Radio spectrum for the internet of things

Simon Forge

Simon Forge is Director at SCF Associates Ltd., Princes Risborough, UK.

Abstract

Purpose – *The aim of this paper is to consider whether it is possible to identify the future spectrum bands most suitable for the Internet of Things (IoT) from the operating factors of a novel set of radio services for a very wide range of applications, as an aid to policy makers now facing decisions in this area.*

Design/methodology/approach – *The approach uses characteristics of spectrum bands against the applications' requirements to focus on specific major traits that can be matched.*

Findings – *The main choice factors for spectrum are the practical application needs and the network cost model, and these are fairly useful as matching parameters. It is forecast that multiple bands will be needed and that these should be of a licence-exempt form to seed the unfettered innovation of IoT technologies and pre-empt the formation of significant market power by concerned interests.*

Practical implications – *The way in which spectrum is allocated today will need to be reconsidered, in the light of evolving IoT requirements, which will have increasing economic and social impacts. Policy recommendations for IoT spectrum demands are outlined, and key policy options to ensure a dynamic and trustworthy development of the IoT are put forward. For instance, regulatory barriers globally will need to be removed.*

Originality/value – *Current interests in the technical requirements of the IoT have not yet given a suitable analysis of the potential spectrum uses, because too often, it is assumed that previous models of spectrum allocation will continue in the future, without consideration of the economic pressures and social context.*

Keywords *Public policy, Communication technologies, Internet of things, Standards, Radiofrequencies*

Paper type *General review*

1. Introduction

Our economy and society will increasingly come to rely on the Internet of Things (IoT). The IoT, however, is not just a single complex system like the current Internet, rather it is a collection of autonomous or semi-autonomous networked systems, linking many independent agents. A key foundation for this new infrastructure will be radio communications, and this radio network dependence has policy implications for spectrum management. Our future society may expect to see a critical dependence on the IoT, but only if it can be trusted. That requires the IoT to not just be inherently stable and resilient but also affordable, ubiquitous globally and freely open to new uses and users. Thus, IoT spectrum requirements will form a growing part of future radio spectrum policy.

Significantly, we are now at a key point of decision. A major upheaval occurred in 2012 at the World Radiocommunication Conference (WRC-12). Certain countries requested the release of the 700 MHz band from broadcast services to use for mobile and other purposes. The use of this band for IoT radio communications raises critical questions and new opportunities. Moreover, the debate on spectrum utility is moving to higher frequencies for small cell networks, termed "5G", in the millimetric bands and those between ultra high

Received 16 November 2015
Revised 16 November 2015
Accepted 16 November 2015

frequency (UHF) and millimetric as a part of the WRC-15 and future WRC-19 debates. This opens a wider debate over IoT spectrum use and the possible frequencies, both lower and very high in the spectrum, despite various uncertainties today over 5G.

2. Finding radio spectrum for the IoT is essential

If we consider all applications that rely on the radio spectrum today, the greater part in terms of social and economic impact are mobile communications and also broadcast digital TV (DTV), digital terrestrial TV (DTT)[1] and satellite. Both are centred largely on the UHF range, with some radars, specialist satellite, microwave links and navigational aids positioned in this band. But many are sited far above UHF, for instance, radars at 5 GHz and microwave links in the 20 to 40 GHz ranges.

Below the UHF range, there are numerous private mobile radio networks for utilities logistics vehicles and so on, as well as the ubiquitous amplitude modulated (AM) and frequency modulated (FM) radio services in the very-high-frequency (VHF) bands with diverse navigational aids. Further down at the low-frequency end are global communications to submarines and other special military services, such as over the horizon radars (the previous Russian Woodpecker system in the Ukraine for instance), as well as in-mine communication systems. In general, radio is becoming a far more important part of the economy (Kende, 2012), especially with the evolution of IoT applications.

Finding the spectrum for the IoT will be a major challenge. Society will increasingly rely on the IoT, but it is not just a single complex system like the Internet, rather it is a collection of autonomous or semi-autonomous complex networked systems, with many independent agents. This is important, as spectrum management that supports the IoT deserves an open, balanced and fair approach that will benefit society and the economy. In contrast, poor IoT spectrum management would threaten the development of a key component of our future infrastructure, by stifling competition and open access to the spectrum needed. At the moment, many IoT initiatives are turning to existing spectrum allocations in the instrument, scientific and medical (ISM) bands. This paper considers what could be the allocations to IoT in consideration of its economic importance and the innovative preplanning of the traditional spectrum allocations, now underway in the world's spectrum fora.

Following the second digital dividend (DD2)[2] developments at WRC-12, the management of the radio spectrum in the series of WRC meetings in 2015 and 2019 presents new opportunities, not just challenges to the status quo. Re-organising the global attribution of key swathes of spectrum is at hand. We should view future demands over the next decade in a different way to the past use of our key public asset. Expansion in spectrum needs from the IoT community for new applications and associated spectrum capacity will become increasingly apparent over the coming decade and especially beyond 2025. Thus, spectrum availability will be an essential controlling factor of the IoT's basic infrastructure, innovation capability, growth rate and development paths.

Various novel forms of radio networks are slowly emerging for IoT systems and more may be expected. These range from slow frequency hopping and direct spread spectrum schemes for energy smart grids, deployed in the USA and the EU, or command-response networks for reading radio frequency identification (RFID) tags based on the ISO/IEC 18000-7 norm (or DASH7) at 433 MHz, an initiative originally from the US Department of Defence. That has generated a major ecosystem, especially in the defence industry.

Pressures for a revised policy for spectrum are intensified by the current climate of expanding demand from the mobile network operators (MNOs) for further long-term evolution (LTE) roll-out of up to 1.9 GHz by current International Telecommunication Union (ITU) estimates (ITU, 2013). This should be seen against the counter persistence of the terrestrial broadcasters with DTT networks using DTV-D2 technology in some countries, even if they migrate to single frequency networks (SFNs) (EBU, 2013).

Consequently, there is much uncertainty as to where such spectrum might come from and how to leverage existing licence-exempt (LE) ISM bands optimally, because of the relatively long expected process of global roll-out of the IoT, perhaps of 15 to 25 years, and the competition for spectrum in allocated bands that continues today. As one EU national regulatory authority (NRA) noted recently:

> We have tried to move away from spectrum allocations to complete service neutrality – but it is proving highly contentious – and wins us no friends in the user industries.

