IoT Connectivity in Radar Bands: A Shared Access Model Based on Spectrum Measurements

Zaheer Khan, Janne J. Lehtomäki, Stefano Iellamo, Risto Vuohtoniemi, Ekram Hossain, and Zhu Han

Abstract

To address the challenge of more spectrum for the Internet-of-things (IoT) connectivity, this paper proposes a shared access (SA) framework with rotating radars. The proposed framework is based on the results of our measurement campaign in which we measured spectrum usage patterns and signal characteristics of three different ground-based fixed rotating radar systems near Oulu, Finland. In our work, we review different IoT protocols and their use of licensed or unlicensed spectrum. We make the case that IoT systems generate much data which cannot be accommodated with licensed/unlicensed spectrum, which already suffer from congestion. We identify the suitability of shared access between different rotating radars and IoT networks. We then present a zone-based SA framework in rotating radar spectrum for the operators providing IoT services, highlight its benefits, and also specify challenges in its implementation. To fully develop the considered zone-based SA method that ensures coexistence of IoT devices with no harmful interference to the rotating radars, we propose an Radio Environment Map (REM)-enabled architecture for the SA. The proposed architecture provides principles and rules for using the SA for the IoTs, and it does not require modifications in the incumbent radar systems.

Index Terms

Internet of things (IoT), radar bands, shared access, gateways, spectrum occupancy measurements, radio environment map (REM), database.

INTRODUCTION

The Internet of things (IoT) is regarded as the next stage in digital communications with a wide range of applications, such as tasked sensors, controllers, smart metering, security systems and industrial control [1], [2]. Communication is the 'glue' that binds all the sensors, actuators, management platforms and databases together to form the IoT. Wireless communications are the key to provide connectivity in the IoT, and as a result IoT can further congest the wireless networks. For the regulators, this means freeing up more spectrum for wireless communications at a time when we are already running out of frequency spectrum [1], [2].

Z. Khan, J. J. Lehtomäki, R. Vuohtoniemi are with the University of Oulu, Finland, S. Iellamo is with Institute of Computer Science at FORTH, Greece, E. Hossain is with University of Manitoba, Canada, and Zhu Han is with University of Houston, USA.

This work was funded by Academy of Finland under the grant number 26687 and in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC).

There is a plethora of new wireless technologies for IoT connectivity currently being developed. However, there is much uncertainty as to where spectrum might come from to efficiently support millions of connected devices once these technologies are deployed globally. The problem of spectrum scarcity in the wireless world has triggered regulators' interest in novel spectrum sharing mechanisms, which enable coexistence between distinct radio technologies and services. In terms of new spectrum sharing models, the potential use of shared access (SA) between radar and wireless communications systems has generated particular interest [3]. One reason for this interest is the fact that communications systems and radar systems jointly consume most of the highly desirable spectrum below 6 GHz [4], [5]. However, different works and reports have shown that existing sharing models either do not take into account the real spectrum usage of radar systems or they are often counter-productive to the goals of spectrum sharing in the radar bands [5].

To address the challenge of more spectrum for the IoT, in this paper, we present results of our measurement campaign and identify the suitability of frequency spectrum used by the rotating radars for providing connectivity to the IoT (sensors, actuators, and gateways) on the basis of a SA framework. Our contributions in this paper include the following:

- First, we present results of our measurement campaign in which we measured spectrum usage patterns and signal characteristics of different ground-based fixed rotating radar systems in Finland.
- Based on the measured/analyzed features of three different radar systems, we identify the suitability of measured frequency spectrum for providing connectivity to the IoT on the basis of SA. To the best of our knowledge, our study represents the first evaluation of more spectrum for the IoT under SA in the radar spectrum.
- We propose the use of a Radio Environment Map (REM) architecture as an enabler to provide SA to the IoT networks in frequency channels used by different rotating radar systems. REM is a cognitive tool which can be utilized to enhance the awareness of the IoT entities of their operational radio environment [6].

It is important to note that our work in [7] presented measurement results for the spectrum usage of a weather radar in the 5GHz band. Different from [7], in this work we present results for three different rotating radar systems. Each of the measured radars is used for a different application, operates in a different spectrum band and has channel bandwidth utilization between 10 to 30 MHz (see Fig. 2, for illustration). Moreover, different from [7], we identify the suitability of providing SA for the IoT in the frequency channels used by rotating radar systems, and also propose the use of an REM architecture as an enabler to provide SA.

The rest of the paper is organized as follows. We overview different IoT wireless technologies and their use of radio spectrum. Then, we present results of our measurement campaign and also provide the reasons for the suitability of SA for the IoT. To this end, we present a REM based SA framework before we conclude our work.

