IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A Trust-based Cooperative System for Efficient Wi-Fi Radio Access Networks

A. Raschellà [1], M. Hashem Eiza [1], M. Mackay [1], Q. Shi [1] and M. Banton[2]
[1]School of Computer Science & Mathematics, Liverpool John Moores University (LJMU), Liverpool UK
[2] Department of Computer Science, University of Sunderland, UK

Corresponding author: A. Raschellà (e-mail: a.raschella@ljmu.ac.uk).

ABSTRACT This paper proposes a novel trust-based cooperative system to facilitate efficient Wi-Fi network access trading to solve the network congestion problem in a beneficial manner for both service providers and customers. The proposed system enables service providers to improve their users' application performance through a novel cooperative Access Point (AP) association solution. The system is based on a Software-Defined Wireless Network (SDWN) controller, which has a global view of users' devices, requirements, and APs. The SDWN controller is supported by Smart Contracts (SCs) as code of law, to liaise control among service providers according to the terms of their mutual agreements. Evaluation results in dense Wi-Fi network environments show how the system can significantly improve the overall performance for the cooperating network. Specifically, the results have been compared against the standard AP association approach and other centralised algorithms dealing with the same problem, in terms of the data bit rate provided to the users' stations (STAs), Quality of Experience (QoE), bandwidth and energy consumed by the APs.

INDEX TERMS Access Point Association, Blockchain, Radio Access Network (RAN), Smart Contract, Software-Defined Wireless Network (SDWN).

I. INTRODUCTION

The wireless communication sector is witnessing a significant increase of devices connecting to the Internet, driven by the emergence of a range of innovative mobile applications and online services. As a result, wireless traffic is estimated to grow at an annual rate of approximately 54% between 2020 and 2030 [1]. Moreover, 2030 is foreseen to be the year in which 6th Generation (6G) networks will begin to be introduced to provide performance superior to the current 5th Generation (5G) and to serve emerging services. For instance, 6G technology promises to provide continuous wide area coverage, peak data rates of at least 1 Tb/s, and improved energy efficiency of 10–100 times that of 5G, along with higher reliability [2].

However, it is also undoubtedly the case that wireless networks are becoming increasingly overcrowded by this massive number of users, heterogeneous technologies, and applications. This will have serious repercussions for modern wireless network customers, Internet Service Providers (ISPs), Network Providers, and Mobile Network Operators (MNOs). These repercussions are mainly related to spectrum congestion with consequent high harmful interference, and network congestion, especially for Wi-Fi networks, which represents a cheaper and more diffuse alternative for many wireless users and stakeholders. Hence, there is an urgent need for new solutions and mechanisms to optimise network performance. Note that for simplicity, in this paper, we will consider only the term stakeholder to refer to any entity that provides services for accessing and using the Internet, and that operates its own network elements.

Spectrum and network congestion affects the quality of the network performance leaving customers unsatisfied and potentially downgrading stakeholders' reputation, for instance increasing the so-called churn rate. This metric indicates the rate of dissatisfied customers who decide to cease their relationships with a certain stakeholder due to its poor performance, and switch to one of that stakeholder's competitors for better performance [3]. It is worth noting that 45% of smartphone user churn happens due to network quality issues[1]. Today, therefore, all the telecommunication operators

[1] https://www.linkedin.com/pulse/impact-churn-telecom-industry-how-bi-can-potentially-solve-chowdary/ (last access October 2023).

are challenged to optimise the use of finite radio spectrum resources and, at the same time, satisfy their customers to efficiently provide ever-increasing connectivity and capacity.

In this context, and staying with Wi-Fi networks, we believe that existing Radio Resource Management (RRM) solutions that do not rely on cooperation, such as works [4], [5] and [6], can benefit from coordination among Wi-Fi networks to enhance their performance. Specifically, a centralised management of the Wi-Fi Access Points (APs) that belong to different stakeholders, who agree to cooperate in a dense environment, would present a global view of the networks and provide crucial input for efficient RRM solutions. Examples of this information includes channel occupation (needed in [4] and [6]) and available data rate in a certain AP which depends on the interference caused by adjacent APs (needed in [5] and [6]).

To address these requirements, Software-Defined Wireless Network (SDWN) is a suitable tool in this context. However, the mere use of this technology is not enough for the implementation of a proposed system. Specifically, an SDWN-based deployment may fail due to a lack of trust, incentives, transparency, and accountability among the actors. Stakeholders do not necessarily know or trust each other and definitely would not yet trust an unknown SDWN-based system that would be controlled by other stakeholders aiming to achieve their own benefits, hence jeopardising the potential cooperation. Therefore, to rectify these problems, we propose to use Smart Contracts (SCs) as code of law to liaise control among all stakeholders according to the terms of their mutual agreements. SCs are event-driven programmes that are executed on top of a Blockchain network and offer a mechanism to initiate transactions according to a defined business logic and, if valid and approved by participants, update the ledger records. Depending on the Blockchain, SCs can be developed using different programming languages. For instance, in Ethereum, SCs are written in a high-level language called Solidity [7] while Hyperledger Fabric (HLF) allows the use of standard programming languages such as Node.js or Java [8].

At the same time, Blockchain ensures data consistency among distributed nodes in a Peer-to-Peer (P2P) network without a trusted third party by utilising the Distributed Ledger Technology (DLT), where every node has a copy of the records (i.e., the ledger) of all transactions [9]. Changes are only committed to the ledger if nodes reach consensus on the validity of these changes. Transactions are arranged in blocks chained to each other using an immutable cryptographic signature (i.e., hash). The blocks can be only appended to the chain, hence, once a transaction has been added to the ledger, it cannot be changed. All nodes update their copies of the ledger with the same transactions in the same order once the transactions are approved (i.e., a consensus is reached). Blockchains can be either 1) permissionless where virtually any node can participate in the network and can do so anonymously (e.g., Bitcoin [10] and Ethereum) or 2) permissioned where participants' identities are verified before they can join the network (e.g., Hyperledger Fabric [8] and R3 Corda [11]). Permissioned aka Consortium Blockchains do not require mining activities thus, consensus can be reached quicker and with less computational power. Still, the benefits of decentralisation, immutability, provenance, and finality exist.

Based on the above, this paper aims to develop and evaluate a proof of concept of a trust-based cooperative system among dense Wi-Fi networks, utilising SCs, to address the network congestion problem. This is possible by allowing user associations to any AP based on their ongoing application requirements but regardless of their stakeholder, as long as they are participants of the cooperative system. Furthermore, the system advocates the use of smart, privacy-aware, and transparent cooperation agreements along with incentivisation mechanisms that will encourage stakeholders to share relevant information crucial for the proposed radio spectrum resource use. This cooperation will be implemented in a smart controller with a global view of users' devices, access nodes, and ongoing applications, and will be applied in real-time due to the high dynamicity of the dense Wi-Fi network radio environment. Moreover, the controller must be able to handle APs with different vendor interfaces along with their monitoring capabilities. This management should be done based on 'Plug-and-Connect' where the details of technologies, protocol stacks, interfaces, etc. are abstracted away from stakeholders' administrators. The SCs will be executed on top of an HLF [8] Blockchain network to support the SDWN-based controller, and facilitates a transparent architecture for spectrum and radio access sharing.

The rest of the paper is structured as follows. In Section II, we discuss related works in the literature in terms of cooperation among wireless networks and AP association, and our novel contributions. Section III presents the trust-based cooperative system including its architecture and implemented functionalities. Section IV illustrates the algorithm for AP association. Section V explains the case study considered in this paper to evaluate the proposed cooperative system and algorithm, while Section VI presents the performance results. Finally, the paper's conclusions and future research directions are illustrated in Section VII.

II. RELATED WORKS

A. COOPERATION AMONG WIRELESS NETWORKS

Cooperation to solve the problems of spectrum and network congestion is an attractive solution that has already been proposed in international projects [12] and several papers such as [13], [14], [15], [16], [17], [18], [19], [20], [21], [22]. Specifically, the work in [12] presented *Wi-5*, a spectrum programming architecture developed to cooperatively address spectrum congestion in unlicensed frequency bands. Nagaraj *et al.* [13] and Bouhafs *et al.* [14] addressed the interference problem in Wi-Fi networks through cooperative

AP channel assignments. Additionally, Ali *et al.* [15] discussed the potential of Unlicensed Long-Term Evolution (LTE-U) and Wi-Fi cooperating in heterogeneous networks as key technologies for future Beyond 5th Generation (B5G) systems. Moreover, they proposed a Mesh Adaptive Direct Search (MADS)-based resource allocation approach for LTE-U and Wi-Fi to maximise the throughput. Candal-Ventureira *et al.* [16] introduced and evaluated two solutions for MNOs or ISPs to dynamically divide the radio resources of a shared channel between Wi-Fi and cellular technologies to enhance spectrum efficiency.

