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

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

FAYCAL BOUHAFS[1] (Senior Member, IEEE), ALESSANDRO RASCHELLA[2], MICHAEL MACKAY[2], MAX HASHEM EIZA[2], AND FRANK DEN HARTOG[1,3] (Senior Member, IEEE)

[1] School of Systems and Computing, University of New South Wales Canberra, Canberra, Australia
[2] School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK
[3] Network Engineering and Cyber Security, University of Canberra, Canberra, ACT 2617, Australia

CORRESPONDING AUTHOR: A. Raschella (e-mail: a.raschella@ljmu.ac.uk).

ABSTRACT The upcoming introduction of 6G will provide an opportunity to build on and expand the vertical use cases currently supported by 5G. The Internet of Things (IoT) has been a major component for many of these use cases. Moving forward, 6G will need to connect more IoT devices, often densely deployed in urban areas, to support similar use cases in the future. This makes simply accessing the wireless medium an issue as current generation networks are not designed to support many thousands of devices attempting to send/receive data simultaneously. In this paper, we present a model for trading wireless network resources in massive IoT scenarios inspired by the concept of Sharing Economy. It is based on a new architecture for highly dynamic sharing of physical-layer network resources between providers using the novel concept of spectrum programming. We also utilise smart contracts and blockchain to guarantee trust, provide fair incentives, and enforce accountability. We simulated a massive IoT network and evaluated the scalability of the system when managed using our platform compared to standard fifth generation (5G) deployments. The experiments show how the proposed scheme can improve network resource allocation by up to 80% when compared to standard 5G allocation solutions. This is accompanied by similar improvements in interference and device energy consumption. Finally, we performed evaluations that demonstrate how the proposed platform can benefit all the stakeholders that decide to join the scheme.

INDEX TERMS 6G, Massive IoT, Blockchain, Sharing Economy, Spectrum Access, Spectrum Programming

I. 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, 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.

5G aims to provide network access on this scale, but for network operators to be able to accommodate so many wireless devices 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 massive IoT, the ITU set a requirement for 5G to support at least one million devices per km^2, or 1 per m^2 [1.5]. In this paper we will explain and evidence why 5G will never fulfill 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 massive IoT in wireless networks [2] [2.5]. 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 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, so we propose a high-level architecture that can scale to the required density level for massive IoT. The proposed architecture and focusses 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 rest of this paper is organised as follows. Section 2 first describes the challenges of supporting massive IoT in 5G and then demonstrates the shortcomings of existing approaches. Section 3 introduces the concept of sharing economies as they are applied in this paper. The next section describes what challenges can be encountered if sharing economy principles are to be applied in the context of future 6G networks, given the state of the art. This is also where we introduce our concept of spectrum programming. Section 5 presents our architecture based on a sharing economy for massive IoT networks, whilst our evaluation is described in section 6. Finally, section 7 presents our conclusions and further work.

II. THE CHALLENGE OF RADIO ACCESS IN 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 [3] 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 [4, 5] 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 a 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 massive IoT [6, 7]. 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 80m x 80m. The IoT devices have 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 from the IoT devices to 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 to get all the devices successfully transmitting 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 get a bit rate at least equal to their requirement represented as R_i and R_{reqi}. When all the devices are connected, lines 20 and 21 of Algorithm 1 interrupts the *while* command to record the final sets *Iterations* and *Satisfaction* as represented in Figure 1.

Algorithm 1 – Access Node

```
1:  all_satisfied = 0
2:  iteration = 0
3:  Iterations ← Ø
4:  Satisfaction ← Ø
5:  get set N
6:  while all_satisfied == 0 do
7:      connect all devices ∈ N to their best allowed gNB

8:      iteration += 1
9:      satisfied = 0
10:     N' = N
11:     for each i ∈ N do
12:         if Ri ≥ Rreqi do
13:             remove i from set N'
14:             satisfied += 1
15:         end if
16:     end for
17:     M = (satisfied / N) * 100
18:     Iterations ← Iterations ∪ {iteration}
19:     Satisfaction ← Satisfaction ∪ {M}
20:     if M == 100 do
21:         all_satisfied = 1
22:     else do
23:         N = N'
24:     end if/else
25: end while
26: plot(Iterations, Satisfaction)
```

The plot in this figure shows that it takes over 40 attempts for all the IoT devices to be satisfied. Moreover, the number of iterations results in more delay as, after each collision, a device needs to back off before retransmitting again.

To better quantify the delay incurred by such number of attempts, we assume that radio access in the IoT network described above is based on Pure ALOHA [8]. Accordingly, an IoT device that will reach n attempts to transmit its data, on the n^{th} attempt will have to wait for a period of time $T_{wait} = T_{Propagate} \times r$, where $r \in \{0, 2^n\}$, and $T_{Propagate}$ is the time necessary for device message to propagate through the wireless medium. If we assume an IoT device message needs only 1ms to propagate but the IoT device is already in its 40^{th} attempt, then it must wait between 0ms and 2^{40}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.

