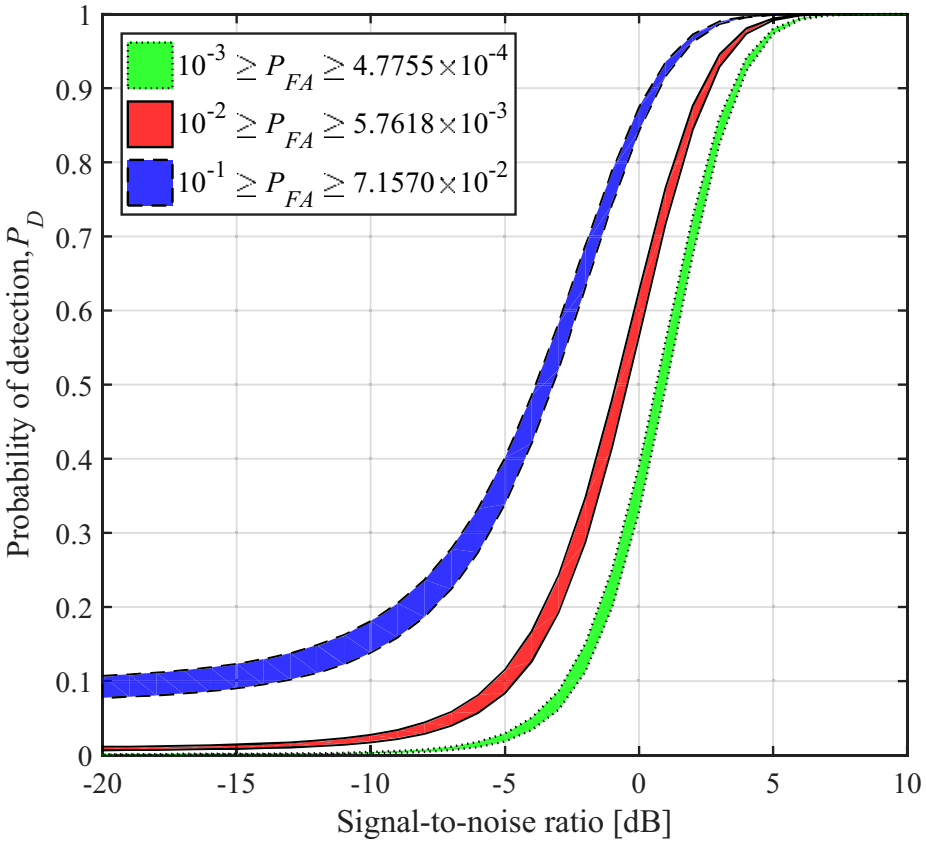

Fig. 24. Probability of detection with respect to nominal SNR with ±0.1 dB noise uncertainty.

where σ^2 is the maximum value of noise in (14) and $\Gamma_{\text{up}}^{-1}(\cdot,\cdot)$ denotes the inverse upper incomplete gamma function [76]. By using these values of γ, the upper limits of the P_{FA} areas in the following figures are obtained from (3) with maximum noise uncertainty $\sigma^2 = \rho\sigma_n^2$ and the lower limits of the areas with minimum noise uncertainty $\sigma^2 = \frac{1}{\rho}\sigma_n^2$.

In Figs. 24, 25, and 26, three differently-bordered areas depict the detection performance with respect to SNR with different detection thresholds. The figures show the overall behaviour of energy detectors with noise uncertainty. The widths of the areas show the effect of the noise uncertainty. From the figures, it is seen that when the noise uncertainty becomes larger at low signal-to-noise ratios, the detection probability obtains values from a wider region, i.e., the median detection probability is not exactly known for a certain SNR. Moreover, in Fig. 26, all the areas of probability of detection

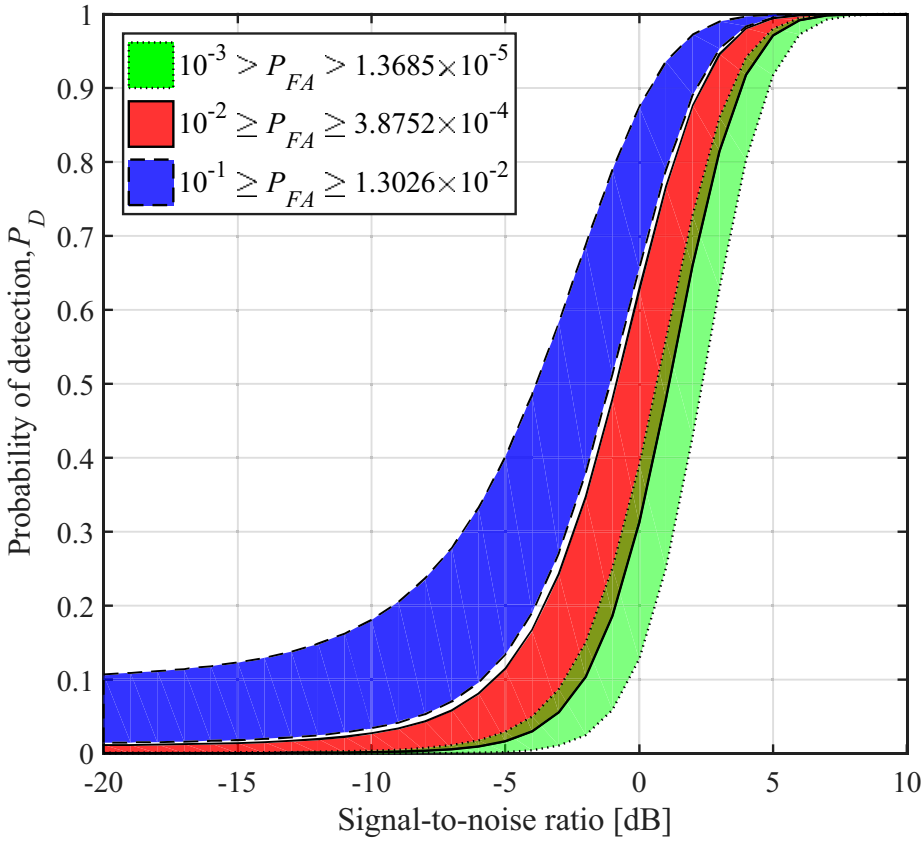

Fig. 25. Probability of detection with respect to nominal SNR with ±0.5 dB noise uncertainty.

overlap. Therefore, the detection probability can be the same for a particular SNR value, when P_{FA} is planned to be at maximum 0.1 or 0.001.

From Figs. 24 - 26, it is seen that the uncertainty directly affects to the detection and false detection probabilities. Thus the energy threshold selection cannot be directly used for designing a detector with certain false and detection probabilities with respect to a certain low SNR. However, in practice, detection can still occur at low SNR. In this setting, the overall detection design needs to consider the noise uncertainty. One approach is to estimate the noise with a training phase and by bounding the false detection probability while obtaining the best possible detection probability. This approach is called constant false alarm rate detector [48]. Another approach, for example, is to bound the distances within which the detected or undetected transmitters are, given

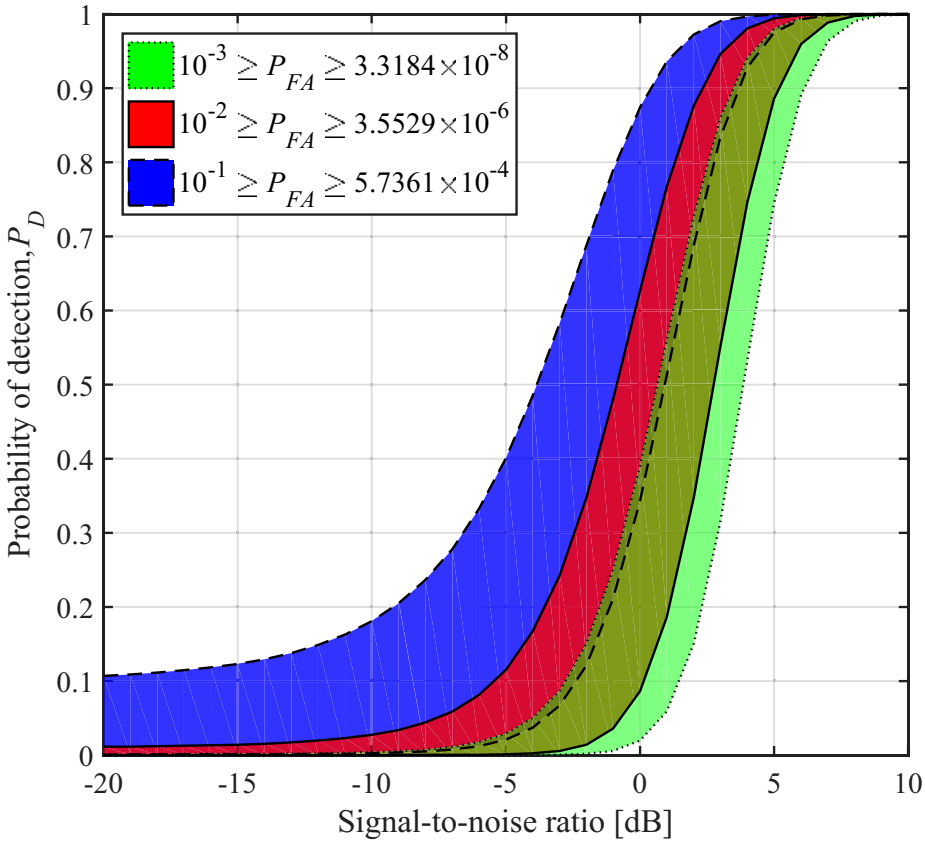

Fig. 26. Probability of detection with respect to nominal SNR with ±1 dB noise uncertainty.

that there might be noise uncertainty. This is the topic of the simulations in the next subsection.

5.2.2 Attenuation simulations

In this section, the detection probability bounds and the detection distances are found out individually for different incumbents that have different transmission parameters. More specifically, simulations are presented of detecting a macro as well as an outdoor and an indoor pico LTE access point by using an energy detector. It is assumed that another LTE access point is used as a sensor, as they are specified to sense the channels [140]. Therefore, typical values of $f = 2655$ MHz, NF $= 5$ dB are assumed. Then, the noise uncertainty x is at maximum 1 dB [139]. Moreover, without loss of generality,

Table 4. The parameters of different types of base stations.

Incumbent type	p_t	G_t	d_{inc}	Base station height
Macro	43 dBm	15 dBi	4.33 km	50 m
Outdoor pico	37 dBm	4.5 dBi	1 km	35 m
Indoor pico	22 dBm	0 dBi	250 m	17 m

the incumbent base station bandwidth is considered to be 5 MHz within which the sensed bandwidth is chosen to be a single narrowband channel of $B_r = 200$ kHz [141] with an antenna gain of $G_r = 6$ dBi. The incumbent maximum transmitted power is assumed to be uniformly distributed over the base station bandwidth and the underlying resource blocks as done in frequency division duplex LTE base stations. Moreover, the incumbent signal is assumed to be a continuous transmission by the base station. From now on, unless otherwise stated, the probability of false alarm P_{FA} is 10^{-3} when the noise has maximum noise uncertainty 1 dB. The antenna height of the sensor is 4 m unless otherwise stated. The rest of the simulation parameters are shown in Table 4. Distance d_{inc} is a reference value for the incumbent LTE cell radius. For a macro base station, d_{inc} can be evaluated from [142]. For pico base stations, the values for d_{inc} are evaluations from our trials done with a rapidly deployed LTE network [109]. The value of d_{inc} is here as a parameter with which the sensing distance can be compared.

Note that the median SNR falls between 0-5 dB for each base station in Table 4 at their respective distances d_{inc}, when their propagation loss is simulated with the rural extended Hata model (7) and by using NF = 7 dB and antenna height H_m = 2 m. This is just enough for having an LTE connection [143].

