Toward secure trading of unlicensed spectrum in cyber-physical systems

Frank den Hartog
School of Engineering and Information Technology
UNSW Canberra
Canberra, Australia
Frank.den.Hartog@unsw.edu.au

Fayçal Bouhafs
Department of Computer Science
Liverpool John Moores University
Liverpool, United Kingdom
f.bouhafs@ljmu.ac.uk

Qi Shi
Department of Computer Science
Liverpool John Moores University
Liverpool, United Kingdom
q.shi@ljmu.ac.uk

***Abstract*— Cyber-physical systems rely more and more on wireless technologies that operate in unmanaged, unlicensed frequency bands. Already today, this leads to security issues and a significant degradation of network performance due to interference and traffic congestion. Only collaboration between stakeholders leads to a sustainable solution. To facilitate collaboration, we designed a novel platform that heavily relies on the concept of Software-Defined Networking, introducing a central controller for programmable radio parameters. Part of this solution is a Brokering Platform that automates negotiation for spectral resources between access point (AP) operators. In this article we present a novel architecture for such a platform. We also propose the distribution of Brokering Platform functionality over the APs using blockchain.**

***Keywords*— Cyber-physical systems, unlicensed spectrum, blockchain.**

I. Introduction

Cyber-Physical Systems (CPSs) are well-integrated systems based on tightly networked and controlled hardware and software. It is a container term for "Smart" systems currently being developed and deployed, such as Smart Homes, Smart Cities, Smart Health, Smart Grids, and Smart Transportation. CPSs are therefore envisaged as being the foundation of our future critical infrastructure [1].

CPSs rely more and more on wireless technologies that operate in unmanaged, unlicensed frequency bands, such as Wi-Fi, Zigbee, LoRa, and sometimes 5G. This means that, in most cases, individuals do not need to obtain a special license before they can operate supported wireless devices, and as such introduce mutual interference and traffic congestion, negatively influencing the performance of the CPS. In [2] we have shown that in typical apartment blocks this already leads to a degradation of Wi-Fi performance by 85%, today. Ultimately, interference and congestion will not only threaten the CPSs' performance, but also their security: the CPSs can be "jammed", i.e. undergo a wireless Denial-of-Service (DoS) attack, with little chance of attribution, as the attack is easily hidden in the noise of other systems.

Although these dangers seem obvious, one could wonder why this has not stopped the industry from massively rolling out such networked systems or devices. One reason is that the logical alternative, having the devices work on licensed frequency bands, will often be commercially unattractive: it comes with too much technical complexity and managerial hassle (e.g. SIM cards), and would likely limit the use of a device to a single managed domain (network operator). Another reason is that the wireless networking industry is traditionally more focused on solving coverage issues than congestion issues. Most "solutions" for bad Wi-Fi performance currently being propagated can be summarized as better placement of the AP, or otherwise putting in additional APs and repeaters. To battle congestion, however, these "solutions" make things only worse [2]. A third reason is that the industry still believes that the typical back-off and spectrum optimization mechanisms that wireless Medium Access Control (MAC) protocols embed, including beamforming, MIMO (Multiple Input Multiple Output), OFDMA (Orthogonal Frequency Division Multiple Access), channel bonding, and TPC (Transmitted Power Control), would automatically take care of fair distribution of access to spectral resources among the devices. However, in [2] and [3] we have proven that this is not the case. Unlicensed spectrum turns out to be a shared-resource system where its users, acting independently according to their own self-interest, *deplete* that resource through their collective action.

This work has been carried out in the framework of the Wi 5 project, which was partly funded by the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement no. 644262.

The last issue above is well-known in economic literature to have only two types of sustainable solutions: either enlarge the pool of resources (i.e. making more frequency bands available for unlicensed communication), or enact some method of collaboration between the users. Adding frequency bands is indeed happening, but apparently not fast enough [3]. And platforms that could facilitate collaboration do not yet exist.

The Horizon 2020 Wi-5 project (www.wi5.eu) has taken up the challenge to design novel platforms and business models to enable effective collaboration between independent operators of APs that are in each other's range. One of the functionalities that Wi-5 proposes is a Brokering Platform. This platform continuously collects information about the spectral resources offered and demanded by independent APs that are in each other's range, and facilitates negotiation. The outcome of the negotiation then leads to the creation of dynamic policies and contracts to be executed by the AP operators.

