Bouhafs, F, Raschella, A, MacKay, M, Hashem Eiza, M and Hartog, FD

Optimizing Radio Access for Massive IoT in 6G Through Highly Dynamic Cooperative Software-Defined Sharing of Network Resources

future internet

MDPI

Article

Optimizing Radio Access for Massive IoT in 6G Through Highly Dynamic Cooperative Software-Defined Sharing of Network Resources

Faycal Bouhafs [1], Alessandro Raschella [2,*], Michael Mackay [2], Max Hashem Eiza [2] and Frank den Hartog [1,3]

[1] School of Systems and Computing, University of New South Wales, Canberra, ACT 2600, Australia; f.bouhafs@unsw.edu.au (F.B.); frank.denhartog@canberra.edu.au (F.d.H.)
[2] School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, L3 3AF, UK; m.i.mackay@ljmu.ac.uk (M.M.); m.hashemeiza@ljmu.ac.uk (M.H.E.)
[3] Network Engineering and Cyber Security, University of Canberra, Canberra, ACT 2617, Australia
* Correspondence: a.raschella@ljmu.ac.uk

Abstract: The Internet of Things (IoT) has been a major part of many use cases for 5G networks. From several of these use cases, it follows that 5G should be able to support at least one million devices per km^2. In this paper, we explain that the 5G radio access schemes as used today cannot support such densities. This issue will have to be solved by 6G. However, this requires a fundamentally different approach to accessing the wireless medium compared to current generation networks: they are not designed to support many thousands of devices in each other's vicinity, attempting to send/receive data simultaneously. In this paper, we present a 6G system architecture for trading wireless network resources in massive IoT scenarios, inspired by the concept of the sharing economy, and using the novel concept of spectrum programming. We simulated a truly massive IoT network and evaluated the scalability of the system when managed using our proposed 6G platform, compared to standard 5G deployments. The experiments showed how the proposed scheme can improve network resource allocation by up to 80%. This is accompanied by similarly significant improvements in interference and device energy consumption. Finally, we performed evaluations that demonstrate that the proposed platform can benefit all the stakeholders that decide to join the scheme.

Keywords: 6G; massive IoT; blockchain; sharing economy; spectrum access; spectrum programming

Citation: Bouhafs, F.; Raschella, A.; Mackay, M.; Hashem Eiza, M.; den Hartog, F. Optimizing Radio Access for Massive IoT in 6G Through Highly Dynamic Cooperative Software-Defined Sharing of Network Resources. *Future Internet* **2024**, *16*, 442. https://doi.org/10.3390/fi16120442

Academic Editor: Paolo Bellavista

Received: 6 October 2024
Revised: 8 November 2024
Accepted: 21 November 2024
Published: 28 November 2024

1. Introduction

The Internet of Things (IoT) is revolutionising the way we interact with the objects and services we use in our daily life and over time has evolved into a vision for a ubiquitous network that seamlessly connects all physical objects to the digital infrastructure, the so-called massive IoT. We are currently witnessing this vision being realised as the number of deployed IoT devices continues to grow at a tremendous rate. According to [1], the number of IoT devices is expected to exceed 38 billion devices by 2029.

Fifth-generation (5G) networks aim to provide network access on this scale, but for network operators to be able to accommodate so many wireless devices it requires a major investment in their telecommunication infrastructures. Moreover, a 5G network is not only required to provide access to many IoT devices, but also at high densities. For a massive IoT, the ITU set a requirement for 5G to support at least one million devices per km^2, or one per m^2 [2]. In this paper, we will first explain and evidence why 5G will never fulfil that promise: the radio access schemes used today are not adapted to meet these densities and the data traffic pattern of IoT devices, which are characterised by short and asynchronous transmissions, and are not the focus of existing wireless protocol optimisations.

We will then show how 6G networks could provide an opportunity for new ways to support a massive IoT in wireless networks [3,4]. Specifically, we aim to tackle the

problem of access in future 6G networks by applying the concept of a sharing economy. This approach represents a paradigm shift in wireless network deployment as operators will be encouraged to step away from the traditional isolated and competitive model and increasingly embrace cooperation for a mutual benefit. As such, we describe the challenges this approach poses from a practical perspective and introduce the technologies that can be leveraged to address them. Crucially, we also introduce our new concept of spectrum programming, which meets the outstanding key challenges and collectively provides a cohesive framework to solving this problem.

The position of this paper is that we are approaching a tipping point whereby sharing economy-based solutions can now realistically be considered. Therefore, we propose a high-level architecture that can scale to the required density level for a massive IoT. The proposed architecture focuses on addressing the key features of heterogeneity, connectivity management, and cooperation and transparency. We then explain how each feature is designed and can interoperate between operators. Finally, we validate our claims through a simulated evaluation of a realistic massive IoT deployment to demonstrate the potential benefits our architecture delivers.

The key contributions of this paper can therefore be summarised as follows:

- We found that the problem we are trying to solve, namely the lack of scalability of 5G to truly achieve a massive IoT, is not well identified and explained in the literature. We therefore start with presenting a novel analysis of the actual problem.
- We then propose a novel, transparent, trusted, and accountable cooperative spectrum-sharing system based on the shared economy paradigm, which relies only on the dynamic matching of the offer and demand of network resources. Moreover, the system provides a method to incentivise any stakeholder (e.g., an end user or an internet service provider) interested in sharing the radio spectrum through our system in a beneficial way for all the actors involved.
- We provide an accurate analysis of the proposed system in terms of transparency and accountability. The analysis also illustrates the benefits achieved by the stakeholders that share their spectrum through our system.

The rest of this paper is organised as follows. Section 2 elaborates the problem we are trying to solve: the lack of scalability of 5G to truly achieve a massive IoT. As this is not clearly presented as such in the current literature, we illustrate the problem by performing a simulation of 5G networks using current default implementations and configurations. We will then use the results as the baseline/benchmark to use for a comparison with our proposed solution for 6G. The core of that solution lies in the realisation of highly granular, dynamic, automated spectrum sharing, using programmable networks. Section 3 is therefore dedicated to a study of the state of the art regarding the application of a spectrum-sharing economy to wireless networks. It first describes existing spectrum-sharing approaches for a massive IoT and then introduces the concept of sharing economies as it is applied in this paper.

Before we can move forward to describe the architecture of our solution, as we do in Section 5, we first need to introduce the key requirements (design challenges) and components that comprise the architecture of our system. Many of these concepts are relatively novel and thus require some explanation. We do so in Section 4. These concepts include softwarisation, virtualisation, network programmability, spectrum programmability, and blockchains. Section 5 thus presents our architecture, which is then evaluated in Section 6 against the standard 5G implementation as was analysed in Section 2. Finally, Section 7 presents our conclusions and further work.

2. Motivation: The Challenge of Radio Access in a Massive IoT

The nature of wireless communication technologies, i.e., being a radio medium, along with the easy and cheap deployment of some of the more mature technologies available today, make them the best candidate for IoT applications in many cases. A key component of wireless technologies is the Medium Access Control (MAC) protocol, which is responsible

for providing access to the radio spectrum for a wireless node to send data. Several MAC schemes and protocols for wireless networks can be found in the literature [5] and are deployed today. They can broadly be classified into two categories: scheduled access and random access. In scheduled access, a central entity, the RAN, grants access for a wireless node to transmit its data following a specific time schedule. In random access, on the other hand, wireless nodes compete for access to the shared wireless medium using randomisation procedures. Two well-known MAC schemes based on random access are ALOHA [6,7] and its variation, Carrier-Sensing Multiple Access (CSMA).

Random access is often preferred for IoT communication due to its simplicity, making it easy to implement, which is important for resource constraint IoT devices. In addition, IoT devices do not necessarily always have data to send and, therefore, adopting schedule-based access could be a waste of a scare resource. However, the contention-based nature of random access, although manageable for small to medium networks, does not scale with the sizes and densities associated with a massive IoT [8,9]. To better illustrate this limitation, we simulated in MATLAB an IoT network of 4000 devices and 20 5G base stations (gNBs) deployed in an open area of 80 m $\times$ 80 m. The IoT devices had transmission power capabilities varying between 1 and 10 dBm and data rates varying between 8 and 128 kbps for uplink transmissions. For the radio access for the IoT devices from the base stations, we adopted the ALOHA access model.

Figure 1 shows the number of attempts necessary for all devices to successfully transmit all their data using the pseudocode implemented as illustrated in Algorithm 1. Specifically, the number of attempts needed for all the devices to successfully transmit their data is stored in the set *Iterations*, while the percentage of devices satisfied at each attempt is stored in the set *Satisfaction*, defined in lines 3 and 4, respectively. The *while* loop in line 6 of Algorithm 1 is executed until all the IoT devices achieve a bit rate at least equal to their requirement, represented as R_i and R_{reqi} respectively. When all the devices are connected, lines 20 and 21 of Algorithm 1 interrupt the *while* command to record the final sets *Iterations* and *Satisfaction*, as represented in Figure 1.

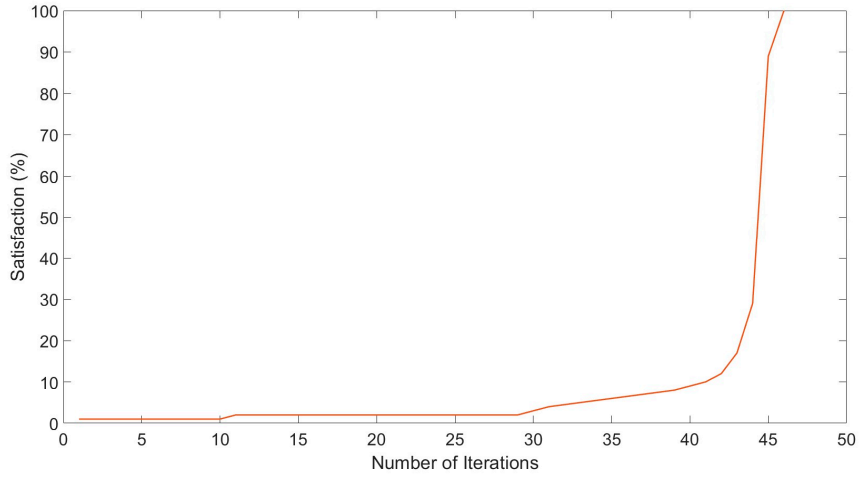


Figure 1. Transmission success rate as a function of the number of attempts to access the medium.

Figure 1 shows that it takes over 40 attempts for all the IoT devices to be satisfied. Moreover, the number of iterations results in more delays as, after each collision, a device needs to back off before retransmitting again. To better quantify the delay incurred by such a number of attempts, we assume that radio access in the IoT network described above is based on Pure ALOHA [10]. Accordingly, an IoT device that will reach n attempts to transmit its data will have to wait for a period of time of $T_{wait} = T_{Propagate} \times r$ on the nth attempt, where r is $\in \{0, 2n\}$ and $T_{Propagate}$ is the time necessary for the device message to propagate through the wireless medium. If we assume an IoT device message needs only 1 ms to propagate but the IoT device is already on its 40th attempt, then it

must wait between 0 ms and 240 ms before transmitting again. This demonstrates that consecutively failing to transmit due to collisions significantly hinders the ability of IoT devices to transmit their data in a timely manner.

These results, in addition to what was published earlier in, e.g., [8,9], illustrate the limitations of the random-access model when used in the context of massive IoT networks, and several approaches to solve this have already been proposed in the literature. Narrowband (NB) [11,12] has been proposed to address this limitation by dividing the band into many channels. This approach aims to provide more access opportunities for IoT devices to transmit at the expense of bandwidth. However, although NB could support thousands of connections, it is only applicable in the context of a cellular IoT where transmissions follow a schedule set by the base station [13].