First, the detection probability of an outdoor pico LTE base station is studied. Fig. 27 plots its detection probability for a median path loss with a different number of samples N as a function of the transmitter distance. The figure gives insight into the average sensor performance. In this figure, the detection probability is again shown as an area, because the exact probability is unknown, as the noise obtains unknown values with noise uncertainty $\sigma^2 \in [\frac{1}{\rho}\sigma_n^2, \rho\sigma_n^2]$.

As expected, the detection is more probable with a high number of samples for longer distances. From Fig. 27, it is also noticed that the area for possible detection probability is wider with $N = 200$ than with a smaller number of samples. Note that the uncertainty of detection probability is caused by $N = 200$ summation of the unknown noise uncertainty. This is known as the "SNR wall" phenomenon [103] with increasing number of samples at low SNR. It prevents reliably knowing the detection probability with higher distances.

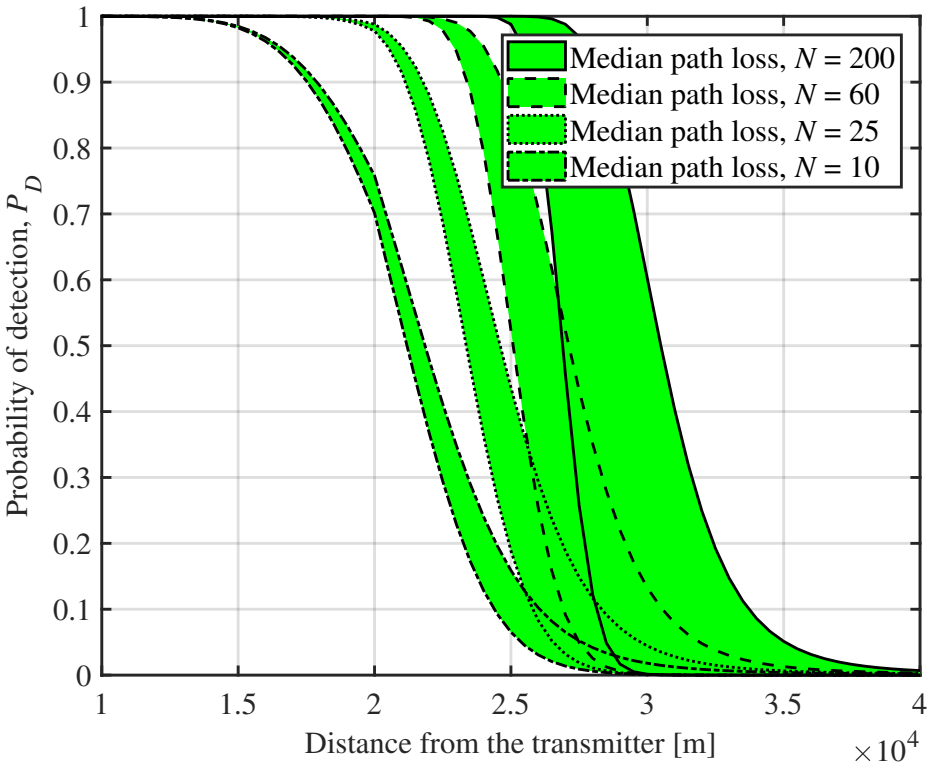

Fig. 27. Median detection probability of a 5 W macro base station with ± 1 dB noise uncertainty. The radio horizons are at 8.2 km and at 24.4 km for the sensor and for the base station, respectively.

However, while the exact detection probability is unknown, it is also seen from Fig. 27 that it is possible to map the distance for which the median detection probability is, for example at least 0.9 or at most 0.1. Here, the median detection probability can be bounded for a known distance between the sensor and the incumbent transmitter. Furthermore, a sensor network can be planned to satisfy at least a certain median detection probability for the required area by selecting a proper distance between the sensors.

The following simulations consider the effect of shadowing. Figs. 28 - 33 show the probability of detection of a macro, an outdoor pico, and an indoor pico base station as a function of the distance of the transmitter. The number of energy samples per measurement, N, is 60.

The shadowing is simulated for independent location points as follows. The simulated points (shown as "+"-markers) in Figs. 28 - 33 are values of detection

probability in (3) for the corresponding distances with received power (12). Furthermore, the received power (12) includes a normally distributed variable part $T(G(\sigma_{\text{hata}}))$ with deviation (6) for random slow fading that is independently simulated for each point of distance. In these independently simulated points, the noise power N_{dBm} is considered as having noise uncertainty $x = 0$ dBm.[9] The effect of shadowing can be seen from Figs. 28 - 33. In the figures, as is natural, approximately half of the independently-simulated points have lower detection probability than the median. Thus, while the median detection probability is known, the randomness in the propagation loss makes knowing the exact detection probability uncertain for different distances.

The propagation loss of a possible incumbent LTE base station can be evaluated to be within certain limits, as the exact value of it is unknown. The propagation loss with constructive and destructive shadowing channels is evaluated by using $p = 0.9$ and $p = 0.68269$ curves.[10] In the figures, the p curves present the probability of detection curves between which random draws of shadowing channel fall p of the time, while additionally considering the possible noise uncertainty. More specifically, the noise uncertainty is taken into account in the lower destructive shadow fading p curves by considering minimum -1 dB noise uncertainty. Conversely, in the upper constructive shadow fading p curves, maximum 1 dB noise uncertainty is assumed.

Fig. 28 plots the detection probability of a macro base station. This type of sector base station can offer approximately 4.33 km cell radius in an open rural setting [142]. From Fig. 28, it is seen that the base station can be sensed much further away. From the simulations, it is seen that the transmitter could be detected further than $d_{\text{t}} = 84.5$ km[11] away in good channel conditions. This natural as the sensing antenna is located higher, has a higher antenna gain, and the sensor has a lower noise figure than the LTE user equipment. In this setting an incumbent macro base station might be detected even though the spectrum could be utilized at the point of the detector. Here, the constructive shadowing increases the possible detection distance.

Detection distance d_{f} is 27.6 km in the scenario simulated in Fig. 28. Note that the frequency reuse distance is sometimes designed to be three times the full cell range, which is, in this setting, $3 \times 2d_{\text{inc}} \approx 26$ km. Thus, as the distance 27.6 km is reliably

[9]The effect of the noise uncertainty is better seen from Fig. 27. The maximum or minimum noise uncertainty would increase, or decrease, the detection probability with the same magnitude as in this figure.

[10]The seemingly random $p = 0.68269$ is selected, because it limits the effect of shadowing between $[-\sigma_{\text{hata}}, \sigma_{\text{hata}}]$ dB.

[11]The maximum total line of sight distance (sensor and base station radio horizons summed together) for these antenna heights is approximately 37.4 km, which could also be used as a maximum value for d_{t} in this scenario.

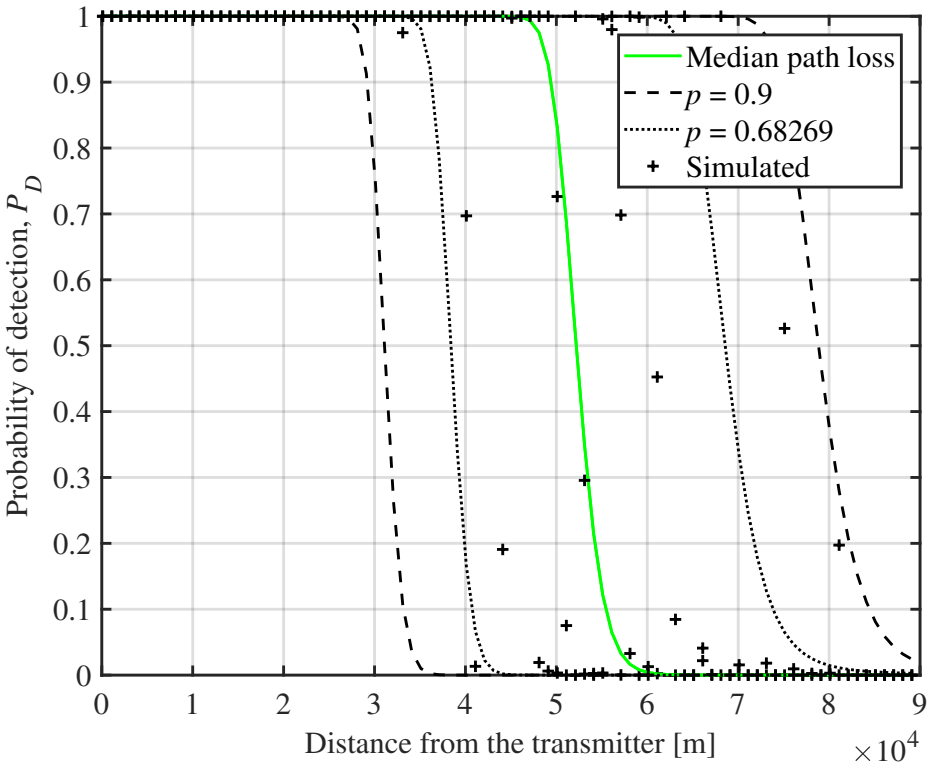

Fig. 28. Detection probability of a 20 W macro base station. The radio horizons are at 8.2 km and at 29.1 km for the sensor and for the base station, respectively.

detected free of incumbent transmitters, the incumbent is not within this frequency reuse distance. Thus, in this setting, the PS actor can directly put its similar 4.33 km cell radius base stations to the location of the sensor.

Note that the incumbent might also use smaller cells. Fig. 29 plots the detection probability of a smaller transmit power outdoor pico base station. This type of a pico base station can cover around a $d_{\text{inc}} = 1$ km LTE cell radius in an open setting. For this base station and antenna height, detection can happen even from a distance of $d_{\text{t}} = 50$ km. Moreover, detection happens with a high probability from a distance of $d_{\text{f}} = 8.7$ km. Thus, if there is no detection, at least 8.7 km can be considered being free of incumbent 1 km cell radius LTE transmitters. Therefore, given that the frequency reuse distance would be approximately $3 \times 2d_{\text{inc}} = 6$ km, the PS users can set their own pico base station with a 1 km cell radius to the location of the sensor without a major disturbance to an undetected incumbent.

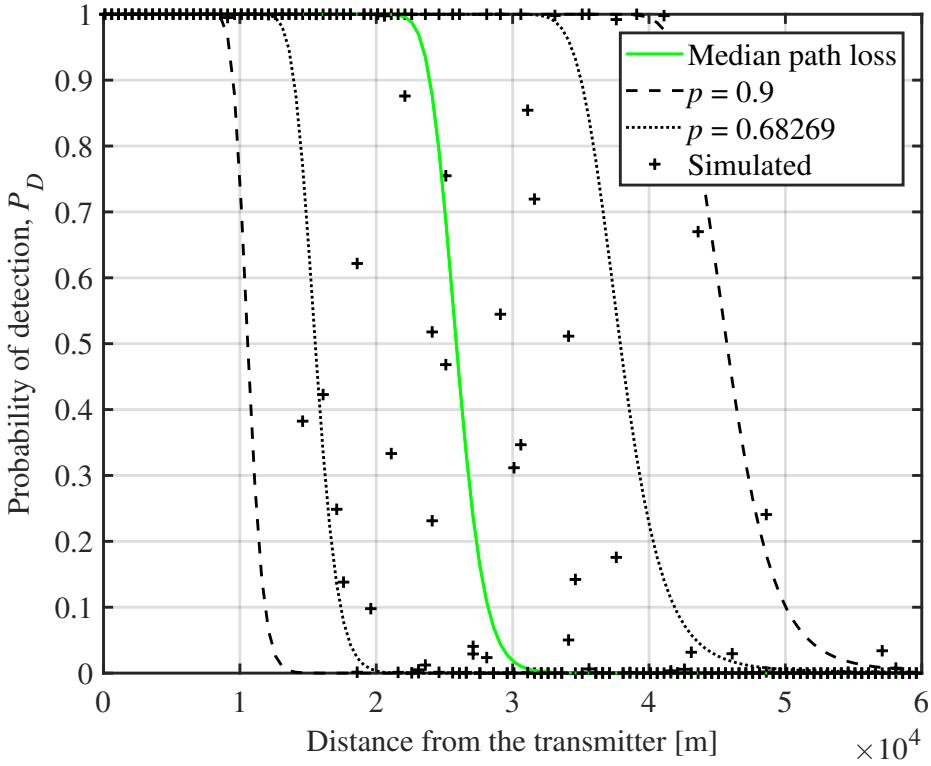

Fig. 29. Detection probability of a 5 W outdoor pico base station. The radio horizons are at 8.2 km and at 24.4 km for the sensor and for the base station, respectively.