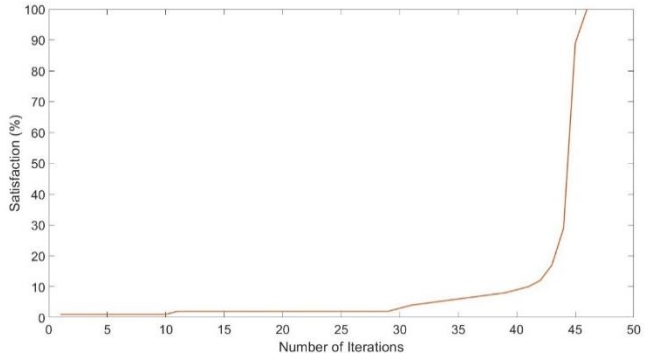


FIGURE 1. Transmission success rate as a function of the number of attempts to access the medium.

These results, in addition to what was published earlier in e.g. [6, 7], illustrate the limitations of the random-access model when used in the context of massive IoT networks and several approaches this solve this have already been proposed in the literature. Narrowband (NB) [9, 10] 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 cellular IoT where transmissions follow a schedule set by the base station [11].

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 waiting for access to the medium. To showcase the benefits of network densification, we conduct another experiment with 2000 IoT devices in the same open area of 80m x 80m 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. As we can observe from this figure, the number of iterations decreases linearly as the number of deployed access nodes increases.

In theory, therefore, network densification could be considered as the perfect solution to meet the requirements of massive IoT. However, such an increase in the access nodes infrastructure will come at a cost that might be prohibitive for many operators. Studies such as in [12, 13] estimated 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 plot the success rate of an IoT device transmitting its data calculated against the cost incurred by the number of gNBs. The success rate is calculated as the reciprocal function of the number of attempts. The cost incurred by the number of necessary gNBs is calculated as the number of gNBs multiplied by €82,000. As shown in Figure 3, an operator needs to spend over one million Euros just to reach the connection success rate of 11%. These results demonstrate the challenge telecommunication operators face in terms of infrastructure investment to meet the requirements of massive IoT.

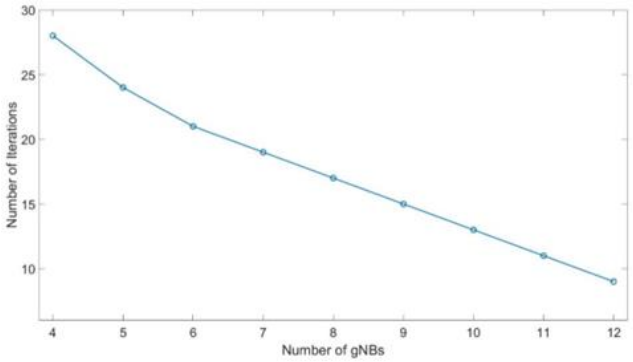


FIGURE 2. Number of attempts necessary to achieve 100% satisfaction as a function of the number of gNBs.

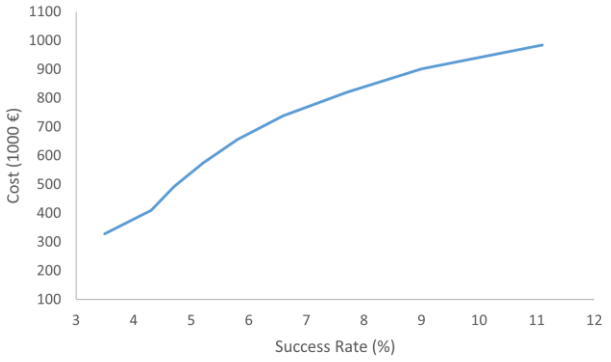


FIGURE 3. Cost incurred by operators to increase the success rate of IoT devices to access the RANs.

III. 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 [14]. It is therefore natural to consider if this model could be applied to the field of wireless communications in the context of 6G [15], [15.5].

A study conducted in [16] investigated the main trends the telecommunication industry are 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 are they to actually happen) and the degree of impact (if they happen, how much will this 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 actually happening.

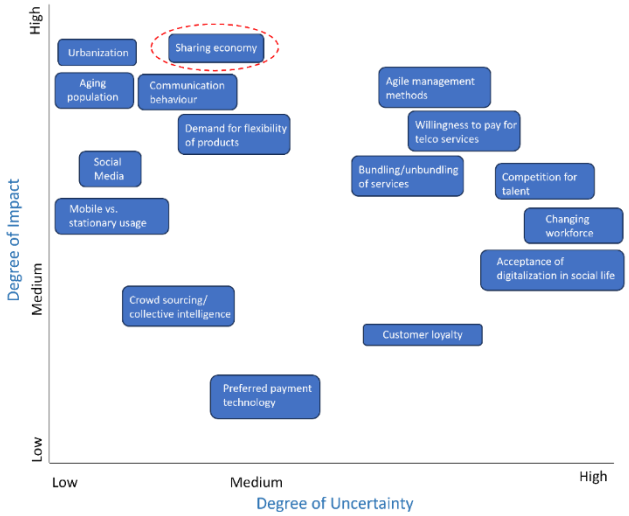


FIGURE 4. Degree of uncertainty of telecommunication landscape drivers and their degree of impact [16].

There have already been several studies that investigated the introduction of a sharing economy in wireless communication networks. In [17] and [18] the authors discussed the potential of "uberisation" in making the telecommunication market more competitive and transparent. The authors of [17] also proposed an Uber-like business model for trading communications and computing resources, with the focus on cloud computing resources. In [19], the authors proposed a pricing scheme to realise a uber-like spectrum sharing model between wireless users using Non-Orthogonal Multiple Access (NOMA) and the authors in [20] 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 [21], the authors investigate the application of blockchain to realise spectrum sharing and addressed the scalability issues that arise from the application of blockchain 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 it is the case in 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.