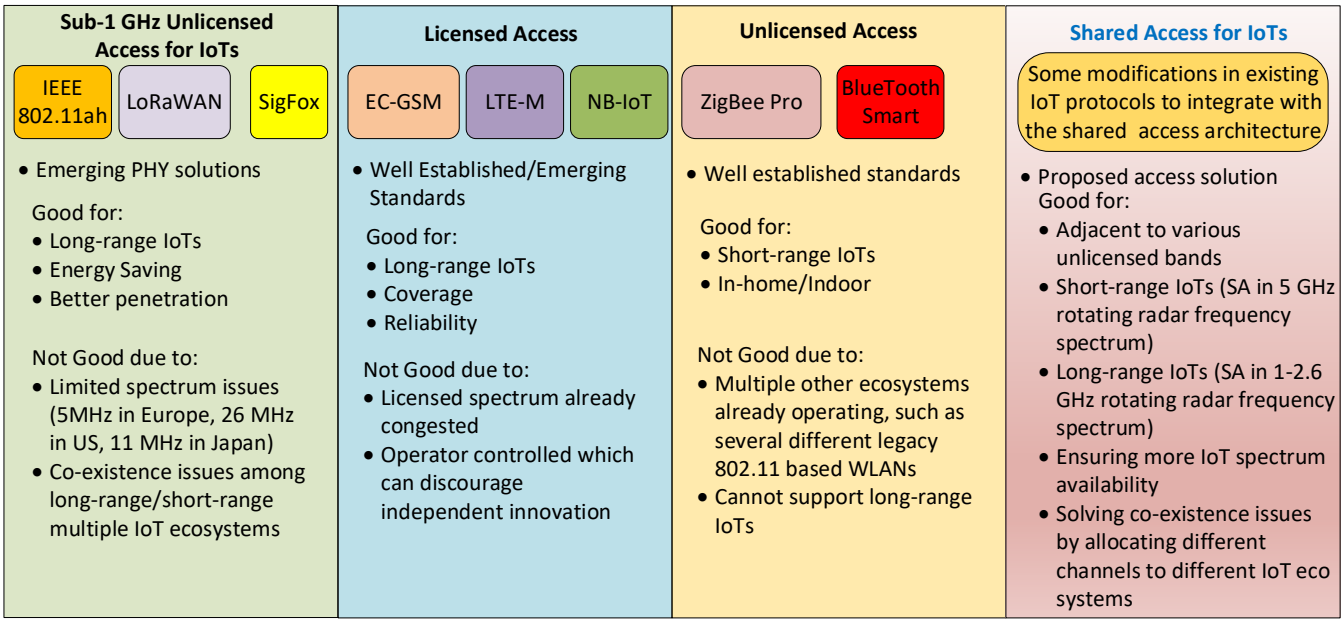


Fig. 1: Comparison of different wireless connectivity schemes for the IoT and their spectrum usage.

Different IoT Wireless Technologies and their Use of Radio Spectrum

Typically, the IoT can generate different spectrum demands. In terms of spectrum usage, in general, there are three alternative tracks for the IoT services: 1) Licensed spectrum; 2) Unlicensed spectrum; and 3) SA spectrum. In Fig. 1, we highlight and compare the different spectrum usage approaches for the IoT that are either currently being used or are under consideration for use to meet the needs of different types of IoT services.

Licensed Spectrum and IoT

Cellular networks operate on licensed spectrum and are being rapidly evolved with new functionalities to form an attractive solution for emerging low power wide area IoT applications. NB-IoT is a narrowband radio technology specially designed for the Internet of Things (IoT) and can be deployed in GSM and LTE licensed spectrum. Ericsson and Orange are testing EC-GSM (Extended Coverage GSM) using the 900 MHz licensed band, with the aim to enhance device reachability by up to 20 dB or seven-fold improvement in the range of low-rate applications. This extends the coverage of GSM to reach challenging locations such as deep indoor basements, where many smart meters are installed. LTE for machine to machine (LTE-M) is another cellular IoT solution which utilizes the licensed spectrum and is based on LTE [8].

Unlicensed/Sub-GHz Unlicensed Spectrum and IoT

In 2.4 GHz and 5 GHz unlicensed spectrum, Bluetooth Smart is a modified Bluetooth technology based protocol for IoT applications which require low power connectivity over short ranges of typically within two hundred metres. ZigBee PRO and ZigBee Remote Control are based on the IEEE802.15.4