Fig. 30 plots the detection probability of an indoor pico base station in an outdoor setting. These types of base stations are mainly used indoors, where they cover around a 50 m radius. The reason to study the detection distances of an indoor base station in an outdoor setting is for obtaining insight in detecting PS actors which are out of reach and are using similar-powered base stations outdoors. When used outdoors, indoor pico base stations can cover around a $d_{\mathrm{inc}} = 250$ m radius. For this base station and antenna height, d_{f} is 1.6 km and d_{t} is 18.7 km. Thus, if there is no detection, at least 1.6 km can be considered being free of incumbent transmitters. In this setting, detection distance d_{f} is over six times longer than the incumbent cell radius, d_{inc}.

To show the effect of antenna height, Figs. 31, 32, and 33 plot the detection probabilities of the previous base stations when the sensor has been lowered to 1.5 m height. By comparing these figures with the previous figures 28, 29, and 30, it can

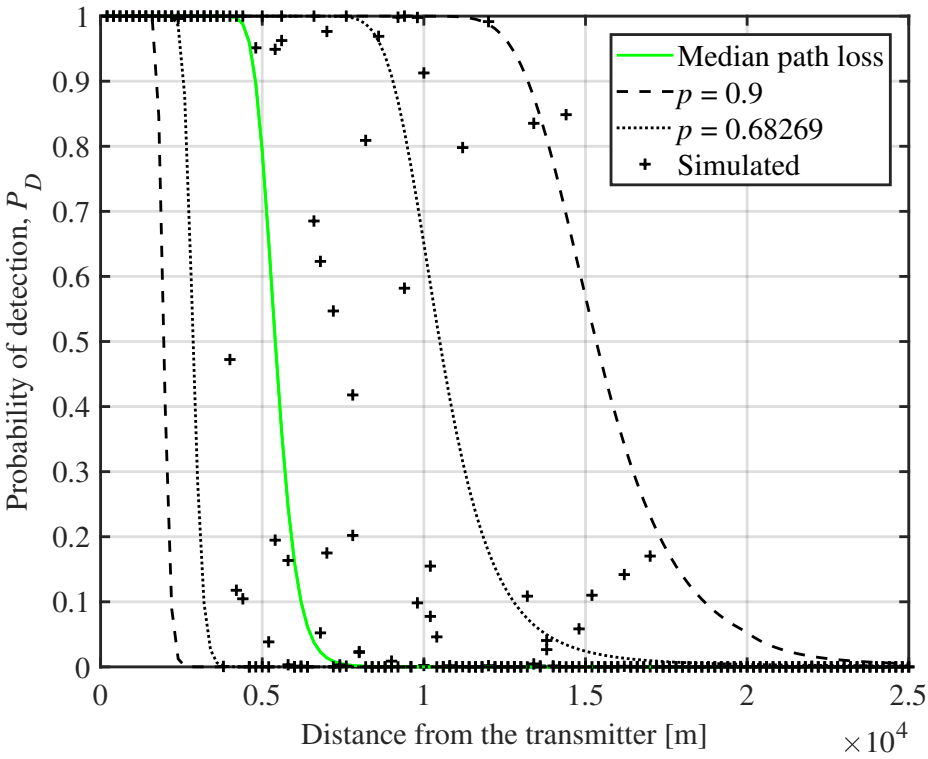

Fig. 30. Detection probability of a 0.15 W indoor pico base station. The radio horizons are at 8.2 km and at 17 km for the sensor and for the base station, respectively.

be concluded that the antenna height plays a big role in detecting the incumbent base stations.

From Figs. 28-33, it can be inferred that the individual simulated points with random noise uncertainty mainly lie in between the $p = 0.68269$ curves. In this case, the detection distances could also be estimated by using the $p = 0.68269$ curves. This would increase the accuracy of available spectrum information, which promotes more efficient spectrum use. In LSA scenarios, fine tuning these distances becomes a trade-off between incumbent protection and spectrum use efficiency.

The p curves are used as follows to find out the distances d_f and d_t defined in Section 5.1.3. Here, distances for d_f are located at the figures from the lower $p = 0.9$ curves at points where $P_D = 0.99$. Distances for d_t are located at the upper $p = 0.9$ curves at points where $P_D = 0.1$. The resulting distances d_f and d_t are in Table 5.

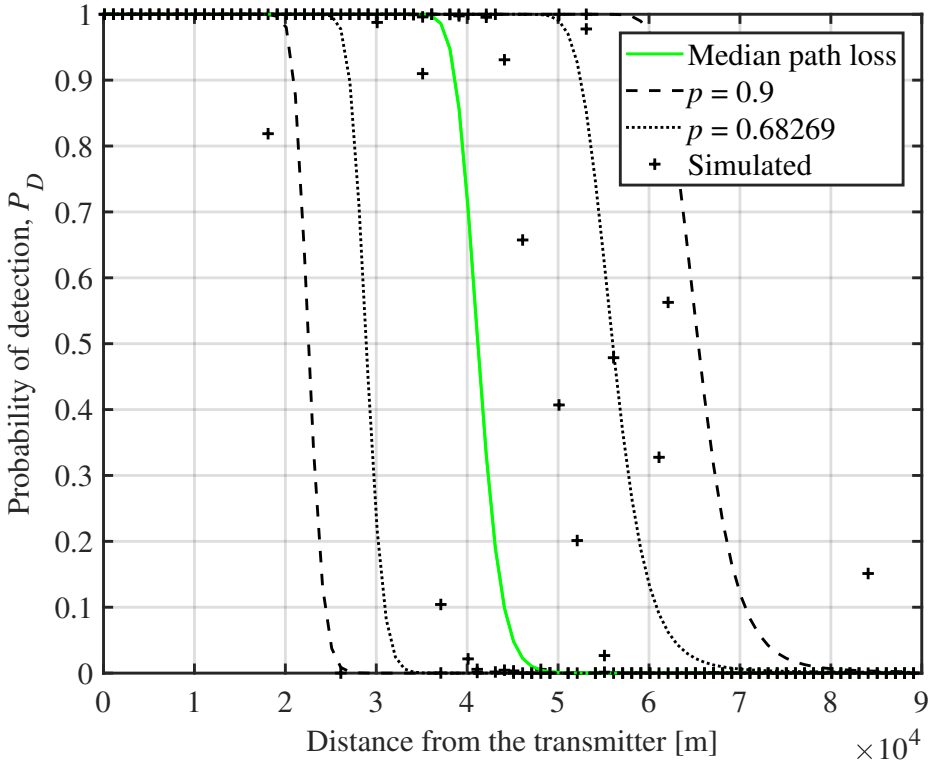

Fig. 31. Detection probability of a 20 W macro base station with a sensor at 1.5 m. The radio horizons are at 5 km and at 29.1 km for the sensor and for the base station, respectively.

The results in this section show that the energy detector with a sensor at 4 m height can detect a single incumbent from much further than the intersite distance, which is generally three times the cell radius when sectored cells are considered [142]. Therefore, with respect to the considered system, the spectrum can be used by the licensee if there is no detection. Moreover, it could sometimes be possible to utilize the spectrum without disturbing the primary spectrum user even when an energy detector detects the incumbent. This is when the incumbent is far enough but has constructive fading. Note that more sophisticated methods would then be needed to verify that the detected incumbent is far enough. One possibility could be collaboratively sensing the angle, time, or power difference of arrival from multiple locations. (See section 1.3.)

The results also show that the transmitter-free distance d_{f} with a sensor antenna at 1.5 m is less than the intersite distance of the corresponding incumbent. Therefore, in this scenario, the LSA licensee cannot be certain that the channel is free for its use if the

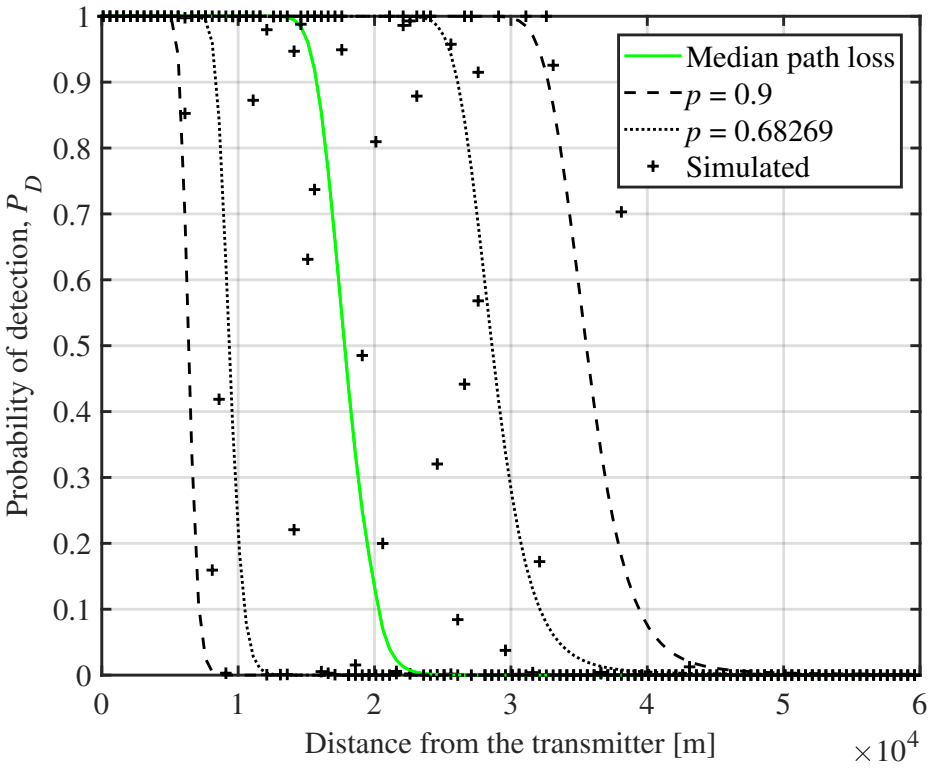

Fig. 32. Detection probability of a 5 W outdoor pico base station with a sensor at 1.5 m. The radio horizons are at 5 km and at 24.4 km for the sensor and for the base station, respectively.

channel is sensed free. However, a detected incumbent can be detected to be closer to the sensor with a low antenna height, as d_t is shorter than with a high antenna height. This can be beneficial, for example, when there is only one incumbent that needs to be located.

Detection distance tables such as Table 5 provide information that can be deducted from the specific sensor information and from the environment and the incumbent characterization. Thereafter, with binary detection results from the sensors, this information can be utilized in calculating the protection zone around a detected or undetected incumbent. This is the theme of the next section.