In circumstances where there are associated long payback times for IoT investments, some stability of spectrum award is necessary to assure roll-out and operations. Without suitable policy choices, this could become a complex spectrum management process, especially as the core IoT players expect many advances in applications with various new generations of technologies, standards and business models – yet the communications must get through.

3. Understanding spectrum demands for the IoT from the IoT architecture

Today's Internet still corresponds to a set of quite limited needs for radio spectrum compared to those of the future IoT, although its architecture will hopefully prove to be adaptable to the new constraints and demands. For future IoT users and suppliers, the question is whether the current underlying Internet architecture will be flexible enough to stretch to all of the potential IoT models of (radio-based) networking?

In essence, today we have only *Intranets* of Things – single, isolated networks that are company-wide but no more. Heterogeneity of technologies in the IoT world is significantly higher than in traditional computing systems or the Internet. This technology range extends from RFID and sensor networks to embedded systems, mesh networks and cellular mobile technologies, so the sum tends to contain multiple address spaces – not just one, as in the Internet or for mobile cellular networks.

There still is too little cross-sectoral reuse of technology and exchange of knowledge in the IoT technology world to produce common architectures or design approaches that leads to fragmented vertical and proprietary company architectures, with no coherent unifying concepts. IoT solutions tend to exist in isolation, in specific application silos. Few coherent approaches to implement the IoT have been proposed, yet, across the many types of applications – and possibly never will be – as industries pick their own winners, currently, and may continue to do so.

Thus many "island" solutions co-exist but are more notable for their uniqueness than commonality. The range includes near field RFID, smart city energy grids with FHSS or pollution-monitoring sensor nets spread over thousands of kilometres, using very low data rates. Networks are designed for purpose, so at a detail level they seem to be all quite different.

That could change. One of the commoner IoT themes is the orientation towards industrial control in the real world, with some notion of real time. Master-slave activity contrasts with today's Internet model "publish and subscribe" styles of processing in protected environments.

4. The IoT is different to the existing Internet

Today's Internet has basic operational principles that date from 1971, with concepts from even earlier, when it was really a research network for a set of trusted correspondents. Originally, the Internet was designed for large file transfers and only later for inter-process communications for co-ordinated computing and email exchanges, really post 1983. Major increments have been more at a user interface level, such as the World Wide Web, from 1994, with the market entry of multiple browsers (Nelson, 2009).

Today's Internet is still largely based on a single processing, communications and storage model, most usually intended for publishing information globally and accessing information with equal ubiquity on a best efforts basis. Thus, its commonest use is for non-real-time delivery mostly for humans in a sheltered environment (home, street, office or data centre).

The Internet's top-down naming and addressing is more oriented to a hierarchical fixed network, with a peer-to-peer model of working, carefully avoiding any centralised *locus* of control, as befits its heritage. The current key application on top of the Internet communications layer, the World Wide Web is based on publish-and-subscribe functions, using a mode of a thin client with an intelligent server. This model is implemented using various document formatting or mark-up languages for presentation of content in the browser, sent from responding webserver sites.

Address space has been expanded with the move from IPv4 to IPv6, so the Internet should now support those hundreds of billion IoT objects expected in coming decades. Moreover, the Internet has remained open to all to join, and its infrastructure has no intellectual property rights constraints. However, on the mobile Internet side, the leading market players are trying to shape the application environments for their operating systems (e.g. Apple iOS and Google's Android and variants), so patent battles may intrude strongly in the future into the IoT world of sensors and actuators if proprietary "platforms" wage their battles.

In contrast to today's Internet for content publishing, the IoT's architecture must be scoped to be a fairly close extension of the physical infrastructure that society uses for its applications – energy distribution, factory automation or rail traffic control. Thus a needs analysis for IoT applications highlights a range of quite diverse operational demands for the critical requirements even at an overview level. Further notable differences to the Internet is that much of the IoT operation is event driven and also that it may need tiers of networking that inter-operate.

Moreover, the IoT is event driven with non-peer-peer processes (e.g. master-slave for real-time control) and fragmented networks. So it has different traffic patterns, latency constraints and levels of scaling compared with today's Internet. These are the hallmarks of real-time industrial processes that must be highly resilient to failure[3]. There are also many radio protocols for industrial applications with different air interfaces – ZigBee, Wi-Fi, in various versions, Bluetooth for short range, near field communications (NFC) for very short range plus proprietary protocols such as Z-Wave, Insteon and C-Bus all being strongly promoted as well as "*domotique*" networks, a term dating from the early 1980s.

The latter has become the latest IoT manifestation as Silicon Valley climbs aboard the domotique bandwagon. One example is Apple's Homekit platform, which may be used by current smart home automation products from Hive, for instance. Alphabet's (or Google's) Nest home controllers use Wi-Fi.

Also there are many existing cabled industrial protocols MODBUS, CAN, Common Industrial Protocol over Ethernet and so on; in fact, just for smart building there are about 40 proprietary industrial protocols which may migrate to being radio based. But which air interface that will be used is unclear. Some are already present, such as smart energy grid control over radio bearers in the 915-921 MHz LE band from Silver Spring Networks, which also operates in other LE bands.

They are generally fairly different to the standard Internet architecture aimed at guaranteed delivery in a short latency (perhaps less than one millisecond) for a short data message. Industrial protocols are usually far from the Internet's concepts, for best effort for the content delivery of documents. The IoT must serve large sensor and actuator networks to efficiently and safely control manufacturing and processing plant, urban environments, smart buildings, homes and hospitals and energy grids in continually interactive command-response modes. These are needed in process automation, industrial control,

building automation, electrical power distribution, generation and meter reading, rail, aerospace and automobile industries (SCF Associates Ltd., 2014).

As well as controlling our built infrastructure, we will also expect the IoT to monitor environmental parameters on land and sea, high in the atmosphere and below ground. That speaks of a different order of security measures for critical and potentially vulnerable systems, which assume no correspondent or intervening network component is to be trusted.

Such physical implementations demand additional constraints and capabilities compared to today's Internet. IoT applications may become "mission critical" and involve safety of life. Their performance should often be faster and certainly guaranteed to be safer and more resilient than the standard best effort mode of the Internet we know. "Best effort" will not be enough.