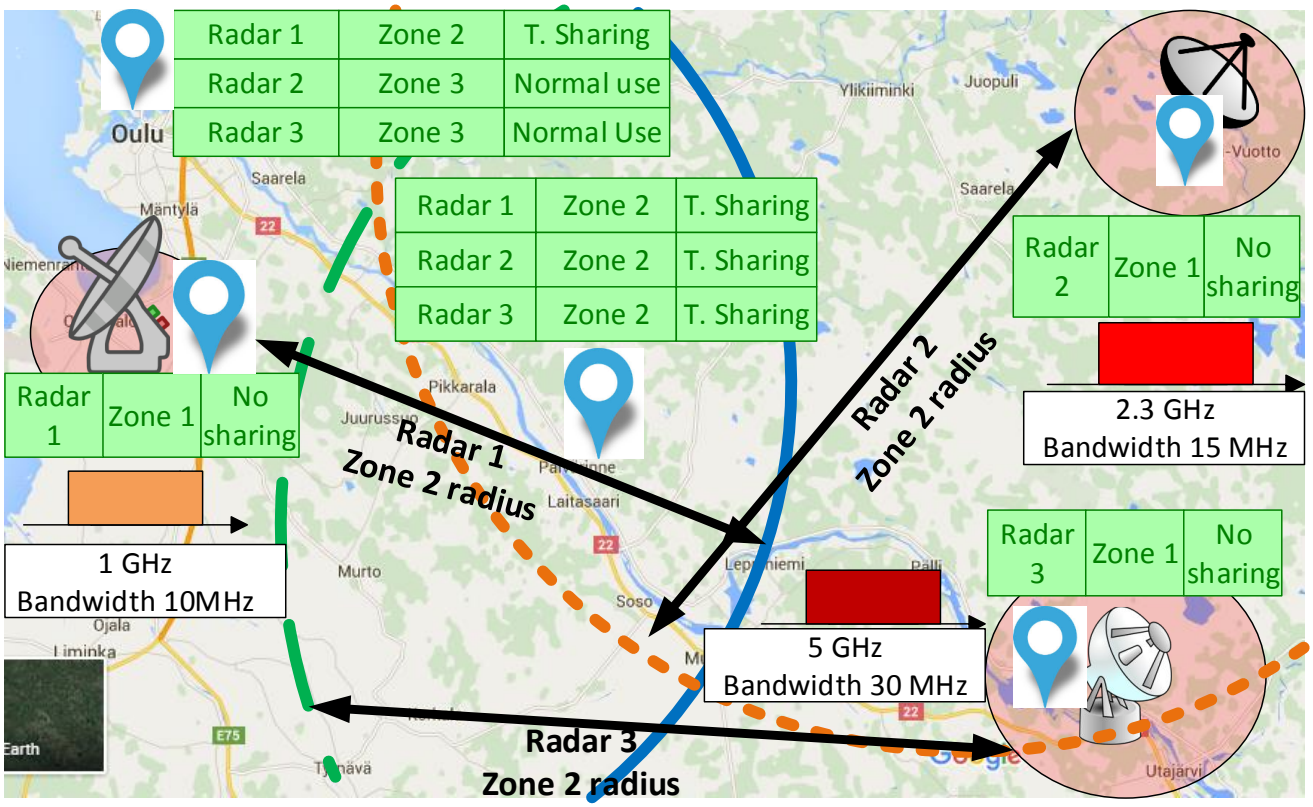


Fig. 2: Approximate locations, spectrum band utilization, bandwidth of each of the utilized channels, and different sharing zones at five different locations (blue location markers) for each of the three different radar systems measured by the authors. “T. Sharing" means temporal sharing.

protocol and use unlicensed spectrum for access. It target applications that require relatively infrequent data exchanges, low data-rates, and coverage of within a 100m range such as in a home or building.

The WiFi alliance is working on a new IEEE 802.11ah standard which can manage Low Power Wide Area Network (LPWAN) connectivity for IoT devices. IEEE 802.11ah intends to operate over a set of unlicensed radio bands in the sub-1 GHz unlicensed band. Some of the prominent features of the new IEEE 802.11ah are its energy saving mechanisms, its use of spectrum below 1 GHZ ensures wider coverage for LPWAN IoT. To power the IoT with new communication solutions independent IoT network groups have devised two different solutions for LPWANs which are called SigFOX and LoRaWAN. SigFox is a narrowband technology and uses a standard radio transmission method called binary phase-shift keying (BPSK). LoRaWAN looks at a wider amount of spectrum than SigFox [9]. Both LoRa and SigFox are planned to share spectrum with other solutions in the sub-1 GHz license-exempt bands.

Shared Access (SA) Spectrum and IoT

The total demand of thousands of IoT in a given area using heterogeneous access protocols can have significant effect on future radio spectrum use. The number of IoT devices and the nature of traffic will thus require far more frequency spectrum than is commercially available for them today. Given that radar

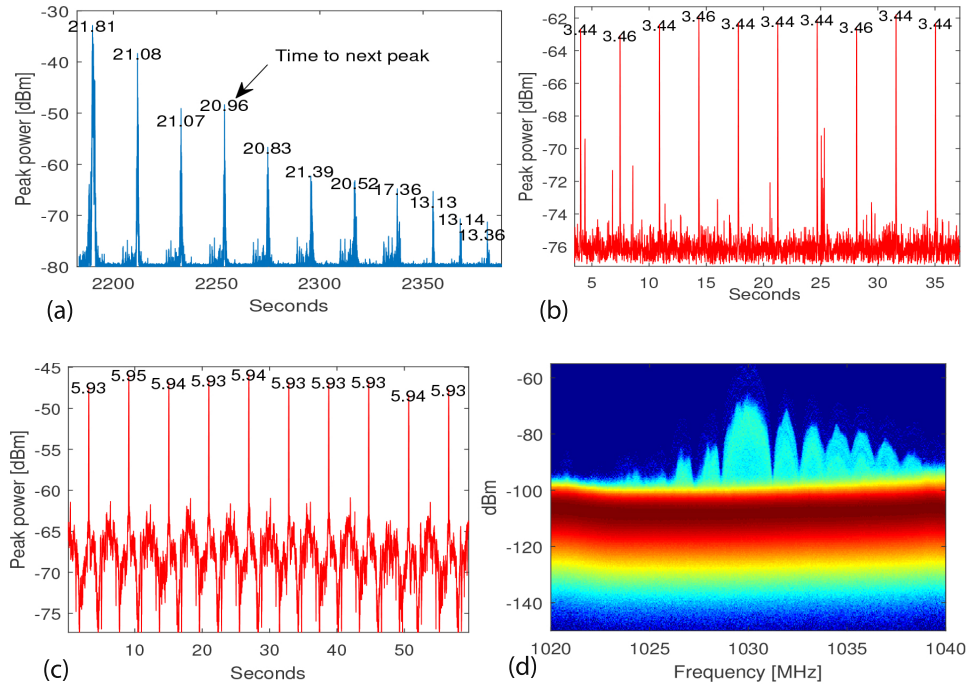


Fig. 3: Example measurement results showing the measured times between the main beam peaks of the three rotating radar systems, and the logarithmic two-dimensional spectrograms of the recorded power values of the airport surveillance radar signals.

bands are now also a potential candidate for sharing between wireless communication systems and radar systems [1], [4], [5], in the context of making available more spectrum, SA in radar spectrum for IoT is an important and useful idea.

In the next section, based on measurements of spectrum usage of different rotating radars, we will describe the suitability of rotating radar channels for wireless connectivity of the IoT devices.

Measurement Results, Zone-Based SA, and the Suitability of the SA for IoT

Measurement Strategy, Setup, and Results

The rotating radars that operate in different bands have highly directional rotating antennas and provide coverage of applications over a large area (e.g., they can have a range of 150-200 km). The presented measurement results in this section include spectrum usage behavior of three ground-based fixed rotating radar systems in Finland: a weather radar system in the 5.6 GHz band, uplink of an airport aircraft surveillance radar system in the 1.03 GHz band, and a surveillance radar in the 2.3 GHz band. These radars transmit a narrow beam and they perform more listening than talking. For example, a weather radar may emit a pulse for 2 μs then listen for approximately 2 ms. They rotate to scan horizontally 360 degrees, and some of them also tilt vertically. In Fig. 2, we illustrate approximate locations, spectrum band utilization, and the utilized channel bandwidths for each of the three different radar systems measured by the authors near the city of Oulu. Measurements were performed with an Agilent N6841A RF sensor

connected to a wideband, omnidirectional antenna (ARA CMA-118/A) [10]. For both surveillance radars, the measurements were based on recording continuous (no time domain gaps) stream of I/Q samples. The sampling rate was (depending on the scenario) 2 MHz, or 10 MHz, leading to the minimum time resolution of 0.5 μs. For weather radar case, measurements were based on recording continuous stream of FFT processed outputs (with 20 MHz sampling rate). Each measurement duration was more than 50 minutes at each location.