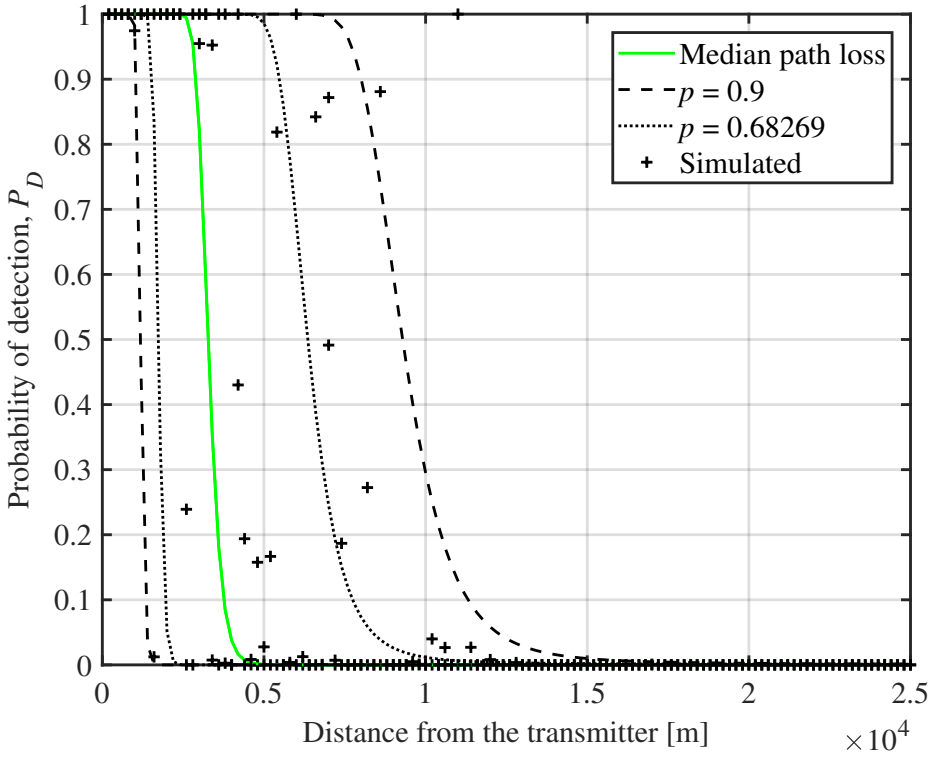

Fig. 33. Detection probability of a 0.15 W indoor pico base station with a sensor at 1.5 m. The radio horizons are at 5 km and at 17 km for the sensor and for the base station, respectively.

5.3 Spectrum information utilization

The rest of the chapter describes how to utilize sensors and their information. Subsection 5.3.1 introduces a collaborative decision method for locating the possible incumbent and describes how to find a protection zone around the possible incumbent. This collaborative method enables the actual use of spectrum information from multiple, possibly contradicting, sensors together with LSA in public safety applications. Subsection 5.3.2

Table 5. Transmitter-free distances, d_f, and transmitter within these distances, d_t, for base stations with different transmit powers.

Cell type	Sensor at 4 m height		Sensor at 1.5 m height	
	d_f	d_t	d_f	d_t
Macro	27.6 km	84.5 km	19.5 km	70.6 km
Outdoor Pico	8.7 km	50 km	5.2 km	39.4 km
Indoor Pico	1.6 km	18.7 km	915 m	11.3 km

describes how the distributed LSA controllers can utilize multiple spectrum information sources, such as sensors and the LSA repository. Therein, the spectrum use agreements between the incumbent and the LSA licensee, i.e., sharing arrangements, determine whether the use is allowed or not. Subsection 5.3.3 describes how to control false and missed detections. The final Subsection 5.3.4 describes the practical use of sensors, so that LTE base stations of the PS do not interfere with the sensing. This could happen when the PS base stations are transmitting and the sensors need to simultaneously sense whether there are incumbent base stations.

5.3.1 Collaborative decision method

This subsection introduces how multiple detectors can be used collaboratively to decide whether the channel is free or not. More specifically, it is shown how to calculate a protection zone for a possible incumbent user.[12] The basic principle is shown in Figs. 34 and 35.

First, circles with radius d_{f} are drawn around the sensors that do not detect the incumbent. Second, the union of these circles is taken, seen in Fig. 35 inside the solid thin red line. Finally, to mitigate the hidden node problem, the area within distance d_{inc} (i.e., cell range) from the edge is removed at the boundary of the union. See value examples for d_{inc} in Table 4. The remaining area is free of incumbent receivers. This area is seen in Fig. 35 inside the solid and rounded thick green line. Its complement is the protection zone, which is the area within which the incumbent receivers must not be subjected to harmful interference caused by PS actors.

The above method can also be utilized when there might be multiple incumbent LTE base stations, but no detection. Note that multiple independent incumbent transmitters would increase detected power and thus increase the distance from which the incumbent activity can be detected. Therefore, the transmitter-free distance calculated for a single incumbent d_{f} is also free from transmitters in the multiple independent transmitter scenario.

If there is only one incumbent transmitter, multiple sensors can be used to roughly locate it. The basic principle can be seen from Fig. 36. In this example, two sensors have sensed an incumbent and one sensor has not. First, circles with radius d_{t} are drawn

[12] The principles behind the protection zone calculation work also with other sensing methods, for example with feature detectors for primary and secondary synchronization signals [138]. This only requires determining the probable detection distances for these methods.

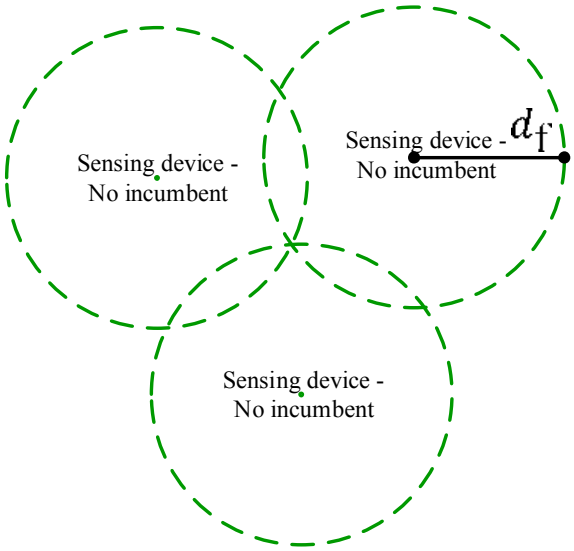

Fig. 34. Three sensors with no detection ([105] ©2018 Springer).

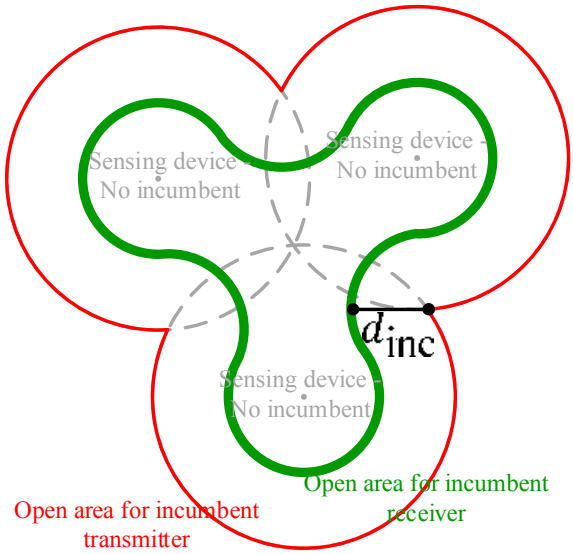

Fig. 35. Three sensors do not sense an incumbent. LSA controllers calculate an incumbent-free zone for a possible incumbent, whose receiver is within distance d_{inc} from the transmitter ([105] ©2018 Springer).

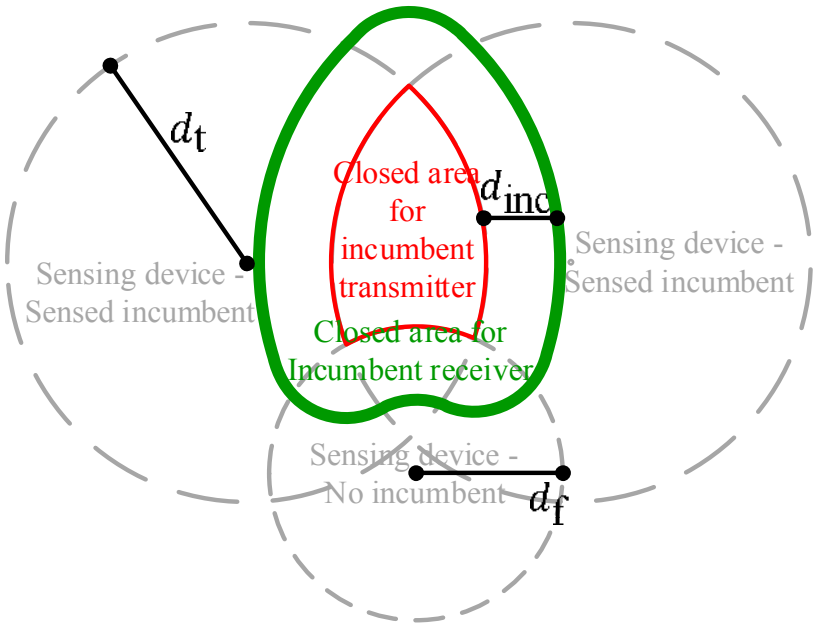

Fig. 36. Two sensors notice the same incumbent and LSA controllers calculate a closed protection zone for it, which is seen here as a green thick line. A detected transmitter is most probably closer to the sensors than d_t. Moreover, a distance d_f is likely free of transmitters, given that there is no detection ([105] ©2018 Springer).

around the sensors that detect the incumbent and an intersection between these circles is taken. Second, circles with radius d_f are drawn around all the sensors that do not detect an incumbent. Third, these circles are removed from the intersection. This is the area free of the incumbent transmitter. Finally, the area within distance d_{inc} at the boundary of the remaining area is added. The resulting area might have incumbent receivers. This area is seen in Fig. 36 inside the solid and rounded thick line. This is the protection zone, or the area within which the incumbent receivers must not be subjected to harmful interference caused by PS base stations. The transmission details must be further agreed in the spectrum sharing arrangements.

5.3.2 Spectrum sharing arrangements for combining contradicting spectrum information

In this subsection, it is described how the distributed LSA controllers can use the protection zones described above for combining and verifying the spectrum information from different sources. The spectrum information sources are: the sensors, the LSA

repository and the other LSA controllers that synchronize spectrum use of their corresponding base stations. Moreover, lack of commercial network services can indicate that there are unused spectrum resources.

Fig. 37 shows the logic for the distributed operations and management system (dOMS) of Fig. 23. The system keeps a synchronized data base of the other LTE base stations at "other nodes". Furthermore, the sensing information is kept at the "sensor manager" data base and the LSA information is at an "LSA server" data base. The "inquire available channels" is a subprogram that decides the channel allowability.

The distributed LSA controllers determine if channel use is allowed or not and share the allowed channels between each other, while selecting the channel allocations and power levels. The controllers have event-based listeners for noticing changes in the spectrum information and in the availability of the channels. This listener initiates a channel change for the base stations, if needed.

In Fig. 37, when "configuring available channel" to the access point, the secondary user has to adjust the secondary cell emitted power levels according to the sharing arrangements. For example, the incumbent user SNR is allowed to deteriorate a certain predetermined dB value at the known or possible incumbent LTE cell border. In calculating the deterioration, the attenuation model should be naturally selected according to the environment.

If the channel is allowed or not depends on the LSA sharing arrangement with the incumbents. The logic is executed in "inquiring of the available channels". The arrangements should be agreed separately for different location types. Types of locations can, for example, be areas with unknown commercial networks and areas with broken commercial networks. Additionally, criticality of the missions and the quality of service measurements of the commercial network can be taken into account.

In a highly critical scenario, where the commercial network is down, it would be straightforward for the controllers to only select the least congested LSA channel from the nearest sensor. This channel is not likely used in this particular location. Furthermore, it has the least interference. Amongst other things, the critical use has to be agreed in the sharing arrangements.