Here, we propose a novel architecture for a Brokering Platform to facilitate independent parties, which operate wireless networks in each other's vicinity using unlicensed frequency bands, to negotiate and securely trade spectral resources with each other. In the following section we summarize the overall Wi-5 architecture as presented in [4,5,6]. We then describe the internal design of the Brokering Platform, which would be most easily deployed as a cloud service. However, as actors may distrust such a solution, and mutual interference is inherently local, we also propose a distributed deployment using blockchain.

II. Wi-5 System Architecture

The Wi-5 solution proposed in [4] and [5] is heavily relying on the concept of Software-Defined Networking

(SDN). SDN is a relatively new technology that enables the routing tables of routers in a data network to be programmed via an SDN controller in the control plane. This provides network operators with the opportunity to have very tight but also very flexible, policy-defined control over the traffic flows in the network. The application of SDN to wireless networks, also called Software Defined Wireless Networks (SDWN), therefore provides great opportunities to make these networks more resilient: traffic can be deflected from areas with much spectral congestion and interference [6].

However, like SDN, SDWN only concerns the programmability of routing tables, i.e. the manipulation of traffic flows. Wi-5 therefore extended SDWN by making also radio configuration parameters programmable [4,5]. This includes channel selection, TPC, and various media access control parameters. By taking the configuration of these parameters out of the distributed MAC protocol layer, and making them programmable via open APIs (Application Programming Interfaces), operators acquire a much tighter and more flexible, policy-defined control over the use of radio resources, enabling better optimized interference avoidance, device handovers, etc.

The Wi-5 system architecture is schematically shown in Figure 1. Two entities form its heart: the Wi-5 Controller (operated by the Wi-5 System Operator) and the Brokering Platform (operated by the Spectrum Broker). The Wi-5 Controller resides with the SDWN controller in the control plane. It makes radio parameters programmable via an open Southbound API to the wireless Access Points (APs, but not limited to Wi-Fi), and an open Northbound API to various applications. Intelligent algorithms use these applications to achieve a specific goal set by policies that are communicated to the Wi-5 Controller by the Brokering Platform. The Wi-5 Controller also includes a Flow and Network Monitoring Module (FNMM, not shown in the figure) [7]. The FNMM takes regular measurements from the APs, monitors the characteristics of new flows in the network, and sends this information to the management algorithm. We implemented the Wi-5 Controller in open source (https://github.com/Wi5) and successfully tested various scenarios [5].

III. The Brokering Platform

A. *Functionality*

The Brokering Platform is what enables the Wi-5 architecture to facilitate collaboration between independent AP operators (called Local AP Managers in Figure 1) in a setting of scarce spectral resources, e.g. in densely built environments. Whereas traditional SDN and SDWN are typically used within a single operator domain, we claim that a combination of Wi-5 Controller and Brokering Platform can be used by independent AP operators to negotiate and execute spectrum sharing policies in an automated way.

In its simplest form, the Brokering Platform is virtual, i.e. it contains non-automated facilities (pen, paper, round table, etc.) that the Spectrum Broker uses to cement a deal between the Local AP Managers. Both interfaces of the Brokering Platform with the Local APs and the Wi-5 Controller are then virtual also.

Alternatively, the Brokering Platform is an IT platform which automates negotiation, in which the local APs with their requirements and offers are represented by agents. The agents then negotiate a deal, e.g. using a negotiating algorithm as described in [7,8,9].

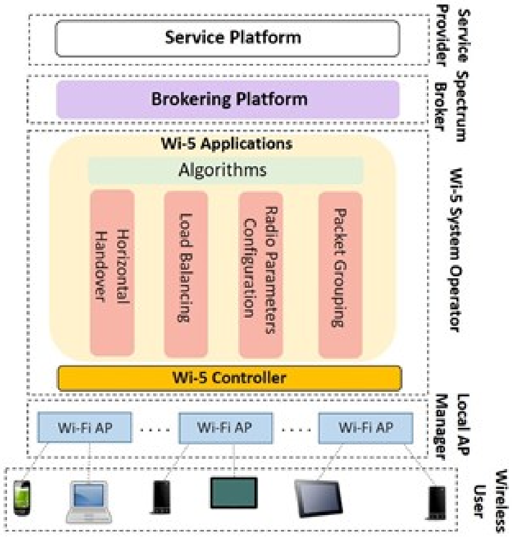

Fig. 1. Wi-5 high-level architecture

To do so, the Spectrum Broker needs information from the APs. This information includes not only current configuration parameters, local radio monitoring results, etc., i.e. everything needed to assess the spectral resources that an AP has on offer, but also a statement regarding how much spectral resources are demanded by the devices that are currently served by an AP. This cumulative demand is determined by the negotiation of individual Wireless Users with their Service Providers. Here a Service Provider is defined as the actor that provides, manages, and controls the Wide Area Network (WAN) connectivity and service access for the wireless access networks. The role of Service Provider can be taken up by several parties together, in collaboration [6]. For instance, to listen to an Internet radio service this role is typically taken by a broadband access WAN network provider, an Internet Service Provider (ISP) and a radio channel content provider.