In Figs. 3a-3c, we present the measured times between main beam peaks of the three rotating radar systems operating in the three different spectrum bands. The three figures also illustrate the received peak power as a function of time in seconds. It can be seen in the three figures that there are pauses in the received signal from the radar, due to its antenna rotation. When the rotating radar's main scan beam points to the measurement locations, a signal peak is received. It can also be seen from the figures that while the radar's pulse interval, i.e., the time between two consecutive pulses received at the same location, are constant (Figs. 3b and 3c) for the measured surveillance radars, however, they are not constant for the weather radar. The pulse intervals of the surveillance radars in Figs. 3b and 3c are periodic with pauses of 3.44 and 5.93 seconds between the scan pulses, however, the pulse intervals of weather radar are quasi-periodic with pauses between the scan pulses that vary from 13.1 seconds to 21.1 seconds. This is due to the reason that the measured radar has two scanning modes: 1) The normal-mode with pulse repetition frequency (PRF) 570 Hz, pulse duration 2 μs, rotation speed 16.9 degrees/s, lowest elevation angle 0.3 degrees. 2) The dual-mode with dual-PRF 900/1200 Hz, pulse duration 0.8 μs, rotation speed 26.7 degrees/s, lowest elevation angle 0.4 degrees.

Figs. 3a-3c also show that, while the received peak power for the two surveillance radars does not vary significantly, for the weather radar, the received power varies over a period of time. The reason for this received peak power variation is that unlike the two surveillance radars, the weather radar scans horizontally 360 degrees at different vertical angles. For the weather radar, the highest received peak power in Fig. 3a are obtained when the radar directs its beam downward to the measurement location. In Fig. 3d, we present logarithmic two-dimensional spectrograms of the recorded power values of the airport surveillance radar signals.

SA in Radar Spectrum

Our measurement results show that there are pauses in the received signal from each of the three rotating radars, due to their antenna rotation (see Figs. 3a-3c). This offers the potential of low power IoT devices to use Zone-based SA in the radar bands [7], [11]. Different from this work, the potential of zone-based SA in the context of small cell networks has been explored by [11], [12].

Previous works in [4] and [5] have proposed the use of large exclusion zones in which the radii of exclusions zones vary, depending on the specific site, between 72 and 121 kms. This model may guarantee 100% protection to the radars; however, different works and reports have shown that large geographic

exclusion zones are unnecessary and counter-productive to the goals of spectrum sharing in the radar bands. In our work, the three different zones around a radar are modeled as follows: At a distance of few kilometres from a rotating radar system a network of sensor devices are deployed in a circle around the radar station. Our measurement results show that for the measured radars approximately within 2 to 3 kms even the the sidelobe signal from the radar can be strong enough to interfere with the wireless communications. So it is suitable for both the radar system and the wireless communication systems to have the radius of Zone 1 of approximately 3 to 4 kms. Due to this reason we call the Zone 1 as the exclusion zone (Zone 1) as any secondary transmissions are forbidden in this zone. The minimum distance from which the aggregate received signal strength at the radar does not exceed a minimum threshold value (defined by a regulatory body) can be used to establish the starting point for the Zone 3 region. This distance needs to be calculated by a regulatory body using extensive measurement campaigns. In Zone 3, the users are free to use the spectrum, as they are outside the interference area of the radar. Finally, in between the Zone 1 and the Zone 3 is Zone 2. In Zone 2, only temporal sharing is allowed in which network is not allowed to transmit during the time when the radar's main beam is pointing to it, and is also not allowed during the guard interval before and after that time period. To avoid any possible interference with the side lobes of a radar, when sensor devices detect aggregate received signal strength exceeding a critical threshold value (defined by a regulatory body), they notify the REM repository, which in turn instructs the IoT gateways to move some of their users to another channel to avoid any possibility of interference. It is easy to see that compared to the GEZ models of [4] and [5], the use of opportunistic temporal spectrum in our Zone-based model allows higher number of secondary user transmissions with the same level of interference protection to the radar system.

In the next section, based on the analyzed features of different rotating radar systems, we will present a REM architecture as an enabler to provide shared wireless access for the IoT devices.

Reasons for Suitability of Zone-based SA, Implementation Challenges, and Spectrum Goodness

In Table I, we provide six reasons for the suitability of zone-based SA for the IoT devices, and also present challenges involved in the implementation of SA in the radar channels. It is also important to identify which rotating radar channels are suitable for which IoT applications. For example, in a given area, a Zone 3 radar channel can be more suitable for applications that are intolerant to delays, whereas delay-tolerant applications can use a Zone 2 radar channel with little or no degradation in performance. In Table I, we also present spectrum goodness metrics that can be utilized for finding a suitable SA channel for an IoT application.