Algorithm 1: Access Node

all_satisfied = 0
iteration = 0
$Iterations \leftarrow \emptyset$
$Satisfaction \leftarrow \emptyset$
get set N
while *all_satisfied* == 0 **do**
  connect all devices $\in N$ to their best allowed gNB
  iteration += 1
  satisfied = 0
  $N' = N$
  for each $i \in N$ **do**
    if $R_i \geq R_{reqi}$ **do**
      remove i from set N'
      satisfied += 1
    end if
  end for
  $M = \left(\frac{satisfied}{N}\right) * 100$
  $Iterations \leftarrow Iterations \cup \{iteration\}$
  $Satisfaction \leftarrow Satisfaction \cup \{M\}$
  if M == 100 **do**
    all_satisfied = 1
  else do
    $N = N'$
  end if/else
end while
plot(Iterations, Satisfaction)

Outside of the area of radio access schemes, network densification has also been proposed to address this challenge by increasing the number of radio access nodes. This approach will also offer more radio channels, improving the opportunities for an IoT device to transmit data, and reduce the delay incurred while waiting for access to the medium. To showcase the benefits of network densification, we conducted another experiment with 2000 IoT devices in the same open area of 80 m $\times$ 80 m while gradually increasing the number of gNBs from 4 up to 12. Figure 2 shows the number of attempts necessary to reach 100% satisfaction in the IoT network as a function of the number of gNBs, calculated using Algorithm 1 described above. Note that the number of attempts corresponds to the number of iterations computed as explained for Algorithm 1 above, and the 100% satisfaction condition means that all the devices have successfully transmitted their data. As we can observe from this figure, the number of iterations decreases linearly as the number of deployed access nodes increases.

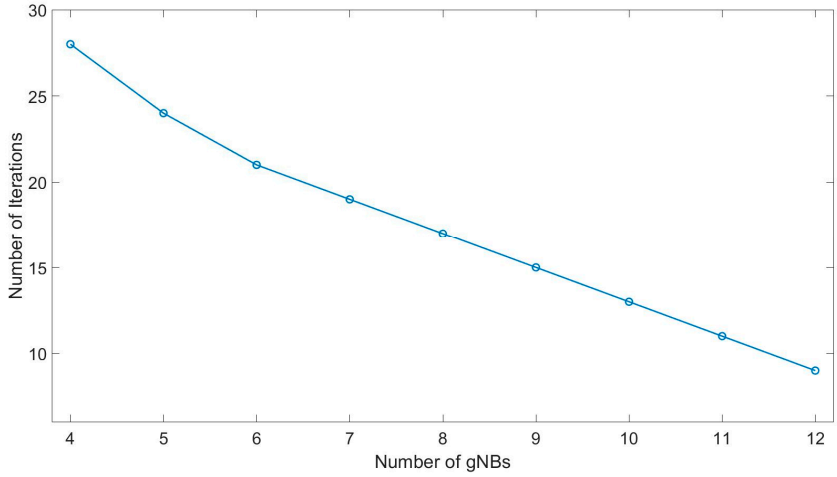


Figure 2. Number of attempts necessary to achieve 100% satisfaction as a function of the number of gNBs.

In theory, therefore, network densification could be considered as the perfect solution to meet the requirements of a massive IoT. However, such an increase in the access node infrastructure will come at a cost that might be prohibitive for many operators. Studies such as in [14,15] estimated that the cost associated with a single gNB could reach up to €82,000, notwithstanding the ongoing cost of operation. Using the results shown in Figure 2, we plotted the success rate of an IoT device transmitting its data calculated against the cost incurred by the number of gNBs. The success rate was calculated as the reciprocal function of the number of attempts. The cost C incurred by the number of necessary gNBs was calculated as follows:

$$C = €82,000 \cdot \mathrm{N} \quad (1)$$

where N is the number of gNBs. As shown in Figure 3, an operator needs to spend over one million EUR just to reach the connection success rate of 11%. These results demonstrate the challenge telecommunication operators face in terms of infrastructure investments to meet the requirements of a massive IoT.

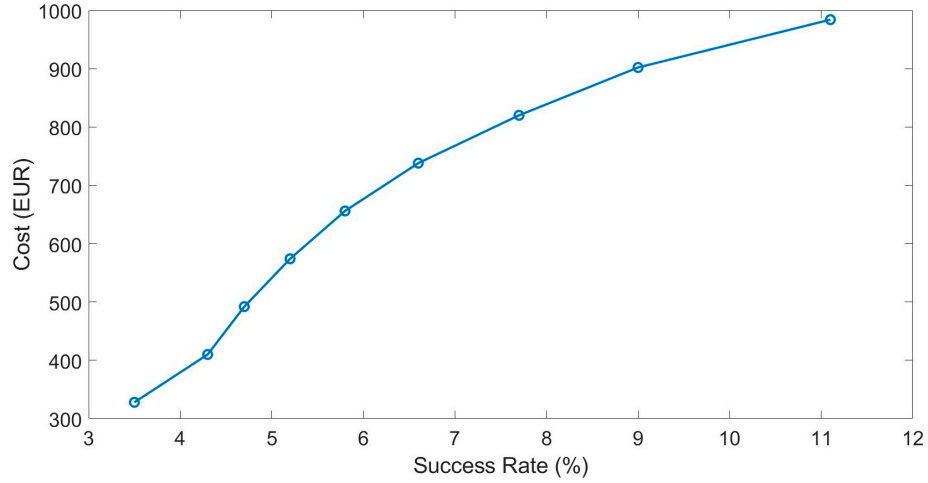


Figure 3. Cost incurred by operators to increase the success rate of IoT devices for accessing the RANs.

3. Literature Review of Spectrum-Sharing Methodologies

3.1. Spectrum Sharing for Massive IoT

5G and the upcoming 6G technologies will benefit several industry areas through massive IoT implementation. Specifically, it is foreseen that over 50 billion IoT devices will be connected by 2030 and, therefore, new solutions that go beyond the traditional

spectrum-sharing models must be found because the available frequency resources are limited [16]. Work in [17] proposed a model for spectrum selection in a massive IoT based on the estimation of the available spectrum for the transmission of ubiquitous data. However, this solution is tailored for a generic architecture that does not take into account mobile networks' specifications and, therefore, its implementation is challenging and not realistic. The authors of [18] presented a multi-operator dynamic spectrum-sharing strategy for massive IoT devices among mobile network operators (MNOs) where a wireless spectrum provider (WSP) addresses spectrum trading through the Stackelberg pricing game. However, this work does not provide a trustful and secure strategy that can encourage and incentivise MNOs to adopt this solution. Moreover, game theory-based approaches often need a prohibitive amount of computational time to find the optimal solution. In [19], we illustrated HODNET (*Heterogeneous on Demand NETwork resource negotiation*), an open platform based on SDWN able to realise a novel vision to trade and allocate the wireless spectrum in 6G communication networks inspired by the concept of the sharing economy. Moreover, we analysed the benefits of our platform with a use case of massive IoT deployment. However, HODNET does not guarantee trust nor provide security guarantees to encourage operators to trade the shared spectrum. The authors of [20] presented a green spectrum-sharing framework targeted for a massive IoT in a Beyond 5G (B5G) network using the concept of crowdsensing. However, the main limitation of this work is that crowdsensing needs (1) complex techniques to minimise possible abnormal users' behaviours through the computation of their trust level and (2) the support of incentive mechanisms to guarantee a minimum number of participants.

Cognitive radio-based IoT systems represent another approach to addressing spectrum sharing supported by spectrum sensing, allowing for the opportunistic utilisation of a spectrum band by the use of licenced channels free of transmission [21]. The cognitive radio spectrum sensing performance, however, necessitates detection accuracy whether primary users are active or not and, therefore, requires more energy effort from the secondary IoT users [22]. In this context, secondary user teamwork can optimise spectrum detection operations in cognitive radio networks [23]. However, recurring teamwork-based spectrum sensing violates the energy restriction in cognitive radio nodes and needs the prediction of the spectrum occupancy to optimise energy efficiency.

In this paper, in a step beyond the current state of the art, we propose a simple, easily implementable, and efficient approach that could fully apply the laws of the market to incentivise a fairer and more consumer-oriented allocation of the spectrum resource.

3.2. Applying a Sharing Economy to Radio Access

A sharing economy is a socio-economic paradigm that promotes the sharing of human and physical assets to deliver a service. This paradigm has emerged as the result of recent societal forces combined with advances in information and communication technologies. In its simplest form, a sharing economy entices entities that in traditional models were considered as consumers of a specific resource to also become providers of that same resource. As a result, a sharing economy enables the discovery and access of resources that were previously unavailable or not conveniently available. Several business models based on a sharing economy have already been successfully introduced into consumer-based services such as transportation and hospitality [24]. It is therefore natural to consider if this model could be applied to the field of wireless communications in the context of 6G [19,25].

A study conducted in [26] investigated the main trends the telecommunication industry is exposed to, and the main findings of this study are illustrated in Figure 4. The figure plots various trends in terms of their perceived degree of uncertainty (how likely they are to happen) and the degree of impact (if they happen, how much this will impact the industry). The study identified sharing economies among the trends that could lead to a major impact on the sector, with a fairly high probability of it happening.

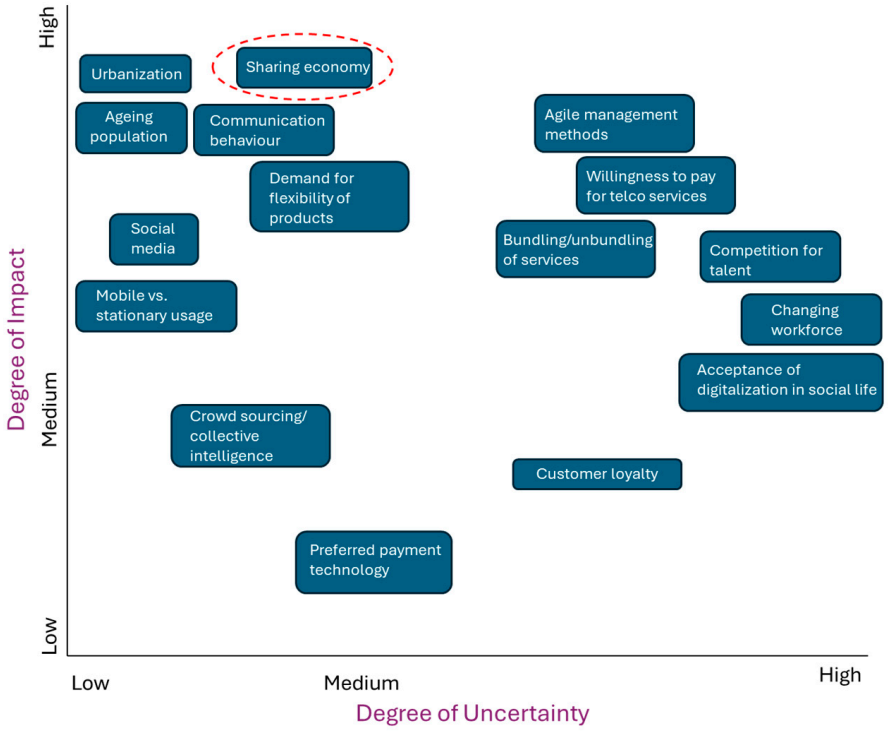


Figure 4. Degree of uncertainty of telecommunication landscape drivers and their degree of impact [26].

There have already been several studies that have investigated the introduction of a sharing economy to wireless communication networks. In [27,28], the authors discussed the potential of "uberisation" in making the telecommunication market more competitive and transparent. The authors of [27] also proposed an Uber-like business model for trading communications and computing resources, with the focus on cloud computing resources. In [29], the authors proposed a pricing scheme to realise an Uber-like spectrum-sharing model between wireless users using Non-Orthogonal Multiple Access (NOMA), and the authors of [30] addressed the challenges related to spectrum sharing in the context of a sharing economy. More specifically, they investigated the possibility of applying a roaming rate to incentivise a service provider (SP) to gain extra revenue when its customers temporarily leverage another SP's service. In [31], the authors investigated the application of a blockchain to realise spectrum sharing and addressed the scalability issues that arise from the application of blockchains in large wireless networks.