All of this must be performed over radio links, which should have a much better failure rate than a typical commercial mobile network (of around 99.8 per cent availability at best but often much less). An ideal IoT radio-based system architecture ought to cover some or all of the points shown in Box 1.

Thus, there is a clear need for an IoT architecture adapted to the constraints of radio communications, *as distinct from the standard Internet architecture*. But whether there can be *a single* IoT architecture or reference model is the question. This is examined below.

5. Choosing radio spectrum to match the various IoT architectures

As radio spectrum is an intrinsic part of the IoT infrastructure, the question is whether the IoT's multiple and varied architectures should influence the choice of spectrum bands. The IoT community is not short on prospective architectural blueprints. Many different designs have been published, from suppliers such as Qualcomm, Huawei, Ericsson and Google. These have been put forward first in Europe and the USA, while now China and Korea are also interested. In Europe alone, there is the Architectural Reference Model from the European Commission (EC)'s IoT-Architecture project and CASAGRAS (EC, 2010), which is more RFID oriented. There is also Sensei, an early M2M model, as well as an ITU-T model, the US's NIST models for Smart Grid and for biometric devices (NIST, 2014), while internationally, ISO/IEC has some applicable standards. The European Telecommunications Standards Institute (ETSI) also has numerous models and standards, especially for sensor networks, M2M, smart metering and low bit-rate networks. All of these standards may have some place potentially.

At a commercial level, platforms for IoT with chipsets are being promoted to win early market share. Samsung has put forward its Artik IoT chipset and integration platform, while Huawei has its Agile IoT architecture and an operating system (LiteOS); Google (or Alphabet) has Android integration with its Brillo project; and Qualcomm and Intel both have their chipsets and integration platforms (Sullivan, 2015).

The various standards and engineering fora also have IoT design initiatives – ETSI, CEPT and the Internet Engineering Task Force (IETF) (IETF, 2011) are notable contributors as well as W3C with its Web of Things and the ITU. All look to supply future developments of the IoT directly or tangentially.

However, few of these models have well-defined specifications for the radio network parameters. Apart from a few relevant targets for limits on latencies, reconfiguration and expected bit error rates and perhaps specification of a common air interface and frequency (such as Wi-Fi), they have few views of the radio interface except what works today.

This is to be expected. We are only perhaps at the dawn of the various architectures that will eventually be used. Possibly, we could see a set of common standards for the air interface emerge in the short term; for instance, ZigBee and Wi-Fi could be revamped to serve many IoT networks. However, there will also be a need for quite different standards

Box 1. Attributes of a radio-based IoT architecture to meet anticipated market and operating conditions

- The radio network must serve many different applications across hundreds of vertical industries for thousands to millions of communicating sensors and actuators. That means each industry may prefer its own type of radio network. The principle of freedom to choose technology becomes paramount. Standards will evolve but only slowly in a world of vertical silos.
- Spectrum sharing can be expected as a core part of the IoT radio architecture. So IoT network implementations will use "spectrum-aware" technologies, such as cognitive radio, possibly databases – although that could be a central point of failure unless suitable failover is designed in.
- Techniques for differentiating the thousands of networks that may share the same spectrum will be a primary concern. Ways of keeping them separated, but also based within common spectrum bands, will require advances in shared spectrum techniques: e.g. via cognitive radio, beam forming, spread spectrum, power budgets, TDM, duty cycles and so on. Hence, a key architectural goal will be band sharing, based on technologies that minimise interference.
- Related to the latter point, receiver design to optimally resist interference will be a primary goal, i.e. with far narrower pass bands, for instance.
- The impacts of failed transmission with lost packets owing to interference can mean that the communications overhead for resends and for an adequate power budget to transmit may increase, perhaps more than for fixed line networks.
- Autonomic operations are required, i.e. radio packet networks that are self-repairing with adaptive self-modifying capabilities for distributed processing. Radio networks typically repair and survive through the formation of new links and relationships adapting internal status to the external environment, as sensors analyse the situation and detect the need for change with a reconfiguration. Thus, improved resilience implies designing in back-up mechanisms as a normal part of the radio network architecture, such as mesh networks with relays and alternative routing, plus routing optimisation strategies based perhaps on power budgets and battery levels.
- Changing protocols upgrades new formats and generally adapting to changing conditions. For instance, during a storm, the passage of ships with marine radar sidebands the appearance of new networks will mean networks cannot be static in operational configuration. They must adapt intelligently to local conditions, usually in the frequency domain. That means software defined radios may need to be incorporated into many designs, despite the cost.
- Depending on the techniques used, how much spectrum is actually needed may be tiny; broadband may not be needed but perhaps very narrow band and for very low data rates in infrequent bursts. Many low data speed machine-to-machine (M2M) networks already exist with comparatively fine amounts of spectrum in the ISM bands[4], while white space device networks for M2M applications are also planned.
- Propagation range is critical for radio-based communications, although the need for known or fixed physical location may not be relevant, especially if the IoT objects are mobile, or give location fixes themselves, or via neighbour triangulation.
- Receiver engineering will form a central part of a successful IoT design. In the LE ISM bands, link budgets may be constrained in terms of output power and duty cycle, perhaps down to 0.01 per cent.

(*continued*)

Box 1. Attributes of a radio-based IoT architecture to meet anticipated market and operating conditions

- Radio networks for M2M communications will tend to avoid the use of relatively expensive mobile connectivity, based on a SIM card. For instance, the savings for a smart energy grid, over 20 years with a commercial mobile cellular connection for meter reading, is of the order of €2 billion, in comparison with a FHSS network for management and energy saving, operating in a LE ISM band for a national smart grid in one country, the UK (SCF Associates Ltd., 2013). And that is for readings being made just once per year; multiple readings may give proportionately greater savings.
- With radio, mobile transceivers may roam and attach to different networks, so they may disappear altogether, only to reappear on a different network later, provoking naming and addressing issues, unless these are catered for in the object identification schema, which may demand databases.
- Suitable cybersecurity and privacy domains should be built in and not added as an afterthought. This will require much effort in design, construction and protection over the long term. Radio networks are obviously vulnerable to the attacks on current radio networks that vary from man-in-the-middle attacks to denial of service, eavesdropping and so on. The security and privacy design has to be designed in end-to-end.

and air interfaces, as new business-driven operational models will define multiple IoT architectures. Here, the Internet may well have a role in many industrial sectors as the *de facto* linking environment.