ENABLING IOT CONNECTIVITY THROUGH REMS

The general concept of REM was first introduced by [6]. In [6], REM is defined as a network entity which enhances the awareness of cognitive radios by providing them information about their

TABLE I: Six reasons for the zone-based SA suitability in frequency channels used by different rotating radars, implementation challenges, and spectrum goodness metrics for IoT applications

Features	Benefits for the operators providing IoT services	Challenges in implementation
Rotating radars operate in various higher and lower frequency spectrum.	To avoid inter-system interference. operators can connect long-range networks for IoT in lower frequency spectrum, and short-range IoT systems in higher frequency spectrum.	Careful design of SA connectivity for the multitude of IoT ecosystems and their appropriate frequency spectrum selection.
Heterogeneous sharing zones due to distinct locations of radar systems.	An operator can allocate networks of delay-tolerant IoT devices to the shared spectrum of Zone 2 radar, and delay-intolerant IoT devices to the shared spectrum of Zone 3 radar.	Appropriate SA IoT allocation design that takes into account delay tolerance/delay intolerance of IoT applications.
Surveillance radars with periodic scanning period	Periodic SA for the gateways and the IoT devices	i) Database assistance for any change in scanning pattern over longer periods. ii) Design of appropriate guard intervals for radar's protection.
Radars with quasi-periodic scanning periods	Quasi-periodic scanning weather radars, have longer scan pulse intervals (between 13 to 22 seconds), and can provide longer communication intervals.	Regular database assistance for any change in scanning and careful design of transmission/quiet periods.
In general, radio navigation frequency reservations are almost similar across the globe.	Operators can have the possibility of designing unified standards under SA for the IoT devices.	Coordination across different regulatory bodies across the globe.
Typically, single radar system per channel, wide coverage area, and co-located transmitter/receiver.	Database-assisted SA systems that require less interaction with the IoT networks.	Design of appropriate database technology.

Type of IoT application	Goodness metric	Explanation
Delay-tolerant	$B_f 1_{[f_{min} \leq f_a \leq f_{max}]}$	Amount of radar channel bandwidth B_f, and its frequency f_a is within radio range requirements of a particular IoT.
Delay-sensitive (time important but not critical)	$B_f 1_{[f_{min} \leq f_a \leq f_{max}]}(d_0/d)$	Along with bandwidth B_f and the frequency range, one needs to also take into account the desired time scale of packet arrival d_o, and its actual delay d.
Delay-intolerant	$B_f 1_{[f_{min} \leq f_a \leq f_{max}]} 1_{[d<d_{max}]}$	Along with bandwidth B_f and the frequency range, actual packet delays d not exceed the defined maximum delay d_{max}.

radio environment. The provided information includes: device locations and their activities, policies and regulation to access spectrum, and other information.

Role of the Gateways

In the proposed REM architecture (Fig. 4), the IoT gateways are used to act as a transparent bridge relaying messages between end-devices and an REM repository server in the back-end. Although internet-connected smart phones and tablets can be used as gateways to collect/transfer data from/to IoT devices, for the IoT to encompass millions of devices, the gateways would be required to operate on a much larger scale. The gateways would require less human intervention to collect and transmit data. To this end, the gateways will be included in hubs for smart homes, into industrial equipment for purposes of tracking and asset management. In general, on one side, the gateways will communicate via wireless technology down-stream and up-stream with the small IoT devices. On the other side, the gateways will be wirelessly