The aim of our work is to leverage the sharing economy paradigm to provide faster access to the wireless medium for IoT devices to send their data when densely deployed, as is the case in a massive IoT. This is different from existing models that try to apply sharing economy principles to wireless and mobile networks, where the focus is mostly on enabling better roaming and providing more bandwidth. More specifically, we aim to use sharing economy concepts to propose a radio access scheme that will maximise the scalability of the wireless network while also considering the limitations of IoT devices, which are often battery-powered and therefore necessitate energy-efficient solutions.

In addition to the conditions identified above, the radio access scheme should incentivise operators to participate in the sharing economy, i.e., we do not assume an a priori given "super operator" or government mandating collaboration and sharing amongst operators. Here, by operator we mean any entity that owns or manages a wireless network and its RANs. This operator should be able to offer wireless connectivity that allows IoT devices to transmit their data. The incentivisation mechanism should also be transparent such that it establishes trust among the participants.

4. Design Challenges and Key Architectural Components

4.1. Design Challenges

The synergy between a sharing economy and telecommunication is yet to be translated into a tangible adoption of this paradigm. In 2006, a startup called FON sold modules that customers could connect to their home gateway enabling the sharing of their Wi-Fi network with other owners of such FON modules. Incumbent operators were quick to disable FON modules to deliver this as an over-the-top service, and although sharing is still possible, an economy never emerged. The work in [27,28] proposed a platform inspired by Uber [32] to share and trade communications and computing resources. However, the authors never addressed the design issues that face the adoption of this paradigm by the telecommunication sector. The main challenges and issues with the works mentioned above are (1) the assumption that the RAN infrastructure works under a single administrative control and (2) the lack of a realistic strategy to guarantee trust, incentives, transparency, and accountability among the actors.

In the context of a massive IoT, this then leads to the following design issues that need to be addressed before sharing economy concepts can be applied to radio access:

- *Heterogeneity.* We aim to leverage the potential of a sharing economy to entice private wireless users to provide their personal devices as access nodes for IoT communications. These devices will have different hardware and software capabilities, and maybe also different Radio Access Technologies (RATs) such as 5G and Wi-Fi. Any solution based on the sharing economy will need to consider this heterogeneity as a core aspect of 6G.
- *Scalability.* Any sharing economy-based solution for massive IoT access needs to support the anticipated scale and density of networks and devices in both current and future deployments.
- *Managerial Complexity.* The sheer size of the IoT networks and the mixture of private and public networks involved in this process along with the heterogeneity imposed will be complex to manage. This involves identifying the operators who agree to participate in the sharing economy model, managing the RANs of these operators, and managing the IoT networks that will use these RANs and all the resources allocated and transactions involved as part of this process.
- *Incentivisation and Transparency*. Actors that will adhere to this sharing economy-based radio access scheme will likely be operating independently from each other with no central authority with the ability to guarantee trust, incentives, transparency, dispute resolution, and accountability among the actors. The designed solution needs to provide this level of guarantee.

Addressing these design challenges as part of 6G will necessitate adopting a different design approach and using different technologies and concepts than what are currently used today [33]. In the following sections, we will cover the most promising trends that could help in achieving a radio access solution based on a sharing economy.

4.2. Softwarisation and Virtualisation

In the last few years, communication networks have witnessed a paradigm shift in the way data traffic and bandwidth resources are managed. The introduction of softwarisation has allowed us to move from running functionalities in hardware to running them as software. Network softwarisation, therefore, offers a high degree of reconfigurability and flexibility in comparison to traditional network management and helps to reduce the network deployment and overheads. Softwarisation has since been adopted for wireless networking using a combination of both SDN and network function virtualisation.

Network function virtualisation is among the most popular softwarisation concepts currently adopted by data network operators. It allows operators to create virtualised instances of the network hardware infrastructure, resources, and physical connections. Virtualisation abstracts away from the complex details of the hardware and makes it possible to move virtual instances across different hardware platforms and technologies

dynamically. Virtualisation could also be used to simplify the management of connections between access nodes and wireless devices. For instance, the architectures presented in [34,35] propose to virtualise wireless access points (APs) by creating Lightweight Virtual Access Points (LVAPs). The use of LVAPs facilitates the management of wireless connectivity and the allocation of radio resources to satisfy QoS requirements. Such features could be useful to addressing the heterogeneity and complexity design issues identified above.

Software-Defined Networking (SDN) is another softwarisation concept that facilitates the management of communications networks and reduces their operational complexity. By separating the control plane from the data plane, SDN can centralise the management of communication networks without compromising scalability. The rise of Software-Defined Wireless Networking (SDWN) [36] represents an extension of SDN to wireless networks. The centralised yet scalable management approach is particularly attractive for IoT networks as it helps to coordinate transmissions and other management operations that would be otherwise be difficult to carry out in a scalable manner [37].

4.3. Programmability

One of the main features inherited from the current advances being made in the network softwarisation domain is the abstraction of the underlying layers, exposing them as an application programming interface (API). The introduction of programmability is currently being investigated in several areas ranging from 5G and O-RAN networks to metasurfaces [38,39]. The diagram in Figure 5 is taken from a study by Deloitte [40] in which they investigated the potential of automation and programmability in telecommunication management. It shows that the scalability and heterogeneity of IoT networks is a major factor behind this trend. Similar studies such as the one by TM Forum [41] have also highlighted the potential of programmability in making large and heterogeneous wireless networks, such as a massive IoT, simpler to manage.

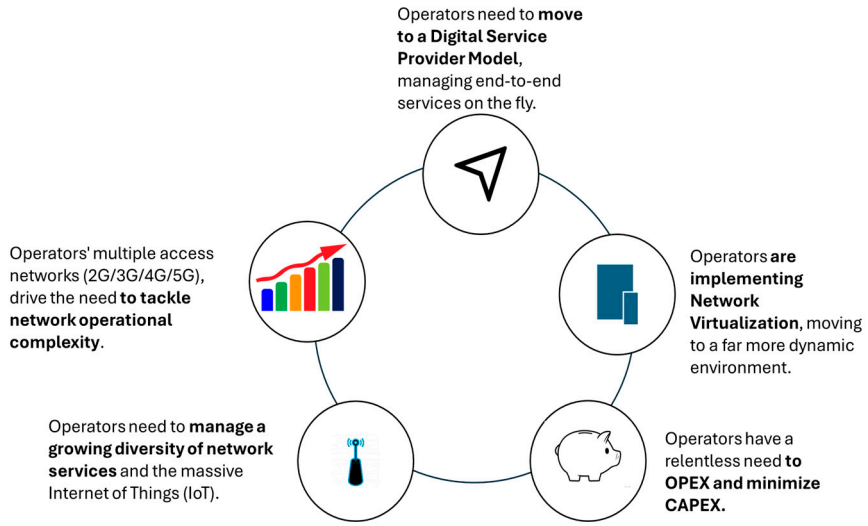


Figure 5. Factors behind the adoption of programmability in telecommunications with the massive IoT as a major driver behind this trend [40].

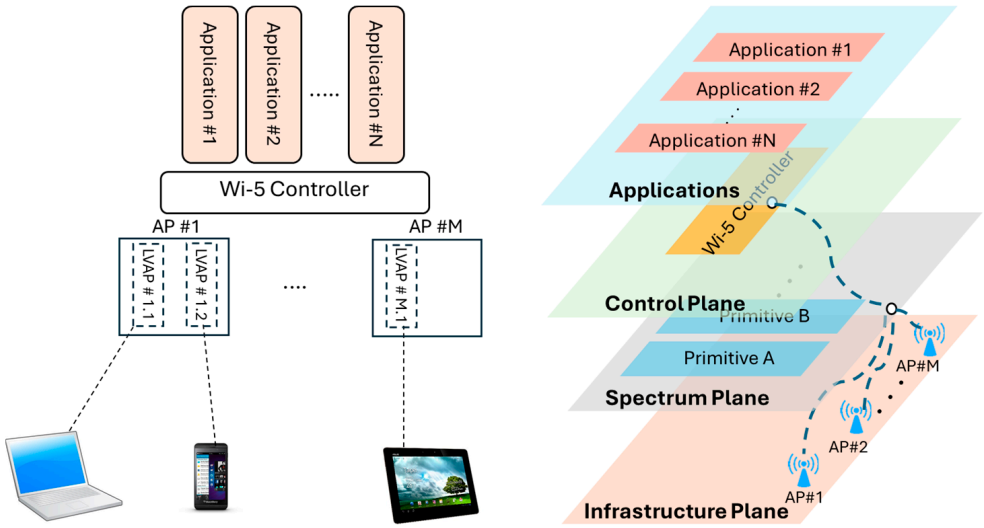
4.4. Blockchain

A blockchain is a distributed system that consists of a chain of interlinked blocks storing encrypted information. The chain grows continuously as new blocks are appended to it. A blockchain works in a decentralised environment and is enabled by comprising several core technologies, such as digital signatures, a cryptographic hash, and distributed consensus algorithms. The main characteristics of a blockchain are decentralisation, immutability, transparency, and auditability. They make blockchains a suitable technology for decentralised verification or transactions, as evidenced by the several applications that utilise it to enforce the transparent trading of resources, including radio resources [42–44]. Therefore, blockchains

could play a major role in enabling a sharing economy such as the one targeted in this work through resolving the incentivisation and transparency design issue.

4.5. Spectrum Programming Architecture and Smart Connectivity Management

In [34], we introduced the concept of spectrum programmability. By that, we mean an extension of the programmability from layer 3 of the networking stack (as in SDN) downwards, such that the use of the radio spectrum itself becomes directly programmable too. We showed that SDWN, virtualisation, and programmability could be combined to provide a centralised and scalable architecture to manage IEEE 802.11 wireless networks. More specifically, we have shown, as illustrated in Figure 6a, that such an architecture can enable wireless network managers to implement specific policies as applications running on top of the central controller. The architecture depicted in Figure 6b extends existing programmable network architectures by introducing the spectrum plane. This plane exposes primitives that allow us to change the configuration of the RANs, i.e., access points, in the infrastructure planes. In addition, the architecture promotes the concept of LVAPs as mentioned above, which are designed to manage connections between end devices and access points.



(a) A high-level depiction of the Wi-5 architecture

(b) Planes and programmability in the Wi-5 architecture

Figure 6. Depiction of the Wi-5 architecture and programmability [34].

In this context, among the controller applications developed that exploit the LVAP concept is a smart connectivity application. This application enables us to seamlessly move the connectivity of a wireless device from one AP to another according to its QoS requirements by making Basic Service Set Identifiers (BSSIDs) (a layer 2 parameter) programmable. This is depicted in Figure 7: the smart connectivity application enables the LVAP associated with a wireless device to move from AP1 to AP2 if the latter can better meet the QoS requirements of the application running on the device. By extending this concept to heterogeneous infrastructures that can support a range of RATs, we therefore resolve a key part of the complexity design issue identified above.

As such, the design challenges that we face when adopting radio access based on a sharing economy could be addressed if recent advances in softwarisation and blockchains are adopted and properly integrated. Table 1 summarises these trends and the design challenges they could help address.

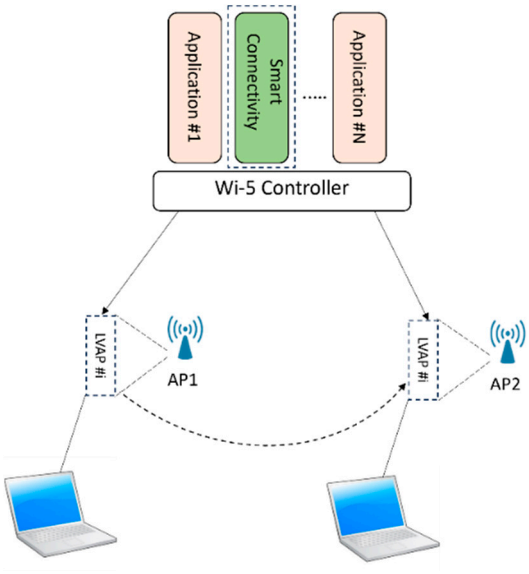


Figure 7. Illustration of using LVAPs to manage connectivity in Wi-5.