6. A pragmatic spectrum policy for a competitive market

To ensure strong competition and ease of market entry, free and open spectrum sharing, preferably via *LE spectrum*, is a key priority for policy. Such a pragmatic spectrum policy for the IoT is of strategic importance.

This policy approach results from a basic assumption about the IoT – there will be no single technical solution. IoT system designs are likely to be very different, according to their application, business model and technologies. So their basic architectures – the blueprint for design – will be equally divergent. That scope for difference leads to important conclusions on the policy for spectrum management, which should address at a minimum the practical issues of:

- Accepting that something new in technology standards may be necessary. The way forward may not be not for one standards body (e.g. the ITU, ETSI or the IEEE) to mandate a specific allocation for a single set of frequencies that correspond to a particular IoT application or technology or architectural model, such as cellular mobile. Instead, the way forward may be to facilitate the maximum choice possible in the use of spectrum so that it may suit any IoT application. As applications are unforeseeable, mandated allocations by application and technology are most likely to become redundant quickly and their utility will be soon lost. Neutrality, at service and technology levels, is necessary for spectrum allocation.
- Access to spectrum on an open and equal basis to give "fair" access to all innovators. This implies adequate access for all to the radio spectrum because so much of the IoT will be connected by radio, so suitable spectrum management is vital.
- Anticipating the market will produce formal common interoperability protocols and gateways between multiple heterogeneous IoT networks. The market will push a whole a set of systems, models and operating processes and so will also need interoperability standards. They are likely to include use of the radio spectrum, because interconnection is likely to be over radio bearers wherever necessary. But

inter-operation should be equally able to use unlicensed spectrum in frequencies as the heterogeneous IoT systems themselves.

- A further consideration is that exclusive IoT spectrum licences could enable monopolies and oligopolies to form or enable operators to gain significant market power (SMP) through control of the spectrum needed by its many potential users. That hold over the key spectrum band could be used to restrict entry of competitors. For instance, most mobile operators see spectrum access as a dual opportunity, both to assure their basic network operations and to effectively restrict the entry of new competitors. In consequence, an exclusive licence could guarantee SMP for its owner and a potential barrier to the rest of the IoT market.

Like other ICT markets, the IoT will be influenced by both the network effect and economies of scale. These two effects could result in enhanced market power for already dominant players, perhaps increasing the risk of abuse of that market power[5] That could lead either to a fragmented ownership of the IoT infrastructure or multiple private fiefdoms rather like those of the mobile networks.

Obtaining equal access for all users, depends on *the form of shared spectrum access rights* and the ease of access that provides to all relevant stakeholders – end-users, IoT product innovators and IoT service suppliers.

Sharing can be achieved in several ways, but three possible directions stand out:

1. The collective use of spectrum model that enables spectrum to be used by more than one user simultaneously without requiring a licence, i.e. LE, so the number of users is unlimited. This is a commons with limits on technical behaviours to eliminate any effects of interference. The interference safeguards are part of the unlicensed conditions and form the basis of the transceiver technology. If the logical choice is that the relevant swathes would be LE, then radio spectrum for the IoT would become like the Internet in several ways due to its nature as a commons:
   - nobody owns it, but all can access;
   - all can use it free, at no charge and as often and as liberally as they desire, as long as they do not cause interference to others, be it a machine or device for human users;
   - many bodies can collectively co-operate to assure its maintenance and sound operation;
   - governance is collective, not managed by commercial diktats or government whims; and
   - global operations can result and seed global markets for equipment, services and devices.
2. Or on the basis of the Licensed Shared Access model in which several agreed users have specific rights to access to a previously exclusive licensed spectrum band to one of the participants. The band may be registered with the NRA which originally licensed the spectrum. The NRA is likely to have a statutory duty of regulatory monitoring of the shared usage.
3. A third possible consideration is for light licensing that implies payment of a fee and conditions on equipment performance but no other restriction and no exclusive use.

The first option, of LE access, is the most attractive for collective use by IoT applications. The advantages it holds are that no contractual negotiations are required – just “manufacture and use”. Also, all may access spectrum to transmit (and receive), free from licence regulation or fees. Manufacturers can build to a standard and so an ecosystem can be built, stretching from semiconductor component manufacturers to radio device

suppliers and distributors. Hence, the availability of unlicensed spectrum promotes production of large numbers of devices at low cost, leveraging economies of scale and making communications technology affordable. This is effectively the Wi-Fi model.

Moreover, the use of LE bands may assure that long-term stability of the spectrum allotment can be achieved, necessary to assure investment, innovation, network roll-out and operations over many decades. The example of Wi-Fi is worth noting, which was originally awarded spectrum in 1985 in the USA by the Federal Communications Commission (FCC) but has flowered tremendously since as an innovative market grew around it.

With a LE commons, the spectrum is assured of being technology and "service" neutral, while being open to all to access it (within the pre-set interference limits) for the long term. And only an award open to all entrants can give this permanence. Furthermore, while spectrum decisions tend to be slow to deliver compared to technology innovations that can happen very quickly, LE gives a spectrum decision that is already given and open to all new users and their innovations. Common global harmonisation for LE spectrum would also raise the debate above national priorities.

Essentially, all these policy requirements point to one solution: multiple license exempt bands for the IoT across many frequency ranges, as suited to each possible IoT system's operating requirements and functions.

Thus, IoT advance in the next decades will increasingly depend on regulators granting shared spectrum access rights for the different IoT networks, using LE swathes far more than in the past. Note that interference limits are a moving target that may require review, possibly as often as every two to three years, say for permitted power, duty cycle and spread of transmitted spectrum skirts as signal processing advances.

7. Which bands should be considered?

The spectrum bands that need to be considered for the IoT should have wide variations in physical properties and utility to match the different IoT applications. This is a case of the right spectrum for the job or "horses for courses". For instance, the frequencies for a body area network are unlikely to be optimal for a national water flow control network.

While broadcast and mobile fight over the prime spectrum area, UHF (300 MHz-3 GHz, especially for its lower range, sub 1 GHz) which gives the best long range propagation, it is likely to also be needed for some IoT devices that must transmit over kilometres or tens of kilometres.

Most interestingly, we are now at a key point, because in 2012, at the World Conference on Radiocommunication and its regulation (WRC-12), a major upheaval occurred, one which provides an example of the possibilities for refarming bands for IoT. Certain countries requested release of the 700 MHz band from broadcast services to for use for mobile and other purposes.