IV. CHALLENGES AND KEY TRENDS TO ADOPT A SHARING ECONOMY FOR MASSIVE IOT

A. 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 to deliver this as an over-the-top service and although sharing is still possible, an economy never emerged. The work in [17] and [18] proposed a platform inspired by Uber [22] 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 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, the mixture of private and public networks involved in this process along with the heterogeneity imposed will be complex to manage. This involves managing the RANs of the operators who agree to participate in the sharing economy model, 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, 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 is currently used today [23]. In the following, we will cover the most promising trends that could help in achieving a radio access solution based on a sharing economy.

B. 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.

1) NETWORK FUNCTION VIRTUALISATION

Virtualisation is among the most popular softwarisation concepts currently adopted by data networks 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 managing connections between access nodes and wireless devices. For instance, the architectures presented in [24, 25] propose to virtualise wireless Access Points (APs) by creating Lightweight Virtual Access Points (LVAP). The use of LVAPs facilitate the management of wireless connectivity and the allocation of radio resources to satisfy QoS requirements. Such features could be useful to address the heterogeneity and complexity design issues identified above.

2) SOFTWARE DEFINED NETWORKING

Software Defined Networking (SDN) is another softwarisation concept that facilitates the management of communications networks and reduces its 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) [26] represents an extension of SDN to wireless networks. The centralised yet scalable management approach is particularly attractive to 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 [27].

C. PROGRAMMABILITY

One of the main features inherited from the current advances made in the network softwarisation domain is the abstraction of the underlying layers and 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 meta-surfaces [28, 29]. The diagram in Figure 5 is taken from a study by Deloitte [30] in which they investigated the potential of automation and programmability in telecommunication management. It shows that the scalability and heterogeneity of IoT networks is as major factor behind this trend. Similar studies such as the one by TM Forum [31] have also highlighted the potential of programmability in making large and heterogeneous wireless networks, such as massive IoT, simpler to manage.

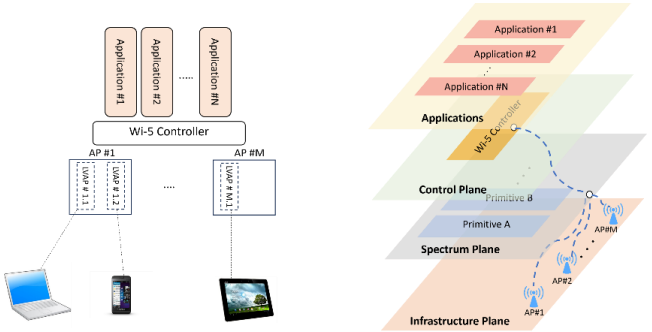
FIGURE 5. Factors behind the adoption of programmability in telecommunication with massive IoT a major driver behind this trend [31].

D. BLOCKCHAIN

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. Blockchain works in a decentralised environment and is enabled by comprising several core technologies, such as digital signatures, cryptographic hash, and distributed consensus algorithms. The main characteristics of blockchain are decentralisation, immutability, transparency, and auditability. They make blockchain a suitable technology for decentralised verification or transactions, as evidenced by the several contributions that utilise it to enforce transparent trading of resources, including radio resources [32-34]. Therefore, blockchain could play a major role in enabling a sharing economy such as the one targeted in this work through the incentivisation and transparency design issue.

E. SPECTRUM PROGRAMMING ARCHITECTURE AND SMART CONNECTIVITY MANAGEMENT

In [24] we introduced the concept of spectrum programmability. With 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 6-(a), 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 6-(b) extends existing programmable networks 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 Wi-5 architecture

(b) Planes and Programmability in Wi-5 architecture

FIGURE 6. Depiction of the Wi-5 architecture and programmability [24].

In this context, among the controller applications developed that exploits 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 solve 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 blockchain are adopted and properly integrated. Table 1 summarises these trends and the design challenges they could help address.

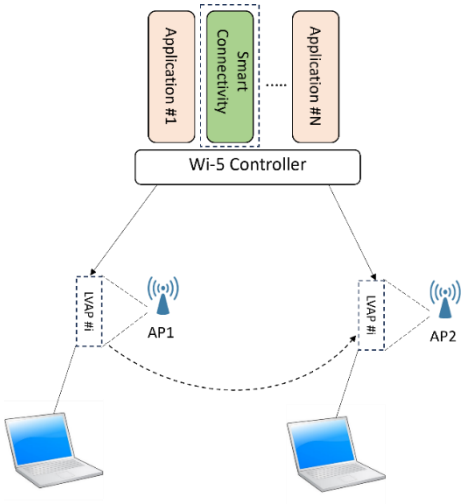


FIGURE 7. Illustration of using LVAPs to manage connectivity in Wi-5.

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

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

V. RADIO ACCESS ARCHITECTURE BASED ON SHARING ECONOMY

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 [24] and 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 massive IoT based on the concept of a sharing economy. The extension covers three dimensions not previously considered in the initial architecture:

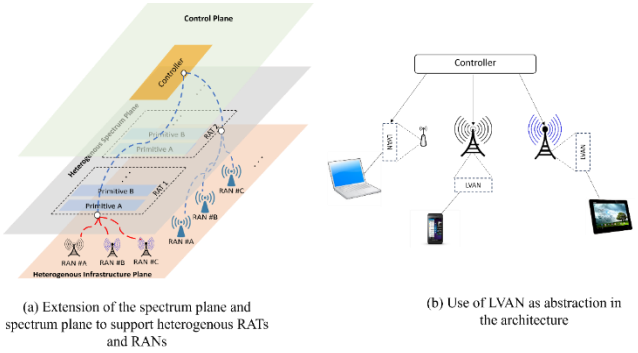
- Heterogeneity Support.
- Connectivity Management.
- Cooperation and Transparency.