In [17], we proposed a framework that addresses the radio access congestion problem in unlicensed bands through radio access node selection, which simultaneously benefits and satisfies both Wi-Fi and 5G users through cooperation managed by centralised controllers. Qin *et al.* [18] proposed a novel architecture including a slicing orchestrator, which coordinates multiple network and service providers to define a slicing allocation through negotiation in a heterogeneous Radio Access Network (RAN). Ling *et al.* [19] presented Blockchain-Radio Access Network (B-RAN) as a novel networking paradigm for B5G wireless networks. Through the lens of network effects, they illustrated how B-RAN improves efficacy and productivity. Giupponi *et al.* [20] proposed the use of B-RAN in the Open Radio Access Network (O-RAN). Zheng *et al.* [21] proposed a Multiple-Operators Spectrum Sharing (MOSS) platform based on the permissioned Blockchain platform Ethereum to implement spectrum trading among multiple operators (multi-OPs). Finally, Zhang *et al.* [22] presented a Blockchain-based system for a distributed spectrum sharing solution for coexistence of multiple operators and multiple Wi-Fi APs.

Nonetheless, these approaches have several limitations. Specifically, to achieve a global view of the network, APs from different stakeholders must exchange relevant information whereas in practice they might not want to trade this knowledge due to security, customers' privacy, and commercial reasons. However, most of the above-mentioned approaches [12], [13], [14], [15], [16], [17] consider that the RAN infrastructure works under a single administrative control. Therefore, they do not provide realistic strategies to guarantee trust and transparency among the stakeholders that decide to cooperate. Moreover, most of these approaches [13], [14], [15], [16], [18], [19], [20], [21], [22] try to optimise objective key metrics in each access node, such as spectral efficiency, throughput, packet losses, and delay without taking into account the actual ongoing applications and corresponding requirements in terms of the bit rate experienced by the wireless users. Furthermore, most of these works [12], [13], [14], [15], [16], [18], [20], [21], [22] do not address AP selection to solve the problem of network congestion.

Finally, none of these approaches consider incentive and trust-based mechanisms to encourage stakeholders to cooperate. Specifically, fostering multiple relationships among stakeholders to stimulate new services and cooperation while striking the balance between decentralisation and transparency on one hand, and secrecy and resilience on the other, is not considered in the current literature. Note that the work in [18] addresses incentives through an orchestrator that plays the role of a third-party entity. The orchestrator helps service providers to maximise their utility and network providers to minimise their costs through an auction mechanism, which guarantees convergence to optimal social welfare. However, it does not guarantee a system with full transparency and trust. Moreover, the optimal social welfare can be reached only if all the service and network providers give, in real-time, their bids needed by the orchestrator, which is prohibitive in dense Wi-Fi networks.

B. AP ASSOCIATION SOLUTIONS

The problem of AP association in Wi-Fi networks has been broadly addressed in the state of the art. Among the most recent published papers on this topic, we can find works in [17] and [19], which are mentioned in the previous section, and works in [23], [24], [25], [26], [27], [28], [29], [30], [31]. Specifically, Saldana *et al.* [23] presented a system managed by a central controller that gathers the capabilities of heterogeneous APs and users' stations (STAs) for efficient load balancing and mobility management. Gómez *et al.* [24] presented a solution relying on SDWN for user association based on a decision-making approach that considers average signal strength, channel occupancy, and AP load. Mao [25] proposed a centralised AP association and transmission time allocation for STAs with different throughput demands in densely deployed Wireless Local Area Networks (WLANs). Seob Oh *et al.* [26] presented a user association scheme for channel load balancing based on channel quality, traffic volume, and channel interference. Ly Dinh *et al.* [27] proposed a distributed user-to-multiple AP association approach that maximises both QoS and AP load constraints. El Khaled *et al.* [28] proposed two algorithms that predict the success of a user association to APs in fixed wireless networks for rural and harsh propagation environments respectively. Finally, in our previous works, we addressed the AP association problem through a function called *Fittingness Factor*, which addresses the suitability of the available spectrum resources to the application requirements [29], including a solution based on Game Theory [30], and another based on a trusted and transparent collaboration among different stakeholders' APs [31].

However, the lack of consideration for satisfying users' requirements as a key input for AP association is a major limitation in many of these approaches [19], [23], [24], [25], [26], [28]. The solutions proposed in [17], [27], [29], [30], [31] address this limitation by presenting AP association solutions that consider the suitability of each traffic with a specific AP in terms of users' requirements. On the other hand, the solution in [27] requires each STA to make use of a Deep Neural Network (DNN) to learn the best set of APs to be connected to, which is unfeasible in dense Wi-Fi

networks that are tremendously dynamic and make solutions based on distributed DNN too complex. Moreover, solutions in [17], [29], [30], [31] do not allow a reallocation of APs to Wi-Fi STAs that can experience different applications with corresponding different requirements while they are connected to the network, which might improve the performance. Furthermore, works in [17], [19], [23], [24], [25], [26], [27], [28], [29], [30] are not supported by a system that can guarantee trust and transparency among the cooperating stakeholders.

C. NOVEL CONTRIBUTIONS

This paper aims to develop a novel trust-based cooperative framework among stakeholders in Wi-Fi networks that addresses the limitations illustrated in Sections II.A and II.B in a unique system. The main novelties of this work with respect to the state of the art can be summarised as follows:

- The design of a system that will always, dynamically and without user input, associate STAs to the best available connection that can be provided by any AP based on their ongoing application and corresponding bit rate requirements. Moreover, the AP association allows STAs to change their connection when they switch to another application when needed.
- The development of a transparent, trusted and accountable cooperation architecture among the participating stakeholders that decide to join the system. This will be facilitated through an attractive solution that leverages the main features of SDWN and SCs in a Blockchain network. This novel solution allows customers to use any AP belonging to any stakeholder to share the unlicensed radio spectrum in a beneficial way for all the actors involved. In fact, so far, to the best of our knowledge, this is the first work that leverages SDWN, SCs and Blockchain network in an architecture to solve the problem of congestion in dense Wi-Fi networks. Note that the research community has already considered the use of Blockchain supported by SDN or SDWN but with other aims, such as for IoT technology [32] or for security purposes [33].

Furthermore, the proposed algorithm that enables this AP association enhances our previous solution presented in [31]. More specifically, in this paper, we provide the following new contributions:

- In terms of design, our new algorithm considers the dynamicity of Wi-Fi network radio environments. This means that the algorithm allows for transferring STA connections among different APs when needed. All the details on the enhancements implemented in the algorithm are provided in Section IV.
- In terms of implementation, a knowledge database has been implemented in the SDWN-based controller to store information on the STAs connected to the APs it manages. As we clarify in the next section, this information is crucial for the AP association algorithm.
- In terms of assessment, we have extended the performance evaluation to analyse the Quality of Experience (QoE) for the STAs, and also evaluate the algorithm for the stakeholders. Moreover, we have considered a further reference algorithm based on another centralised approach relying on SDWN [24], to illustrate how our solution can improve upon the performance of previous papers in the same area.

Finally, the developed algorithm is supported by bespoke SCs that are executed on top of the HLF Blockchain network utilising an SDWN controller to facilitate a transparent, trusted, and accountable collaboration among stakeholders. Transparency and trust here mean that all actions by all parties who join the system should be approved collectively and evidenced at any time thanks to the immutable nature of Blockchain records. Note that this paper focusses on the AP association algorithm implemented in the architecture and the token-based solutions that are designed to incentivise the cooperation among the stakeholders and define the rules of SCs supporting the proposed algorithm can be found in [31].

III. PROPOSED COOPERATIVE SYSTEM

The overall system architecture is illustrated in Figure 1. The centralised nature of SDWN enables the controller to obtain a global view of the network through monitoring and measurements to support all the implemented applications. The SDWN controller developed for the European Union Horizon 2020 (H2020) *What to do With the Wi-Fi Wild West* (Wi-5) project, which addresses spectrum congestion in Wi-Fi networks, is the basis for our architecture [12]. In that implementation, RRM strategies, defined as applications, can be developed on top of the controller through the northbound Application Programming Interfaces (APIs). This API also supports other management tools, which can be provided by third party developers. Moreover, the controller can gather periodic measurements from the radio environment, monitor the users' wireless STAs, and connect these STAs to a certain AP, through the southbound API. Note that the controller is semi-trusted in this context in the sense that it always performs its assigned operations correctly. Therefore, it is semi-trusted by all the stakeholders in the system to conduct its resources allocation and monitoring roles as long as it can provide irrefutable evidence of compliance with the cooperation agreements. Moreover, all the communications in Figure 1 are encrypted to ensure the confidentiality of these transactions.