This "Second Digital Dividend" (DD2) might eventually be an example of an opportunity for the IoT to gain more LE spectrum. If granted, the IoT would secure some prime range spectrum. That could support the needs of large metropolitan area mesh machine networks (M3N) and other applications that require ranges of over 300 metres, with penetration of ferro-concrete structures in buildings, as well as all-weather working for rain, snow and wet leaves environments.

Note that this may mean clawing back spectrum from commercial mobile cellular networks in subsequent WRC events. Various studies analysing the potential release presented to the EC (Forge *et al.*, 2012; Forge and Blackman, 2012), the FCC and other bodies propose that one sub-band of the potential 100 MHz spectrum release at 700 MHz could be reserved for LE devices and that whole band should not just be allocated for licensed mobile use, for LTE roll-out. The European Common Policy documents from CEPT (EC, 2015) are currently being put forward for proposals to WRC-15, as the first round of

talks before WRC-19 proceeds towards a refined bandplan (Ring, 2015). Debate will cover many UHF and adjacent bands as well as higher frequencies for "5G" working, which may hold value for IoT networks.

One possible trajectory for evolution of the 700 MHz band for IoT needs is shown below. It might well be a progressive, rather than a single event. A first allocation could expand with demand if more applications using LE bands come into play over the following two decades. In this scheme, the bandwidth of the LE section could expand from a first range of perhaps 20 MHz for IoT-type applications and other services with 10 MHz for the emergency services[6] also. After 2030, the band in this scenario could perhaps increase to 50 MHz for LE services that would encompass many longer-range IoT demands as well as possible Wi-Fi traffic needed for offload of mobile data. The key approach here is one of a series of phases of progressive migrations, as shown in Figure 1.

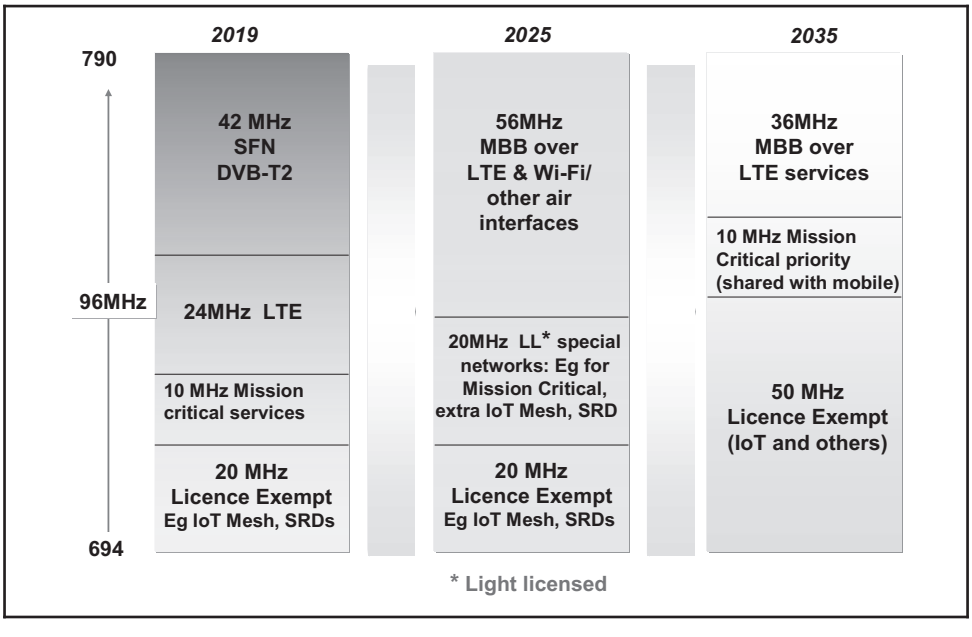
This is just one possible example of repurposing a band that unexpectedly could provide an IoT LE swathe of spectrum with sufficient capacity and range for smart cities and perhaps country-wide networks. Useful propagation range is a parameter which varies inversely with frequency, so it would offer tens of kilometres, being at the lower frequency end of UHF.

8. Future spectrum will be driven by different applications

Future IoT networks may have quite different characteristics that lend themselves to much higher and much lower frequencies than the UHF band of 300 MHz to 3 GHz. These various different types of IoT networks could, and should, be sited in quite different frequencies because of their functional requirements, not just in the UHF band.

This is already the case today, for instance, (NFC) which transmit over millimetres or centimetres for non-contact transactions may be positioned today in the lower frequencies (13.56 MHz) in the high frequency range of the unlicensed ISM band. Interestingly, the power the device needs is also transmitted over these short distances. But NFC ranges may possibly in the future fit the spectrum for much higher frequencies of "millimetre wave" transmissions at the EHF band (Extreme High Frequency, 30-300 GHz).

Figure 1 Refarming for IoT: possible use of the 700 MHz band for the IoT in an LE band



As IoT networks develop towards maturity, with many different forms, architectures and different basic characteristics, so quite diverse bands may seem more attractive or more appropriate to their operational parameters. Eventually, the spectrum bands that could be most appropriate for the IoT would have a wide array of properties, and thus frequencies, to suit the different types of IoT applications, both above and below the prime radio spectrum territory of the sub-1 GHz UHF band.

One obvious alternative to the 700 MHz UHF band is to go further down into the broadcast UHF band to the 400 MHz range (400-500 MHz), more specifically perhaps around 450-480 MHz. That band offers major advantages over 700 MHz, evident in terms of range of propagation and thus investment and operating cost of networks as well as building penetration and wet weather/wet foliage performance. Currently, this band is allocated to TV broadcast users in Regions 1 and 2. But it also hosts military communications (including NATO designated spectrum in Europe) and is used by mission critical services in some countries, such as France and the UK. But at WRC-15, this is already an item for discussion, extending debate from 470 to 690 MHz for Region 2 for the USA (Youell, 2015). Although this is for mobile, again, some bands could be allocated to IoT in the future.