Tables 6 and 7 are two examples of sharing arrangements for what to do with contradicting and congruent spectrum information. The tables show whether spectrum use is allowed or not by the PS base stations. The *old LSA information with available channel* in the tables is a situation when the connection to the LSA repository has been out longer than for how long the spectrum information is valid. The *LSA channel not*

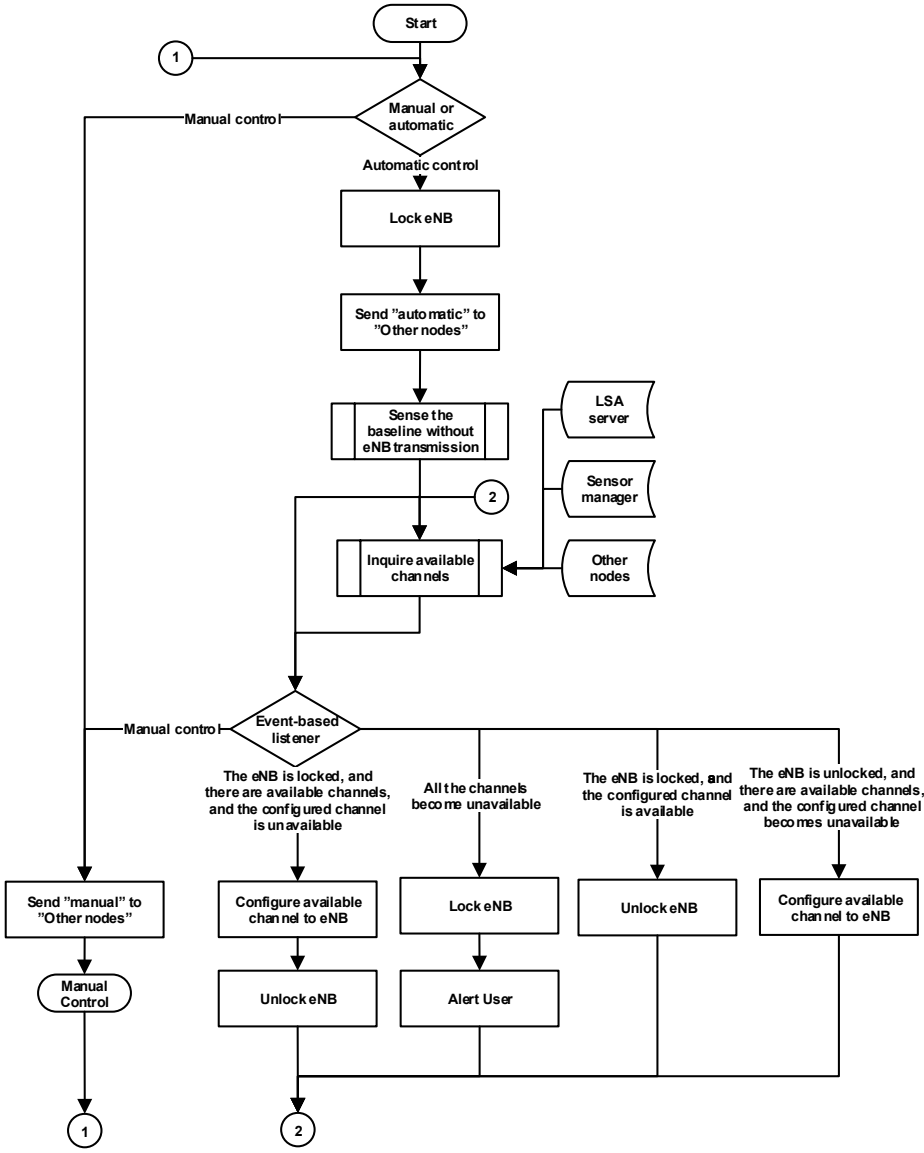

Fig. 37. Example logic for the dOMS for utilizing the LSA and the sensor information.

Table 6. Is the spectrum use allowed? A sharing arrangement table for LSA licensee transmissions in areas with no known commercial networks.

LSA repository information ↓	LSA channel in this area not sensed free	LSA channel in this area sensed free
LSA channel available	No	Allowed
LSA channel not available	No	No
Old LSA information with available channel	No	Allowed

available in Table 7 denotes a situation where the information at the LSA repository is false, e.g., the commercial system is out of order and has not been able to update the information to the LSA repository. Similar sharing arrangements could also be made for commercial network scenarios with existing but insufficient commercial networks.

Note that the details of the allowed transmissions must be further agreed. One agreement pertains to if the incumbent is allowed to transmit without informing the LSA repository. Moreover, the sharing arrangements resolve the transmission power and antenna height limitations, sensing methods and their detection probabilities and false and missed detection probabilities.

5.3.3 False and missed detections

While sensing, some amount of false and missed detections must be tolerated. The amount of these must be agreed with the incumbent with respect to the criticality of the mission. With energy detectors, the maximum false detection probability per sensor can be decided first by selecting the energy threshold correspondingly. Then, in general, the maximum missed detection probability can be made smaller by considering a smaller radius, d_{f}, around the sensor. This radius is considered free of transmitters, given there are no detections. Furthermore, the less there is fading, the higher is the signal strength. Finally, if d_{f} is small, there might be a larger received signal strength and thus increased

Table 7. Is the spectrum use allowed? A sharing arrangement table for LSA licensee transmissions in areas with broken commercial networks.

LSA repository information ↓	LSA channel in this area not sensed free	LSA channel in this area sensed free
LSA channel available	Allowed	Allowed
LSA channel not available	No	Allowed
Old LSA information with available channel	No	Allowed

detection probability. Note that with a smaller d_f there might be a need for multiple sensors[13] to cover the required area.

5.3.4 Sensor control in practice

The use of multiple detectors needs an efficient tool for controlling all the information from all of them. Moreover, the PS requires an application for utilizing the available sensors and for communicating the information to the PS network. This subsection describes methods for the PS network to use available detectors and to notice changes in the channel information.

The PS network has a sensor manager application that extracts the measurement results of LSA licensed channels from the available sensors. The PS actors can utilize their radios and sensors for spectrum information. Moreover, LTE user equipment has built-in sensing capabilities. Note that also the LTE access points themselves are specified to sense the channels [140]. However, this feature is not yet always implemented with a usable application programming interface in the commercial access points.

The sensor manager uses unique commands for the corresponding sensors. Most spectrum sensors have programmable interfaces that use C, Python or standard commands for programmable instruments [144, 145]. The manager provides the measurement results and sensor-specific information for the distributed LSA controllers. The information from the sensors is analyzed at the distributed LSA controllers. More specifically, the sensor-specific information is used by the controllers to estimate the values for d_f and d_t. The sensor-specific information includes at least the sensor antenna height, location and gain as well as the environment of the sensor.

The LSA controllers access the sensing information when the PS transmissions do not disturb the sensing. For doing this, the channels are sensed before the PS base stations start transmitting. The information is saved for later use. However, if there are other nearby PS base stations transmitting, the LSA controller first waits for a communication break. Then it temporarily blocks the nearby base stations via internal private network links before accessing the sensed information. Moreover, sensing can happen periodically during communication breaks to verify that the channel is still available. The time period should be agreed in the sharing arrangements.

[13] Moreover, with more sensors, false detections themselves can be detected if multiple sensors give contradictory results.

5.4 Summary

In this chapter, a sensing method was introduced for PS actors to obtain available spectrum information for their own LTE network. The research started from the application point of view for obtaining spectrum information for a rapidly deployed network when the central frequency repositories are not working or are not up to date. The simulation results showed that simple energy detectors can be used for guaranteeing the availability of channels for the PS LTE network. More precisely, the possible incumbent base stations could be detected far enough in outdoor channels, when the sensors are lifted high enough, free of severe obstacles. In our setting, for example in rural areas, using a single sensor is sufficient for obtaining spectrum information for a secondary licensee base station. In our scenarios, the secondary licensee's base station does not disturb the incumbent cell phone when the primary base stations are not detected.

In contrast, if the incumbents were indoor base stations in a city with low transmission powers, a solution for reliable detection would be a dense sensor network. The detectors should be located sufficiently near to each other to reliably cover the whole area where the secondary licensee base stations emit power. Then, it is important to consider whether it is sensible to utilize the frequencies of incumbents whose detection requires a lot of effort and time. In non-critical scenarios, it might be sensible if no other frequencies are available. Still, when the situation is critical, a PS actor role change from a secondary licence to a primary spectrum user to the channel with the least interference can be justified.

Nevertheless, to efficiently obtain spectrum information, there is a need to design the sensor network according to the scenario and the incumbent type. The used sensing methods have to be verified and the sensors need to be high enough to detect the specific incumbents.

For detecting incumbents with different transmit powers, this chapter introduced reliable detection distances d_f and d_t for an energy detector, which are *distance free of transmitters*, and *distance with the detected transmitter*, respectively. The chapter introduced how to further use the sensing methods for which these distances are known. More specifically, the chapter showed techniques to collaboratively determine the available spectrum and, e.g., to complement LSA spectrum information. These methods are not only bound to energy detection. They work also for other detection methods whose detection distances can be determined.

6 Discussion and open problems

The technological solutions for PS actors to use the LTE networks are readily available and the standardization work, which was described in Chapter 1, enables the PS actors to be priority users. This tailoring allows the commercial network providers to also offer their services to the PS actors. In normal situations, when the commercial networks are fully available, the tailored solutions for PS applications offer a high capacity and functionality. However, in situations when the commercial networks are unavailable, the PS actors can deploy their own rapidly deployed PS networks.

This thesis studied how the PS actors can obtain connectivity and similar capabilities in rapidly deployed networks as in commercial networks, and how PS actors can obtain radio spectrum for their communications in their rapidly deployed networks. To study these questions, they were divided into multiple research problems that were then answered. More specifically, to obtain similar functionality in different networks, interface connection possibilities were studied for connecting the PS actors from one network to another. Moreover, spectrum sharing possibilities in the means of ownership of the spectrum were discussed. Then, a robust LSA system was developed for the PS actors to obtain and to utilize unused and available spectrum with a secondary spectrum licence. The secondary LSA licence is suitable in situations where the PS can primarily rely on commercial networks. The licensed spectrum can then be used by rapidly deployed PS networks in scenarios where there are no commercial networks available. Thus, there is an open need of a coverage-map-based and/or QoS-based application for turning on the rapidly deployed networks, when required.

The LSA system was then extended with a sensing system. It was shown how the PS users can utilize a spectrum sensing system together with an LSA mechanism to find suitable and available spectrum for the rapidly deployed PS networks.

The LSA has been used in trials live with sensing and with rapidly deployable networks [109]. Tests done with the implemented systems in real networks show that the LSA approach can be a part of the solution obtaining spectrum in future rapidly deployed networks. In general, the methods developed in this thesis are already implementable for commercially-available rapidly deployed PS networks.

The PS actors should also be able to utilize their own deployable networks when the commercial LTE networks are operating but are insufficient for their use cases. For these

scenarios, the PS users require more than a secondary spectrum licence. They need guaranteed spectrum resources. The PS actors need a regulative decision that allows flexible spectrum sharing with conditional priority for the critical use cases. In other words, the PS actors require spectrum slots for police, firemen and other PS users for the rare situations when the commercial networks cannot guarantee their requirements.

Here, the rapidly deployed PS networks could primarily use a secondary licence for the available spectrum. If this spectrum is not available, the rapidly deployed PS networks could use the spectrum of the operator that offers commercial network connections to the PS users. On the other hand, this network is also used by the PS users and thus might be occupied. As a final option, the PS should be allowed to use additional suitable spectrum, for example with the least interference to the other spectrum users or other predefined spectrum.

However, it is a political decision about how the PS actors will be integrated into the commercial LTE networks. In Finland, an auction will be organized for the LTE operators for obtaining the PS actors as their customers [122]. The winning operator can also offer its network to commercial users, but has the legal obligation to offer priority services for the PS actors. Then, the winning operator is obligated to offer a wide coverage solution for the PS actors. This can, for example, mean a sufficient amount of connection points for rapidly deployed PS networks countrywide. Organizing the spectrum sharing with the rapidly deployed networks is the responsibility of the operator. An option for this is to use LSA spectrum sharing methods together with sensing, as discussed in this thesis.

A natural extension to the sensing work of this thesis is to consider more specific, possible, and available deployment practices of the PS base stations with a quantitative analysis of real-life scenarios. It is possible to plan the sensing network with other types of channels, where the extended Hata is not suitable. This can be the case when the incumbent users are drones. Additionally, detecting different types of incumbents should be considered, such as time division duplex base stations. Their detection should be done with signal correlation methods [51] rather than energy detection. Note that, at LTE time division duplex base stations, the downlinks are silent for a portion of time depending on the transmission speed [138].

As shown in this thesis, in open rural areas, where the primary user has not placed small cells, a single energy sensor per a single secondary LTE base station can be enough for obtaining available spectrum information from incumbent frequency division duplex base stations.