A. HETEROGENEITY SUPPORT

The support for heterogeneity is 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 that 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.

As shown Figure 8-(a), similarly to the architecture initially proposed in [24], 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 8-(b) 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 [35-37].



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

(b) Use of LVAN as abstraction in the architecture

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

B. CONNECTIVITY MANAGEMENT

Using the extended architecture described in section 5.A, 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 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, the Received Signal Strength Indicator (RSSI) for each IoT device *i* connected to it, and the number of devices connected to it. This part is labelled as step 1 in Figure 9-(a). In terms of the algorithm of the Connectivity Application, the monitoring information is stored in 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 Rb for device *i* in line 7 is computed through the Shannon-Hartley theorem also taking into account the number of IoT devices connected to the corresponding RAN and its capacity in terms of bps. Further details on this computation can be found in [38]. The identity of the chosen RAN is passed by the Connectivity Application to the controller, labelled as step 2 in Figure 9-(a). The controller, then, connects the IoT device to the chosen RAN, which is labelled step 3 in Figure 9-(a).

From an architectural point of view, and as shown in Figure 9-(b), 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.

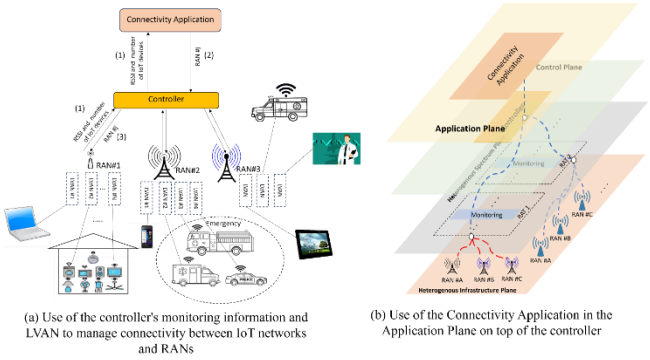
Algorithm 2

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**

C. TRANSPARENCY

At the heart of the proposed solution sits the cooperation and trust among the operators who agree to share their access nodes to IoT networks. To achieve this, we propose a Brokering Plane to be added to our architecture as first suggested in [39]. It resides above the Connectivity Application and acts as an interface between the application and the operators, as shown in Figure 10. The Brokering Plane is based on a permissioned blockchain network, for instance a Hyperledger Fabric (HLF) as described in [40]

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 faster consensus while still guaranteeing decentralisation, immutability, provenance, and finality.



(a) Use of the controller's monitoring information and LVAN to manage connectivity between IoT networks and RANs

(b) Use of the Connectivity Application in the Application Plane on top of the controller

FIGURE 9. Description of the deployment of the connectivity application as part of the proposed solution.

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., 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 could be accessed, the duration of the availability of the RAN and the cost to use it. In [40], 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 to 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 on 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 interaction between the controller and the blockchain network, and keeps a record of the ledger 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.

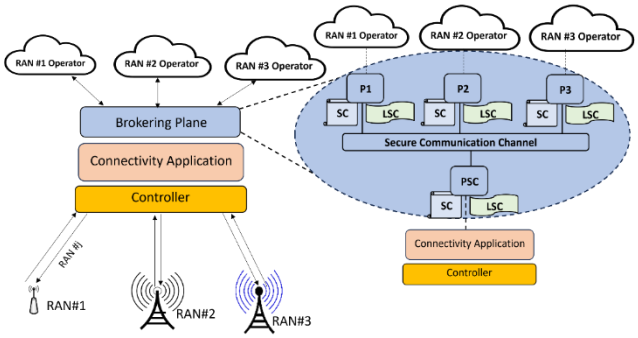


FIGURE 10. Description of the brokering plane and its interaction with operators and the connectivity application.

D. 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 networks 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 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:

$$C_i(\Delta t) = \Delta t.\beta_{given} + ¤_i \quad , \qquad (1)$$

where β_{given} is the bandwidth consumed by other networks when using OP_i RANs and $¤_i$ is the operational cost

associated with the usage of these RANs. The operation cost could include energy consumption, annual cost associated with maintaining each RAN, etc. The gain $G_i(\Delta t)$ can be defined as follows:

$$G_i(\Delta t) = \Delta t.\beta_{received} + \Gamma_i \quad , \qquad (2)$$

where $\beta_{received}$ is the bandwidth gained by 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:

$$G_i(\Delta t) - C_i(\Delta t) \geq 0 \quad , \qquad (3)$$
$$G_j(\Delta t) - C_j(\Delta t) \geq 0 \quad . \qquad (4)$$

If either condition (3) or (4) are not verified, OP_i and OP_j negotiate the initial contract between them via their peers on 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 on the blockchain network to keep records of these steps for any future reference (e.g., in case of a dispute).

VI. EVALUATION

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

A. EVALUATION SCENARIO AND PARAMETERS

In our evaluation, we simulate a dense deployment of 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 energy resources of IoT devices. For that, we consider N RANs that belong to four different operators, as well as M IoT devices, all uniformly distributed in an open-area of 80m x 80m.