The Wi-5 controller has been extended in our architecture in order to monitor information, statistics and events from all the network elements considered in this paper (i.e., wireless stations, Wi-Fi APs based on 802.11 standards and the Blockchain network entities). The RRM applications are implemented on top of the controller and are triggered according to the network needs and leads to actions securely agreed by all the stakeholders through the Cooperation Agreement, which is implemented as a smart contract on top of the Blockchain network. The RRM application developed

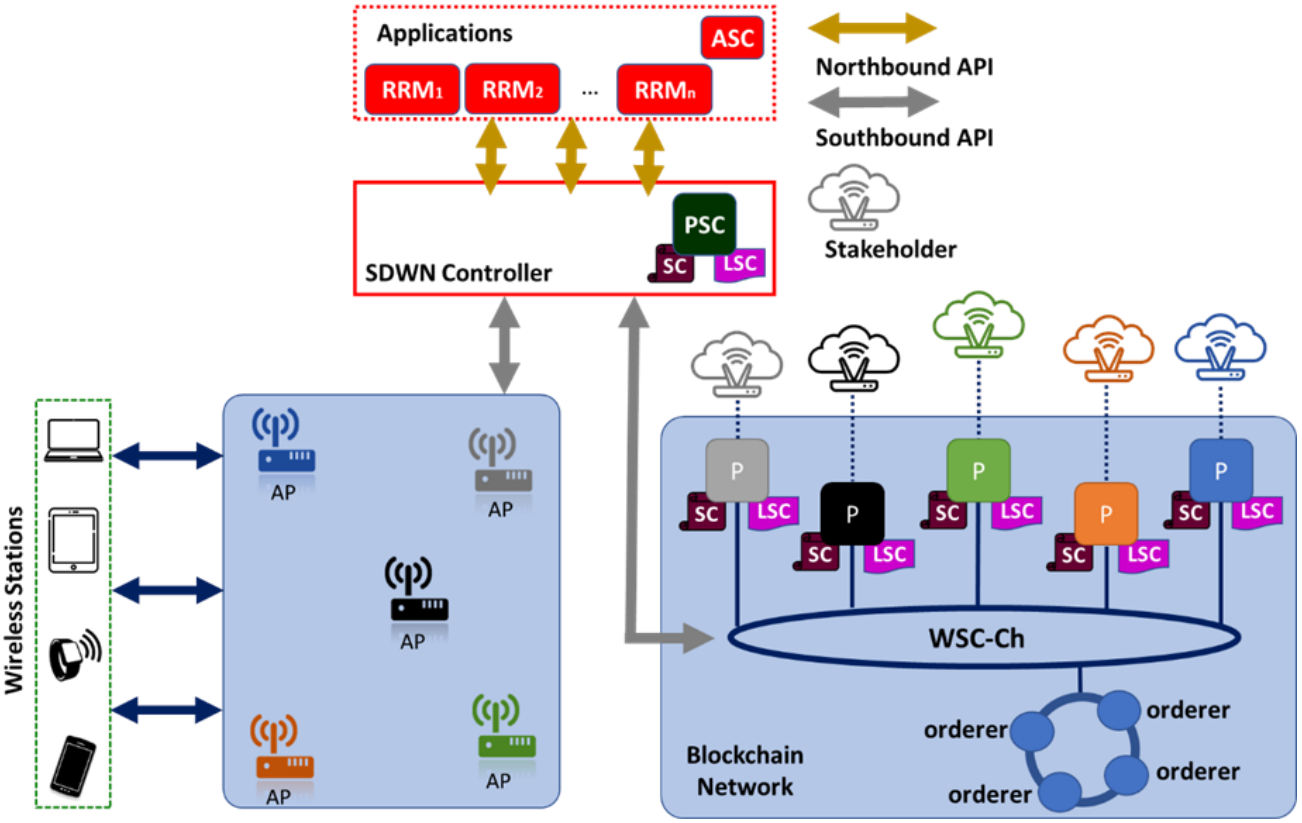


FIGURE 1. System Architecture for Trust-based and Efficient Cooperation including SDWN-based Controller and Blockchain network.

and presented in this paper is the algorithm for AP association as explained in Section IV.

As outlined in Section I, the Blockchain network in Figure 1 is permissioned whereby all peers are identified before they can join the network. This allows the participating stakeholders to monitor who can join the network, handle the communication channels, setup security and privacy policies, and define a bare minimum of trust among each other. To implement the cooperation agreement, the developed SCs give each stakeholder the flexibility to design and agree on the terms and conditions of their agreement with other stakeholders. The SCs are then enforced, and they are legally binding across the architecture. Note that stakeholders can join the system once a cooperative agreement is reached off channel. This is possible by negotiating the terms of the cooperation agreement with the other stakeholders via their administrators. Once agreed, the new stakeholder will be allowed to join the system.

The SDWN Controller Application (ASC) illustrated in Figure 1 is implemented and used by the controller to interact with the SCs on the Blockchain network to update the cooperation records. The ASC is the only way for the controller to access/update the ledgers (i.e., cooperation records) and invoke the SC functions that are responsible for executing the output of the RRM applications. For instance, through the ASC, the controller can create a new STA association to an AP or transfer a current connection to another AP depending on the association algorithm output. This way, updating the cooperation records will be carried out by the controller only, while stakeholders can only read these records. This is an essential element of facilitating a trust-based cooperation among the stakeholders.

Each stakeholder has a peer node *P* in the Blockchain network to negotiate and approve SC updates and transactions, and access the cooperation records (i.e., SDWN Controller Ledger (LSC)), which holds all the information related to the current users' connections. As illustrated in Figure 1, all the internal communications among stakeholders are carried via a dedicated secure and private channel *WSC-Ch* that guarantees secure and private transactions among all peers on the Blockchain network. This is a standard practice in HLF Blockchain network that allows the creation of multiple channels among participants to isolate their operations and keep their transactions private. The SDWN Controller Peer (PSC) is managed by the SDWN controller and gives it access to the cooperation records LSC and SC. The orderer nodes, managed by one or more stakeholder(s), are responsible for ordering transactions, creating a new block of ordered transactions, and distributing a newly created block to all peers on the *WSC-Ch* channel.

The Blockchain network in Figure 1 is implemented using HLF v2.2 in which the cooperating stakeholders are created together with their peers on the network. The channel

WSC-Ch is designed with an administrative policy that requires endorsements from all participants to accept new organisations and/or update the channel configurations. For instance, this will happen when a new stakeholder joins the cooperative system. The ASC application and SCs are developed in Node.js. The endorsement policy is set to all (i.e., all stakeholders must execute and agree on the SC execution result to consider the transaction valid). Note that endorsing the result of a SC function means it has worked according to the SC's specifications. The semantic of the result (e.g., transferring one STA connection from AP_1 to AP_2) is not endorsed because a stakeholder might not have enough information to endorse this decision. That is why it is the controllers' responsibility to do this, and all the records are transparent and available for all stakeholders.

In this paper, we assume that all the stakeholders who agreed to join the trust-based cooperative system will share their APs through the proposed algorithm, which is explained in the next section. This cooperation is incentivised and secured through the definition of SCs that implement operations such as creating connections when an STA is connected to an AP, updating connections' status based on the AP association algorithm, and updating the associated costs of these connections based on the negotiated and agreed terms among the participating stakeholders. Connection records for the AP association algorithm include, for each customer, the AP that is providing the connection, which can belong to any participating stakeholder, the offered bandwidth, and for how long the customers used that bandwidth. To ensure transparent and trust-based cooperation, all the connection records are accessible by the stakeholders and committed to the ledger if and only if the terms and conditions set in the cooperation agreement are satisfied (i.e., SC's execution results are endorsed).

Note that the results of executing these operations are fed to the AP association algorithm proposed in this paper to make decisions and vice versa (i.e., the algorithm will put forward potential proposals to connect and/or transfer connections to APs to do the necessary calculations of costs). The collective results of the interaction between the SC operations and AP association algorithm will set the benefits that every stakeholder will gain in terms of users' satisfaction and earned tokens for servicing other stakeholders' users. Details regarding the definition of the SC operations and the incentive mechanism for the participating stakeholders are out of the scope of this paper and can be found in [31].

Figure 2 illustrates the modules implemented in the central controller to execute the AP association algorithm proposed in this paper. The *Provided quality* module provides the bit rate that each AP in the network can give for a new STA requiring connection and is measured at the physical layer connection. This metric is calculated through the computation of the link capacity available for each new STA in terms of the bit rate that, in turns, depends on the channel bandwidth assigned to each AP, the computed inter-

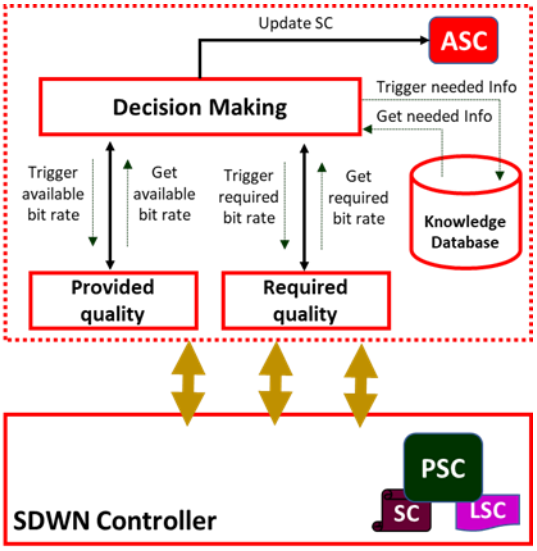


FIGURE 2. Modules implemented using SDWN for AP Association.

AP interference, and the location of the STA requiring the connection. The details of this computation are given in Section IV.

The *Required quality* module translates the QoS requirements of an STA requesting connection into a bit rate metric. Note that the bit rate requirements represent the minimum data bit rate of the STAs requesting connection, which is commonly available for online applications such as Voice over IP (VoIP) and YouTube, as explained in Section V. This can be obtained through, for instance, a Machine Learning (ML) based solution (e.g., [34]), which can easily be implemented in our system. Further details on ML-based classification approaches which could be considered here can be found in [29].