After devising a spectrum sharing policy, or contract, the Brokering Platform passes the contract on to the Wi-5 Controller. As such, the Brokering Platform also provides network operators the opportunity to automate re-negotiation of policies when needed, e.g. when there are new entrants.

B. *Existing architectures*

Very few elaborated architectures of such Brokering Platforms exist today. The one in [8] is the best we know, and it is shown in Figure 2. Here, Zhang *et al* describe a Coordination Wi-Fi Platform (CWP), which talks directly to the APs. First, the APs are represented in CWP as Virtual Agents (VAs) using a bespoke protocol. The VAs then exchange information using a novel AP Talk Protocol (ATP). The Interference Measurement module performs active interference measurement between the APs, reflecting both in-range interference and hidden terminal interference. The Power Coordination module is where negotiation between VAs happens, here using Nash bargaining, the outcome of which will optimize the APs transmission powers. Then there are various management modules, one for managing the VAs (VA Management), one for time synchronization (Slot Management), defining the heartbeat of the system, and one for managing the data being received and held in the Data Storage part of the CWP (File Management). These management modules are in themselves managed by the CWP Manager module.

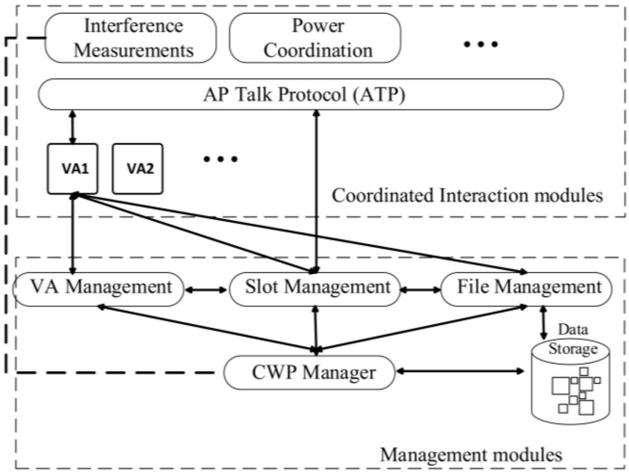

Fig. 2. High-level architecture of the Coordination Wi-Fi Platform as presented in [8].

C. Wi-5 Brokering Platform architecture

We base the architecture of the Brokering Platform on the one presented in Figure 2, but take into account the following differences:

- We optimize mutual interference impact by not only varying the transmit power, but also channel selection, packet grouping parameters, and which AP is best to attach to [5].
- The optimum mutual interference impact is not necessarily the minimum mutual interference impact, as it is determined by Nash bargaining. Neither is it necessarily the mutual interference impact that leads to equal throughput for all. The optimum mutual interference impact is whatever leads to a distribution of performance that the Local AP Managers have agreed upon after negotiation.
- The authors of [8] assume that APs are controlled by a single authority, and therefore are able to optimize the mutual interference impact using cooperative game theory. In our case, participants can choose to drop out if the negotiation does not lead to a satisfactory solution.
- The Brokering Platform only talks to the APs via the Wi-5 Controller. This has two advantages. First, the APs can be monitored and controlled using standard protocols such as OpenFlow (with an extended parameter set). Second, the Brokering Platform only needs to pass a contract on to the Wi-5 Controller, which consequently tunes its optimization algorithms such that the contract is fulfilled.
- The Brokering Platform does not require a full set of monitored low-level radio parameters from the FNMM. Instead, it needs per AP an estimate of spectral resources demanded and on offer (including their inter-AP dependencies), and insight into how possible mismatches between the demand and offer could be settled by a pricing agreement that leads to the equal distribution of satisfaction. Said otherwise, if AP1 has little on offer and much demand, which AP2 cannot deliver without undesired loss of performance for itself, AP1 (or rather its Local AP Manager) may buy some resources from AP2 for a price with which both parties end up equally satisfied (and above a certain absolute minimum satisfaction threshold).