9. Other bands which may be applicable to IOT applications

We are now at a critical point of progressive opening of the spectrum to novel applications, such as IoT networks and systems. This is being driven, first, by a growing spectrum liberalisation, which is much more significant than the changes that have taken place over the past 40 years. These enable innovative communications technologies to enter with a series of measures:

- releases of exclusively licensed and restricted use spectrum, especially from bands reserved for the military;
- refarming of exclusive TV broadcast multiplexes in heavily used parts of the spectrum such as UHF;
- gradual expansion of the critical LE bands; and
- sharing spectrum with use of cognitive radio, white spaces, databases and so on, in heavily used bands for both commercial and government bands.

The second driver is the entry of new technologies that can exploit useful frequencies *outside* the traditional ranges which, in general, are heavily used bands to take advantage of these alternative ranges at the extremes of the spectrum outside the UHF band.

Table I indicates the main bands in the radio spectrum with a brief summary of their attributes and possible limits for IoT networks. Many of these would have seemed odd choices, perhaps even unthinkable, just a few years ago. Also it should be noted that many types of IoT network may use ultra narrow bands for low data rates which could use interstitial or guard bands, as proposed for white spectrum devices.

Note also that the distance ranges cited depend on the power available to the remote transmitter and also on the duty cycle, often applicable in LE bands. Exploiting the longest ranges may require higher power combined with over-the-horizon phenomena. These may include tropospheric scatter, ground waves with ionospheric reflection to follow the earth's curved surface or ionospheric refraction effects. All vary with frequency.

This analysis leads to a perhaps self-evident conclusion: that for the IoT to flourish freely, there is a need not just for a future LE band for the IoT in the 700 MHz band but for IoT LE bands in many of the above swathes. One possible simplified model may be based around the propagation range of systems and reduced to four main types of IoT application, as shown in Table II.

Table I IoT applications against spectrum band

Designation	*Frequency range and useful range*	*IoT applications and propagation mechanisms*	*Description and current applications*
Tremendously low frequency, TLF	<3 Hz Theoretically >1000 km	Possibly very short range organic technology monitoring devices at bps data rate	Not used yet
Extremely low frequency, ELF	3-30 Hz Theoretically[a] >1000 km	Very long range fixed metering networks with very low data rates, if power available for maximum range	Used for submarines globally since 1920s, morse signalling
Super low frequency, SLF	30-300 Hz Theoretically[a] >1000 km	Very long range fixed monitoring/slow control networks with low data rates (bps), if power available for maximum range	Used for submarines globally since 1920s, morse signalling
Ultra low frequency, ULF	300-3000 Hz Theoretically[a] >100 km	Longer range fixed monitoring networks with low data rates, 1 kbps. Also closed environments–mining and tunnel applications, if power	Underground tunnel communications–e.g. mining, also for submarines
Very low frequency, VLF	3-30 kHz Theoretically[a] >100 km	National fixed networks for long-range metering with low data rates. Signals are guided between the earth and the ionosphere	Currently for navigational aids, heart rate monitors, geophysics, time signals, submarine communication
Low frequency, LF	30-300 kHz Theoretically[a] >100 km	National fixed networks for long-range metering with low data rates. Guided between the earth and the ionosphere as ground waves following curvature of the earth	Currently for RFID, AM audio (longwave broadcast Europe and Asia) time signals, navigational aids, amateur radio
Medium frequency, MF	300-3000 kHz Theoretically[a] >100 km	National fixed networks for long-range metering with low data rates of kbs-Mbps. Signals guided between earth and the ionosphere as ground waves following curvature of the earth; best at night, when ionospheric absorption weak	AM (medium-wave) broadcasts, avalanche beacons, amateur radio
High frequency, HF	3-30 MHz Theoretically[a] >100 km	Various different propagation systems possible, based on ionospheric refraction giving both long range (theoretically <1000 km if very high power) or via ionospheric reflection (600 km). Generally medium data rates (Mbps)	Current uses–RFID, shortwave broadcast, marine and PMR mobile radio telephony, Citizens' band radio, over-the-horizon aviation communications and radars, sky-wave (NVIS) communications, amateur radio
Very high frequency, VHF	30-300 MHz Theoretically[a] <100 km	National networks for monitoring with multiple base stations. Generally direct wave. Current technology for longer range is limited by unreliable tropospheric ducting and ionospheric refraction–statistical techniques possible	Current uses–analogue TV broadcast, FM audio, weather radio, land and maritime mobile communications, duplex line-of-sight ground-to-air communications, amateur radio
Ultra high frequency, UHF	300-3000 MHz Theoretically[a] 40-2 km	National networks for monitoring with multiple base stations. Generally direct wave. Could use interleaved WSD or existing licence-exempt ISM bands–e.g. 876 MHz and 915 MHz or 2.4 GHz. Possible mobile applications. Direct wave propagation, with variable tropospheric ducting	Today the most crowded band of all–DTT and analogue broadcast TV, mobile GSM, LTE, UMTS, Wi-Fi WLAN, PMR, PAMR, ZigBee, Bluetooth, GPS, microwave ovens/devices/LoS (Line of Sight) communications, satellites, radio astronomy, amateur radio
Super high frequency, SHF (part of the conventional "5G" initiative)	3-30 GHz Theoretically[a] 2 km-10 mm	Possible "5G" short range mesh networks for monitoring and control. Direct wave propagation	Wi-Fi LAN, military and civil radars, satellite TV broadcasting–DBS, microwave devices/communications, communications satellites, radio astronomy, amateur radio

(*continued*)

Designation	*Frequency range and useful range*	*IoT applications and propagation mechanisms*	*Description and current applications*
Extremely high frequency, EHF (part of the conventional "5G" initiative)	30-300 GHz Theoretically[a] 2 km-10 mm	Possible "5G" short range mesh networks for monitoring and control at very high transfer rates (>10 Gps) with LoS or radiated transmission. Direct wave propagation. limited by O_2 bond absorption for certain frequencies–e.g. 60 GHz	Microwave LoS relays and remote sensing, millimetre wave devices, radio astronomy, amateur radio, directed-energy weapons
Tremendously high frequency (or TeraHertz)	300-3,000 GHz 20 m-100 μm, Possible extensions[a]	LoS short range (10 m) at high transfer rates (>100 GBps). Less likely to be useful for IoT systems, except for specialised sensors. May have in-space LoS capabilities for IOT applications above the atmosphere	Novel applications in medical imaging, spectroscopy, computer processors and internal communications, remote sensing, condensed-matter physics, possibly data transmission

Note: [a]Range depends on power available in remote transmitters and also on duty cycle, if also a constraint