The *Knowledge Database* maintains information on the connections of all the active STAs in the network related to the RAN environment. Specifically, it stores information for all the STAs that are connected to the APs managed by the SDWN controller, the bit rate requirements corresponding to each active STA, the link capacity in terms of the bit rate available for each connected STA in the network, and the duration of the connection (i.e., for how long the STA has been connected to an AP). Such information will be considered in the *Decision-Making* module during the execution of the AP association algorithm.

The *Decision-Making* module is triggered either every time a new STA_i connects to the network or when a connected STA_i changes its application and corresponding bit rate requirements. It first triggers and collects the available information from the *Provided quality* and *Required quality* modules (i.e., available bit rates from APs that can provide connection to STA_i, and required bit rates, respectively, which depend on the radio environment through the southbound API). Furthermore, this module triggers and collects all the information needed for the execution of the algorithm which is stored in the *Knowledge*

Database related to the APs that can provide a connection to STA_i and the currently connected STAs. Then, it considers this information to execute the algorithm for AP association. All the details on the algorithm including how this information is used in the *Decision-Making* module are explained in Section IV. Finally, the *Decision-Making* module updates the STAs' connections based on the results of executing the algorithm, which is then implemented in the SC through the ASC as explained earlier.

IV. AP ASSOCIATION ALGORITHM

In our system, we consider a *legal AP* to be an AP that belongs to a stakeholder and gives services to its customers. Therefore, the legal AP for a certain STA is an AP which belongs to the stakeholder that provides services to that STA. Moreover, we define a *home user* as a user connecting an STA to his/her subscribed *legal AP* and a *guest* as a user connecting an STA to an AP belonging to a stakeholder that he/she is not subscribed to.

The algorithm presented in this paper for an efficient AP association to subscribers through stakeholders cooperating in the system, aims to enhance our previous *Win-Win AP association* approach in [31]. Therefore, in this section we first briefly describe the main principles of the Win-Win AP association algorithm and its main limitations. Then, we introduce the enhanced version that addresses those limitations.

A. WIN-WIN AP ASSOCIATION AND ITS LIMITATIONS

The term Win-Win was used to emphasise that the proposed algorithm can provide performance enhancements for all users in terms of their application performance in comparison to the standard approach that allows STAs to only connect to their legal AP. The Win-Win AP association algorithm allows a certain STA_i to connect to any AP_j belonging to any stakeholder only if such a connection does not negatively affect the other STAs that are already connected to AP_j (i.e., all the STAs connected to AP_j can achieve the minimum bit rates needed for their ongoing applications even after the connection of STA_i). Despite the encouraging performance results obtained through this algorithm in our previous work, it still has the following limitations that should be addressed to improve its performance:

- The algorithm did not prioritise *home users* in their l*egal AP*. Specifically, the system does not disconnect *guests* if *home users* return and want to access their *legal AP*. Furthermore, the algorithm did not allow for the moving or transferring of any user's connection from one AP to another.
- The algorithm did not distinguish among *home users* who are subscribed to their *legal AP*, *greedy home users* who are subscribed to their *legal AP* but also want to add more STAs than other users, and *guests*.
- The algorithm did not provide the STAs with a minimum acceptable bit rate.

B. ENHANCED WIN-WIN AP ASSOCIATION

The enhanced Win-Win AP association algorithm implemented in the SDWN-based controller in this work is presented in Algorithm 1. In detail, each STA_i that tries to connect to its legal AP_j or switches to an application requiring a higher data rate while it is connected to its legal AP_j, triggers the algorithm. The *Decision-Making* module first gets $R_{breq,i}$ the bit rate required by STA_i obtained through the *Required quality* module (line 1 of Algorithm 1). If STA_i is not able to get at least half of its bit rate requirement $R_{breq,i}$, because either it is too far from AP_j or AP_j is too congested, the *Decision-Making* module gets, from the *Knowledge Database*, a set *G* that includes all the guests connected to AP_j in order of arrival (i.e., the STA which has been connected for the longest time is the first one in set *G*, lines 2-3 of Algorithm 1).

ALGORITHM 1 – ENHANCED WIN-WIN AP ASSOCIATION

```
1:  get R_breq,i
2:  if STA_i is not able to get at least R_breq,i/2 in its legal AP_j do
3:        get set G of guests connected to AP_j
4:        found = 0
5:        guests_STA = 1
6:        while found == 0 and guests_STA <= length(G)
7:              compute R_b,i after disconnection of
                  guests STAs ∈ G(1:guests_STA)
8:              if R_b,i >= R_breq,i/2
9:                found = 1
10:             end if
11:               guests_STA ++
12:       end while
13:       if found == 1
14:         connect STA_i to AP_j
15:         connect disconnected guests to their legal AP
              if possible
16:         update R_b for all STAs connected to AP_j
17:       else
18:         get AP_k, k≠j with best RSSI
19:         all_good = 1;
20:         for each STA_x connected to AP_k do
21:                 update R_b,x based on connection of STA_i
                    to AP_k for required R_breq,i
22:                 if R_breq,x > updated R_b,x and x ≠ i do
23:                         all_good = 0;
24:                 end if
25:           end for
26:           if all_good = 1 and R_b,i >= R_breq,i/2 do
27:                 connect STA_i to AP_k
28:           else do
29:                 do not allow connection
30:           end if
31:       end if
32: else
33:    connect STA_i to AP_j
34: end if
```

After that, the *Decision-Making* module triggers the computation of the bit rate $R_{b,i}$ that STA_i could obtain in AP_j (i.e., $R_{b,i}$ after possible disconnections of the *guests* connected to AP_j in order of arrival, lines 4-12 of Algorithm 1) in the *Provided quality* module. Specifically, the Signal to Interference plus Noise Ratio (SINR) $SINR_{i,j}$ experienced by STA_i in AP_j is computed based on its location as follows:

$$\mathrm{SINR}_{i,j} = \frac{g_{i,j} \cdot p_j}{\sum_{y \in A'} g_{i,y} \cdot p_j + N_0} \quad (1)$$

where $g_{i,j}$ is the channel gain from AP_j to STA_i, p_j is the transmit power of AP_j, N_0 is the additive Gaussian white noise, and given A as the set of the APs included in the system, A' is a subset of the set A that includes the APs interfering with STA_i and other interfering APs that are not under the management of the SDWN-based controller, and therefore, affecting its experienced SINR.

Based on the SINR obtained through (1), the link capacity for STA_i is computed. The link capacity of an STA corresponds to the most efficient Modulation and Coding Scheme (MCS) to achieve the highest available bit rate under the interference level constraints. In this work, the MCSs are computed by using the Orthogonal Frequency Division Multiple Access (OFDMA) approach, which has been adopted in the most recent 802.11 protocols (e.g., 802.11 ax/be). According to these standards, a set of defined bit rate levels exist that can be provided by the APs. Each of these bit rate levels represents the maximum link capacity in Wi-Fi APs, defined in this case as $b_{i,j}$ between STA_i and AP_j that can be computed using $SINR_{i,j}$ and BW_j, which is the bandwidth assigned to AP_j in Hz, through the Shannon-Hartley theorem [29]. Hence, the parameter $b'_{i,j}$ is computed through (2) and then, $b_{i,j}$ is achieved by mapping $b'_{i,j}$ to the level closest to but below the bit rate level allowed by OFDMA.

$$b'_{i,j} = \mathrm{BW}_j \cdot \log_2\left(1 + \mathrm{SINR}_{i,j}\right) \quad (2)$$

After that, the bit rate $R_{b,i}$ is calculated from $b_{i,j}$ using the resource allocation algorithm designed in [29] that also considers the number M_j of STAs connected to AP_j and the maximum capacity C_j in bps available in AP_j. Therefore, $R_{b,i}$ can be expressed as the following function f of all these parameters:

$$R_{b,i} = \mathrm{f}\left(b_{i,j}, M_j, C_j\right) \quad (3)$$

If STA_i can achieve at least half of its bit rate requirements $R_{breq,i}$ after a gradual disconnection of one or more guests in AP_j in order of arrival, it is permitted to connect to AP_j (lines 6-14 of Algorithm 1). Moreover, each disconnected *guest* will be connected (i.e., transferred) to its legal AP if it is in the AP's coverage area, and the AP is not congested (line 15 of Algorithm 1).

If this is not possible, the algorithm finds the best AP_k where $k \neq j$ for STA_i in terms of Received Signal Strength Indicator (RSSI) among the available APs (lines 17-18 of Algorithm 1). After that, for each STA_x which is already connected to AP_k, the *Provided quality* module calculates the bit rate $R_{b,x}$ that each STA_x would achieve after a possible connection of STA_i that needs a bit rate $R_{breq,i}$ based on its ongoing application and obtained through the *Required quality* module. $R_{b,x}$ is again computed through (1)-(3). If STA_i can achieve at least half of its bit rate requirement $R_{breq,i}$ without decreasing $R_{b,x}$ for any STA_x to a bit rate lower than its current one, STA_i is permitted to connect to AP_k. Otherwise, its connection request is declined (lines 19-30 of Algorithm 1). Note that this process is transparent to the users and, therefore, they will always appear to be connected to their legal AP. This allows the system to seemingly extend the potential coverage of the legal AP for its users, making it more efficient for the corresponding stakeholder. Finally, the controller updates the *Knowledge Database* and all the connection records based on the new connections.