Table 1. Main trends and their potential in addressing the design challenges raised by adopting a shared economy for radio access in the massive IoT.

	Complexity	***Scalability***	***Heterogeneity***	***Transparency***
Virtualisation	X		X	
SDWN		X		
Programmability	X			
Blockchain				X

5. Sixth-Generation Radio Access Architecture Enabling a Sharing Economy for the Massive IoT

5.1. Approach

A radio access scheme based on shared economy concepts where private wireless users could provide access to IoT devices to transmit their data represents both a cost-effective and more efficient alternative to what is currently available.

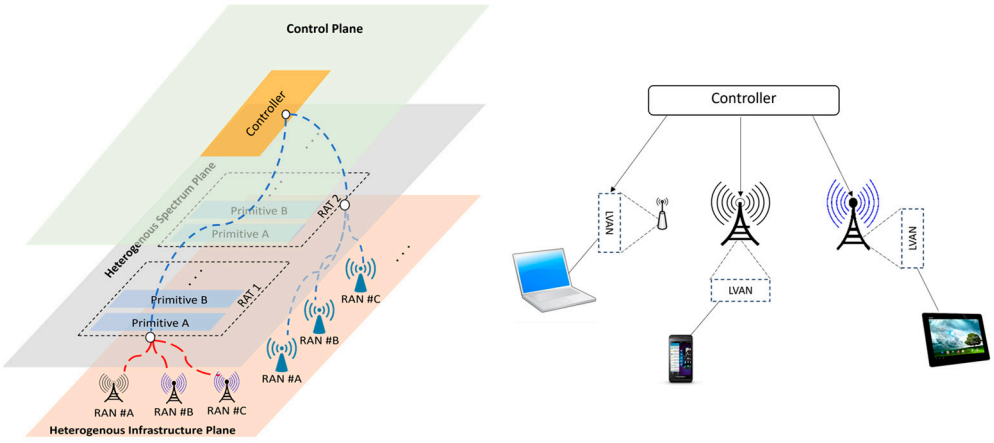
As described above, virtualisation, programmability, and a centralised implementation make the architecture of [34] and that is depicted in Figure 6 a suitable starting point to achieve the objective of this research. Our aim is, therefore, to extend this architecture to realise radio access for the massive IoT based on the concept of a sharing economy. The extension covers three dimensions not previously considered in the initial architecture:

- Heterogeneity support.
- Connectivity management.
- Cooperation and transparency.

5.2. Heterogeneity Support

The support for heterogeneity was achieved by extending the infrastructure plane, the spectrum plane, and the concept of LVAPs to support other RATs beyond IEEE 802.11. Figure 8 shows the proposed extension covering the aforementioned components. RANs that operate different RATs will now be managed by a Heterogenous Infrastructure Plane. Similarly, the Heterogenous Spectrum Plane exposes primitives that will allow us to manage the connection to these RANs and monitor them along with the networks they provide access to. These primitives will be specific to all RATs supported by the architecture. In this paper, we will primarily discuss IEEE 802.11 and 5G in this respect. The LVAP virtualisation will be extended such that any RAN will be able to host a virtual instance,

called a Lightweight Virtual Access Node (LVAN), and to associate it with a device it grants access to.



(a) Extension of the spectrum plane and spectrum plane to support heterogenous RATs and RANs

(b) Use of an LVAN as an abstraction in the architecture

Figure 8. Depiction of the heterogeneous infrastructure plane, heterogeneous spectrum plane, and LVAN in the proposed solution.

As shown in Figure 8a, similarly to the architecture initially proposed in [34], the controller will create and manage the LVANs as well as the connections associated with them using the primitives exposed by the Heterogeneous Spectrum Plane. Figure 8b illustrates an example of how this will work in a real deployment, where the controller creates and manages LVANs for each connection served by each RAN. Such an extension should be feasible as we can see an increasing number of RATs, including 5G, becoming accessible and configurable through SDWN centralised architectures [45–47].

5.3. Connectivity Management

Using the extended architecture described in Section 5.2., we have developed an application to manage the connectivity between IoT devices and the available RANs. The application provides the controller with information related to the identity of the IoT devices that need connection and the identity of the RANs they may be connected to. The allocation of RANs to devices is based on the pseudocode illustrated in Algorithm 2. The aim of the algorithm is to use the information available in the Heterogeneous Spectrum Plane to implement the concept of the sharing economy. Specifically, the algorithm will allow the IoT devices to connect to any available RAN, guaranteeing (1) a fair distribution of the load among the RANs managed by our architecture and (2) the minimum bit rate required by the IoT devices.

The application relies on information obtained from one of the main primitives in the Heterogeneous Spectrum Plane, namely the monitoring primitive. This primitive will measure, for each RAN j, the Received Signal Strength Indicator (RSSI) for each IoT device i connected to it, i.e., $RSSI_{i,j}$, and the number of devices connected to it. $RSSI_{i,j}$ is computed as follows:

$$RSSIi, j = P_j - 10 \cdot \mathrm{n} \cdot log_{10}(d) \quad (2)$$

where P_j is the transmit power of the RAN j, n is the path loss exponent set to 2.5, and d is the distance between the RAN j and the IoT device i. This part is labelled as step 1 in Figure 9a. In terms of the algorithm for the connectivity application, the monitoring information is stored in a set RAN_i that feeds the algorithm (line 1 of Algorithm 2). Then, the algorithm dynamically connects each IoT device i to the RAN (belonging to any of the operators) with the minimum number of connections and providing a sufficient RSSI based on the data rate requirements defined as *minRb* (lines 2–11 in Algorithm 2). If a RAN

providing a sufficient RSSI and *minRb* is not found, the algorithm chooses the RAN with the highest RSSI if the latter is not congested (lines 12–14 in Algorithm 2). Note that the *Rb* for a device *i* in line 7 is computed using the Shannon–Hartley theorem, also taking into account the number of IoT devices connected to the corresponding RAN and its capacity in terms of the bps. Further details of this computation can be found in [48]. The identity of the chosen RAN is passed by the connectivity application to the controller, labelled as step 2 in Figure 9a. The controller, then, connects the IoT device to the chosen RAN, which is labelled step 3 in Figure 9a.

Algorithm 2: RANs Allocation

1: **get** RAN_i
2: $RAN1_i$ = RAN ordered by IoT devices number(RAN_i)
3: $RAN2_i$ = RAN ordered by RSSI(RAN_i)
4: *found* = 0
5: *j* = 1
6: **while** (*found* == 0) && (*j* <= length($RAN1_i$)) **do**
7: **compute** Rb_i
8: **if** Rb_i >= minRb **do**
9: **connect** *i* **to** $RAN1_i$ (*j*)
10: *found* = 1
11: **end if**
12: **if** (*j* == length($RAN1_i$)) && (*found* == 0)
13: **connect** *i* **to** $RAN2_i$ (1) if possible
14: **end if**
15: *j* += 1
16: **end while**

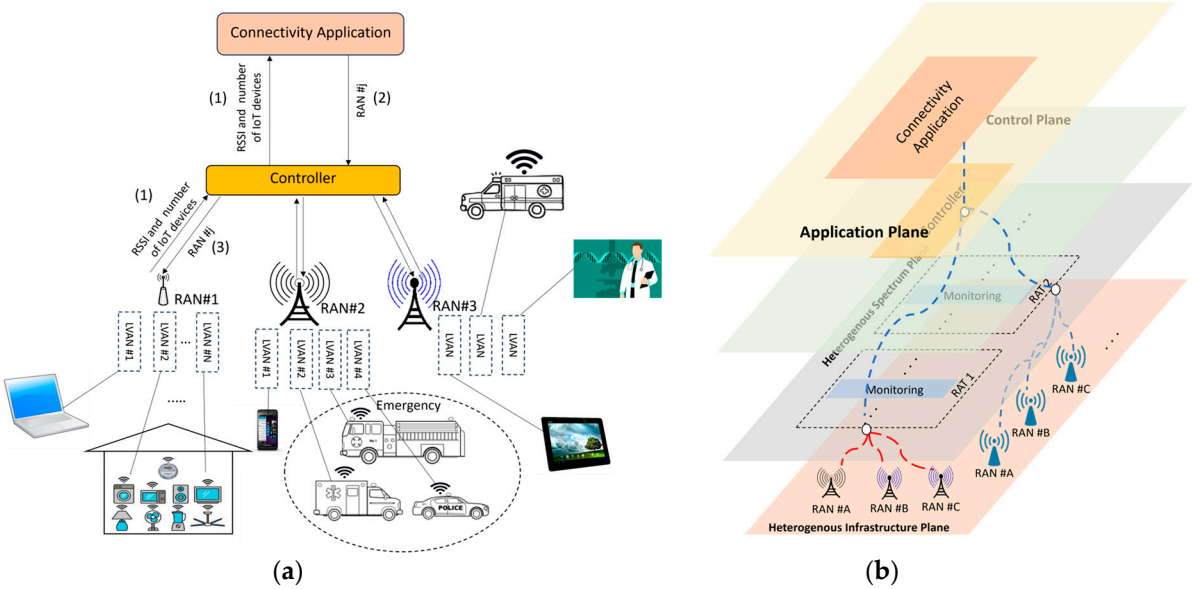


Figure 9. Description of the deployment of the connectivity application as part of the proposed solution. (**a**) Use of the controller's monitoring information and LVAN to manage the connectivity between IoT networks and RANs. (**b**) Use of the connectivity application in the application plane on top of the controller.

From an architectural point of view, and as shown in Figure 9b, the connectivity application sits in the application plane just above the control plane. The controller is able to gather the necessary monitoring information and pass it on to the connectivity application, which in turn provides the controller with the identity of the RAN.

5.4. Transparency

At the heart of the proposed solution sits the cooperation and trust among the operators who agree to share their access nodes with IoT networks. To achieve this, we propose a brokering plane to be added to our architecture as first suggested in [49]. It resides above the connectivity application and acts as an interface between the application and the operators, as shown in Figure 10. When a RAN #n operator intends to join the collaboration, its node (AP, gNb, . . .) identifies itself and its operator to the Brokering Platform. It can use any existing management protocol for that, e.g., Simple Network Management Protocol (SNMP). The brokering plane is based on a permissioned blockchain network, for instance, a Hyperledger Fabric (HLF) as described in [50] where participants' identities are verified before they can join. The choice of this type of blockchain is justified by the unneeded CPU mining which results in a faster consensus while still guaranteeing decentralisation, immutability, provenance, and finality.

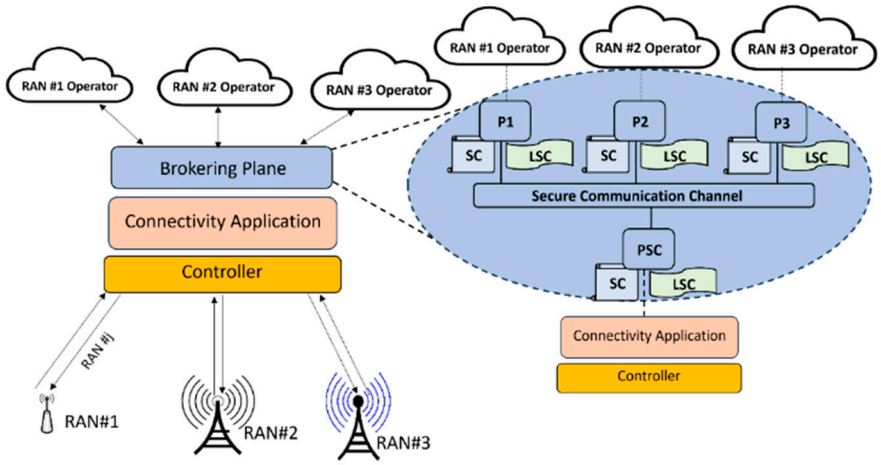


Figure 10. Description of the brokering plane and its interaction with operators and the connectivity application.

