IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 19, 2020, accepted December 30, 2020, date of publication January 5, 2021, date of current version January 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3049180

Attention to Wi-Fi Diversity: Resource Management in WLANs With Heterogeneous APs

JOSE SALDANA[1], (Senior Member, IEEE), JOSÉ RUIZ-MAS[1], JULIÁN FERNÁNDEZ-NAVAJAS[1], JOSÉ LUIS SALAZAR RIAÑO[1], JEAN-PHILIPPE JAVAUDIN[2], (Member, IEEE), JEAN-MICHEL BONNAMY[3], AND MAËL LE DIZES[3]

[1]I3A, University of Zaragoza, 50018 Zaragoza, Spain
[2]Orange Labs, 35510 Cesson-Sévigné, France
[3]Orange Labs, 22300 Lannion, France

Corresponding author: Jose Saldana (jsaldana@unizar.es)

This work was supported in part by the ORANGE as an External Research Contract "Wireless LAN based on use of Light Virtual WiFi Access Points", and in part by the European Social Fund and Government of Aragon, CeNIT Research Group, under Grant T31_20R.

ABSTRACT Many home networks integrate a small number (typically 2-4) of Wi-Fi Access Points (APs), with heterogeneous characteristics: different 802.11 variants, capabilities and security schemes. This paper proposes the consideration of these specific characteristics in order to improve the management of network resources. Three use cases are presented in order to showcase the potential benefits. By the use of a user-space AP, which works in coordination with a controller, the network is able to assign each connected station to the AP that best fits with its characteristics. The system also manages security, avoiding the need of adding specific elements for authentication, encryption or decryption. Extensions are proposed to an existing protocol that defines the communication between the AP and the controller, in order to communicate and store the specific characteristics of each AP and end device. This includes new association and handoff schemes that do not introduce any additional delay. The system has been implemented in a real environment, and a battery of tests has been run using three hardware platforms of different characteristics. The results show that handoffs between bands are possible, and estimate the processing delays, the Round-Trip Time and the handoff delay, which is small enough in order not to produce any significant disruption to the user (10-50 ms). Finally, the scenarios of interest have been replicated in a simulation environment, showing that significant benefits can be achieved if the specific characteristics of each AP and station are considered.

INDEX TERMS 802.11, seamless handoff, software defined wireless network, wireless LAN.

I. INTRODUCTION

In the last years, Wi-Fi (IEEE 802.11) has become the de-facto technology for achieving short- to medium-range connectivity of wireless devices: nowadays, every smart phone, tablet or laptop in a store does incorporate a Wi-Fi card. As a part of the same phenomenon, WLAN (Wireless Local Area Network) deployments including a set of Access Points (APs from now) managed by the same authority are usually deployed in scenarios such as airports, business centers, malls or even entire cities. These solutions, usually known as "Enterprise Wi-Fi," are often proprietary, closed and costly, which in most of the cases makes them unaffordable for many organizations.

Solutions including a number of APs are also considered as a means to provide full Wi-Fi coverage in the house, considering that the number of client devices (STAs[1] from now) in a home network is increasing exponentially: in addition to personal devices (laptops, desktops, tablets, mobile phones, smart watches, fitness trackers, etc.), many IoT devices may also be connected to the Wi-Fi network (home appliances, cameras, voice controllers, light bulbs, smart plugs, etc.).

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenzhou Tang.

[1]As usual in the literature, we will employ the term "STA" as a synonym of the user station, *i.e.* the terminal or the Wi-Fi client.

In fact, specific features included in 802.11ah and 802.11ax are aimed at addressing the range and power concerns of IoT. This trend is making security become a critical feature, since a breach may have disastrous consequences at home.

The Wi-Fi interfaces of all these devices have very heterogeneous characteristics: first, they may implement different versions of 802.11, from 11b to 11ac, or even 11ax, which also implies that they may operate in different bands (mainly 2.4 or 5 GHz). Furthermore, many different capabilities are optional in the latest versions of the standard (bandwidth from 20 to 160 MHz, Short / Long Guard Interval, number of spatial streams, supported rates / MCS, etc.).