Moreover, each RAN can be either a 5G gNB base station or a Wi-Fi 802.11ah AP. In the use case investigated below, the 5G connectivity is provided by 4 gNBs and the Wi-Fi connectivity is offered by 16 802.11ah APs and, hence, N=20. Furthermore, the 20 RANs belong to 4 different operators, where each one manages 5 RANs, i.e., 1 gNB and 4 APs. We also consider 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 128kbps for uplink transmissions. Finally, we assume 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 [41] [42]. The parameters for our evaluation are summarised in Table 2.

TABLE 2. Summary of evaluation parameters.

Area size	80m x 80m
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 x gNB - 16 x 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 compare the performance of the proposed solution against the standard approach currently adopted in 5G and Wi-Fi networks, i.e. 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 focuses 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.

B. 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 will allow 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 in percentage, this metric quantifies 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 assesses the flexibility of the solution in accommodating the requests of as

many IoT devices as possible while minimizing the number of unsuccessful attempts.

1) SIGNAL TO INTERFERENCE PLUS NOISE RATIO (SINR)

The metric considered in this evaluation is the average SINR experienced by all IoT devices in the network. The value of the SINR experienced by device *i* connected to access node *j* is computed through equation 5:

$$SINR_{i,j} = \frac{g_{i,j} \cdot p_i}{\sum_{k \in I'} g_k \cdot p_k + N_0} \qquad (5)$$

Here, $g_{i,j}$ is the channel gain from device *i* to 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 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.

Figure 11, Figure 12, and Figure 13 illustrate the SINR performance results computed through equation 5 and converted to decibels (dB) for different numbers of connected IoT devices. The upper and lower edges of the plotted boxes are the 25th and 75th percentile 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 SINR compared to the standard approach regardless of how many IoT devices are connected to the network.

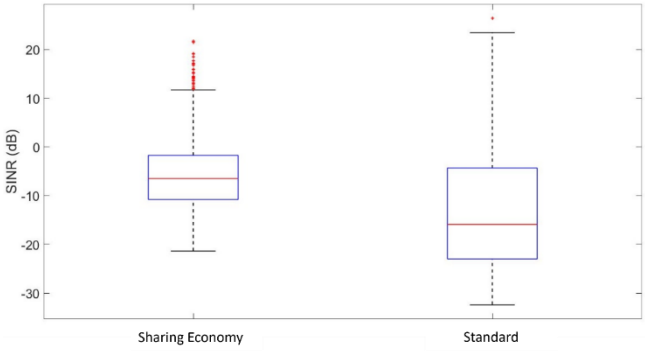


FIGURE 11. Measured SINR when using 5G and Sharing Economy for M=1000.

2) TRANSMISSION SUCCESS

This metric is 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 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 in 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.

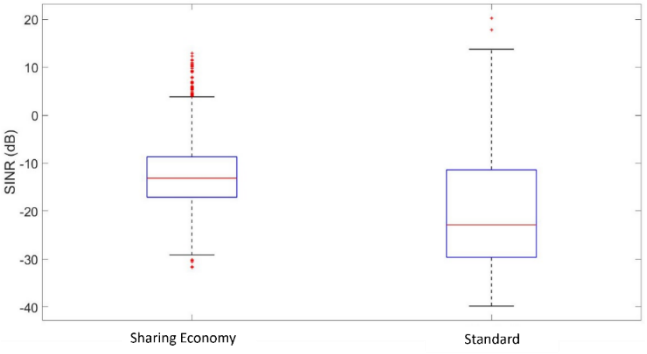


FIGURE 12. Measured SINR when using 5G and Sharing Economy for M=2000.

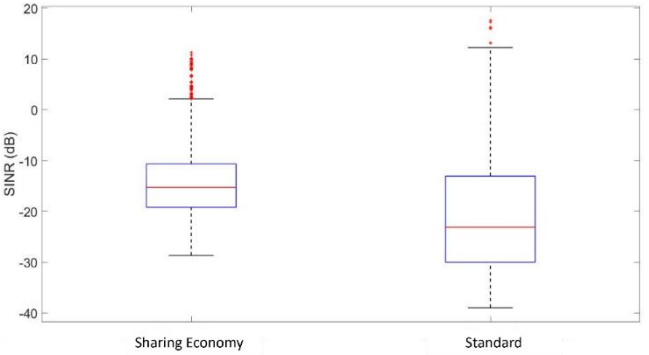


FIGURE 13. Measured SINR when using 5G and Sharing Economy for M=3000.

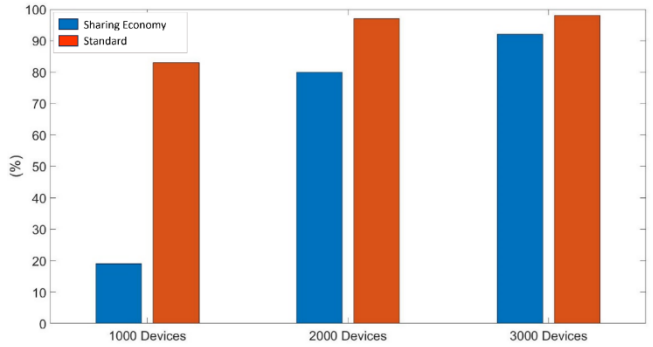


FIGURE 14. Probability of unsuccessful connectivity for different numbers of IoT nodes.