It is worth noting that the order of STAs in G can be changed (e.g., based on experienced data rates). However, this does not affect the results as we illustrate in Section VI. Finally, lines 2-15 of Algorithm 1 allow the system to prioritise *home users* in their *legal AP*. In fact, through the algorithm, it can disconnect *guests* (if needed) when *home users* return and want access to their *legal AP*. Moreover, the algorithm allows the system to move/transfer any user's connection from one AP to another (see line 15 of Algorithm 1). This handover does not affect the STA application performance. As demonstrated in [12] and [35], our system, which is based on the Wi-5 SDWN implementation, allows seamless handover of STAs among APs when needed.

Furthermore, thanks to the algorithm, the system does not need to distinguish between *home users*, *greedy home users* and *guests*. In fact, as *home users* are always prioritised, *greedy home users* and *guests* cannot negatively affect the performance in a certain AP. It is worth noting that the algorithm can be improved in order to provide a better experience to the guest users. For instance, the algorithm might also be triggered in the following cases: 1) when a *guest* switches to an application with higher bit rate requirements to accommodate the new requirement; and 2) to accommodate a *guest* that leaves the connection for a *home user* with any available AP when he/she is not in the area covered by his/her *legal AP*. We will consider enhancements that will also allow us to improve the guest users' experience in the section with our future works. Finally, note that the algorithm allows the system to provide STAs with at least half of the bit rate requirements (see lines 2 and 26 of Algorithm 1). The reason for this will be clarified in the next section.

We now discuss the complexity using the big O notation of our algorithm. Let M be the number of all the STAs connected in the network at a certain time instant t, which are equally distributed among N APs belonging to all the stakeholders that joined the system throughout the network. Moreover, let us assume that half of the STAs are *home users* and the remaining

half are *guests* for the sake of simplicity. Therefore, the *while* cycle in the AP selection algorithm is called *M/2N* times at the most (line 6 in Algorithm 1). Then, Algorithm 1 computes on average *M*/*N* bit rate values in the *for* cycle (lines 20-25 of Algorithm 1) and in line 16. Finally, note that the other operations implemented in the algorithm include only checks, calculations or assignments, do not depend on the input size and, therefore, in big *O* notation they have complexity with order *O*(1). Hence, considering that the number of APs is fixed during the execution of the algorithm, the complexity of our AP selection solution is linearly related only to the number of STAs connected to the network managed by our system and we can define its approximation as *O*(M). Note that the algorithm has the same complexity as the Win-Win AP association and, therefore, the improvements achieved by the enhanced version illustrated in Section V do not add further complexity.

V. SCENARIOS AND METRICS

To evaluate our proposed architecture, we simulated a Wi-Fi network in a Matlab-based simulator managed by the SDWN-based controller illustrated in Figure 1. The SCs are implemented in Node.js and run on top of the HLF Blockchain network running on an Ubuntu 20.04 server. The bidirectional communication between the simulator and HLF is enabled via a database, which is accessible only via the defined interfaces on the Matlab-based simulator and HLF network. This database bridges the simulated part of our evaluation to the running HLF network, and provides the information needed for both the AP association algorithm and SCs to operate successfully. It is worth noting that the system overhead related to Blockchain operations is not considered here since the agreement negotiation is done off channel and does not affect the current users and their connections. Transaction latency and throughput are also not considered given that we are only considering a limited evaluation network. Therefore, benchmarking our implemented HLF network and SC functions are left for future work where we will introduce our novel Dynamic Throttling Strategy (DTS), proposed in [36], to improve the effectiveness of the proposed system in terms of handling queries.

In this evaluation, the SDWN controller manages 5 Wi-Fi APs uniformly distributed in an area of 100m^2 with a minimum distance of 7m between them, and with a transmit power of 25 dBm. The APs are based on the 802.11ax standard also known as Wi-Fi 6 (for the 2.4 GHz and 5 GHz radio band) and Wi-Fi 6E (for the 6 GHz band). For this evaluation, the APs are configured to work on five 6 GHz radio band channels with a bandwidth of 40 MHz, operating with 2 streams and can reach up to 400 Mbps [37], [38]. Moreover, we consider two different scenarios with 500 and 1000 STAs, respectively, which were progressively created and uniformly distributed in the area. We also assume that five stakeholders agreed to cooperate in each scenario with each contributing one AP to the system. Note that these scenarios were designed to represent a common dense network environment [29].

Furthermore, we added two sources of external interference that have been operative for certain periods of time during the simulations in different Radio Frequency (RF) channels selected randomly among the ones used by the APs in the 6 GHz band. We assumed that each time these sources interfered with two of the APs managed via the SDWN-based network, they cause a reduction in the average SINR experienced in the affected APs by 2 dB. Therefore, resulting in a reduction of the available capacity in terms of the bit rates provided to the connected STAs. This assumption about the external interference in the simulated scenarios and its impact on the affected APs are representative of an empirical model explained in [30].

The bit rate requirements of the STAs have been randomly selected from a set varying between 64 kbps to 20 Mbps, to consider the minimum bit rates needed for common online applications such as VoIP and video streaming. Table I summarises these minimum bit rates together with the corresponding codec in the case of VoIP, and video resolution for video on YouTube and Netflix. For each application used by STAs, a duration has been selected from a set varying between 1 to 20 minutes. Moreover, the STAs that have been created in both scenarios remain connected for the entire duration of the simulations and can change their applications and corresponding bit rate requirements over time. Note that, the assumption for lines 2 and 26 of the proposed AP association algorithm helps the STAs connect to an AP providing at least 50% of their bit rate requirements. This means that, for instance, a user who is trying to watch a video on YouTube with HD 1080p resolution needing a minimum bit rate of 5 Mbps can experience a reduction of resolution to HD 720p, which requires a bit rate of 2.5 Mbps. Finally, 50 independent simulation runs were performed to obtain the results which are analysed in the next section.

TABLE I
BIT RATE REQUIREMENTS

Application	Codec/Resolution	Bit Rate
VoIP[2]	G.726	64 kbps
	G.722	128 kbps
YouTube[3]	Standard Definition 360p	0.7 Mbps
	Standard Definition 480p	1.1 Mbps
	High Definition 720p	2.5 Mbps
	High Definition 1080p	5 Mbps
	4K	20 Mbps
Netflix[4]	Standard Definition	1 Mbps
	High Definition 720p	3 Mbps
	High Definition 1080p	5 Mbps
	4K Ultra High Definition	15 Mbps

[2] https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html (last access October 2023)

[3] https://support.google.com/youtube/answer/78358?hl=en-GB (last access October 2023)

[4] https://help.netflix.com/en/node/306 (last access October 2023)

To benchmark the performance of the proposed AP association algorithm, we compare it against the following reference strategies:

- *Win-Win Access Point Association*: This is the previous version of our algorithm [31] that we explained in Section IV.A along with its limitations.
- *Enhanced Wi-Balance* [24]: This solution addresses unfair resource allocations by allowing STAs to migrate to other APs in order to achieve the optimal trade-off between the quality of the signal, load on the RF channels, and load of the APs. We consider this AP association approach because it also relies on a similar centralised system based on SDN. All the analytical details of this algorithm that we implemented in our system, which is illustrated in figures 1 and 2, can be found in [24].
- *Standard* [39]: This is the AP standard association approach that allows each STA to connect only to the legal AP based on the highest RSSI and recommended by the IEEE 802.11 standard, even if another AP belonging to a different stakeholder is available to provide a more efficient connection.

The assessment of all the approaches focuses on the following performance parameters:

- ***Data rate**:* This is the average data bit rate achieved at the end of the simulation by all the STAs that try to connect to the network.
- ***Percentage of STAs with Good Mean Opinion Score (MOS)***: This addresses the QoE of an application provided to an STA as the perceived acceptability from the client's point view [29]. In the context of this work, QoE is assessed using the MOS, which is an arithmetic mean of all the scores obtained by the result of subjective tests that can vary from 1 (worst experience) to 5 (best experience). The meaning of each of these scores is illustrated in Table II in terms of quality and impairment. In this work, the percentage of STAs that achieve at least a *Good* quality (i.e., a perceptible but not annoying impairment) at the end of the simulation is considered as a performance metric. Note that for the applications considered in this work, the successful assignment of the corresponding minimum bit rate requirements illustrated above guarantees the Good MOS shown below in Table II [29].
- ***Bandwidth usage***: This is the capacity at which an STA can transmit in bps and that each stakeholder provides to both *home users* and *guests*.
- ***Energy consumption*** [40]: This is the energy consumed in mJ by the APs during the connection of the served STAs. We consider this parameter as a key metric to evaluate the algorithm for the stakeholders because energy efficiency is one of the crucial performance parameters in Wi-Fi 6 [41].

As explained in the following section, while *Data rate* and *Good MOS* aim to assess the performance experienced by the users, *Bandwidth usage* and *Energy consumption* assess the performance for the stakeholders. All the results are averaged when all the STAs were connected in both scenarios. Finally, for STAs that changed their application during the simulations, the averages of the performance for all the applications have been considered.