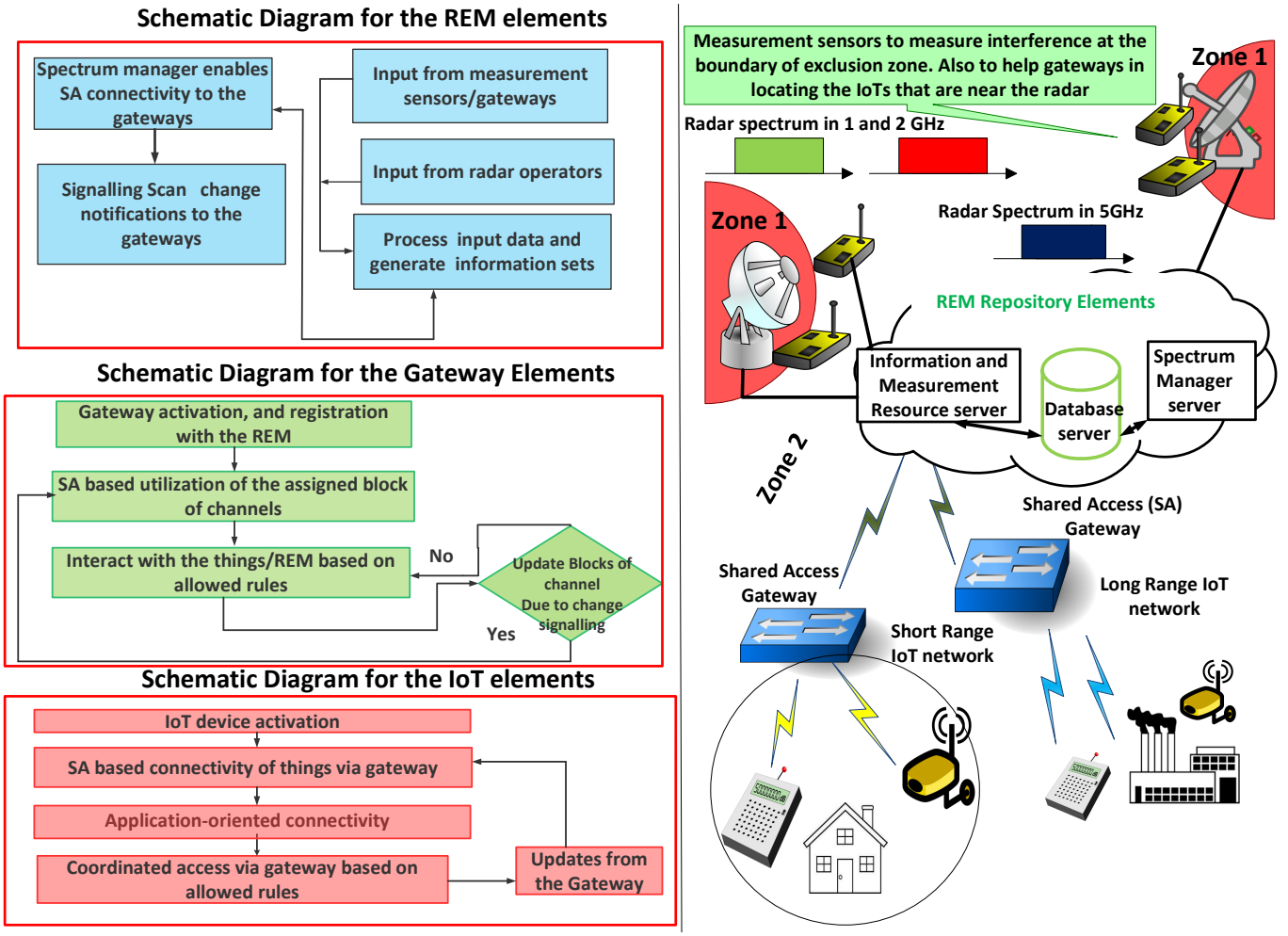


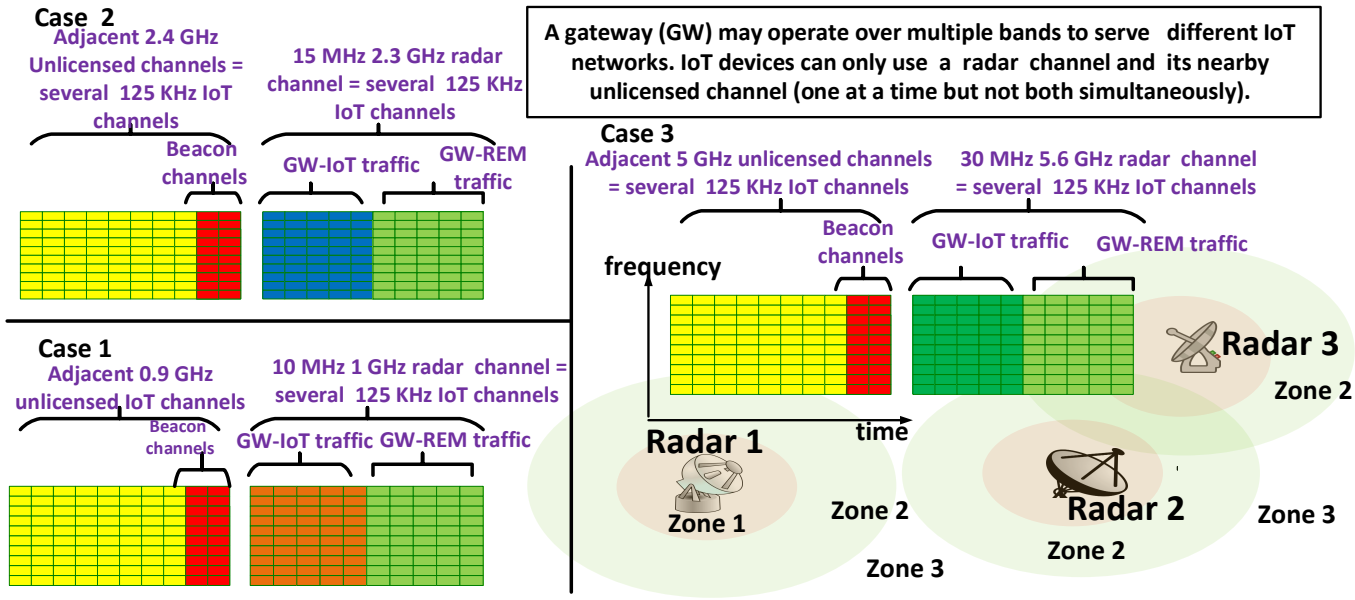
Fig. 4: Different components of the proposed SA architecture and the simplified high level schematic diagrams for different components involved in the proposed architecture.

connected further upwards to the REM server.

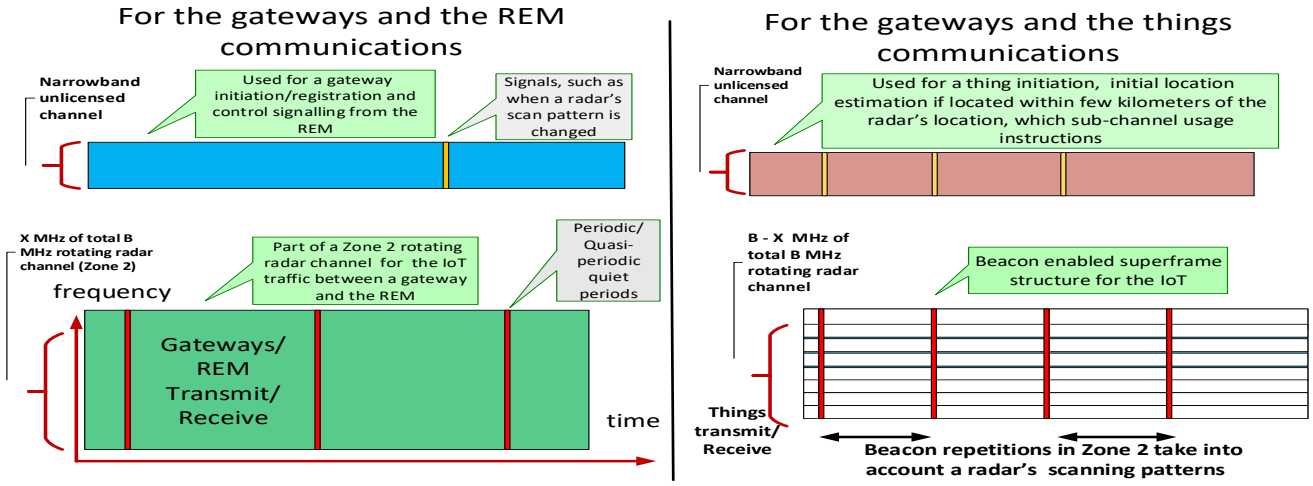
The Proposed Architecture

The novel aspects of our proposed SA architecture relate to the access and operation in both various radar channels and adjacent unlicensed bands to these channels. It is good for our proposal that the unlicensed bands are close to/adjacent to several radar bands. There are already IoT devices that are operating in different unlicensed frequency spectrum. This means that basically same front end with some modifications can be used for our proposed framework.