Each operator that is trading the use of their RAN has a peer node Pi to execute the smart contract (SC) functions and maintain a copy of the cooperation records (i.e., a ledger) as explained below. The SC is the implementation of the sharing agreement between the RAN operator and the IoT operator. The SC includes agreement details such as the identity of the RAN that can be accessed, the duration of the availability of the RAN, and the cost to use it. In [50], all SCs are defined using Node.js in the HLF blockchain network. Note that the SC is installed on all peer nodes and must be approved by all these peers before any transaction can take place. In our work, the cost is determined during the negotiating process by operators who join the system, as will be explained later in our incentive mechanism.

In addition to the SC, the SDWN Controller Ledger (LSC) maintains the records of all connections served by the operators' RANs to the IoT devices as per the agreement in the SC. A dedicated secure communication channel enables all peers in the blockchain network to communicate and transact securely and privately. The ledger records are accessible only for operators, via their peer nodes, who have been granted access to the channel. Hence, a copy of the LSC and SC is available in each operator's peer node Pi in the network. Additionally, there is a peer node that is managed by the controller to allow for interaction between the controller and the blockchain network and keeps a record of the LSC and SC. The SDWN Controller Peer (PSC) keeps records of all LSCs and SCs. The SCs generated during the negotiations are passed to the PSC which then interacts with the connectivity application via the brokering plane to pass on the relevant information such as the identity of the shared RANs. Similarly, the PSC updates the LSCs with the information passed on

by the connectivity application, namely the IoT devices that accessed a specific RAN, the number of connections, and the duration of the access.

5.5. Incentive Mechanism

In our work, we aim to encourage any RAN operator to join the proposed solution and trade their RANs with other operators when needed. To incentivise operators to participate in this framework, we propose to record the cost incurred when they share their RANs with other operators. This cost will later be converted into a reward in the form of the right to use other operators' resources. From a business perspective, participation in any collaborative effort must return a positive value for the operator. In other words, the benefit from collaboration for an operator OP_i, denoted as the gain G_i, must be larger than the cost of participation, denoted as C_i hereafter. It is worth noting that depending on the RAN capacity and the IoT network demands, which are often dictated by the IoT application and the size of the network, costs and gains are not necessarily constant over time. Therefore, adopting the concept of generic tokens as a reward mechanism for incentivising operators to participate is not suitable here given the dynamic nature of these demands. Therefore, a novel direction is needed.

Our incentive mechanism is therefore based on an SC designed to maximise the benefits for participating operators focusing on bandwidth and meeting IoT network requirements. This SC is initially offered by the controller, based on its global view of the RANs, network devices, and conditions at a given time t, and its execution is guaranteed by the blockchain network (i.e., cooperation records). Moreover, this contract is negotiable upon new operators joining the system to ensure the current operators' interests are still maintained. This way, our incentive mechanism can deal with the dynamic nature of changing gains/costs according to network conditions, whereas a simple token-based rewarding scheme cannot.

Without a loss of generality, let $G_i(\Delta t)$ and $C_i(\Delta t)$ be the gain and the cost an OP_i would experience from participating in the collaboration for a period Δt, respectively. The cost $C_i(\Delta t)$ can be defined as follows:

$$C_i(\Delta t) = \Delta t.\beta_{given} + ¤_i \tag{3}$$

where β_{given} is the bandwidth consumed by other networks when using the RANs of the OP_i and $¤_i$ is the operational cost associated with the usage of these RANs. The operation cost could include the energy consumption, the annual cost associated with maintaining each RAN, etc. The gain $G_i(\Delta t)$ can be defined as follows:

$$G_i(\Delta t) = \Delta t.\beta_{received} + \Gamma_i, \tag{4}$$

where $\beta_{received}$ is the bandwidth gained by the operator OP_i when their devices or users access other operators' RANs and Γ_i is the increase in the satisfaction of these devices or users as a result. We assume that the controller is able to obtain the values of $\beta_{received}$, β_{given}, and Γ_i, based on its global view of all networks and devices connected to them.

When at least two operators, OP_i and OP_j, decide to join the collaboration platform, they will receive initial contracts via the controller that contain $\{C_i(\Delta t), G_i(\Delta t)\}$ and $\{C_j(\Delta t), G_j(\Delta t)\}$, where

$$G_i(\Delta t) - C_i(\Delta t) \geq 0, \tag{5}$$

$$G_j(\Delta t) - C_j(\Delta t) \geq 0. \tag{6}$$

If either condition (5) or (6) is not verified, OP_i and OP_j negotiate the initial contract between them via their peers in the blockchain network. The negotiation in this case will focus on accepting the terms of costs and gains, assuming both operators are rational and it is feasible for them to collaborate. The negotiation process is carried out via a designated smart contract maintained by the controller. All the negotiation transactions are performed in the blockchain network to keep records of these steps for any future reference, e.g., in

the case of a dispute; it is transparent for every operator which contracts have been agreed to, which network configurations have been executed accordingly, and what renumeration has been exchanged subsequently. A breach of contract can be followed up by blacklisting and subsequent exclusion from the collaboration by the Brokering Platform.

6. Evaluation

In this section, we will assess the ability of the proposed solution to scale against the network sizes and densities expected in the massive IoT. We will also assess the solution's ability to incentivise operators to participate in the sharing economy model while providing transparency and accountability.

6.1. Evaluation Scenario and Parameters

In our evaluation, we simulated a dense deployment of the massive IoT, reaching the densities predicted in [1]. Such simulation scenarios will help us to reflect the conditions of such dense environments in terms of constrained radio access and the energy resources of IoT devices. For that, we considered N RANs that belong to four different operators, as well as M IoT devices, all uniformly distributed in an open area of 80 m $\times$ 80 m.

Moreover, each RAN could be either a 5G gNB base station or a Wi-Fi 802.11ah AP. In the use case investigated below, the 5G connectivity was provided by four gNBs and the Wi-Fi connectivity was offered by 16 802.11ah APs and, hence, N = 20. Furthermore, the 20 RANs belonged to four different operators, where each one managed 5 RANs, i.e., one gNB and four APs. We also considered several values of M that represent different massive IoT scenarios for the considered area, whilst assuming that IoT devices have transmission power capabilities randomly varying between 1 and 10 dBm and data rates randomly varying between 8 and 128 kbps for uplink transmissions. Finally, we assumed that each RAN offers a 5 MHz uplink channel operating on the 880–915 MHz band or a 4 MHz uplink channel on the 900–928 MHz frequency band in the case of the gNBs and Wi-Fi APs, respectively [51,52]. The parameters for our evaluation are summarised in Table 2.

Table 2. Summary of evaluation parameters.

Area size	80 m $\times$ 80 m
Number of network operators	4
RATs	- 5G - Wi-Fi 802.11ah
Frequency	- 5G: 880–915 MHz - Wi-Fi: 880–915 MHz
Bandwidth	- 5G: 5 MHz - Wi-Fi: 4 MHz
Number of RANs	- 4$\times$ gNB - 16$\times$ Wi-Fi 802.11ah Access Point (AP)
IoT devices' transmit power	1–10 dBm
IoT devices' data bit rates	8–128 kbps

To benchmark the evaluation of our system, we compared the performance of the proposed solution with the standard approach currently adopted in 5G and Wi-Fi networks and considered in several papers analysed in the state of the art [17,20,23], which simply connect each IoT device to the RAN of its operator with the highest received power without access to the connectivity offered by other operators. In contrast, our proposed approach allows the IoT devices to utilise the whole environment through the sharing economy model.

The evaluation of our approach against the standard focused on the performance metrics explained in the following sub-sections, averaged for all IoT nodes after connecting to the corresponding RAN, and these are assessed as M scales upwards.

6.2. Scalability Evaluation

To evaluate the scalability of the proposed solution we opted to measure the following metrics:

- *Signal-to-Interference plus Noise Ratio*: This metric allowed us to assess if the proposed solution is efficient in sharing the uplink connectivity in the RAN between the IoT devices.
- *Transmission Success Rate:* Measured as a percentage, this metric quantified how many IoT devices are not only able to access the RAN but are also able to transmit all their data.
- *Access Delay:* This metric assessed the flexibility of the solution in accommodating the requests of as many IoT devices as possible while minimising the number of unsuccessful attempts.

6.2.1. Signal-to-Interference Plus Noise Ratio (SINR)

The metric considered in this evaluation was the average SINR experienced by all IoT devices in the network. The value of the SINR experienced by a device i connected to an access node j is computed using

$$SINR_{i,j} = \frac{g_{i,j} \cdot p_i}{\sum_{k \in I'} g_k \cdot p_k + N_0} \quad (7)$$

Here, $g_{i,j}$ is the channel gain from the device i to the access node j, which includes the transmitted gain, the receiver gain, and a large-scale path loss model with the path loss exponent set to 2.5. p_i is the transmit power of the device i, N_0 is the additive Gaussian white noise. Moreover, considering I as the set including all the IoT devices, $I' \subseteq I$ represents the sub-set of devices interfering with device i and, therefore, affecting the SINR it experiences. Finally, g_k and p_k are the channel gain from the interfering device k to the access node it is connected to and its transmit power, respectively.

Figures 11–13 illustrate the SINR performance results computed using Equation (7) and converted to decibels (dB) for different numbers of connected IoT devices. The upper and lower sides of the plotted boxes are the 25th and 75th percentiles of the values. The median values are indicated by the central red lines. The values which we considered as outliers are indicated by red dots. The figures show that our sharing economy-based solution results in better performance in terms of the SINR compared to the standard approach regardless of how many IoT devices are connected to the network.

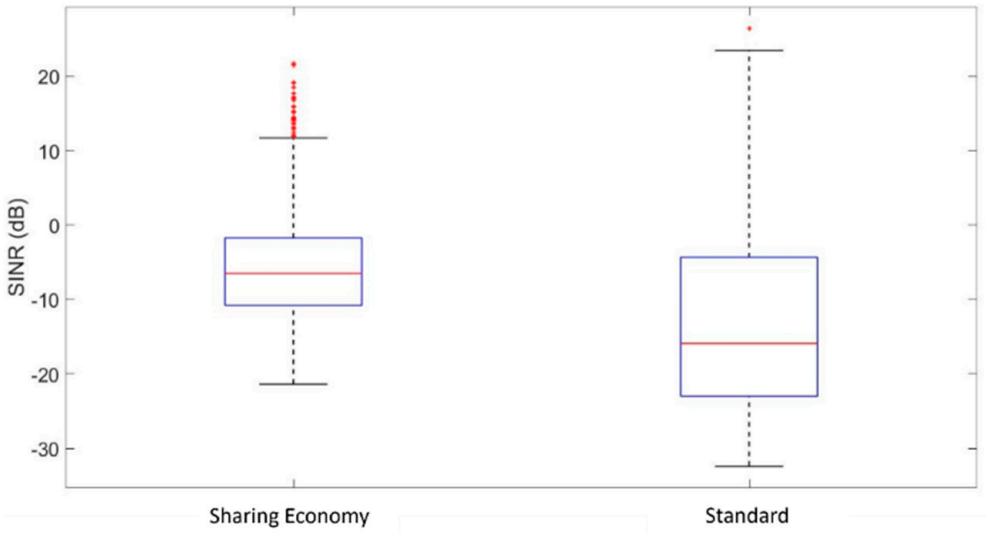


Figure 11. Measured SINR when using 5G and sharing economy for M = 1000.