Table II Suggested bands for new licence exempt swathes

Typical Iot Application	*Frequency region*
TYPE 1: IoT application consisting of long distance low-cost networks with low data rates and narrowband applications–e.g. national monitoring networks for utilities for instance, possibly extending to regional networks across countries. These may include environmental monitoring and low speed industrial applications–e.g. national water network management. Data rates are of less than a few kbps and time constants in hundreds of milliseconds or longer. They are examples of low throughput networks (LTN) in ETSI parlance, for M2M communications	Ultra low frequency, ULF 300-3000 Hz Theoretically, range >100 km Very low frequency, VLF 3-30 kHz Theoretically, range >100 km
TYPE 2: Mesh and cellular type network systems, with ranges of at least 20-30 km that may be used for transport, industrial and utility applications	VHF bands (50-300 MHz)
TYPE 3: Medium range networks of 1-10 km for the diverse low cost industrial applications–e.g. smart city monitoring, alarms and in-building	Sub 1 GHz (e.g. 850-876 and 915-921 MHz) plus some new bands in the 700 MHz band and the 300-600 MHz ranges, as discussed
TYPE 4: SRDs and NFC types at 30 GHz- 100 GHz for metre, centimetre and millimetre range applications with some directional beam applications having high power for ranges up to 1 km possibly indoor but less likely for building penetration	Above 5 GHz, i.e. 5-30 GHz SHF and EHF

Note: SRDs = short range devices

The analysis in Table II implies that the expansion of LE and LE bands will be needed *in each major frequency band.* For high reuse of the same LE bands, future directions for R&D in radio technology will be concentrated on:

- Receiver pass band improvements, to limit detection ranges and so interference within each LE swathe.
- Cognitive radio techniques for heightened listen before talk operation.
- Transmitter performance to reduce out-of-band emissions, especially in sideband suppression using low cost computing power, or analogue techniques for sharper filters and focussed generation.
- Future use of an online registration database for devices in the field to track interference transgressors in IOT applications.

10. Options may vary by region – and what is a region could change

A dimension of varying international preferences for spectrum access is becoming increasingly present in debates surrounding the IoT. Conventional ideas of global standardisation of spectrum use by bands have held up fairly well since the ITU first defined the debate with the publishing of the Radio Regulations (RR) in the last century. It has been most useful in encouraging international standards to build equipment with the global scales of manufacturing volumes and far lower prices. The RR set standards, for instance, for UHF broadcast frequencies in the 485-694 MHz bands for DTT and before that for analogue TV and satellite, as well as the VHF bands for FM radio and the analogue AM bands. The ITU RR applies with differing recommendations by global geographic area (ITU Regions 1, 2 and 3 as defined in ITU Radio Regulations).

Traditionally, these ITU recommendations have always been challenged at a national level, with various derogations within the Regional Recommendations. Today that is being further challenged within the regional level. The new "unit" of commonality in allocations may be an economic one that is smaller than the ITU Regions 1, 2 and 3 but much larger than national. It would be based on common choices for economic and social reasons for allocations on the uses of spectrum – for broadcast, mobile, military and IoT and so on.

For example, at WRC-12, despite being in Region 1, Africa, with some neighbouring regions, had a preference for using the UHF TV bands for mobile, nomadic or fixed radio communications, as TV had never become widespread and DTT was less in demand. This surprised many nations used to leadership, more by the Organisation for Economic Co-operation and Development community. Thus, the most logical spectrum allocations may differ significantly in form and content from those of the past. This is important for development of the IoT.

11. Policy recommendations for IoT spectrum demands

There are various policy actions for spectrum that governments globally should proactively pursue to increase the proportion of shared access spectrum. Key actions are required at a policy level to obtain shared access, through LE spectrum, which would be critical for IoT application roll-out:

- First, the WRC-15 groundwork and subsequent WRC-19 preparations should take advantage of a key window of opportunity that has just opened for LE access in the 700 MHz band, as covered in various DD2 studies, and possibly DD3 (transfer of the broadcast 470-694/8 MHz band) using the principles of shared spectrum. That band may be attractive to some users, but many others are opening up a much wider debate, conventionally in going higher up the spectrum than 6 GHz for small cells under the "5G" umbrella. More unconventionally, the debate in the future could also swing to much lower parts of the spectrum, below 300 Mhz and the UHF band.

- This preparation will require liaising with the relevant ITU and other working groups globally and with the associated bodies (e.g. in the EU, this would include the ECO, CEPT and RSPG for the NRAs, as well as ETSI).
- Preparations also require engaging with the key incumbent players – the MNOs with their industry association, the GSMA – and broadcasters, collectively (e.g. the through the EBU in the EU).
- It will also demand co-operation between various governments on policy matters. At the same time, it would be beneficial to create a significant funding programme for research and for the first commercial roll-out into the market for novel sharing mechanisms for LE radio architectures and interference mitigation mechanisms (e.g. CR, FHSS, MIMO, mesh and so on).
- A further key goal will be to ensure that any research and development initiatives produce purely open source software and open IP (intellectual property), just as was done for the Internet, to create a patent-free zone for new innovative technologies (e.g. novel forms of FHSS). They will create a platform for industry and can gain international standards bodies' approval.

Thus, policy makers, such as the European Commission and NRAs, have a key role in ensuring that rights to spectrum access are configured in a way that promotes the growth of innovation and development of IoT applications, including the harmonisation of conditions across the globe. Studies analysing the potential release, and which have already been presented to the European Commission, propose that one sub-band of the potential 100 MHz spectrum release should be reserved for LE devices and that whole band should not just be reserved for licensed mobile use for LTE roll-out (Forge and Blackman, 2012). Naturally, this might be progressive with a first reservation expanding as more applications using LE come into play over the next two decades.

Fundamentally, there is a single key message: IoT architectural design must form a part of future spectrum policy at a global level. This may be interpreted simply as the right spectrum for the right type of IoT application and its network. Here, the four major IoT application classes, as described in Table II, are summarised in frequency terms, as each requires specific spectrum for its type of application:

1. *Above 5 GHz*: Small-cell networking, also short range devices and NFC types at 30 to 100 G Hz with some directional beam applications with high power for ranges up to 0.5 km for frequencies from 5 to 30 GHz as in the "5G" plans for a new architecture.
2. *Sub-1 GHz (e.g. ISM bands such as 850-876 MHz and 915-921 MHz) but with new bands added in 700 MHz and 300-600 MHz*: Medium range networks of 1 to 20 km per hop or cell radius.
3. *VHF bands*: mesh- and cellular-type network systems (50-300 MHz) with ranges of at least 20 to 30 km.
4. *VLF bands (below 10 MHz down to 1 kHz)*: National and global networks for slow speed signalling with global range.