TABLE II
MEAN OPINION SCORES (MOSS)

MOS	Quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

VI. PERFORMANCE ANALYSIS AND DISCUSSION

Figure 3 illustrates the performance results in terms of the data rate. Specifically, from the figure we can observe that the Win-Win algorithm we presented in [31] and the enhanced version proposed in this paper outperform the other solutions from the state of the art in terms of the data rate. In fact, the enhanced Win-Win algorithm outperforms the enhanced Wi-Balance by 29% and the standard approach by 69%, in the first scenario when all 500 STAs are connected to the network. The results in Figure 3 also show that the Win-Win algorithm outperforms the enhanced Wi-Balance algorithm and the standard approach by 27% and 67%, respectively. Moreover, in the second scenario, when all 1000 STAs are connected, the enhanced Win-Win version and the Win-Win algorithm outperform the enhanced Wi-Balance by 39% and 38%, and the standard approach by 71% and 70%, respectively in terms of the data rate.

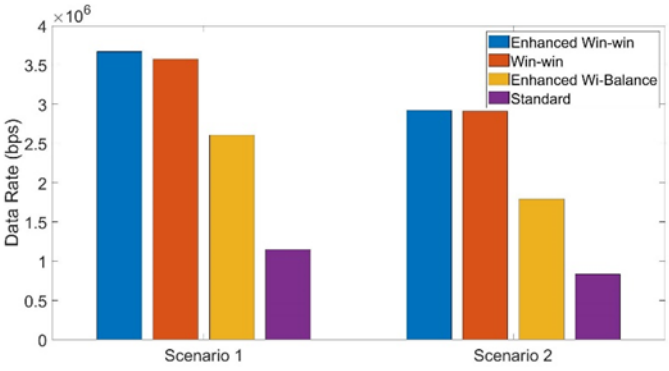


Figure 3. Performance in terms of Data Rates.

Figures 4 and 5 present the performance results in terms of Good MOS for the first and second scenario respectively. Specifically, in the figures, the left-hand side illustrates the performance achieved in the case of Voice applications (i.e., VoIP calls), whereas the right-hand side illustrates the performance obtained in the case of Video applications (i.e., streaming on YouTube and Netflix).

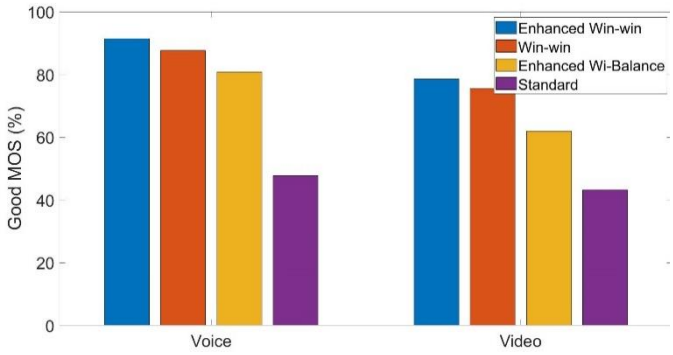


Figure 4. **Performance in terms of Good MOS for the first scenario.**

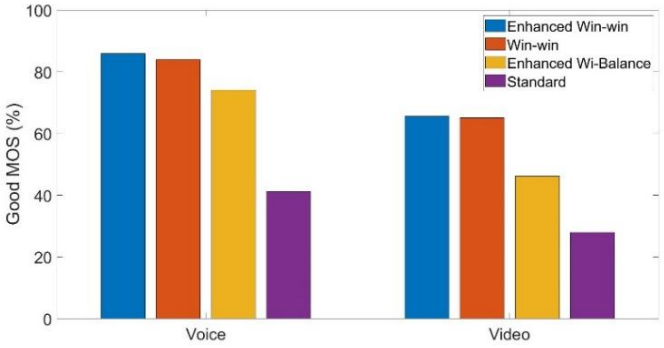


Figure 5. **Performance in terms of Good MOS for the second scenario.**

In both scenarios, the Win-Win algorithm and its enhanced version outperform the other approaches from the state of the art in terms of Good MOS. Specifically, in the first scenario, the enhanced Win-Win algorithm outperforms the enhanced Wi-Balance by 12% and the standard approach by 48% in the case of Voice applications, and 21% and 45% in the case of Video applications, respectively. The results in Figure 4 also illustrate that the Win-Win algorithm outperforms the enhanced Wi-Balance algorithm and the standard approach by 8% and 45% in the case of Voice applications, and 18% and 43% in the case of Video applications, respectively.

Furthermore, in Figure 5 we can observe that, in the second scenario, the increased number of STAs affects the Video applications most significantly, whereas in the case of Voice applications, the performance results are only slightly affected due to the lower bit rate requirements. The gains achieved by both Win-Win algorithms in comparison to the other approaches are approximately the same as in the first scenario. In detail, in the second scenario the enhanced Win-Win version and the Win-Win algorithm outperform the enhanced Wi-Balance by 30% and 57%, and the standard approach by 29% and 57%, respectively in terms of Good MOS for Video applications.

It is also worth noting that the enhanced Win-Win algorithm achieved a slight improvement over the previous version of this approach in terms of both Data Rate and Good MOS for both scenarios. For instance, the enhanced Win-Win outperform the Win-Win algorithm in terms of the Data Rate illustrated in Figure 3 by 2% and 1% in Scenario 1 and Scenario 2, respectively. However, as we will illustrate in the next results, the improvements achieved through the enhanced version of the algorithm are more tangible in terms of bandwidth usage and energy consumption.

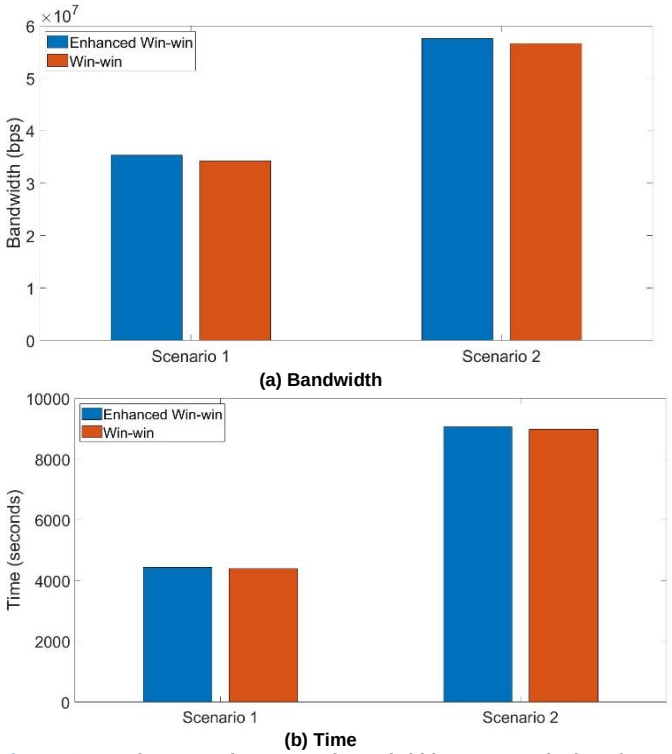


Figure 6. **Performance in terms of Bandwidth usage and Time for stakeholders' own customers.**

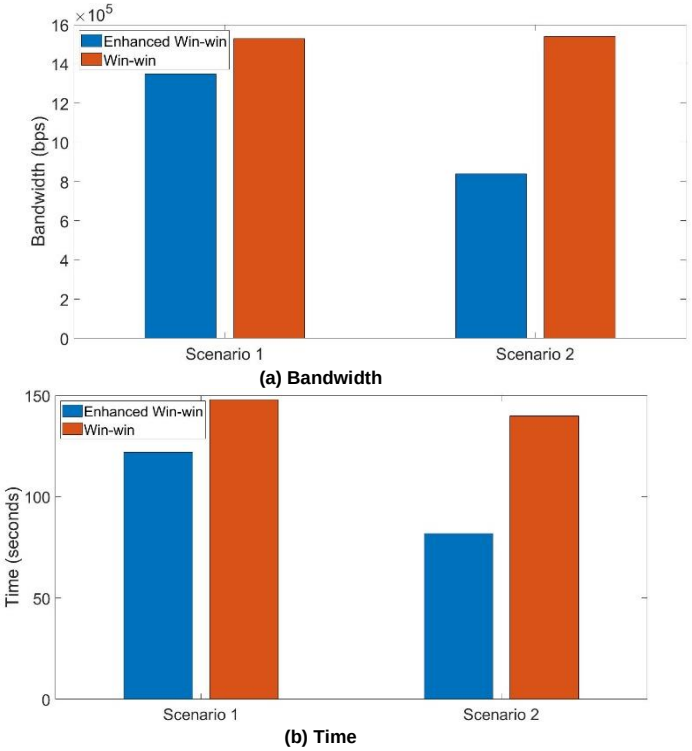


Figure 7. **Performance in terms of Bandwidth usage and Time for stakeholders' other customers.**

In this respect, Figure 6 illustrates the bandwidth in terms of network capacity that on average the stakeholders provided to their own customers (i.e., Figure 6(a) represents the bandwidth in bps and Figure 6(b) shows, on average, for how long the customers used that bandwidth). For STAs that changed their application during the simulations, the average duration of all such applications has been considered. In Figure 6, we can observe that on average, all the stakeholders provide similar amounts of bandwidth for similar durations to their customers in the case of both enhanced Win-Win version and Win-Win algorithm for both scenarios.