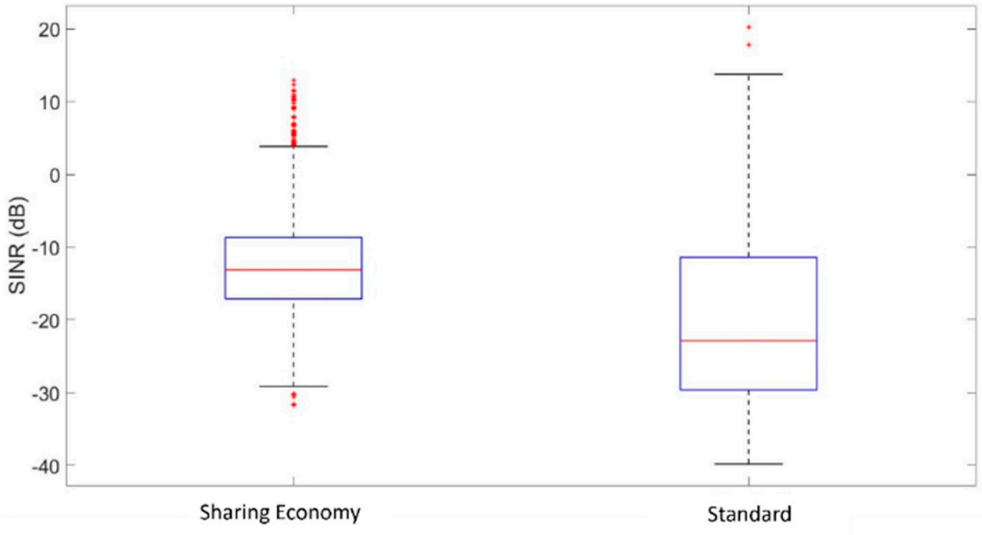


Figure 12. Measured SINR when using 5G and sharing economy for M = 2000.

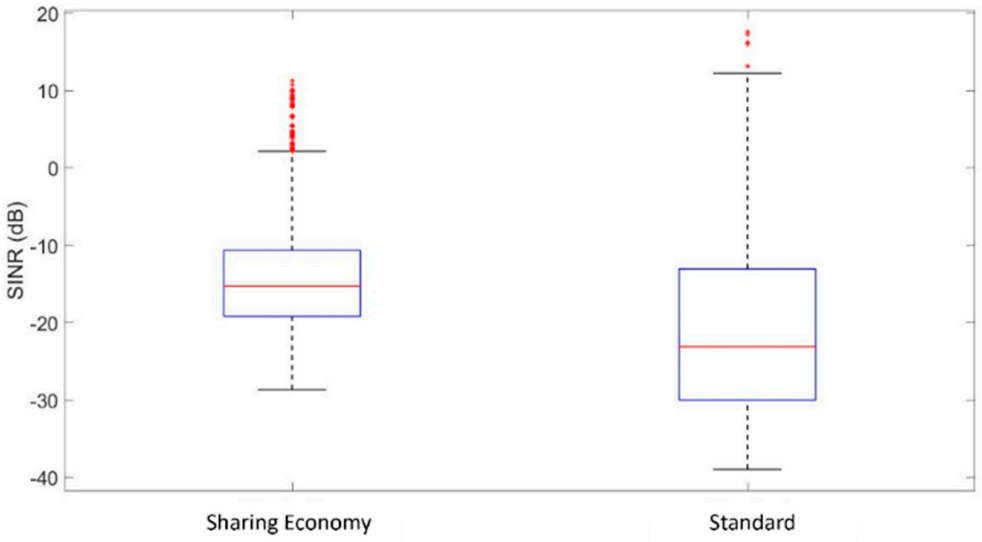


Figure 13. Measured SINR when using 5G and sharing economy for M = 3000.

6.2.2. Transmission Success

This metric was measured by counting the number of IoT devices able to send their data according to their bit rate requirements in a single attempt and those that are blocked due to congestion. Figure 14 illustrates the percentage of IoT devices not able to send their data from the first attempt. This illustrates how the overall increase in the SINR shown in the previous sub-section also leads to improved connectivity. Specifically, it shows that the probability of an IoT device being denied transmission on its first attempt decreases by 77%, 18%, and 6%, for M = 1000, 2000, and 3000, respectively, when the sharing economy-based solution is applied compared to the standard connectivity scenario.

However, this result also shows that, while IoT devices have a greater chance of successfully transmitting their data in the proposed network resource-sharing model, the ability of both models to satisfy IoT devices decreases dramatically as the number of nodes increases. This is confirmed by Figure 15, which shows the percentage of IoT nodes able to transmit their data in relation to the IoT network's density, i.e., the #devices/area in the figure. Therefore, while our sharing economy-based solution can offer extra spectrum capacity and help in optimising its utilisation, the performance of this approach will eventually reach a saturation point dictated by the density of the network and the access technology. In other words, applying a sharing economy paradigm enables the better

optimisation of available (spectral) resources, but does not create additional resources needed to satisfy exceedingly high densities of devices even in a fully optimised way.

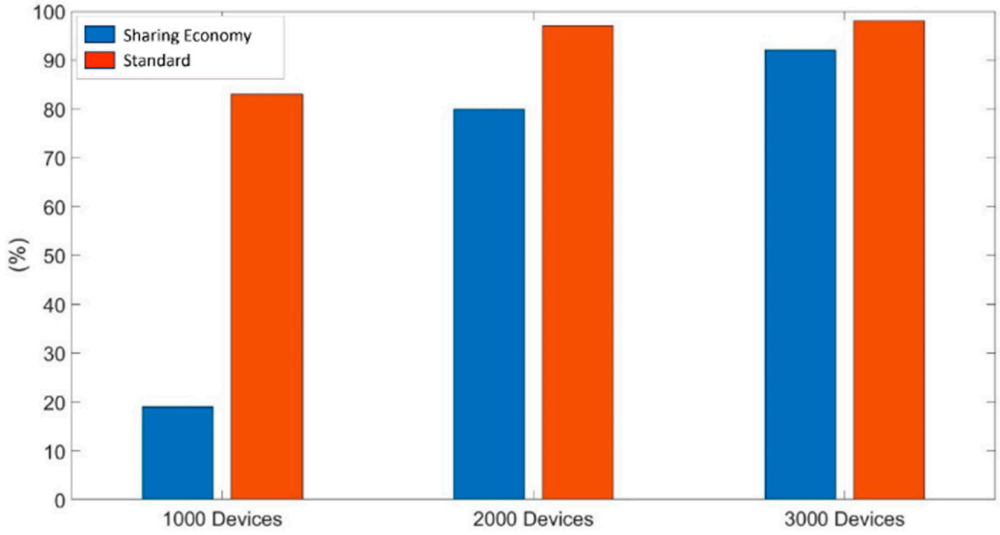


Figure 14. Probability of unsuccessful connectivity for different numbers of IoT nodes.

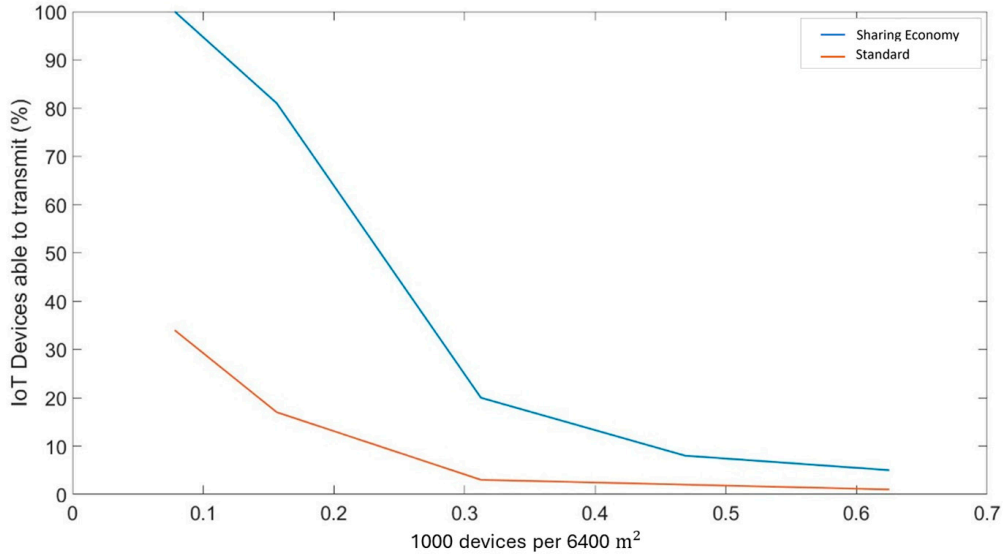


Figure 15. Percentage of satisfied IoT nodes as a function of IoT network density.

6.2.3. Access Delay

This metric was represented by the number of attempts it takes before all IoT nodes are able to transmit their data. Figure 16 illustrates this metric as the number of iterations in relation to the percentage of IoT nodes able to transmit their data (i.e., the success rate) computed using Algorithm 1.

From the figure, we can see that it takes a little more than ten attempts for all the IoT nodes to be satisfied using our sharing model, which is roughly a quarter of the attempts it takes to reach the same result in the standard 5G approach. This result shows that, even though fundamental limitations exist in the access technologies currently available, a sharing approach can scale much better than the standard approach.

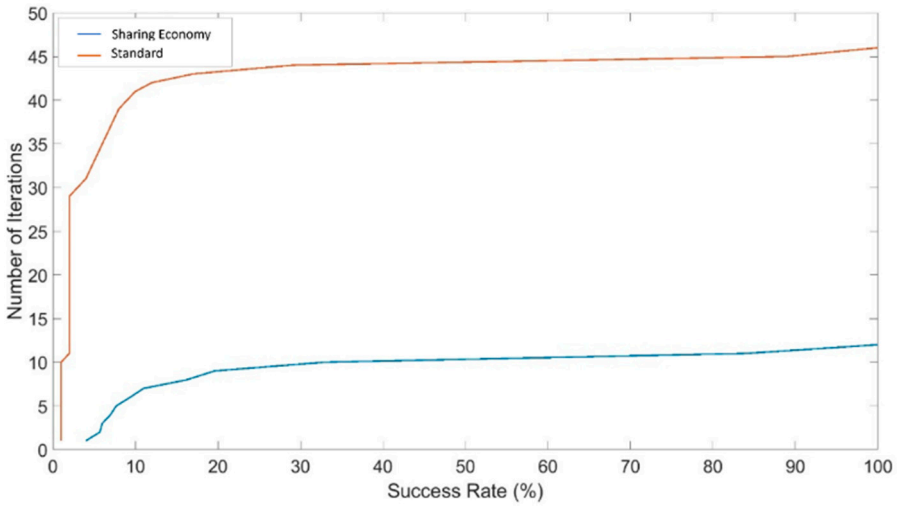


Figure 16. Number of iterations in relation to success rate.

6.3. Energy Efficiency

This metric was assessed by measuring the average number of bits transmitted by all IoT devices divided by the average power consumed by all IoT devices in the network for different numbers of connected IoT devices [9]. Figure 17 shows the number of bits successfully transmitted per mJ spent across the IoT devices in the network and computed based on [9].

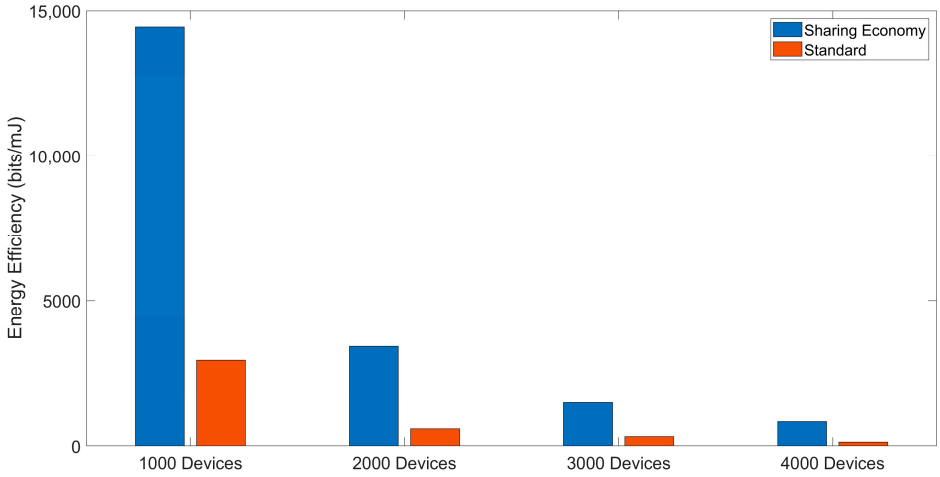


Figure 17. Energy averaged for different numbers of connected IoT nodes.