Home users not only demand consistent performance in terms of throughput and connectivity, but also good Wi-Fi coverage throughout the house. Therefore, consumers often deploy more than one AP to provide that coverage at home. The network operator usually provides one device that includes a Wi-Fi AP, but in many cases the users add one (or more) extra APs to the home network, and this results in a heterogeneous deployment with 2-4 APs from different vendors. The result is usually a heterogeneous network with different 802.11 versions, capabilities, and frequency bands. As an example, it may happen that the network operator provides an 802.11n AP in 2.4 GHz, and the one(s) bought by the user are 802.11ac, working in the 5 GHz band. Finally, legacy devices including 802.11g or even 11b can still be found.

As far as security is concerned, heterogeneity is also observable: statistics[2] still report a significant amount of Wi-Fi routers implementing obsolete security schemes as WPA (5%) or WEP (5%). The take of WPA2 is 67%.

All in all, in these scenarios a set of heterogeneous APs has to bring service to a set of heterogeneous devices. This often results in a collection of unmanaged and isolated radio cells, some of them with advanced technologies, but with an overall poor (or null) capacity in terms of radio resource management and cell handover and roaming. Spectrum is used in a very inefficient way, and problems such as the ''sticky client'' [1] appear: if there is some coverage overlap, once a Wi-Fi device gets associated to an AP, it may remain connected to it, even if the user has moved to another place where there is a closer AP (or an AP with more advanced capabilities) that could give a better service. It may also happen that a multi-band device is connected to the most occupied band, thus contributing to the saturation.

Some solutions exist in the market that may overcome these problems: enterprise-grade coordination solutions provide many of these features [2]. They are designed for managing big networks in campus-like scenarios, but they are not suitable (nor affordable) for home networks. Another option is the so-called Wi-Fi *Mesh Networks*, in which a group of APs that communicate wirelessly to each other create a single Wi-Fi network that provides connectivity throughout the house. Many of the big vendors have developed these kinds of solutions, consisting of a set of identical APs that are usually sold together. The Wi-Fi Alliance has created the *EasyMesh* certification program (version 3.0 has been released recently) [3], which provides a standardized way for the coordination of different APs.

Some works can also be found in scientific literature [4]–[6], proposing open-source solutions that permit different resource management methods to be implemented by a controller. Many of them propose fast handoff schemes based on the use of virtual APs. Security is also addressed by some of them [7].

In this paper we focus on home scenarios with heterogeneous APs and STAs, and our main proposal is to gather their capabilities, and to consider them as input parameters for a better resource management (load balancing, mobility management) of the WLAN. It can be said that this is the most specific contribution of the paper: the attention paid to the heterogeneity of the APs and STAs, which permits new optimizations based on the assignment of each of the STAs to the AP that better fits its characteristics. The contributions will be explained in more detail in Section III, once the review of the state of the art has been presented in Section II.

The paper is mainly practical, and the proposal has been implemented and tested with real equipment, as an enhancement our previous work, presented in [1]. It is a significant step forward, as the system is now able to consider the heterogenous characteristics of the APs and STAs, ranging from 802.11g to 11n, 11ac and beyond. In addition, in order to complement the practical and qualitative approach, the scenarios of interest have been replicated in a simulation environment, which has allowed us to obtain some quantitative results that support our proposal: significant benefits can be achieved if this approach is followed and the specific characteristics of each AP are considered.

The software running in the AP has been built from scratch as a user-space standalone application. It does no longer make use of Click Modular Router, which did not allow to use 802.11n and subsequent versions. The software running in the controller is an update of the one used in our previous work.

In addition, WPA2-PSK (Wi-Fi Protected Access with Pre-Shared Key) security has been included in a way that does not require a specific central element in charge of it, as it happened in other proposals [6], [7]. Furthermore, the handoff scheme has been designed in a way that makes not necessary to perform a security re-association when the STA moves between APs. As a consequence, the handoff delay is the same reported in [1], in the order of some tens of milliseconds.

The next section summarizes the state of the art regarding Wi-Fi mobility standards, and commercial and research solutions, including how they address security. Next, a more detailed explaining of our proposal and the contribution is provided in Section III by means of three use cases. Section IV presents the architecture of the system. The tests carried out in a real setup are presented in Section V.

[2]Wigle statistics, see https://wigle.net/stats

Section VI details the simulation environment and the obtained results. The paper ends with the Conclusion.

II. STATE OF THE ART

In this section we will first provide a summary of the standards employed for Wi-Fi mobility. Then, a short summary of existing commercial solutions will be provided: the ones that follow the standards are able to manage mobility in certain ways that are fast, but require a re-association. On the other hand, alternative approaches, usually proposed by research projects, adopt different mechanisms and some of them permit seamless handoffs that are totally transparent for the STA. Finally, we will summarize the ways in which security has been included in these solutions.