If the incumbents are, e.g., indoor base stations with low transmission powers, reliable detection might require a sensor network. Therein, the sensors should be located sufficiently near to each other to cover the whole area where the secondary base stations emit power. However, building a dense sensor network in a critical situation might be impractical. An alternative to this type of sensor network can be, e.g., a drone that senses the area. It could circulate the necessary area and measure the required spectrum information and communicate this information to the ground. Naturally, the rapid implementation of this type of a drone solution would require more planning. In normal situations, the PS actors need their communication equipment to be automatically up and running within one minute from powering on.

The sensor scenarios considered in this thesis had a hidden assumption of simple and coarse detectors for frequency division duplex incumbents. A problem in using energy detectors in our scenario is that sometimes the incumbents might be sensed even when the spectrum could be used by the secondary user, i.e., the incumbent base stations emit interference far away above the tree level, while their actual service range is much closer. To solve this problem, it is possible to consider more sophisticated sensing methods, such as angle of arrival [41], time difference of arrival [42], frequency difference of arrival [43, 44], power difference [45] of arrival, gain ratio of arrival [46] and ID-aided locating techniques. The information obtained with these techniques can be statistically combined for locating the detected incumbent users with higher accuracy. This is especially true when multiple collaborative or mobile sensors are used at a sufficient distance from each other. Then, the spectrum use could be allowed for similar base stations, given that the detected base stations can be located to be further than their intersite distance.

The collaborative decision method principles presented for the sensing results in this thesis can also be modified for other incumbent-specific scenarios. The practices can, for example, be utilized in the environmental sensing capability of the SAS spectrum sharing method, which is planned for sharing the 3.5 GHz band in the United States.

References

[1] "Radio technology beyond lte," Accessed Jan. 2019. [Online]. Available: http://www.3gpp.org/DynaReport/38-series.htm

[2] ETSI EN 300 392-1, "Terrestrial trunked radio (TETRA); voice plus data (V+D); part 1: General network design," *V1.4.1*, 2009.

[3] ETSI EN 300 392-2, "Terrestrial trunked radio (TETRA); voice plus data (V+D); part 2: Air interface (AI)," *V3.8.1*, 2016.

[4] "Ukkoverkot commercial service," Accessed Jun. 2016. [Online]. Available: http://www.ukkoverkot.fi/

[5] 3rd Generation Partnership Project, "Evolved universal terrestrial radio access (E-UTRA); carrier aggregation; base station (BS) radio transmission and reception," *3GPP TR 36.808 V10.0.0*, 2013.

[6] Electronic Communications Committee, "Licensed shared access (LSA)," *ECC Report 205*, 2014, Accessed Jun. 2016. [Online]. Available: http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP205.PDF

[7] ETSI, "Reconfigurable radio systems (RRS); system architecture and high level procedures for operation of licensed shared access (LSA) in the 2 300 MHz - 2 400 MHz band," *ETSI TS 103 235 V1.1.1*, 2015, Accessed Jun. 2016. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/103200_103299/103235/01.01.01_60/ts_103235v010101p.pdf

[8] ETSI, "Electromagnetic compatibility and radio spectrum matters (ERM); system reference document (SRdoc); mobile broadband services in the 2 300 MHz - 2 400 MHz frequency band under licensed shared access regime," *ETSI TR 103 113 V1.1.1*, 2013, Accessed Feb. 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103100_103199/103113/01.01.01_60/tr_103113v010101p.pdf

[9] Electronic Communications Committee, "Broadband wireless systems usage in 2300-2400 MHz," *ECC Report 172*, 2012, Accessed Jun. 2016. [Online]. Available: http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCRep172.pdf

[10] European Radiocommunications Committee, "Handbook on radio equipment and systems videolinks for ENG/OB use," *ERC Report 38*, 1995, Accessed Jun. 2016. [Online]. Available: http://www.erodocdb.dk/Docs/doc98/official/pdf/REP038.pdf

[11] "Cisco visual networking index: Global mobile data traffic forecast update, 2016-2021," *Cisco White Paper*, 2017, Accessed Nov. 2017. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf

[12] "The 1000x mobile data challenge," *Qualcomm Presentation*, 2013, Accessed Jun. 2016. [Online]. Available: http://www.qualcomm.com/media/documents/files/1000x-mobile-data-challenge.pdf

[13] The White House, "Realizing the full potential of government-held spectrum to spur economic growth," *President's Council of Advisors on Science and Technology*, 2012, Accessed Nov. 2017. [Online]. Available: https://www.obamawhitehouse.gov/sites/default/files/microsites/ostp/pcast_spectrum_report_final_july_20_2012.pdf

[14] ECC, "The european table of frequency allocations and applications in the frequency range 8.3 kHz to 3000 GHz (eca table)," *ERC REPORT 25*, 2017.

[15] ——, "Cross-border coordination for mobile/fixed communications networks (MFCN) and between MFCN and other systems in the frequency band 2300-2400 MHz," *Recommendation (14)04*, 2014, Accessed Nov. 2017. [Online]. Available: http://www.erodocdb.dk/Docs/doc98/official/pdf/REC1404.PDF

[16] ——, "Harmonised technical and regulatory conditions for the use of the band 2300-2400 MHz for mobile/fixed communications networks (MFCN)," *Decision (14)02*, 2014, Accessed Nov. 2017. [Online]. Available: http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCDEC1402.PDF

[17] A. M. Foster, "Spectrum sharing," in *Discussion paper of the global symposium for regulators*, Pattaya, Thailand, 2008.

[18] S. Bhattarai, J. J. Park, B. Gao, K. Bian, and W. Lehr, "An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research," *IEEE Transactions on Cognitive Communications and Networking*, vol. 2, no. 2, pp. 110–128, June 2016.

[19] Viestintävirasto, "Frequency allocation table," *annex to regulation M4W*, 2017, Accessed Nov. 2017. [Online]. Available: https://www.viestintavirasto.fi/attachments/maaraykset/Taajuusjakotaulukko_12.6.2017_E.pdf

[20] ITU, "General principles and methods for sharing between radiocommunication services or between radio stations," *Recommendation ITU-R SM.1132-2*, 2001.

[21] Wireless innovation forum, "Signaling protocols and procedures for citizens broadband radio service (CBRS): Spectrum access system (SAS) - citizens broadband radio service device (CBSD) interface technical specification," *WINNF-TS-0096 V 1.3.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://workspace.winnforum.org/higherlogic/ws/public/download/6482/

[22] M. M. Sohul, M. Yao, T. Yang, and J. H. Reed, "Spectrum access system for the citizen broadband radio service," *IEEE Communications Magazine*, vol. 53, no. 7, pp. 18–25, 2015.

[23] M. Palola, V. Hartikainen, M. Mäkeläinen, T. Kippola, P. Aho, K. Lähetkangas, L. Tudose, A. Kivinen, S. Joshi, and J. Hallio, "The first end-to-end live trial of CBRS with carrier aggregation using 3.5 GHz LTE equipment." in *IEEE International Symposium on Dynamic Spectrum Access Networks*, Baltimore, MD, USA, 2017.

[24] (Accessed Nov. 2017) CORE++ project web page. [Online]. Available: http://core.willab.fi

[25] ETSI, "Reconfigurable radio systems (RRS); system requirements for operation of mobile broadband systems in the 2 300 MHz - 2 400 MHz band under licensed shared access (LSA)," *ETSI TS 103 154 V1.1.1*, 2014, Accessed Feb. 2019. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/103100_103199/103154/01.01.01_60/ts_103154v010101p.pdf

[26] ——, "Reconfigurable radio systems (RRS); information elements and protocols for the interface between LSA controller (LC) and LSA repository (LR) for operation of licensed shared access (LSA) in the 2 300 MHz - 2 400 MHz band," *ETSI TS 103 379 V1.1.1*, 2017. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/103300_103399/103379/01.01.01_60/ts_103379v010101p.pdf

[27] E. Commission, "Standardisation mandate to CEN, CENELEC and ETSI for reconfigurable radio systems (RSS)," *European Commission mandate M/512 EN*, 2012.

[28] J. Kahtava, "An evolutionary spectrum authorisation scheme for sustainable economic growth and consumer benefit," *Frequency Management Working Group, Presentation*, 2011, Accessed Nov. 2017. [Online]. Available: https://cept.org/Documents/cg-crs/363/

[29] R. S. P. Group, "Report on collective use of spectrum CUS and other spectrum sharing approaches," *RSPG11-392 Final*, 2011.

[30] ETSI, "Reconfigurable radio systems (RRS); use cases for spectrum and network usage among public safety, commercial and military domains," *ETSI TR 102 970 V1.1.1*, 2013, Accessed Jun. 2016. [Online]. Available: http://www.etsi.org/deliver/etsi_tr/102900_102999/102970/01.01.01_60/tr_102970v010101p.pdf

[31] E. Villebrun, "France's path to PPDR broadband," *Presentation*, 2018, Accessed Feb. 2019. [Online]. Available: https://snir.fr/images/pmr-2018/VILLEBRUN-MinInt.pdf

[32] ETSI, "LTE;telecommunication management; licensed shared access (LSA) controller (LC) integration reference point (IRP); requirements," *ETSI TS 128 301 V15.0.0*, 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/128300_128399/128301/15.00.00_60/ts_128301v150000p.pdf

[33] ——, "LTE;telecommunication management; licensed shared access (LSA) controller (LC) integration reference point (IRP); information service (is)," *ETSI TS 128 302 V15.0.0*, 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/128300_128399/128302/15.00.00_60/ts_128302v150000p.pdf

[34] ——, "LTE;telecommunication management; licensed shared access (LSA) controller (LC) integration reference point (IRP); solution set (SS) definitions," *ETSI TS 128 303 V15.0.0*, 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/128300_128399/128303/15.00.00_60/ts_128303v150000p.pdf

[35] T. Tuukkanen, S. Yrjölä, M. Matinmikko, P. Ahokangas, and M. Mustonen, "Armed forces' views on shared spectrum access," in *International Conference on Military Communications and Information Systems*, 2017, pp. 1–8.

[36] M. Matinmikko, H. Okkonen, M. Palola, S. Yrjola, P. Ahokangas, and M. Mustonen, "Spectrum sharing using licensed shared access: the concept and its workflow for LTE-advanced networks," *IEEE Wireless Communications*, vol. 21, no. 2, pp. 72–79, April 2014.

[37] M. Matinmikko-Blue, "Stakeholder analysis for the development of sharing-based spectrum governance models for mobile communications," *Ph.D. dissertation, Faculty of Technology, University of Oulu, Finland*, vol. 2018, Accessed Nov. 2018. [Online]. Available: http://urn.fi/urn:isbn:9789526220512

[38] 3rd Generation Partnership Project, "Technical specification group services and system aspects; telecommunication management; study on OAM support for licensed shared access (LSA)," *3GPP TR 32.855 V14.0.0*, 2016.

[39] ITU, "Spectrum occupancy measurement and evaluation," *Report ITU-R SM. 1880-2*, 2017.

[40] ——, "Spectrum monitoring evolution," *Report ITU-R SM. 2355-0*, 2015.

[41] J. Wang, J. Chen, and D. Cabric, "Cramer-rao bounds for joint RSS/DoA-based primary-user localization in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1363–1375, 2013.

[42] C. Knapp and G. Carter, "The generalized correlation method for estimation of time delay," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 24, no. 4, pp. 320–327, 1976.

[43] K. C. Ho and W. Xu, "An accurate algebraic solution for moving source location using tdoa and fdoa measurements," *IEEE Transactions on Signal Processing*, vol. 52, no. 9, pp. 2453–2463, Sept. 2004.

[44] K. C. Ho, X. Lu, and L. Kovavisaruch, "Source localization using tdoa and fdoa measurements in the presence of receiver location errors: Analysis and solution," *IEEE Transactions on Signal Processing*, vol. 55, no. 2, pp. 684–696, 2007.