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

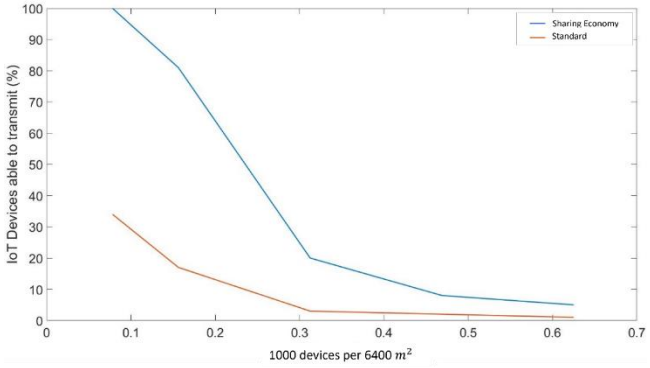


FIGURE 15. Probability of unsuccessful connectivity for different numbers of IoT nodes.

3) ACCESS DELAY

This metric is 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., success rate) computed through **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.

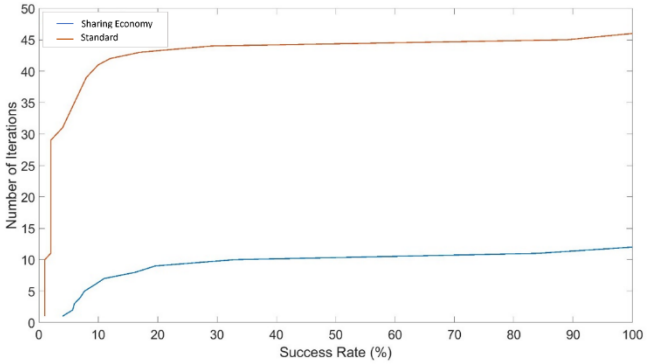


FIGURE 16. Number of iterations in relation to success rate.

C. ENERGY EFFICIENCY

This metric is 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 [7]. Figure 17 shows number of bits successfully transmitted per mJ spent across the IoT devices in the network and computed based on [7].

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., by 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.

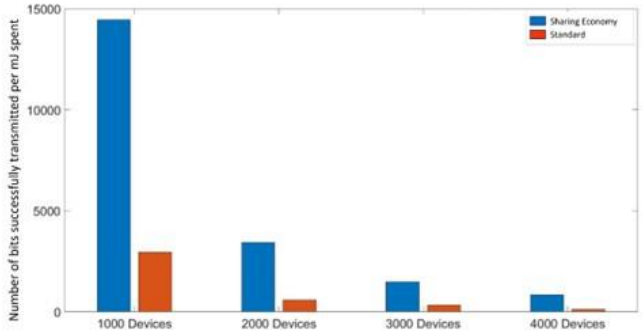


FIGURE 17. Energy averaged for different numbers of connected IoT nodes.

D. INCENTIVISATION AND TRANSPARENCY

In the following experiment, we measure the cost incurred and gain made by the four operators (OP1-OP4) when participating in the proposed sharing economy solution. The connection cost/gain is calculated through equation (1) and (2) described in section 5.D 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 is fixed across all connections for our evaluation and agreed in advance in the cooperation agreement but can also change dynamically as explained before.

Figure 18, Figure 19, and Figure 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, 3000 devices, respectively. Across these results, we can make the following observations. The difference between 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 to +0.70 for OP4 in the same case. This shows that some operators are in a less favourable location 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 is about 3. We, therefore, assume that such gains and losses are acceptable to all operators involved (also given the other benefits in terms of 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. Absolute gain here means that an operator's gain is higher that its incurred cost (i.e., positive net gain) beyond what they gain in terms of users' satisfaction and energy saving as shown in previous figures. Figure 18, Figure 19 and Figure 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 hence, absolute gains.