The proposed architecture can be divided into four components (see Fig. 4): 1) REM repository; 2) Different radar operators; 3) Measurement capable devices (MCD), such as a network of interference measurement and location estimation sensors, which are deployed at the boundary of a radar's exclusion zone; 4) IoT network entities, such as gateways and the IoT devices. In our proposed framework, the REM repository is a collection of resources that can be accessed by the IoT gateways. The REM repository



(a)



(b)

Fig. 5: Examples of beacon and traffic channel blocks for the proposed SA for IoT devices.

consists of: 1) an Information and Measurement Resource Module (IMRM); 2) a database module (DM); and 3) a spectrum manager (SM).

In Fig. 4 we present simplified high level block diagrams for different components involved in the proposed REM-based SA architecture for IoT. Next we explain the components of the proposed architecture.

The REM repository elements

i) Information and Measurement Resource Module (IMRM):

- *(Input from the radar operators)* The IMRM module of the REM repository takes low-overhead static and dynamic information from different radar operators as input. *The static (one time) information*

includes: 1) location of a radar system; 2) a particular radar system allows temporal sharing or not, and an exclusion zone established by a regulatory body to prohibit secondary transmissions in a specific area around a radar; 3) a reference power threshold to ensure that a secondary network entity does not fall into the exclusion zone; 4) The rotation rate of a radar. Also the time radar's rotating main beam spends at a reference point. *The dynamic information includes*: 1) Any change in scan speed of radar systems that are periodic/quasi-periodic rotating radars. A low-overhead message using few bits can be utilized by a radar system operator to provide information about scan change notifications. Note that this does not require any changes in the operation of a radar system itself.

- *(Input from measurement sensors/gateways)*
  - *Information about the radio environment:* The sensors collect information about the interference environment. For example, a sensor network deployed at the boundary of the Zone 1 of a radar can particularly facilitate interference free temporal sharing in Zone 2 with the radar. By deploying interference measurement sensors, an operator can know when and where the reference power threshold (defined by a regulatory body) is exceeded, if any, due to aggregate transmissions of the IoT entities. In the case of aggregate power received at the sensors exceeds the threshold, the REM repository instructs the gateways to move some of its users to another channel. The REM also uses the Zone 1 sensors and the gateways (that are located near the Zone 1) to perform *sensor-gateway triangulation* for the location estimation of the IoT devices. The location estimation near Zone 1 helps determine whether an IoT devices is within the exclusion zone or outside it. If the device is within Zone 1 then it can only use unlicensed channels, else it can use the rotating radar channels adjacent to the unlicensed channels.

ii) Database Module (DM): The DM module processes information from the IMRM module and generates instruction sets for the IoT gateways operating in the area. Based on the processed information from IMRM, it lists channels that are available in an area for sharing, and also lists rules of sharing for a particular channel.

The instruction set generation at the DM provides a secure way of ensuring sharing with such radar systems, as the access is controlled and managed by a trustworthy authority (cellular/IoT operator) which is authorized to operate in a given area by an official regulatory body.

iii) Spectrum Manager (SM): The SM on one side interacts with different gateways, such as it interacts with a gateway when its activated to collect its location information, and transmission power characteristics, and on the other side, it collects generated instructions from the DM. It then processes the obtained two-sided information and notifies the gateways about which portion of spectrum is available to them for utilization.

The gateway elements

i) Gateway activation/registration: Depending on how many different applications it can serve, a

gateway can operate over multiple bands or a single band. For example, if a gateway is deployed by a residential home, it may require only short range IoT connectivity, and hence may operate only in the higher 5 GHz bands. On the other hand, if a gateway is deployed by an operator to provide connectivity in a given area, it may be required to provide long range and/or short range connectivity to a variety of different IoT applications. Hence, it may be required to operate over multiple bands.

When activated, a gateway, in order to obtain channel access authorization, needs first to register with the SM module. This procedure can be carried out as follows: an unlicensed channel adjacent to a rotating radar channel is partitioned into several subchannels of 125 KHz bandwidth. A small set of these subchannels, called beacon channels, is used for the beacon transmissions (see Fig. 5). On activation, a gateway first listens to one of these beacon channels and registers with the REM repository. The registration of a gateway involves providing its location information, and transmission power characteristics in order for the list of available/forbidden channels to be computed.

ii) SA based utilization of the channels: The gateway obtains from the REM repository a list of available channels, which is a set of unlicensed channels and available radar channels, and also obtains the rules for sharing in each of the available channels. Each of the available unlicensed/radar channels, whose bandwidth may vary between 10-30 MHz, is partitioned into several subchannels of 125 KHz bandwidth. A set of these subchannels is utilized by the gateway to communicate with the REM repository, and the other subchannels are utilized to communicate with the IoT devices (see Fig. 5 for illustrative examples).

The things elements

At a given time, an IoT device can operate only over a single radar channel or an adjacent unlicensed channel but not both. Each gateway continuously transmits information, such as its identification number (ID), on the beacon unlicensed channels adjacent to the radar channels on which it can operate. When the signal is picked up by a nearby IoT device, which is just initiated, it responds to the signal. The gateway selects a set of subchannels for exchanging traffic with the IoT device. When the radar channel is not available in the area the gateway selects this subchannel set from the unlicensed channel adjacent to the radar channel, otherwise it selects the set from the radar channel.