These requirements lead to a proposal for the Wi-5 Brokering Platform architecture as presented in Figure 3. Here, FNMM and Interference Optimization Algorithms are as described in [7], but in addition to regular measurements from the APs and new flows entering the network, it should also register demands, satisfaction levels, and price sensitivities, and communicate these to the Brokering Platform. The Management Modules function in pretty much the same way as in Figure 2. The VAs communicate with each other via the Coordination Module, which tries to steer the negotiation towards an equilibrium. The obtained equilibrium is then communicated to the Wi-5 Controller as a set of weights with which the Interference Optimization Algorithms are consequently tuned.

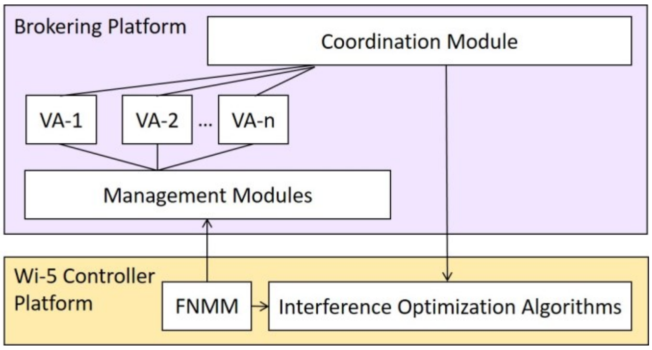

Fig. 3. Proposed high-level architecture of the Brokering Platform

D. Towards a distributed Brokering Platform architecture

In the Wi-5 project, we initially assumed that the Wi-5 architecture could be deployed in a centralized fashion, i.e. the Wi-5 Controller and the Brokering Platform could run on a central local server, or in the cloud, operated by independent 3rd party Wi-5 System Operators and Spectrum Brokers. However, after intensive discussion with many existing Wi-Fi network operators, we realized that such deployment may fail due to a lack of trust between the actors: Wi-Fi network operators do not necessarily know or trust each other, and would definitely not trust an yet unknown Wi-5 System Operator and Spectrum Broker who both have a controlling monopolistic position in the value chain. This, then, would demand for a distribution of the responsibilities of the Wi-5 System Operator and the Spectrum Broker over the existing Local AP Managers, and thus of the functionality of the Wi-5 Controller and the Brokering Platform over the APs. However, if we would attempt to take out the Wi-5 Controller and let the APs directly talk to each other, we would be back at the status quo, which is just not an option.

Distributing the Brokering Platform over the APs, however, deserves further study. Our proposal is to employ distributed ledger technology, a.k.a. blockchain, to achieve this. A blockchain is a peer-to-peer network that can be used as a secure but distributed information carrier for any transaction of value. The technology enables applications that could previously run only through a trusted intermediary, to operate in a decentralized fashion, without the need for a central authority. Its key property is that it distributes trust by sharing a digitally signed and verified log of all value transactions among the participants.

Blockchain is best known as a carrier for cryptocurrencies. But also other digital representations of value can be supported. Smart Contracts are an important example: instead of currency, the records consist of code that can execute business logic (contracts) to posted transactions [10]. This is what is most likely needed in the case of trading unlicensed spectrum: access rights to spectral resources are exchanged for e.g. money. So, the idea is to forget about creating VAs in a centralized platform as shown in Figure 3, and let the Coordination Module run in a distributed fashion on the physical APs, where APs exchange value directly with each other, and synchronize the state using some type of blockchain. The state is then communicated to the Interference Optimization Algorithms using FNMM.

IV. FUTURE WORK

Before we can design a distributed Brokering Platform architecture, we first need to gain a deeper understanding of the internals of the Coordination Module. A very simple business logic was proposed in one of Wi-5's deliverables [11], where we assumed that a Local AP Manager who contributes twice as much money compared to the other Local AP Managers to cover the costs of network operations, would also retain the right on double the wireless capacity. But real negotiations may be more complicated, and have to be studied, e.g. by serious games with real stakeholders.

Although many different types of blockchain exist, they generally have high demands on computation, storage and communication in order to deliver high-level security, leading to high overhead, delays, and low scalability. This is in stark contrast with the capabilities of a CPS network, often consisting of APs and small wireless devices and sensors that need efficient communication and have limited storage and computation capacities. This requires new lightweight solutions to the mining and blockchain construction without compromising security too much.