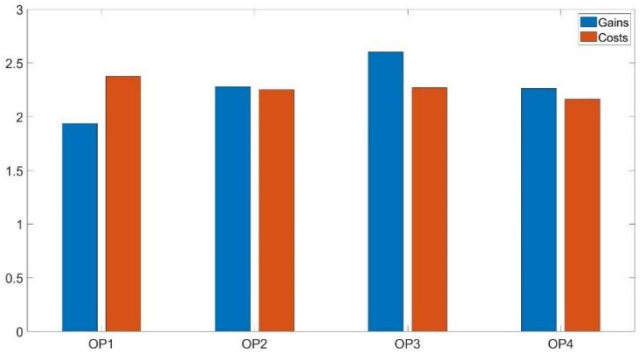


FIGURE 18. **OPs gains and costs for M=1000.**

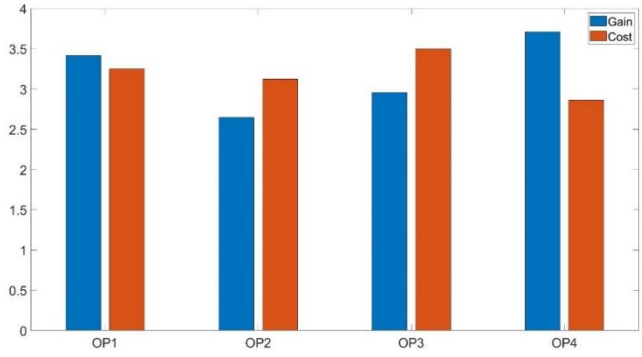


FIGURE 19. **OPs gains and costs for M=2000.**

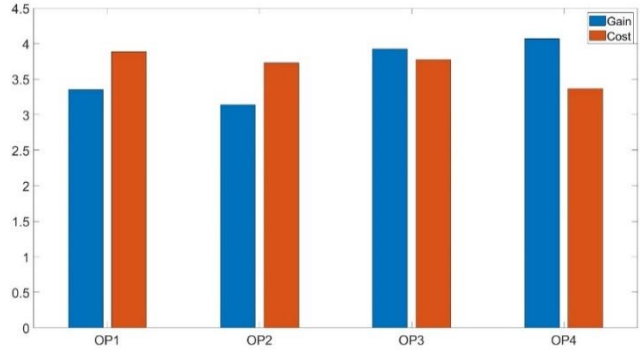


FIGURE 20. **OPs gains and costs for *M*=3000.**

E. DISCUSSION

These evaluation results show that the sharing economy-based radio access can help operators in satisfying 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 massive IoT and the challenges it poses for 6G. The results presented above in this paper also show that operators assisted 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 Figure 14 and Figure 15 show that the gains achieved through this model are curtailed. This is expected as a dense IoT network results in high contention to access the spectrum and, as the density increases, the contention grows which 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 massive IoT based on a sharing economy.

VII. CONCLUSIONS

In this paper we have proposed a solution to the issues of maximising access for 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 for 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 propose the need for cooperative spectrum usage as a solution. As such, we have applied the concept of sharing economy in this paper and reviewed the challenges and technological solutions that can 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 massive IoT while remaining practical through the trustworthy and incentivised sharing of resources. We then evaluated our architecture through simulation to verify the required density of devices 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 (WiFi 8, 6G), and RAN architectures (O-RAN) will ultimately meet the needs of 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.

REFERENCES

[1] Ericsson, "Ericsson Mobility Report," November 2023.

[1.5] "Minimum requirements related to technical performance for IMT-2020 radio interface(s)", ITU Report M.2410-0 (11/2017).

[2] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. Leung, "Enabling massive IoT toward 6G: A comprehensive survey," IEEE Internet of Things Journal, vol. 8, no. 15, pp. 11891-11915, 2021.

[2.5] A. Slalmi, H. Chaibi, A. Chehri, R. Saadane and G. Jeon, "Enabling Massive IoT Services in the Future Horizontal 6G Network: From Use Cases to a Flexible System Architecture," in IEEE Internet of Things Magazine, vol. 6, no. 4, pp. 62-67, December 2023

[3] L. Oliveira, J. J. Rodrigues, S. A. Kozlov, R. A. Rabêlo, and V. H. C. d. Albuquerque, "MAC layer protocols for Internet of Things: A survey," Future Internet, vol. 11, no. 1, p. 16, 2019.

[4] G. Hattab and D. Cabric, "Unlicensed spectrum sharing for massive Internet-of-Things communications," arXiv preprint arXiv:.01504, 2019.

[5] S. B. Yaala and R. Bouallegue, "On MAC layer protocols towards internet of things: From IEEE802. 15.4 to IEEE802. 15.4 e," in IEEE 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2016, pp. 1-5.

[6] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Kovács, P. Mogensen, and M. Sorensen, "Interference impact on coverage and capacity for low power wide area IoT networks," presented at the 2017 IEEE Wireless Communications and Networking Conference (WCNC), 2017.

[7] G. Deepak, F. Bouhafs, A. Raschellà, M. Mackay, and Q. Shi, "Radio resource management framework for energy-efficient communications in the Internet of Things," Transactions on Emerging Telecommunications Technologies, vol. 30, no. 12, p. e3766, 2019.

[8] N. Abramson, "The ALOHA system: Another alternative for computer communications," in Proceedings of the November 17-19, 1970, fall joint computer conference, 1970, pp. 281-285.

[9] E. M. Migabo, K. D. Djouani, and A. M. Kurien, "The narrowband Internet of Things (NB-IoT) resources management performance state of art, challenges, and opportunities," IEEE Access, vol. 8, pp. 97658-97675, 2020.

[10] E. Rastogi, N. Saxena, A. Roy, and D. R. Shin, "Narrowband internet of things: A comprehensive study," Computer networks, vol. 173, p. 107209, 2020.

[11] J. Xu, J. Yao, L. Wang, Z. Ming, K. Wu, and L. Chen, "Narrowband internet of things: Evolutions, technologies, and open issues," IEEE Internet of things journal, vol. 5, no. 3, pp. 1449-1462, 2017.

[12] E. J. Oughton and Z. Frias, "The cost, coverage and rollout implications of 5G infrastructure in Britain," Telecommunications Policy, vol. 42, no. 8, pp. 636-652, 2018.

[13] E. J. Oughton, Z. Frias, S. van der Gaast, and R. van der Berg, "Assessing the capacity, coverage and cost of 5G infrastructure strategies: Analysis of the Netherlands," Telematics Informatics, vol. 37, pp. 50-69, 2019.

[14] K. Frenken and J. Schor, "Putting the sharing economy into perspective," in A research agenda for sustainable consumption governance: Edward Elgar Publishing, 2019, pp. 121-135.

[15] F. Bouhafs, A. Raschellà, M. Mackay, and F. den Hartog, "A Spectrum Management Platform Architecture to Enable a Sharing Economy in 6G," Future Internet, vol. 14, no. 11, p. 309, 2022.