[45] B. R. Jackson, S. Wang, and R. Inkol, "Emitter geolocation estimation using power difference of arrival," *Defence R&D Canada Technical Report DRDC Ottawa TR*, vol. 40, 2011.

[46] K. C. Ho and M. Sun, "Passive source localization using time differences of arrival and gain ratios of arrival," *IEEE Transactions on Signal Processing*, vol. 56, no. 2, pp. 464–477, 2008.

[47] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[48] S. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*. Prentice-Hall, 1998, vol. 2.

[49] J. Lehtomäki, "Analysis of energy based signal detection," *Ph.D. dissertation, Faculty of Technology, University of Oulu, Finland*, vol. 2005.

[50] J. Benko, "A PHY/MAC proposal for IEEE 802.22 WRAN systems, part 1: The PHY," *IEEE 802.22-06/0004r1*, 2006. [Online]. Available: http://www.ieee802.org/22/Meeting_documents/2006_Mar/22-06-0004-02-0000_ETRI-FT-I2R-Motorola-Philips-Samsung-Thomson_PHY_Spec.doc

[51] H. Tang, "Some physical layer issues of wide-band cognitive radio systems," in *IEEE International Symposium on Dynamic Spectrum Access Networks*, 2005, pp. 151–159.

[52] M. Oner and F. Jondral, "Cyclostationarity based air interface recognition for software radio systems," in *IEEE Radio and Wireless Conference*, Sept. 2004, pp. 263–266.

[53] W. A. Gardner, "Signal interception: a unifying theoretical framework for feature detection," *IEEE Transactions on Communications*, vol. 36, no. 8, pp. 897–906, 1988.

[54] T. Yucek and H. Arslan, "Spectrum characterization for opportunistic cognitive radio systems," in *IEEE Military Communications conference*, 2006, pp. 1–6.

[55] M. Höyhtyä, A. Mämmelä, M. Eskola, M. Matinmikko, J. Kalliovaara, J. Ojaniemi, J. Suutala, R. Ekman, R. Bacchus, and D. Roberson, "Spectrum occupancy measurements: A survey and use of interference maps," *IEEE Communications Surveys Tutorials*, vol. 18, no. 4, pp. 2386–2414, 2016.

[56] M. Matinmikko, M. Mustonen, M. Höyhtyä, T. Rauma, H. Sarvanko, and A. Mämmelä, "Distributed and directional spectrum occupancy measurements in the 2.4 GHz ISM band," in *International Symposium on Wireless Communication Systems*, Sept. 2010, pp. 676–980.

[57] R. J. Matheson, "Strategies for spectrum usage measurements," in *IEEE International Symposium on Electromagnetic Compatibility*, 1988, pp. 235–241.

[58] W. innovation forum, "CBRS operational security technical specification," *WINNF-TS-0071 V 1.0.0*, 2017, Accessed Mar. 2018. [Online]. Available: https://workspace.winnforum.org/higherlogic/ws/public/download/4487/

[59] 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. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S187449071000039X

[60] M. Subhedar and G. Birajdar, "Spectrum sensing techniques in cognitive radio networks: A survey," *International Journal of Next-Generation Networks*, vol. 3, 07 2011.

[61] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of tv transmissions in support of dynamic spectrum sharing," in *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2005, pp. 338–345.

[62] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *IEEE International Conference on Communications*, vol. 4, 2006, pp. 1658–1663.

[63] H. Uchiyama, K. Umebayashi, Y. Kamiya, Y. Suzuki, T. Fujii, F. Ono, and K. Sakaguchi, "Study on cooperative sensing in cognitive radio based ad-hoc network," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Sept. 2007, pp. 1–5.

[64] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *IEEE International Symposium on Dynamic Spectrum Access Networks*, 2005, pp. 131–136.

[65] S. Joshi, K. B. S. Manosha, M. Jokinen, T. Hanninen, P. Pirinen, H. Posti, and M. Latva-aho, "Esc sensor nodes placement and location from moving incumbent protection in cbrs," in *Wireless Innovation Forum European Conference on Communications Technologies and Software Defined Radio*, 2016, p. 119âĂŞ125.

[66] T. T. Nguyen, M. R. Souryal, A. Sahoo, and T. A. Hall, "3.5 GHz environmental sensing capability detection thresholds and deployment," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 3, pp. 437–449, Sept. 2017.

[67] M. Clark and K. Psounis, "Designing sensor networks to protect primary users in spectrum access systems," in *Wireless On-demand Network Systems and Services*, 2017, pp. 112–119.

[68] M. Souryal, M. Ranganathan, J. Mink, and N. E. Ouni, "Real-time centralized spectrum monitoring: Feasibility, architecture, and latency," in *IEEE International Symposium on Dynamic Spectrum Access Networks*, Sept. 2015, pp. 106–112.

[69] M. Cotton, J. Wepman, J. Kub, S. Engelking, Y. Lo, H. Ottke, R. Kaiser, D. Anderson, M. Souryal, and M. Ranganathan, "An overview of the ntia/nist spectrum monitoring pilot program," in *2015 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2015, pp. 217–222.

[70] Z. M. Zheleva, R. Chandra, A. Chowdhery, P. Garnett, A. Gupta, A. Kapoor, and M. Valerio, "Enabling a nationwide radio frequency inventory using the spectrum observatory," *IEEE Transactions on Mobile Computing*, vol. PP, no. 99, pp. 1–1, 2017.

[71] I. Sobron, W. A. Martins, M. L. R. de Campos, and M. Velez, "Incumbent and LSA licensee classification through distributed cognitive networks," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 94–103, Jan 2016.

[72] V. Frascolla, A. J. Morgado, A. Gomes, M. M. Butt, N. Marchetti, K. Voulgaris, and C. B. Papadias, "Dynamic licensed shared access - a new architecture and spectrum allocation techniques," in *IEEE Vehicular Technology Conference*, Sept. 2016, pp. 1–5.

[73] C. Ghosh, C. Cordeiro, D. P. Agrawal, and M. B. Rao, "Markov chain existence and hidden markov models in spectrum sensing," in *2009 IEEE International Conference on Pervasive Computing and Communications*, March 2009, pp. 1–6.

[74] N. Wang, Y. Gao, F. Yang, Q. Bi, W. Xie, and C. Parini, "Energy detection-based spectrum sensing with constraint region in cognitive LTE systems," *Trans. Emerging Telecommunications Technologies*, vol. 28, no. 11, 2017.

[75] F. F. Digham, M. S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," in *Proceedings IEEE International Conference on Communications*, vol. 5, Anchorage, Alaska, USA, 2003, pp. 3575–3579 vol.5.

[76] M. Abramowitz and I. A. Stegun, “Handbook of mathematical functions with formulas, graphs, and mathematical tables,” in *National Bureau of Standards, Applied Math. Series 55*, Dover Publications, 1965.

[77] J. Mathews and K. Fink, *Numerical methods using MATLAB*. Prentice Hall, 1999.

[78] R. Hallahan and J. M. Peha, “Enabling public safety priority use of commercial wireless networks,” *Homeland Security Affairs 9, Article 13*, 2013, Accessed Jun. 2016. [Online]. Available: http://www.hsaj.org/articles/250

[79] T. Doumi, M. F. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, and D. Flore, “LTE for public safety networks,” *IEEE Communications Magazine*, vol. 51, no. 2, pp. 106–112, February 2013.

[80] ETSI, “3GPP public safety (individual to/from authority) communications,” *V0.0.4*, 2014.

[81] ——, “LTE for public safety (authority-to-authority) communications,” *V0.0.4*.

[82] ——, “LTE; mission critical services common requirements,” *ETSI TS 122 280 V15.3.0*, 2018.

[83] ETSI, “LTE;mission critical data over LTE,” *ETSI TS 122 282 V15.1.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/122200_122299/122282/15.01.00_60/ts_122282v150100p.pdf

[84] ——, “LTE; mission critical video over LTE,” *ETSI TS 122 281 V15.2.0*, 2018, Accessed Aug 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/122200_122299/122281/15.01.00_60/ts_122281v150100p.pdf

[85] ——, “Digital cellular telecommunications system (phase 2+) (GSM); universal mobile telecommunications system (UMTS); LTE; network architecture,” *ETSI TS 123 002 V15.0.0*, 2018, Accessed Nov. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123000_123099/123002/15.00.00_60/ts_123002v150000p.pdf

[86] 3rd Generation Partnership Project, “Technical specification group services and system aspects; study on isolated evolved universal terrestrial radio access network (E-UTRAN) operation for public safety,” *3GPP TR 22.897 V13.0.0*, 2014.

[87] ETSI, “Universal mobile telecommunications system (UMTS); LTE; isolated evolved universal terrestrial radio access network (E-UTRAN) operation for public safety; stage 1,” *ETSI TS 122 346 V15.0.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/122300_122399/122346/15.00.00_60/ts_122346v150000p.pdf

[88] ——, “Universal mobile telecommunications system (UMTS); LTE; mission critical push to talk (MCPTT) over LTE; stage 1,” *ETSI TS 122 179 V15.2.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/122100_122199/122179/15.02.00_60/ts_122179v150200p.pdf

[89] ——, “LTE; group communication system enablers for LTE (GCSE_LTE),” *ETSI TS 122 468 V15.0.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/122400_122499/122468/15.00.00_60/ts_122468v150000p.pdf

[90] ——, "LTE; group communication system enablers for LTE (GCSE_LTE); stage 2," *ETSI TS 123 468 V15.0.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123400_123499/123468/15.00.00_60/ts_123468v150000p.pdf

[91] ——, "LTE; general packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRAN) access," *ETSI TS 123 401 V15.4.0*, 2018, Accessed Aug 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123400_123499/123401/15.04.00_60/ts_123401v150400p.pdf

[92] ——, "Universal mobile telecommunications system (UMTS); LTE; multimedia broadcast/multicast service (MBMS); architecture and functional description," *ETSI TS 123 246 V15.0.0*, 2018, Accessed Aug. 2017. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123200_123299/123246/15.00.00_60/ts_123246v150000p.pdf

[93] ——, "Universal mobile telecommunications system (UMTS); LTE; proximity-based services (ProSe); stage 2," *ETSI TS 123 303 V15.1.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123300_123399/123303/15.01.00_60/ts_123303v150100p.pdf

[94] 3rd Generation Partnership Project, "Technical specification group services and system aspects; feasibility study for proximity services (ProSe)," *3GPP TR 22.803 V12.2.0*, 2013.

[95] ETSI, "Universal mobile telecommunications system (UMTS); LTE; proximity-based services (ProSe); security aspects," *ETSI TS 133 303 V15.0.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133300_133399/133303/15.00.00_60/ts_133303v150000p.pdf

[96] ——, "Digital cellular telecommunications system (phase 2+) (GSM); universal mobile telecommunications system (UMTS); LTE; policy and charging control signalling flows and quality of service (QoS) parameter mapping," *ETSI TS 129 213 V15.3.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/129200_129299/129213/15.03.00_60/ts_129213v150300p.pdf

[97] ——, "Universal mobile telecommunications system (UMTS); LTE; policy and charging control (PCC); reference points," *ETSI TS 129 212 V15.3.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/129200_129299/129212/15.03.00_60/ts_129212v150300p.pdf

[98] ——, "Digital cellular telecommunications system (phase 2+) (GSM); universal mobile telecommunications system (UMTS); LTE; policy and charging control architecture," *ETSI TS 123 203 V15.3.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123200_123299/123203/15.03.00_60/ts_123203v150300p.pdf

[99] B. Forum, "Policy convergence for next generation fixed and 3GPP wireless networks," *TR-300*, 2014, Accessed Dec 2017. [Online]. Available: https://www.broadband-forum.org/technical/download/TR-300.pdf

[100] ETSI, "LTE; universal mobile telecommunications system (UMTS); LTE; non-access-stratum (NAS) protocol for evolved packet system (EPS); stage 3," *ETSI TS 124 301*

V15.3.0, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/124300_124399/124301/15.03.00_60/ts_124301v150300p.pdf

[101] Elektrobit, "Enhancing the link network performance with EB tactical wireless IP network (TAC WIN)," *EB Defense Newsletter*, 2014, Accessed Nov. 2018. [Online]. Available: www.bittium.com/file.php?fid=785

[102] ETSI, "Monte carlo simulation methodology for the use in sharing and compatibility studies between different radio services or systems," *Report ITU-R SM.2028-2*, 2017.