Superframe-based Communication Format:

On a radar channel, the communication format consists of a periodic/quasi-periodic superframe. The superframe starts with a beacon signal transmitted by a gateway (See the beacon signals on the right of the Fig. 5b). More than one gateway in an area can transmit beacon messages at the same time and avoid interference by using a spread spectrum radio modulation used in existing IoT protocol like LoRaWAN [9]. The beacon signal notifies the IoT devices about the beacon repetition rate, i.e., when to listen for the next beacon, communication period message which notifies the length of the period after the beacon signal during which the devices can transmit/receive their traffic (for the illustration, see Fig. 5b).

In a Zone 3 radar channel, the superframe duration can be adjusted to any length suitable for the

network. In a Zone 2 periodic radar channel, such as the radars in the 1 GHz and the 2.3 GHz, the beacon can be transmitted to the devices after the radar's main beam leaves the slice in which the network is located. The network stays quiet during the time the radar's main beam spends on the slice T_s and also during the guard intervals time T_g before and after that slice. This means that if the radar's main beam points every T_r seconds at the slice, then a superframe of length $T_r - T_s - 2T_g$ can be utilized for the IoT traffic. For example, with $T_s = T_g = 0.5$ seconds this can be equal to $T_r - 1.5$ seconds.

In a Zone 2 quasi-periodic radar channel, such as the radar in the 5 GHz (see Fig. 3a), the time T_r can vary over different periods. To take into account of this quasi-periodicity due to the slow scan mode and the fast scan modes of the radar, the length of the superframe can be set to be $min(T_r) - T_s - 2T_g$ for the IoT traffic.

CONCLUSIONS AND FUTURE DIRECTIONS

Radar bands are a potential candidate for spectrum sharing between wireless communications and incumbent systems. To better understand the operating principles of various rotating radars which operate in different spectrum bands, and to determine their spectrum usage patterns, we ran an extensive measurement campaign near the city of Oulu in Finland. During the campaign, the spectrum usage behavior of three ground-based fixed rotating radar systems at different locations was measured. Based on the measurement results, in this paper, we identify the suitability of the rotating radar spectrum for the IoT shared spectrum access. We present reasons for the proposed SA suitability, identify related implementation challenges, and discuss spectrum goodness metrics for IoT applications. We also propose a framework that enables SA for the IoT devices through REMs. For potential future work, this research can be extended to explore the challenges in the implementation of the proposed REM-based SA in the rotating radar's channels. Challenges such as the required number of measurement sensors to support the REM, update rate of the REM, its algorithmic complexity, and security issues. The prototype can also be developed to enable SA through REMs for the IoT connectivity.

REFERENCES

[1] H. R. Schindler, J. Cave, N. Robinson, V. Horvath, P. J. Hackett, S. Gunashekar, M. Botterman, S. Forge, and H. Graux, "Europe's policy options for a dynamic and trustworthy development of the Internet of Things," Tech. Rep., 2013, Accessed on: 17-10-2016. [Online]. Available: http://www.rand.org/pubs/research_reports/RR356.html

[2] S. Forge, "Radio spectrum for the internet of things," Tech. Rep., 2016, Accessed on: 17-10-2016. [Online]. Available: {http://www.emeraldinsight.com/doi/abs/10.1108/info-11-2015-0050}

[3] Federal Communications Commission, "Enabling Innovative Small Cell Use In 3.5 GHz Band NPRM & Order," *Docket 12-148*, 2012, Accessed on: 17-10-2016. [Online]. Available: https://www.fcc.gov/document/enabling-innovative-small-cell-use-35-ghz-band-nprm-order

[4] CSMAC Committee, "Interference and Dynamic Spectrum Access," National Telecommunications and Information Administration (NTIA), USA, Tech. Rep., November, 2010, Accessed on: 17-10-2016. [Online]. Available: {https://www.ntia.doc.gov/files/ntia/publications/csmac_interferencecommitteereport_01102011.pdf}

[5] M. Cotton, M. Maior, F. Sanders, E. Nelson, and D. Sicker. (March, 2012) Developing Forward Thinking Rules and Processes to Fully Exploit Spectrum Resources: An Evaluation of Radar Spectrum Use and Management. Accessed on: 17-10-2016. [Online]. Available: {http://www.its.bldrdoc.gov/publications/2669.aspx}

[6] Y. Zhao, "Enabling cognitive radios through radio environment maps," Ph.D. dissertation, Virginia Tech, USA, 2007, Accessed on: 17-10-2016. [Online]. Available: https://theses.lib.vt.edu/theses/available/etd-05212007-162735/

[7] Z. Khan, J. J. Lehtomäki, R. Vuohtoniemi, E. Hossain, and L. A. DaSilva, "On opportunistic spectrum access in radar bands: Lessons learned from measurement of weather radar signals," *IEEE Wireless Communications Magazine*, vol. 23, no. 3, pp. 40–48, 2016, Accessed on: 17-10-2016.

[8] Nokia, "LTE-M: Optimizing LTE for the Internet of Things," White Paper , Tech. Rep., 2015, Accessed on: 17-10-2016. [Online]. Available: https://iotfuse.com/wp-content/uploads/2016/02/nokia_lte-m_-_optimizing_lte_for_the_internet_of_things_white_paper.pdf

[9] Technical Marketing Workgroup, "LoRaWAN: What is it?" LoRa Alliance, Tech. Rep., 2015, Accessed on: 17-10-2016. [Online]. Available: https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf

[10] Agilent Technologies, "Agilent radar measurements," Application Note, Tech. Rep., 2014, Accessed on: 17-10-2016. [Online]. Available: http://cp.literature.agilent.com/litweb/pdf/5989-7575EN.pdf

[11] M. Tercero, K. Sung, and J. Zander, "Temporal secondary access opportunities for WLAN in radar bands," in *Proceedings of the 14th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2011, pp. 1–5, Accessed on: 17-10-2016.

[12] F. Hessar and S. Roy, "Spectrum sharing between a surveillance radar and secondary wifi networks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 52, no. 3, pp. 1434–1448, June 2016, Accessed on: 17-10-2016.