Similarly, Figure 7 illustrates the bandwidth that on average the stakeholders provided to other stakeholders' customers due to the cooperation. It can be observed that in the case of the enhanced Win-Win algorithm, on average, the stakeholders provide a reduced amount of bandwidth for a shorter duration to other stakeholders' customers in comparison to the original Win-Win algorithm. Specifically, the enhanced Win-Win version allows a reduction of granted bandwidth and time with respect to the Win-Win algorithm: 12% and 18% in the first scenario, and 45% and 41% in the second scenario, respectively. This has important implications on the energy consumption illustrated in Figure 8, which shows an average of the energy consumed by legal APs used by guests. In fact, in Figure 8 we can observe that the enhanced Win-Win solution allows a reduction of this consumed energy by 12% and 38% in comparison to the Win-Win algorithm in the first and second scenario, respectively. This means that stakeholders achieve performance improvements for their customers and, at the same time, manage to save energy when they allow other stakeholders' customers to use their own AP with the enhanced version of our algorithm.

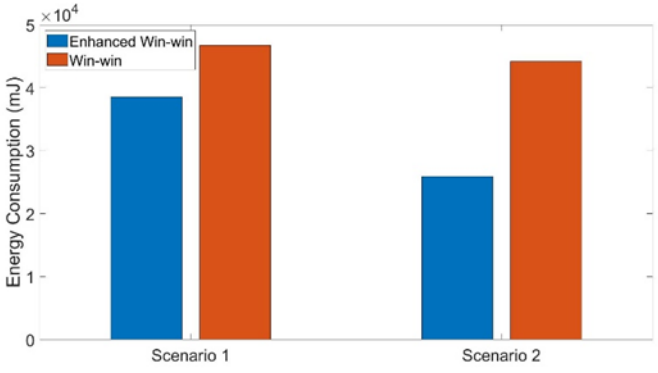


Figure 8. AP energy consumption for cooperating stakeholders.

In summary, Figures 7 and 8 show that stakeholders gave less bandwidth and spend less on energy in their AP because of cooperating in the proposed system under the enhanced algorithm. Yet, they managed to give their customers better QoE and data rate compared to the previous version of the algorithm and the state of the art, as illustrated in Figures 3 to 6 above. Table III summarizes these gains in terms of all the parameters achieved through the enhanced Win-Win algorithm in comparison to the previous version presented in [31]. From this table we can conclude that while the solution proposed in this paper gives a slight improvement in the performance experienced by the users, it results in a significantly more efficient allocation of stakeholders' resources for their customers in terms of network capacity provided to others, and energy efficiency that improves further in denser scenarios.

TABLE III
GAINS ACHIEVED THROUGH THE ENHANCED WIN-WIN ALGORITHM

Parameter	Gain (%)	
Data Rate	2	
Good MOS Voice	4	
Good MOS Video	2	Scenario 1
Bandwidth	12	
Energy Consumption	12	
Data Rate	1	
Good MOS Voice	4	
Good MOS Video	1	Scenario 2
Bandwidth	45	
Energy Consumption	38	

VII. CONCLUSION AND FUTURE DIRECTIONS

This paper has proposed a trust-based cooperative system for trading network access to solve the problems of Wi-Fi network congestion. The architecture utilises an SDWN-based controller that has an overview of users' requirements and APs' status, to connect STAs to suitable APs. Moreover, the cooperation in the system is governed by a Smart Contract that implements the cooperation agreement among stakeholders. The Wi-Fi radio access network is addressed through an algorithm implemented in the central controller that guarantees an efficient AP association to users, which can be served by the cooperating stakeholders in the system. To demonstrate the benefits provided by our algorithm, we have presented an accurate analysis of its performance in comparison to the standard AP selection approach and other solutions considered in the literature that address the same problem. We have illustrated how our algorithm obtains important improvements in two dense Wi-Fi environments in terms of the data rate assigned to the users, their QoE, bandwidth usage and energy consumed by the APs.

For future works, we will extend the proposed architecture to improve the experience of guest users and to include link and MAC layers' operations that will help exchange customers' account information among stakeholders when STAs migrate between APs. Moreover, we will extend the presented system to include other technologies such as 5G and B5G radio access networks and evaluate our algorithm in a heterogeneous environment. In terms of the Blockchain network, we will improve the provisioning of SCs among the participating stakeholders by including a ML-based module to setup cooperation agreements that can be dynamically updated based on changes in the operating environment with minimal interference from stakeholders' administrators. The

use of ML will also address possible system overhead related to Blockchain operations. Finally, we will redesign the blocks and transactions to meet our system goals and benchmark the newly developed Blockchain operations.

REFERENCES

[1] A. Slalmi, H. Chaibi, A. Chehri, R. Saadane, G. Jeon, "Toward 6G: Understanding network requirements and key performance indicators", *Wiley trans. on telecom. Tech.*, vol. 32 issue 3, Mar. 2021, doi.org/10.1002/ett.4201.

[2] C.-X. Wang, et al., "On the Road to 6G: Visions, Requirements, Key Technologies and Testbeds", *IEEE Comms. Surveys & Tutorials*, early access, Feb. 2023.

[3] S. Agrawal, A. Das, A. Gaikwad, and S. Dhage, "Customer Churn Prediction Modelling Based on Behavioural Patterns Analysis using Deep Learning", presented at the *IEEE International Conf. on Smart Computing and Electronic Enterprise* (*ICSCEE*), Kuala Lumpur, Malaysia, 11-12 Jul., 2018.

[4] L. Zhang, H. Yin, S. Roy, L. Cao, "Multiaccess Point Coordination for Next-Gen Wi-Fi Networks Aided by Deep Reinforcement Learning", *IEEE Syst. Journal*, vol. 17, issue 1, pp. 904-915 Jun. 2022, 10.1109/JSYST.2022.3183199.

[5] M. Alsakati, C. Pettersson, S. Max, V. N. Moothedath, J. Gross, "Performance of 802.11be Wi-Fi 7 with Multi-Link Operation on AR Applications", *IEEE Wireless Comms. and Networking Conf.* (*WCNC*), 26-29 Mar. 2023, Glasgow, Scotland, UK.

[6] V. N. Ha, G. Kaddoum, G. Poitau, "Joint Radio Resource Management and Link Adaptation for Multicasting 802.11ax-Based WLAN Systems", *IEEE Trans. on Wireless Comms.*, vol. 20, issue 9, pp. 6122-6138 Apr. 2021, 10.1109/TWC.2021.3072051.

[7] Ethereum, Solidity. Accessed Oct. 2023. [Online]. Available: https://docs.soliditylang.org/en/v0.8.7/.

[8] E. Androulaki, et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proc. EuroSys Conf.*, Porto, Portugal, Apr. 2018, pp. 1–15.

[9] B. Hu, et al., "A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems," *Patterns*, vol. 2, no. 2, Feb. 2021, doi.org/10.1016/j.patter.2020.100179.

[10] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," Accessed Oct. 2023. [Online]. Available: https://bitcoin.org/en/bitcoinpaper.

[11] M. Hearn, and R. G. Brown, "Corda: A distributed ledger," Aug. 2019. Accessed Oct. 2023. [Online]. Available: https://www.corda.net/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf.

[12] F. Bouhafs, et al., "Wi-5: A Programming Architecture for Unlicensed Frequency Bands", *IEEE Comms Magazine*, vol. 56, issue 12, pp. 178-185, Dec. 2018, 10.1109/MCOM.2018.1800246.

[13] S. Nagaraj, M. Sarkar, "Preliminary Results on Overlaid Cooperation Channels Between Nearby IEEE 802.11 Access Points", presented at the *IEEE Int. Black Sea Conf. on Comms. and Networking* (*BlackSeaCom*), Sofia, Bulgaria, 6-9 Jul. 2022.

[14] F. Bouhafs, M. Seyedebrahimi, A. Raschellà, M. Mackay, Q. Shi, "Per-Flow Radio Resource Management to Mitigate Interference in Dense IEEE 802.11 Wireless LANs", *IEEE Trans. on Mobile Computing*, vol. 9, issue 5, pp. 1170-1183 May 2020, 10.1109/TMC.2019.2903465.

[15] M. Ali, S. Qaisar, M. Naeem, W. Ejaz and N. Kvedaraite, "LTE-U WiFi HetNets: Enabling Spectrum Sharing for 5G/Beyond 5G Systems," *IEEE IoTs Magazine*, vol. 3, issue 4, pp. 60-65, Dec. 2020, 10.1109/IOTM.0001.2000024.

[16] D. Candal-Ventureira, F. González-Castaño, F. Gil-Castiñeira and P. Fondo-Ferreiro, "Coordinated Allocation of Radio Resources to Wi-Fi and Cellular Technologies in Shared Unlicensed Frequencies," *IEEE Access*, vol. 9, pp. 134435-134456 Sep. 2021, 10.1109/ACCESS.2021.3115695.

[17] A. Raschellà, et al., "A Centralized win-win Cooperative Framework for Wi-Fi and 5G Radio Access Networks", *Hindawi Wireless Comms and Mobile Computing*, vol. 2021, Sep. 2021, doi.org/10.1155/2021/5515271.

[18] Q. Qin, N. Choi, M. R. Rahman, M. Thottan and L. Tassiulas, "Network Slicing in Heterogeneous Software-defined RANs," presented at the *IEEE Int. Conf. on Computer Comms.* (*INFOCOM*), Toronto, ON, Canada, 06-09 Jul. 2020.