[15.5] Yrjölä, S., Matinmikko-Blue, M. and Ahokangas, P., "The evolution of mobile communications." In The Changing World of Mobile Communications: 5G, 6G and the Future of Digital Services (pp. 13-43). Cham: Springer International Publishing (2024)

[16] Deloitte, "The Future of the Telco Business Model — To Be or Not to Be," 2017.

[17] F. d. Hartog, P. Kempker, A. Raschella, and M. Seyedebrahimi, "Network Uberization," 2017, Available: https://www.slideshare.net/secret/JzIFRIPkLXS5Zz.

[18] H. Bogucka and B. Kopras, "Uberization of telecom networks for cost-efficient communication and computing," IEEE Communications Magazine, vol. 61, no. 7, pp. 74-80, 2023.

[19] Y. Song, W. Wang, and K. Sohraby, "Uberization of NOMA Wireless Network Resource Sharing: A Driver-Passenger Game-Theoretic Approach," presented at the IEEE 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2022.

[20] H.-B. Chang and K.-C. Chen, "Cooperative spectrum sharing economy for heterogeneous wireless networks," presented at the 2011 IEEE GLOBECOM Workshops (GC Wkshps), 2011.

[21] Z. Li, W. Wang, Q. Wu, and X. Wang, "Multi-operator dynamic spectrum sharing for wireless communications: A consortium blockchain enabled framework," IEEE Transactions on Cognitive Communications Networking, vol. 9, no. 1, pp. 3-15, 2022.

[22] N. Daidj, "Uberization (or uberification) of the economy," in Encyclopedia of Information Science and Technology, Fourth Edition: IGI Global, 2018, pp. 2345-2355.

[23] C.-X. Wang et al., "On the road to 6G: Visions, requirements, key technologies, and testbeds," IEEE Communications Surveys and Tutorials, vol. 25, no. 2, pp. 905-974, 2023.

[24] F. Bouhafs et al., "Wi-5: A programming architecture for unlicensed frequency bands," IEEE Communications Magazine, vol. 56, no. 12, pp. 178-185, 2018.

[25] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao, "Towards programmable enterprise WLANS with Odin," presented at the The first workshop on Hot topics in software defined networks, 2012.

[26] K. Nisar et al., "A survey on the architecture, application, and security of software defined networking: Challenges and open issues," Internet of Things, vol. 12, p. 100289, 2020.

[27] K. Sood, S. Yu, and Y. Xiang, "Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review," IEEE Internet of Things Journal, vol. 3, no. 4, pp. 453-463, 2015.

[28] A. Arnaz, J. Lipman, M. Abolhasan, and M. Hiltunen, "Toward integrating intelligence and programmability in open radio access networks: A comprehensive survey," IEEE Access, vol. 10, pp. 67747-67770, 2022.

[29] R. Riggio, M. K. Marina, J. Schulz-Zander, S. Kuklinski, and T. Rasheed, "Programming abstractions for software-defined wireless networks," IEEE Transactions on Network Service Management, vol. 12, no. 2, pp. 146-162, 2015.

[30] Deloitte, "The Age of Telecom Network Automation," 2021.

[31] T. Forum, "Unleashing creativity with the programmable telco," Accessed on: 24th May 2024Available: https://inform.tmforum.org/features-and-opinion/unleashing-creativity-with-the-programmable-telco

[32] Y. Le et al., "Resource sharing and trading of blockchain radio access networks: Architecture and prototype design," IEEE Internet of Things Journal, vol. 10, no. 14, pp. 12025-12043, 2021.

[33] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," IEEE Access, vol. 7, pp. 117134-117151, 2019.

[34] Q. Wu, W. Wang, Z. Li, B. Zhou, Y. Huang, and X. Wang, "SpectrumChain: a disruptive dynamic spectrum-sharing framework for 6G," Science China Information Sciences vol. 66, no. 3, 2023.

[35] L. Baldesi, F. Restuccia, and T. Melodia, "ChARM: NextG spectrum sharing through data-driven real-time O-RAN dynamic control," presented at the IEEE INFOCOM 2022-IEEE Conference on Computer Communications, 2022.

[36] E. Coronado, S. N. Khan, and R. Riggio, "5G-EmPOWER: A software-defined networking platform for 5G radio access networks," IEEE Transactions on Network Service Management, vol. 16, no. 2, pp. 715-728, 2019.

[37] P. K. Taksande, P. Jha, A. Karandikar, and P. Chaporkar, "Open5G: A software-defined networking protocol for 5G multi-RAT wireless networks," presented at the 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2020.

[38] A. Raschellà, M. H. Eiza, M. Mackay, Q. Shi, and M. Banton, "A Trust-based Cooperative System for Efficient Wi-Fi Radio Access Networks," IEEE Access, vol. 11, pp. 136136-136149, 2023.

[39] M. H. Eiza, A. Raschellà, M. Mackay, Q. Shi, and F. Bouhafs, "Towards trusted and accountable win-win SDWN platform for trading Wi-Fi network access," in 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), 2023, pp. 1-6: IEEE.

[40] E. Androulaki et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in Proceedings of the thirteenth EuroSys conference, 2018, pp. 1-15.

[41] Technical Specification 38.211, NR; Physical channels and modulation.

[42] M. Park, "IEEE 802.11 ah: sub-1-GHz license-exempt operation for the internet of things," IEEE Communications Magazine, vol. 53, no. 9, pp. 145-151, 2015.