From Figure 17, we can see that our sharing economy-based solution could save a significant amount of energy in comparison to the standard approach, i.e., 80%, 83%, 78%, and 85% for M = 1000, 2000, 3000, and 4000, respectively. This means that, by using our strategy, IoT devices can send more bits using the same amount of transmit power compared to the standard approach.

6.4. Incentivisation and Transparancy

In the following experiment, we measured the cost incurred and gains made by the four operators (*OP1–OP4*) when participating in the proposed sharing economy solution. The connection cost/gain was calculated using Equations (3) and (4) described in Section 5.5 and using the time of connection of the IoT device, the assigned data rate, and the charging rate (Mbps/¤) for connecting to another RAN other than those belonging to the subscribed network operator. Note that the charging rate was fixed across all connections for our

evaluation and agreed in advance in the cooperation agreement but could also change dynamically as explained before.

Figures 18–20 show the average gains made and the average costs incurred by every operator after participating in the sharing economy, in the case of 1000, 2000, and 3000 devices, respectively. Across these results, we can make the following observations. The difference between the net gains (i.e., the gain minus the cost) for each operator in all cases is between −0.58 for *OP2* in the case of 3000 devices and +0.70 for *OP4* in the same case. This shows that some operators are in a less favourable position than others and thus have to pay more than they gain. The observed net gains or net losses are relatively small given that the average gain and cost are about three. We therefore assume that such gains and losses are acceptable to all operators involved (also given the other benefits in terms of the satisfaction percentage and energy savings) and can be relatively easily acquitted by, e.g., financial compensations. The second observation is related to the absolute gains for each operator. The absolute gain here means that an operator's gain is higher that its incurred cost (i.e., a positive net gain) beyond what they gain in terms of users' satisfaction and energy saving as shown in previous figures. Figures 18–20 show that 50% (in the case of 2000 and 3000 devices) to 75% (in the case of 1000 devices) of participating OPs experience positive net gains, and hence, absolute gains.

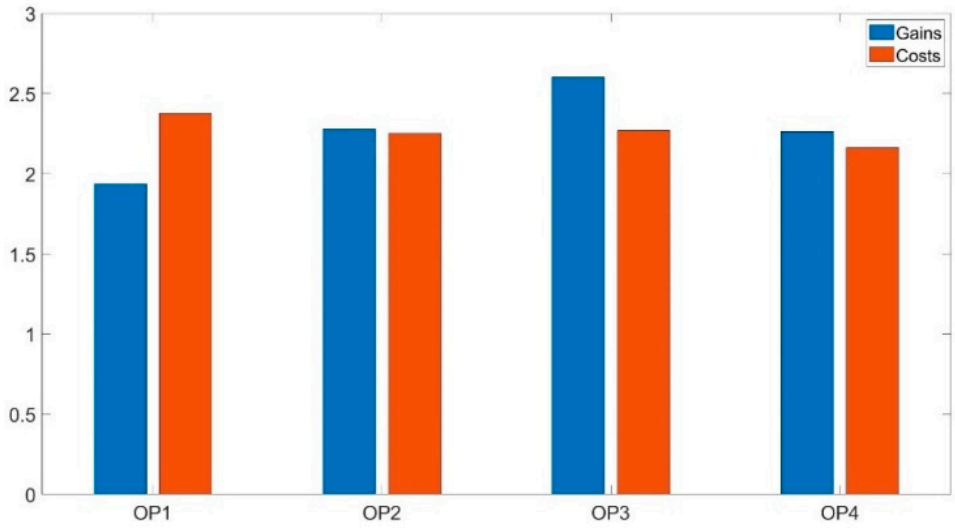


Figure 18. Ops' gains and costs for M = 1000.

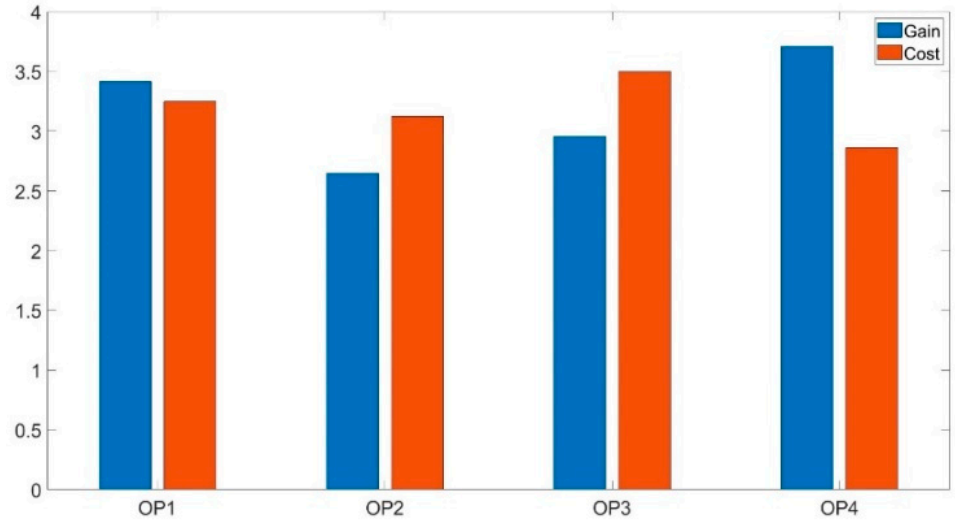


Figure 19. OPs' gains and costs for M = 2000.

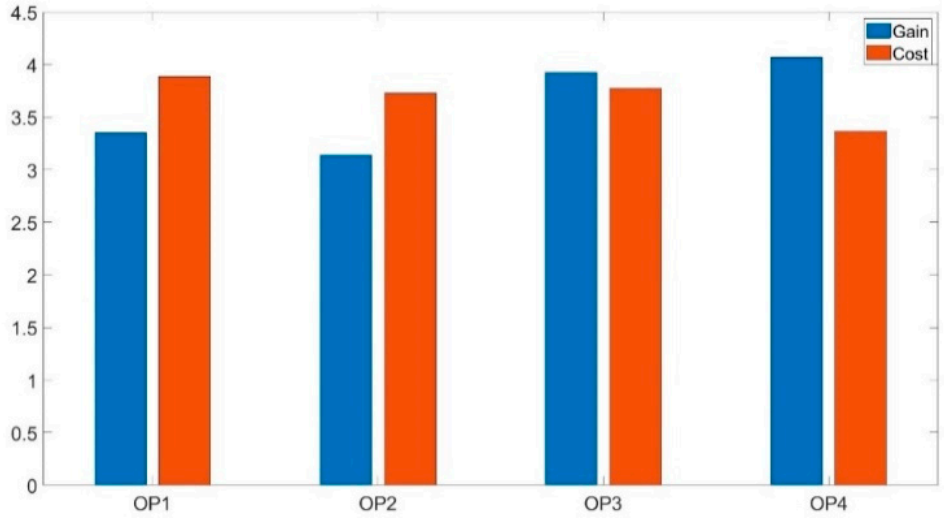


Figure 20. OPs' gains and costs for M = 3000.

6.5. Discussion

These evaluation results show that sharing economy-based radio access can help operators to satisfy the requirements of IoT devices better than they could achieve individually without cooperation. More importantly, the results show that the concepts of a sharing economy can be applied well to the nature of the massive IoT and the challenges it poses for 6G.

The results presented in this paper also show that operators assisting with such a scheme could scale better with the increasing size of the IoT network. This is visible through the time it takes IoT nodes to access the medium using the proposed scheme in comparison to the operator-oriented model, as shown in Figure 16. Since the data rate requirements of these nodes are quite low, they free the medium quickly and, thus, provide other nodes with the opportunity to transmit in subsequent iterations. However, such gains will always be limited by the density of the IoT network. The results presented in Figures 14 and 15 show that the gains achieved through this model are curtailed. This is expected as a dense IoT network results in high competition to access the spectrum and, as the density increases, the competition grows, resulting in more collisions and less access time.

Moreover, as shown in Section 6.4, the impact on the operators of joining such a scheme is not significant and can even produce modest additional income depending on the deployment of their resources in a given scenario. This is, of course, notwithstanding the implied overheads of establishing and maintaining such a scheme, but here we believe there is the potential for new business roles to be introduced that could provide this service as a trusted third party. This, taken in the context of the above benefits in terms of user satisfaction, node access, and energy efficiency, provides a compelling case for cooperative approaches to spectrum access in the massive IoT based on a sharing economy.

7. Conclusions

In this paper, we have proposed a solution to the issues of maximising access to massive IoT networks in future 6G networks. This is anticipated to be one of the key use cases for wireless networks going forward and presents very specific challenges based on the scalability and density requirements, but also because it deviates from traditional network usage paradigms and is therefore not necessarily as well supported in current protocols.

We have shown how existing approaches to the provisioning and deployment of wireless networks, both in unlicensed and cellular domains, are not suitable to address this problem without the need for prohibitive investment from operators and therefore present the need for cooperative spectrum usage as a solution. As such, we have applied the concept of the sharing economy in this paper and reviewed the challenges and technological solutions that can be used in this context. Specifically, we have described how spectrum

programming, that is, the extension of programmability into the lower layers of the protocol stack, will be a fundamental technology to support this vision.

Based on our analysis, we described how these technologies can be integrated into an architecture that maximises the available spectrum to solve the scalability challenges of the massive IoT while remaining practical through the trustworthy and incentivised sharing of resources. We then evaluated our architecture through simulation to verify the maximum density of devices that can be supported while additionally respecting their application requirements and minimising energy consumption. Moreover, we produced these results whilst demonstrating how such an architecture can realistically be deployed between competing operators to maintain isolation and trust, in addition to providing compelling incentives for participation.

In conclusion, therefore, we believe there is a compelling argument to utilise such an architecture to support massive IoT deployments in future 6G networks. The technologies being integrated into the architecture are all either in current use or very realistically achievable and the sharing economy concept has been validated many times already in other industries. This approach, coupled with the advancements being developed in hardware design (antennas, processors), new protocols (Wi-Fi 8, 6G), and RAN architectures (O-RAN), will ultimately meet the needs of a future massive IoT with densities up to and beyond 1–10 devices per m^2.

For future work on this project, we will expand on the blockchain-based incentivisation platform to investigate how to maximise adoption and identify new business roles. We will also attempt an implementation of this architecture as a real-world proof of concept. The application and scope of the massive IoT is still evolving as the technologies mature. Therefore, an important part of this future work will be to understand and align our architecture as closely as possible with these real-world use cases to maximise the performance gains.

Moreover, the economic aspects of the massive IoT and the supporting wireless infrastructure, as outlined in this paper, will play a crucial role in the viability of these deployments. In this paper, we provided a preliminary techno-economic analysis of the economic benefits of the cooperative sharing of wireless resources in 6G, and these results look promising. However, a more detailed economic analysis, balancing the real-world savings gained by resource sharing with the capital and operational costs of this new technology, needs to be performed.