Perhaps as a second message, there is the need for a progressive growth in unlicensed spectrum for free innovation, placing LE bands in each major frequency band identified above. Naturally, the concentration on LE bands requires certain technology advances, particularly in two areas:

1. Politeness protocols for sharing LE bands advance so that higher duty cycles and signal powers are possible for more simultaneous users to share the band.
2. Receiver discrimination, with pass band filtering improvements, to limit interference. Equally, enhanced transmitter pass band performance in adjacent bands that could

overlap should also reduce interference as in the 2.3 GHz LTE/2.4 GHz Wi-Fi debate currently.

To track interference transgressors in IoT application bands, national and global databases of online registered devices may be useful. Note that the above all is predicated on *frequency-dependent* technology models. Future technologies may increasingly look to alternative approaches (e.g. UWB types).

Notes

1. Digital terrestrial television – the replacement technology for analogue broadcasting.
2. The second digital dividend – release of the 700 MHz for mobile use from DTT in much of the world.
3. For example, any interruption of the smart electricity grid is very expensive – in the case of the UK, this would cost over €8 billion for a major outage of a large region for 12 hours (SCF Associates Ltd., 2013).
4. For example, those from Sigfox of France for national coverage of water distribution networks at low cost.
5. The classic example of the network effect is a telephone network – the more subscribers who can be connected, the greater is the value of the network, as AT&T Inc. quickly understood in the 1920s in the USA. Increasing returns with scale applies to networks as well as to products – a typical example is a software programme, whose cost to produce one more copy is miniscule, compared to the cost of developing it (Wynants and Cornelis, 2005, pp. 489-503).
6. That could imply a new generation of mission critical first responder services, perhaps based on commercial mobile networks with priority conditions and additional shared spectrum in the 2017-2025 era.

References

EBU (2013), "SFN Frequency planning and network implementation with regard to T-DAB and DVB-T", available at: https://tech.ebu.ch/docs/techreports/tr24.pdf/ (accessed 24 October).

EC (2010), "CASAGRAS 2 Workpackage 2 Architecture and platforms for the IoT", available at: www.iot-casagras.org/WPA2

EC (2015), "Proposals for a council decision on the position to be adopted on behalf of the European Union in the ITU WRC-15", European Commission, 29 May.

Forge, S. and Blackman, C. (2012), "Europe's spectrum bonanza: strategies, market opportunities and challenges for a second digital dividend", Research Report, PolicyTracker, August.

Forge, S., Horvitz, R. and Blackman, C. (2012), "Perspectives on the value of shared spectrum access", Final Report for the European Commission, *SCF Associates Ltd.*, February, available at: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/scf_study_shared_spectrum_access_20120210.pdf

IETF (2011), "The internet of things- concept and problem statement", available at: www.tools.ietf.org/html/draft-lee-iot-problem-stament-00

ITU-R (2013), "ITU-R Report M.2290", ITU, Geneva.

Kende, M. (2012), "Impact of radio spectrum on the UK economy and factors influencing future spectrum demand", *Department of Business, Innovation and Skills, and Department for Culture*, Media and Sport, London.

Nelson, T. (2009), *Geeks Bearing Gifts*, Mindful Press, San Francisco, CA.

NIST (2014), *Smart Grid Framework*, National Institute of Standards and Technology, available at: www.nist.gov/el/smartgrid-100114.cfm

Ring, S. (2015), "IoT Spectrum on WRC-15 Agenda", *EE Times*, 14 October, available at: www.eetimes.com/author.asp?section_id=36&doc_id=1328000

SCF Associates Ltd. (2013), "Consultation submission to ofcom: consultation on 870-876 MHz and 915-921 MHz, update and way forward", available at: http://stakeholders.ofcom.org.uk/consultations/870-915/?showResponses=true&pageNum=2#responses

SCF Associates Ltd. (2014), "Is commercial cellular suitable for mission critical broadband?", A study prepared for the European Commission, DG Communications Networks, Content & Technology,

available at: https://ec.europa.eu/digital-agenda/en/news/use-commercial-mobile-networks-and-equipment-mission-critical-high-speed-broadband

Sullivan, M. (2015), "Too many platforms may make the IoT a confusing place", *VentureBeat*, 21 May, available at: www.venturebeat.com/2015/05/21/too-many-platforms-may-make-the-IoT-a-confusing-place/

Wynants, M. and Cornelis, J. (2005), *How Open is the Future: Towards an EU Policy for Open Source Software*, VUB University Press, Brussels.

Youell, T. (2015), "US negotiators reaffirm commitment to global mobile allocation for 470-694/8 MHz band", *PolicyTracker*.

Further reading

CEPT (2011), "ECO, Weber, T., ECC activities and principles applied for the IoT Future spectrum use",12 November, Brussels.

EC (2011a), "Internet of things architecture IoT-A project deliverable D1.2 – initial architectural reference model for IoT", available at: www.iot-a.eu/public/public/documents/documents-1

EC (2011b), "Internet of things architecture, IoT-A project deliverable D6.2 – updated requirement list", 31 January, IoT-A (257521), European Commission, FP-7, available at: www.meet-iot.eu/deliverables-IOTA/D6_2.pdf

EC (2012c), "Internet-of-things architecture, IoT-A, deliverable D1.3 – updated reference model for IoT", 16 July, v1, IoT-A (257521), European Commission, FP-7, available at: www.meet-iot.eu/deliverables-IOTA/D1_3.pdf

ETSI (2014), "Report GS LTN 003 V1 Low throughput networks (LTN): protocols and interfaces; & ETSI Report GS LTN 002 V1, Low throughput networks (LTN): functional architecture".

ITU (2005), "ITU internet reports 2005: the internet of things", Executive Summary, International Telecommunication Union, Geneva.

ITU (2008), "The international identification plan for public networks and subscriptions", ITU.212, International Telecommunication Union, Geneva.

Corresponding author

Simon Forge can be contacted at: simon.forge@whsmithnet.co.uk