[103] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE Journal of selected topics in Signal Processing*, vol. 2, no. 1, pp. 4–17, 2008.

[104] K. Lähetkangas, H. Saarnisaari, and A. Hulkkonen, "Licensed shared access system development for public safety," in *Proceedings European Wireless Conference*, Oulu, Finland, 2016.

[105] K. Lähetkangas, H. Posti, H. Saarnisaari, and A. Hulkkonen, "LSA system development with sensing for rapidly deployable LTE network," in *Proceedings 13th EAI International Conference on Cognitive Radio Oriented Wireless Networks*, Ghent, Belgium, 18-19 Sept. 2018.

[106] M. Palola, T. Rautio, M. Matinmikko, J. Prokkola, M. Mustonen, M. Heikkilä, T. Kippola, S. Yrjölä, V. Hartikainen, L. Tudose, A. Kivinen, J. Paavola, J. Okkonen, M. Makelainen, T. Hanninen, and H. Kokkinen, "Licensed shared access (LSA) trial demonstration using real LTE network," in *Proceedings 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Oulu, Finland, 2014, pp. 498–502.

[107] M. Palola, M. Matinmikko, J. Prokkola, M. Mustonen, M. Heikkilä, T. Kippola, S. Yrjölä, V. Hartikainen, L. Tudose, A. Kivinen, J. Paavola, and K. Heiska, "Live field trial of licensed shared access (LSA) concept using LTE network in 2.3 GHz band," in *Proceedings IEEE International Symposium on Dynamic Spectrum Access Networks*, McLean, VA, USA, 2014, pp. 38–47.

[108] (Accessed Nov. 2017) CORNET project web page. [Online]. Available: http://www.oulu.fi/cornet/

[109] M. Höyhtyä, K. Lähetkangas, J. Suomalainen, M. Hoppari, K. Kujanpää, K. Trung, T. Kippola, M. Heikkilä, H. Posti, J. Mäki, T. Savunen, A. Hulkkonen, and H. Kokkinen, "Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control," *IEEE Access*, 2018. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8550640

[110] A. Alshalan, S. Pisharody, and D. Huang, "A survey of mobile VPN technologies," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1177–1196, 2016.

[111] IEEE, "Virtual LANs," *IEEE 802.lQ*, 2005.

[112] K. Kompella and Y. Rekhter, "Virtual private LAN service (VPLS) using BGP for auto-discovery and signaling," 2007.

[113] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[114] 3rd Generation Partnership Project, "Technical specification group services and system aspects; telecommunication management; study on management and orchestration of network slicing for next generation network," *3GPP TR 28.801 V15.1.0*, 2018.

[115] ETSI, "Universal mobile telecommunications system (UMTS); LTE; service aspects; service principles," *ETSI TS 122 101 V15.6.0*, 2018.

[116] Motorola, "The future is now: Public safety LTE communications," *White Paper*, 2012, Accessed Jan 2018. [Online]. Available: https://www.motorolasolutions.com/content/dam/msi/docs/business/_documents/white_paper/_static_files/4g_lte_public_safety_communications_systems_white_paper2.pdf

[117] Nokia, "Enhance first responders' situational awareness with mobile broadband," 2017, Accessed Dec. 2018. [Online]. Available: https://onestore.nokia.com/asset/201467

[118] Motorola, "Response to australian productivity commission from motorola solutions australia," *Response letter*, 2015, Accessed Dec 2018. [Online]. Available: https://www.pc.gov.au/__data/assets/pdf_file/0017/190313/sub012-public-safety-mobile-broadband.pdf

[119] "Anonymity online," Accessed Nov. 2018. [Online]. Available: https://www.torproject.org

[120] "The invisible internet project," Accessed Nov. 2018. [Online]. Available: https://geti2p.net/

[121] E. Gamma, *Design patterns: elements of reusable object-oriented software*. Pearson Education India, 1995.

[122] Finnish ministry of transport and communications, "Viranomaisille laajakaistainen viestintäpalvelu virve-verkon tilalle," *press release*, 2018, Accessed Oct. 2018. [Online]. Available: https://www.lvm.fi/-/viranomaisille-laajakaistainen-viestintapalvelu-virve-verkon-tilalle-987114

[123] D. Mitton and M. Beadles, "Network access server requirements next generation (NASREQNG) NAS model," *Informational, RFC 2881*, 2000, Accessed Mar. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc2881

[124] P. Mockapetris, "Domain names - implementation and specification," *INTERNET STANDARD STD 13 RFC 1035*, 1987, Accessed Mar. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc1035

[125] 3rd Generation Partnership Project, "Technical specification group services and system aspects; 3g security; network domain security (NDS); IP network layer security," *3GPP TS 33.210 V15.1.0*, 2018.

[126] S. L. Thomas, "Backdoor detection systems for embedded devices," *Ph.D. dissertation, Faculty of , University of Birmingham, UK*, 2018, Accessed Dec. 2018. [Online]. Available: https://www.cs.bham.ac.uk/~garciaf/theses/badseed.pdf

[127] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J. Seifert, “Practical attacks against privacy and availability in 4g/lte mobile communication systems,” 2016. [Online]. Available: http://arxiv.org/abs/1510.07563

[128] K. Nohl, “Mobile self-defense,” *Chaos Communication Congress*, 2014, Accessed Nov. 2017. [Online]. Available: https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf

[129] 3rd Generation Partnership Project, “Technical specification group services and system aspects; 3GPP system architecture evolution (SAE); security architecture,” *3GPP TS 33.401 V15.5.0*, 2018.

[130] T. C. C. B. Group, “Critical communications and mobile network operators, options for new revenue streams and new market segments,” *White Paper*, 2018, Accessed Feb. 2019. [Online]. Available: https://tcca.info/fm_file/2018-may_critical_communications_mobile_network_operators-pdf/

[131] D. Kanakidis, E. Sdongos, A. Amditis, D. Lavaux, N. McCrone, J. Jackson, M. Tsagkaropoulos, J. Burns, T. Lavender, P. Tyczka, H. Gierszal, P. S. AntÃşnio, and M. Casoni, “The strategic roadmap for next generation (broadband) PPDR communication systems, reviewing users needs and technology evolutions towards recommendations for future critical communications policy making and technology migration,” *PPDR-TC White Paper*, 2016, Accessed Feb. 2019. [Online]. Available: http://inw.dei.unipd.it/wp-content/uploads/2017/01/PPDR-White-Paper.pdf

[132] J. S. Marcus, J. Burns, V. Jervis, R. Wählen, K. R. Carter, I. Philbeck, and P. Vary, “PPDR spectrum harmonisation in germany, europe and globally,” *Public Report*, 2010, Accessed Feb. 2019. [Online]. Available: https://www.cept.org/Documents/fm-49/1552/FM49_11_Info2_WIK_Report_PPDR_Spectrum_Harmonisation

[133] J. Stewart, M. Colville, and A. Bellis, “Award of 700MHz, 900MHz and 2.3GHz spectrum in denmark - spectrum for PPDR use,” *Report for the Danish Energy Agency*, 2017, Accessed Feb. 2019. [Online]. Available: https://ens.dk/sites/ens.dk/files/Tele/analysys_mason_-_final_report_on_ppdr.pdf

[134] S. Department of Finance and A. I. . D. G. Innovation, “Request for proposal for national public safety mobile broadband proof of concept (poc),” *Archived Tenders*, 2018, Accessed Feb. 2019. [Online]. Available: https://tenders.nsw.gov.au/dfs/?event=public.rft.showArchived&RFTUUID=A0BFBFF0-B999-6717-A0F1D3320BD7DBAF

[135] M. Jokinen, M. Mäkeläinen, and T. Hänninen, “Demo: co-primary spectrum sharing with inter-operator D2D trial,” in *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking*, New York, NY, USA, 2014, pp. 291–294.

[136] 3rd Generation Partnership Project, “Technical specification group radio access network; TDD operating band in the L-band for LTE,” *3GPP TS 36.753 V15.0.0*, 2017.

[137] ——, “Technical specification group radio access network; TDD 3300-3400 MHz band for LTE,” *3GPP TR 36.758 V15.0.0*, 2018.

[138] ——, “Technical specification group radio access network; evolved universal terrestrial radio access (E-UTRA); physical channels and modulation,” *3GPP TS 36.211 V15.4.0*, 2018.

[139] S. Shellhammers and G. Chouinard, “Spectrum sensing requirements summary,” *IEEE P802.22 Wireless RANs*, vol. 2006.

[140] ETSI, “Evolved universal terrestrial radio access (E-UTRA); physical layer; measurements,” *ETSI TS 136 214 V15.2.0*, 2018, Accessed Aug. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/136200_136299/136214/15.02.00_60/ts_136214v150200p.pdf

[141] 3rd Generation Partnership Project, “Evolved universal terrestrial radio access (E-UTRA); user equipment (UE) radio transmission and reception,” *3GPP TS 36.101 V16.0.0*, 2019.

[142] Electronic Communications Committee, “Compatibility between the mobile service in the band 2500-2690 MHz and the radiodetermination service in the band 2700-2900 MHz,” *ECC Report 174*, 2012, Accessed Mar. 2017. [Online]. Available: http://www.erodocdb.dk/Docs/doc98/official/Pdf/ECCRep174.pdf

[143] L. Anbieter, “SINR and signal to noise ratio,” Accessed Jul. 2019. [Online]. Available: https://www.lte-anbieter.info/technik/sinr.php

[144] CRFS, “RFeye node wideband intelligent spectrum system for remote distributed RF monitoring,” Accessed Nov. 2017. [Online]. Available: http://agc.com.br/files/media/67/54c68fbde6c26.pdf

[145] Anritsu Company, “Programming manual for spectrum master ms2722c, ms2723c, ms2724c, ms2725c, and ms2726c,” Accessed Nov. 2017. [Online]. Available: https://dl.cdn-anritsu.com/en-us/test-measurement/files/Manuals/Programming-Manual/10580-00278D.pdf

[146] K. Lähetkangas, H. Saarnisaari, and A. Hulkkonen, “Licensed shared access system possibilities for public safety,” *Mobile Information Systems*, pp. 1–12, 2016.

[147] K. Lähetkangas, H. Posti, H. Saarnisaari, and A. Hulkkonen, “Sensing LTE base stations with energy detectors for public safety,” *IEEE Transactions on Cognitive Communications and Networking, submitted*, 2018.

Original publications

I Lähetkangas K, Saarnisaari H and Hulkkonen A (2016) Licensed Shared Access System Possibilities for Public Safety, in Mobile Information Systems, vol. 2016, Article ID 4313527, pp. 1-12. URI: https://doi.org/10.1155/2016/4313527

II Lähetkangas K, Posti H, Saarnisaari H and Hulkkonen A. (2019) Sensing LTE Base Stations with Energy Detectors for Public Safety, submitted in IEEE Transactions on Cognitive Communications and Networking.

III Höyhtyä M, Lähetkangas K, Suomalainen J, Hoppari M, Kujanpää K, Trung K, Kippola T, Heikkilä M, Posti H, Mäki J, Savunen T, Hulkkonen A and Kokkinen H (2018) Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control, in IEEE Access, vol. 6, pp. 73572-73582. URI: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8550640

Original publications are not included in the electronic version of the dissertation.

Book orders:
Granum: Virtual book store
http://granum.uta.fi/granum/

UNIVERSITY OF OULU P.O. Box 8000 FI-90014 UNIVERSITY OF OULU FINLAND

ACTA UNIVERSITATIS OULUENSIS

UNIVERSITY of OULU
OULUN YLIOPISTO

ISBN 978-952-62-2393-3 (Paperback)
ISBN 978-952-62-2394-0 (PDF)
ISSN 0355-3213 (Print)
ISSN 1796-2226 (Online)