Author Contributions: Conceptualization, F.B., A.R., M.M. and F.d.H.; methodology, F.B., A.R., M.M. and F.d.H.; software, A.R.; validation, A.R. and M.H.E.; formal analysis, F.B., A.R., M.M., M.H.E. and F.d.H.; writing—original draft preparation, A.R.; writing—review and editing, F.B., M.M., M.H.E. and F.d.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ericsson. *Ericsson Mobility Report*; Ericsson: Stockholm, Sweden, 2023.
2. *Minimum Requirements Related to Technical Performance for IMT-2020 Radio Interface(s)*; ITU Report M.2410-0 (11/2017); ITU: Geneva, Switzerland, 2017.
3. Guo, F.; Yu, F.R.; Zhang, H.; Li, X.; Ji, H.; Leung, V.C. Enabling massive IoT toward 6G: A comprehensive survey. *IEEE Internet Things J.* **2021**, *8*, 11891–11915. [CrossRef]
4. Slalmi, A.; Chaibi, H.; Chehri, A.; Saadane, R.; Jeon, G. Enabling Massive IoT Services in the Future Horizontal 6G Network: From Use Cases to a Flexible System Architecture. *IEEE Internet Things Mag.* **2023**, *6*, 62–67. [CrossRef]
5. Oliveira, L.; Rodrigues, J.J.; Kozlov, S.A.; Rabêlo, R.A.; de Albuquerque, V.H.C. MAC layer protocols for Internet of Things: A survey. *Future Internet* **2019**, *11*, 16. [CrossRef]
6. Hattab, G.; Cabric, D. Unlicensed spectrum sharing for massive Internet-of-Things communications. *arXiv* **2019**, arXiv:1903.01504.

7. Yaala, S.B.; Bouallegue, R. On MAC layer protocols towards internet of things: From IEEE802. 15.4 to IEEE802. 15.4 e. In Proceedings of the IEEE 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 22–24 September 2016; pp. 1–5.
8. Vejlgaard, B.; Lauridsen, M.; Nguyen, H.; Kovács, I.; Mogensen, P.; Sorensen, M. Interference impact on coverage and capacity for low power wide area IoT networks. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017.
9. Deepak, G.; Bouhafs, F.; Raschellà, A.; Mackay, M.; Shi, Q. Radio resource management framework for energy-efficient communications in the Internet of Things. *Trans. Emerg. Telecommun. Technol.* **2019**, *30*, e3766.
10. Abramson, N. The ALOHA system: Another alternative for computer communications. In Proceedings of the Fall Joint Computer Conference, Houston, TX, USA, 17–19 November 1970; pp. 281–285.
11. Migabo, E.M.; Djouani, K.D.; Kurien, A.M. The narrowband Internet of Things (NB-IoT) resources management performance state of art, challenges, and opportunities. *IEEE Access* **2020**, *8*, 97658–97675. [CrossRef]
12. Rastogi, E.; Saxena, N.; Roy, A.; Shin, D.R. Narrowband internet of things: A comprehensive study. *Comput. Netw.* **2020**, *173*, 107209. [CrossRef]
13. Xu, J.; Yao, J.; Wang, L.; Ming, Z.; Wu, K.; Chen, L. Narrowband internet of things: Evolutions, technologies, and open issues. *IEEE Internet Things J.* **2017**, *5*, 1449–1462. [CrossRef]
14. Oughton, E.J.; Frias, Z. The cost, coverage and rollout implications of 5G infrastructure in Britain. *Telecommun. Policy* **2018**, *42*, 636–652. [CrossRef]
15. Oughton, E.J.; Frias, Z.; van der Gaast, S.; van der Berg, R. Assessing the capacity, coverage and cost of 5G infrastructure strategies: Analysis of the Netherlands. *Telemat. Inform.* **2019**, *37*, 50–69. [CrossRef]
16. Parvini, M.; Zarif, A.H.; Nouruzi, A.; Mokari, N.; Javan, M.R.; Abbasi, B.; Ghasemi, A.; Yanikomeroglu, H. Spectrum Sharing Schemes From 4G to 5G and Beyond: Protocol Flow, Regulation, Ecosystem, Economic. *IEEE Open J. Commun. Soc.* **2023**, *4*, 464–517. [CrossRef]
17. Prem Jacob, T.; Pravin, A.; Ramachandran, M.; Al-Turjman, F. Differential spectrum access for next generation data traffic in massive-IoT. *Microprocess. Microsyst.* **2021**, *82*, 103951. [CrossRef]
18. Qian, B.; Zhou, H.; Ma, T.; Yu, K.; Yu, Q.; Shen, X. Multi-Operator Spectrum Sharing for Massive IoT Coexisting in 5G/B5G Wireless Networks. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 881–895. [CrossRef]
19. Bouhafs, F.; Raschellà, A.; Mackay, M.; den Hartog, F. A Spectrum Management Platform Architecture to Enable a Sharing Economy in 6G. *Future Internet* **2022**, *14*, 309. [CrossRef]
20. Wang, X.; Umehira, M.; Akimoto, M.; Han, B.; Zhou, H. Green Spectrum Sharing Framework in B5G Era by Exploiting Crowdsensing. *IEEE Trans. Green Commun. Netw.* **2023**, *7*, 916–927. [CrossRef]
21. Fernando, X.; Lăzăroiu, G. Spectrum sensing, clustering algorithms, and energy-harvesting technology for cognitive-radio-based internet-of-things networks. *Sensors* **2023**, *23*, 7792. [CrossRef]
22. Li, X.; Zheng, Y.; Khan, W.U.; Zeng, M.; Li, D.; Ragesh, G.K.; Li, L. Physical Layer Security of Cognitive Ambient Backscatter Communications for Green Internet-of-Things. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1066–1076. [CrossRef]
23. Shi, Z.; Gao, W.; Zhang, S.; Liu, J.; Kato, N. AI-enhanced cooperative spectrum sensing for non-orthogonal multiple access. *IEEE Wirel. Commun.* **2020**, *27*, 173–179. [CrossRef]
24. Frenken, K.; Schor, J. Putting the sharing economy into perspective. In *A Research Agenda for Sustainable Consumption Governance*; Edward Elgar Publishing: Cheltenham, UK, 2019; pp. 121–135.
25. Yrjölä, S.; Matinmikko-Blue, M.; Ahokangas, P. The evolution of mobile communications. In *The Changing World of Mobile Communications: 5G, 6G and the Future of Digital Services*; Springer: Cham, Switzerland, 2024; pp. 13–43.
26. Deloitte. *The Future of the Telco Business Model—To Be or Not to Be*; Deloitte: London, UK, 2017.
27. den Hartog, F.; Kempker, P.; Raschella, A.; Seyedebrahimi, M. Network Uberization. 2017. Available online: https://www.slideshare.net/secret/JzIFRIPkLXS5Zz (accessed on 20 November 2024).
28. Bogucka, H.; Kopras, B. Uberization of telecom networks for cost-efficient communication and computing. *IEEE Commun. Mag.* **2023**, *61*, 74–80. [CrossRef]
29. Song, Y.; Wang, W.; Sohraby, K. Uberization of NOMA Wireless Network Resource Sharing: A Driver-Passenger Game-Theoretic Approach. In Proceedings of the IEEE 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Paris, France, 2–4 November 2022.
30. Chang, H.-B.; Chen, K.-C. Cooperative spectrum sharing economy for heterogeneous wireless networks. In Proceedings of the 2011 IEEE GLOBECOM Workshops (GC Wkshps), Houston, TX, USA, 5–9 December 2011.
31. Li, Z.; Wang, W.; Wu, Q.; Wang, X. Multi-operator dynamic spectrum sharing for wireless communications: A consortium blockchain enabled framework. *IEEE Trans. Cogn. Commun. Netw.* **2022**, *9*, 3–15. [CrossRef]
32. Daidj, N. *Uberization (or uberification) of the economy In Encyclopedia of Information Science and Technology*, 4th ed.; IGI Global: Hershey, PA, USA, 2018; pp. 2345–2355.
33. Wang, C.X.; You, X.; Gao, X.; Zhu, X.; Li, Z.; Zhang, C.; Wang, H.; Huang, Y.; Chen, Y.; Haas, H.; et al. On the road to 6G: Visions, requirements, key technologies, and testbeds. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 905–974. [CrossRef]

34. Bouhafs, F.; Mackay, M.; Raschella, A.; Shi, Q.; den Hartog, F.; Saldana, J.; Munilla, R.; Ruiz-Mas, J.; Fernandez-Navajas, J.; Almodovar, J.; et al. Wi-5: A programming architecture for unlicensed frequency bands. *IEEE Commun. Mag.* **2018**, *56*, 178–185. [CrossRef]
35. Suresh, L.; Schulz-Zander, J.; Merz, R.; Feldmann, A.; Vazao, T. Towards programmable enterprise WLANS with Odin. In Proceedings of the First Workshop on Hot Topics in Software Defined Networks, Helsinki, Finland, 13 August 2012.
36. Nisar, K.; Jimson, E.R.; Hijazi, M.H.A.; Welch, I.; Hassan, R.; Aman, A.H.M.; Sodhro, A.H.; Pirbhulal, S.; Khan, S. A survey on the architecture, application, and security of software defined networking: Challenges and open issues. *Internet Things* **2020**, *12*, 100289. [CrossRef]
37. Sood, K.; Yu, S.; Xiang, Y. Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review. *IEEE Internet Things J.* **2015**, *3*, 453–463. [CrossRef]
38. Arnaz, A.; Lipman, J.; Abolhasan, M.; Hiltunen, M. Toward integrating intelligence and programmability in open radio access networks: A comprehensive survey. *IEEE Access* **2022**, *10*, 67747–67770. [CrossRef]
39. Riggio, R.; Marina, M.K.; Schulz-Zander, J.; Kuklinski, S.; Rasheed, T. Programming abstractions for software-defined wireless networks. *IEEE Trans. Netw. Serv. Manag.* **2015**, *12*, 146–162. [CrossRef]
40. Deloitte. *The Age of Telecom Network Automation*; Deloitte: London, UK, 2021.
41. Tele Management Forum. Unleashing Creativity with the Programmable Telco. Available online: https://inform.tmforum.org/features-and-opinion/unleashing-creativity-with-the-programmable-telco (accessed on 24 May 2024).
42. Le, Y.; Ling, X.; Wang, J.; Guo, R.; Huang, Y.; Wang, C.X.; You, X. Resource sharing and trading of blockchain radio access networks: Architecture and prototype design. *IEEE Internet Things J.* **2021**, *10*, 12025–12043. [CrossRef]
43. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
44. Wu, Q.; Wang, W.; Li, Z.; Zhou, B.; Huang, Y.; Wang, X. SpectrumChain: A disruptive dynamic spectrum-sharing framework for 6G. *Sci. China Inf. Sci.* **2023**, *66*, 130302. [CrossRef]
45. Baldesi, L.; Restuccia, F.; Melodia, T. ChARM: NextG spectrum sharing through data-driven real-time O-RAN dynamic control. In Proceedings of the IEEE INFOCOM 2022-IEEE Conference on Computer Communications, Virtual, 2–5 May 2022.
46. Coronado, E.; Khan, S.N.; Riggio, R. 5G-EmPOWER: A software-defined networking platform for 5G radio access networks. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 715–728. [CrossRef]
47. Taksande, P.K.; Jha, P.; Karandikar, A.; Chaporkar, P. Open5G: A software-defined networking protocol for 5G multi-RAT wireless networks. In Proceedings of the 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Seoul, Republic of Korea, 25–28 May 2020.
48. Raschellà, A.; Eiza, M.H.; Mackay, M.; Shi, Q.; Banton, M. A Trust-based Cooperative System for Efficient Wi-Fi Radio Access Networks. *IEEE Access* **2023**, *11*, 136136–136149. [CrossRef]
49. Eiza, M.H.; Raschellà, A.; Mackay, M.; Shi, Q.; Bouhafs, F. Towards trusted and accountable win-win SDWN platform for trading Wi-Fi network access. In Proceedings of the 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2023; pp. 1–6.
50. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; de Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
51. 3GPP. Technical Specification 38.211, NR; Physical Channels and Modulation (3GPP TS 38.211 version 16.2.0 Release 16) July 2020. Available online: https://www.etsi.org/deliver/etsi_ts/138200_138299/138211/16.02.00_60/ts_138211v160200p.pdf (accessed on 20 November 2024).
52. Park, M. IEEE 802.11 ah: Sub-1-GHz license-exempt operation for the internet of things. *IEEE Commun. Mag.* **2015**, *53*, 145–151. [CrossRef]