[19] X. Ling, J. Wang, Y. Le, Z. Ding and X. Gao, "Blockchain Radio Access Network Beyond 5G," *IEEE Wireless Comms.*, vol. 27, no. 6, pp. 160-168, Oct. 2020, 10.1109/MWC.001.2000172.

[20] L. Giupponi, F. Wilhelmi, "Blockchain-Enabled Network Sharing for O-RAN in 5G and Beyond", *IEEE Networks*, vol. 36, issue 4, pp. 218-225, Jul./Aug. 2022, 10.1109/MNET.103.2100489.

[21] S. Zheng, T. Han, Y. Jiang and X. Ge, "Smart Contract-Based Spectrum Sharing Transactions for Multi-Operators Wireless Communication Networks," *IEEE Access*, vol. 8, pp. 88547 – 88557, May 2020, 10.1109/ACCESS.2020.2992385.

[22] H. Zhang, S. Leng, Y. Wei, J. He, "A Blockchain Enhanced Coexistence of Heterogeneous Networks on Unlicensed Spectrum", *IEEE Trans. on Vehicular Tech.*, vol. 71, issue 7, pp. 7613-7624 Jul. 2022, 10.1109/TVT.2022.3170577.

[23] J. Saldana, et al., "Attention to Wi-Fi Diversity: Resource Management in WLANs With Heterogeneous APs", *IEEE Access*, vol. 9, pp. 6961 – 6980, Jan. 2021, 10.1109/ACCESS.2021.3049180.

[24] B. Gómez, E. Coronado, J. Villalón, R. Riggio, A. Garrido, "User Association in Software-Defined Wi-Fi Networks for Enhanced Resource Allocation", presented at the *IEEE Wireless Comms. and Networking Conf.* (*WCNC*), Virtual Conference, 25-28 May 2020.

[25] Z. Mao, "Throughput Optimization Based Joint Access Point Association and Transmission Time Allocation in WLANs", *IEEE Open Journal of the Comms. Society*, vol. 2, pp. 899-914 Apr. 2021, 10.1109/OJCOMS.2021.3072573.

[26] H. Seob Oh, D. Geun Jeong, W. Sook Jeon, "Joint Radio Resource Management of Channel-Assignment and User-Association for Load Balancing in Dense WLAN Environment", *IEEE Access*, vol. 8, pp. 69615-69628 Apr. 2020, 10.1109/ACCESS.2020.2986581.

[27] T. Ha Ly Dinh, et al., "Distributed user-to-multiple access points association through deep learning for beyond 5G", *Elsevier Computer Networks*, vol. 197, Oct. 2021, doi.org/10.1016/j.comnet.2021.108258.

[28] Z. El Khaled, H. Mcheick, W. Ajib, "Machine learning-based approaches for user association and access point selection in heterogeneous fixed wireless networks", *Springer Wireless Networks*, vol. 28, pp. 3503–3524, Jul. 2022, https://doi.org/10.1007/s11276-022-03053-2.

[29] A. Raschellà, F. Bouhafs, M. Seyedebrahimi, M. Mackay, Q. Shi, "Quality of Service Oriented Access Point Selection Framework for Large Wi-Fi Networks", *IEEE Trans. on Network and Service Mgmt.*, vol. 14, issue 2, pp. 441-455, Jun. 2017, 10.1109/TNSM.2017.2678021.

[30] A. Raschellà, et al., "A dynamic access point allocation algorithm for dense wireless LANs using potential game", *Elsevier Computer Networks*, vol. 167, Feb. 2020, https://doi.org/10.1016/j.comnet.2019.106991.

[31] M. Hashem Eiza, A. Raschellà, M. Mackay, Q. Shi, F. Bouhafs, "Towards Trusted and Accountable Win-Win SDWN Platform for Trading Wi-Fi Network Access", presented at the *1st Int. Workshop on SDWN, of the IEEE Consumer Comms & Networking Conf.* (*CCNC*), 8-11 January 2023, Las Vegas, NV, USA.

[32] A. Rahman, et al., "SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT", *IEEE Access*, vol. 9, pp. 28361-28376, Feb. 2021, 10.1109/ACCESS.2021.3058244.

[33] L. Xiao, Y. Gao, B. Liu, and T. Fang, "An Attack Detection and Defense Method for SDWN Oriented Blockchain Network", presented at the *Int. Conf. on Blockchain and Trustworthy Systems* (*BlockSys*), Dali, China, 6-7 Aug. 2020.

[34] T. T. T. Nguyen, G. Armitage, P. Branch, and S, Zander, "Timely and continuous machine-learning-based classification for interactive IP traffic," *IEEE/ACM Trans. on Networking*, vol. 20, no. 6, pp. 1880-1894, Dec. 2012, 10.1109/TNET.2012.2187305.

[35] L. Sequeira, J. L. de la Cruz, J. Saldana, J. Ruiz-Mas, J. Almodóvar, "Building a SDN Enterprise WLAN Based On Virtual APs", *IEEE Comm. Letters*, vol. 21, issue 2, pp 374-377, Nov. 2016, 10.1109/LCOMM.2016.2623602.

[36] L. Alevizos, V. T. Ta, and M. H. Eiza, "A Novel Efficient Dynamic Throttling Strategy for Blockchain-Based Intrusion Detection Systems in 6G-Enabled VSNs," *Sensors*, vol. 23, no. 18, pp. 8006, Sep. 2023, doi.org/10.3390/s23188006.

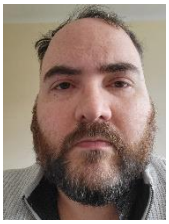
[37] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements, May 2021, https://doi.org/10.1109/IEEESTD.2021.9442429.
[38] F. Vergés, "MCS Table (Updated with 802.11ax Data Rates) – SemFio Networks". Accessed Oct. 2023. [Online]. Available: https://semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates/.
[39] G. Judd and P. Steenkiste, "Fixing 802.11 access point selection," *ACM SIGCOMM Computer Comm. Review*, vol. 32, no. 3, pp. 31, Jul. 2002, doi.org/10.1145/571697.571720.
[40] V. Namboodiri, L. Gao, "Energy-Efficient VoIP over Wireless LANs", *IEEE Trans. on Mobile Computing*, vol. 9, no. 4, pp. 566 – 581, Apr. 2010, 10.1109/TMC.2009.150.
[41] R. Liu, N. Choi, "A First Look at Wi-Fi 6 in Action: Throughput, Latency, Energy Efficiency, and Security", *ACM on Measurement and Analysis of Computing Systems*, vol. 7, no 1, pp. 1-25, Mar. 2023, doi.org/10.1145/3579451.

Alessandro Raschellà received the B.Sc. and M.Sc. degrees in Telecommunications Engineering from the University Mediterranea of Reggio Calabria (UNIRC), Italy in 2004 and 2007, respectively, and the Ph.D. degree in Wireless Communications from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain in 2015. From 2007 to 2009, he was a research assistant with UNIRC. He joined the School of Computer Science and Mathematics of Liverpool John Moores University (LJMU), UK in 2015, working as a Research Fellow and now he is a Senior Lecturer. His research interests include wireless networks optimization, software-defined networking, cognitive radio, IoT and heterogeneous networks.

Max Hashem Eiza is a Senior Lecturer in computer security at the School of Computer Science and Mathematics, LJMU. Max received his PhD in secure QoS routing in vehicular networks from Brunel University London in 2015. Max's research interests revolve around cybersecurity and data privacy issues in distributed and cyber-physical systems with the aim of developing novel schemes/protocols for various applications. During his career, Max published over 20 journal and conference papers.

Michael Mackay is a Reader in Wireless and Edge systems at Liverpool John Moores University and leads the Networking and Distributed systems research group. He received a BSc in Computer Science from Lancaster University in 2000 and a PhD from the same institution in 2005. He joined LJMU as a Senior Lecturer in 2010. His main research interests are in networking protocols, and his current focus is on Beyond 5G and 6G wireless systems. He is also widely published in a range of research areas focussed around networking technologies including IPv6, IP mobility, QoS and CDNs, Grid networking, and more recently Cloud and Edge Computing and the Internet of Things.

Qi Shi is a Professor in Computer Security and the Director of the PROTECT Research Centre in the Department of Computer Science at Liverpool John Moores University (LJMU) in the UK. He received his PhD in Computing from the Dalian University of Technology, P.R. China. He then worked as a Research Associate at the University of York in the UK. Qi then joined LJMU, working as a Lecturer and then a Reader before becoming a Professor. He has many years research experience in a number of areas, e.g. computer networks and security, secure service composition, privacy-preserving data aggregation, cryptography, computer forensics, formal security models and cloud security. He has published over 200 papers in international conference proceedings and journals, and served in a number of conference IPCs and journal editorial boards. He has also played a key role in many research and development projects related to his research topics.



Matthew Banton received B.Sc. in Cyber Security from Liverpool John Moores university in 2017, and completed his PhD in Deep Learning and Cyber Security in 2020. From 2020 to 2022 he was a post doctoral research fellow with the University of St Andrews, connected to the Horizon funded SERUMS project. From 2022-2023 he was a research fellow with the University of Stirling and joined the University of Sunderland as a Lecturer part way through 2023. His research interests include Cyber Security and anomaly detection in software defined networks as well as wireless networking.