The latter will not be trivial. One reason is that we are dealing with relatively few devices, as the area in which devices interfere with each other is generally quite small (~100 m). Normally, the larger the network of miners/peers, the stronger is the blockchain's security and availability.

Also, we do not expect trading to happen very often in CPSs. Less frequent trading makes a blockchain more vulnerable to be compromised. A common way to prevent this is to allow the initial transfer to take effect only after a predefined number of new blocks have been added to the chain after the transfer, meaning delayed implementation. This would have ramifications for the performance of the wireless network as a whole. Mechanisms have to be developed to mitigate these risks.

Another shortcoming of blockchain is non-protection of data/ledger confidentiality. Nodes and their users generally expect to preserve their privacy/data confidentiality during their interaction with the blockchain, but this contrasts with the need to hold users accountable, e.g. for billing and mobility purposes. Verifiable encryption or zero knowledge proof techniques are useful for solving such a problem, but they are not efficient and some of them need support from a trusted or semi-trusted third party. Hence, new/better algorithms and protocols are needed.

V. CONCLUSIONS

Sustainable spectrum sharing in unlicensed frequency bands by CPSs in densely populated areas requires collaboration between the stakeholders. Such collaboration needs to be facilitated by platforms such as the one developed in Wi-5. These platforms are based on the concept of SDN, and also include a Brokering Platform. This is an IT platform that automates negotiation between Local AP Managers, in which the local APs with their requirements and offers are represented by agents.

In this article we presented a novel architecture for such a Brokering Platform. We initially assumed that it could be deployed in a centralized fashion, e.g. on a central local server or in the cloud, operated by an independent Spectrum Brokers. However, such deployment may fail because Wi-Fi network operators do not trust a yet unknown Spectrum Broker with a controlling monopolistic position. We therefore propose the distribution of Brokering Platform functionality over the APs, using blockchain technology. However, to the best of our knowledge, blockchain technology that is suitable for this use case does not yet exist. We therefore conclude this paper with various requirements with which a suitable blockchain must comply.

REFERENCES

[1] National Institute Standards and Technology, "Cyber-Physical Systems", available from http://www.nist.gov/cps/, accessed on 24 October 2017.

[2] F. den Hartog, P. Kempker, B. Boltjes, A. Raschella, F. Bouhafs, and M. Seyedebrahimi, "A Pathway to solving the Wi-Fi Tragedy of the Commons in apartment blocks", in Proc. of the International Telecommunication Networks and Applications Conference (ITNAC 2017), Melbourne.

[3] F. den Hartog and J. de Nijs, "The role of regulation in preventing Wi-Fi over-congestion in densely populated areas", Australian Journal of Telecommunications and the Digital Economy, vol. 5, no. 2, article 93, May 2017.

[4] F. Bouhafs, M. Mackay, F. den Hartog, J. Saldana, and A. Arsal, "Wi-5 final architecture", Deliverable D2.5 of the H2020 Wi-5 project.

[5] F. Bouhafs, *et al*, "Wi-5: A programming architecture for unlicensed frequency bands", accepted for publication in IEEE Commun. Mag.

[6] F. den Hartog, and K. Dittrich, "Towards a viable business model for collaborative use of unlicensed frequency bands in densely populated areas", submitted to International International Telecommunication Networks and Application Conference (ITNAC), Sydney, 2018.

[7] A. Raschellà, *et a*l, "AP selection algorithm based on a potential game for large IEEE 802.11 WLANs", In Proc. of IEEE/IFIP Network Operations and Management Symposium (NOMS), Taipei, 2018.

[8] Y. Zhang, C. Jiang, Z. Han, S. Yu, and J. Yuan, "Interference-aware coordinated power allocation in autonomous wi-fi environment," IEEE Access, vol. 4, pp. 3489–3500, 2016.

[9] D. DebBarma, Q. Wang, I. M. Niemegeers, S. Heemstra de Groot, and A. Lo, "Coalition game-theory-based congestion control in hybrid Fi-Wi indoor network", In Proc. of the 3rd International Conference on Future Generation Communication Technology (FGCT), pp. 25-32, August 2014.

[10] K. Christidis, and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things.", IEEE Access, vol. 4, pp. 2292-2303 (2016).

[11] F. den Hartog, K. Dittrich, J. de Nijs, M. van Heesch, P. Wissink, and F. Bouhafs, "Regulatory and game-theoretical considerations regarding the Wi-5 business model", Deliverable D2.6 of the H2020 Wi-5 project, April 2018.