Extensive surveys have been presented previously, for example in [1], and also in [7] and [8], so the reader can use these works if further information is needed.

A. STANDARDS FOR WIFI MOBILITY

802.11k [9] and 802.11r [10] were designed to create a more seamless roaming experience for wireless clients. They enable seamless Basic Service Set (BSS) transitions in WLAN environments, which is particularly useful for applications where long roaming times can result in a very noticeable impact on performance as *e.g.* VoIP, video conferencing, online games, etc. A long disruption in the connection may significantly harm the quality experienced by the user.

Both standards, which are usually implemented together, define measures to reduce the impact of roaming on the performance:

- 802.11k provides information to discover the best available AP, thus reducing the time required to roam. The current AP provides information regarding neighboring APs and their channels, so when the client is ready to roam, it has a better idea of where it will be roaming to.
- 802.11r uses Fast Basic Service Set Transition (FT) to allow encryption keys to be stored on all of the APs in a network. The initial handshake with the new AP occurs before the client roams to it, so the client does not need to perform the complete authentication process to a backend server.

In addition, 802.11v [11] is used by some solutions to allow STAs to exchange information about the network topology, including information about the radio environment.

CAPWAP [12] stands for Control and Provisioning of Wireless Access Points, and enables an Access Controller (AC) to manage a collection of wireless termination points (WTPs), which are called Access Points in many other places. The goals of CAPWAP are: *a*) to centralize the authentication and policy enforcement functions for a wireless network; *b*) to enable shifting of the higher-level protocol processing from the WTP; and *c*) to provide an extensible protocol that is not bound to a specific wireless technology: its generic encapsulation and transport mechanism, enables it to be applied to many AP types in the future.

B. PROPRIETARY AND COMMERCIAL SOLUTIONS

In this subsection we provide an overview of some of the proprietary solutions available in the market. As it will be seen, many of them are designed for managing big networks in campus-like scenarios. Some of them use the CAPWAP protocol, but many other features are proprietary thus reducing the interoperability.

As explained in [13], Miercom was engaged by Cisco Systems Inc. in May 2019, to conduct an independent competitive analysis of leading wireless infrastructure packages, *i.e.* wireless controllers and their corresponding APs. The solutions tested were from Cisco, Aruba, Ruckus and Huawei. It should be noted that, although this report was paid by Cisco Systems, Miercom is an independent company.

Four categories of tests were carried out, namely Availability, Security, Deployment and Programmability & Telemetry. Regrettably, no results about ''user mobility management'' were reported. For further details, the report itself can be obtained from [2]. These solutions can usually handle thousands of APs, and tens of thousands of wireless clients. Many of them support different types of roaming (intracontroller, intercontroller or intersubnet) by means of CAPWAP. Their cost is typically of some tens of thousands of dollars, which makes them unaffordable for home scenarios in which a reduced number of APs is managed by a single controller.

The Wi-Fi Alliance, through the Wi-Fi *EasyMesh* certification program [3], proposes a similar approach: a set of coordinated APs (called *agents)* connect between them using wired or wireless backhaul links, to create a single Wi-Fi network. They allow the mobility of STAs that implement 802.11v. This permits the inclusion of self-organizing, self-optimizing and load balancing features, since the network can react according to the number of STAs and the wireless conditions. Certified devices from multiple vendors can interact.

Extensive reviews of Wi-Fi *mesh network*, solutions have been carried out [14], [15]. Vendors typically sell together 2 or 3 identical APs (with the possibility of adding more), which cost may range between $100 and $400. These vendors usually provide the surface where they can provide coverage, typically between 1,500 and 4,500 square feet (139 to 418 square meters), which corresponds to the size of a house.

Although *EasyMesh* has many features in common with the solution proposed in the present paper, the approach is quite different, as our solution follows a Software Defined Wireless Network (SDWN) approach. It brings programmability through the use of a central controller which obtains a global view of the network, and offers a northbound interface that exposes primitives, allowing the network administrator to develop resource management solutions [4]. In *EasyMesh*, handoffs follow the standard procedures defined in the 802.11 amendments, and they do not make use of solutions such as Virtual APs that allow very fast handoffs (we will see them in detail in the next subsection).

C. OPEN RESEARCH SOLUTIONS ALLOWING FAST HANDOFFS

The Lightweight Virtual AP (LVAP) is the abstraction that enables seamless handovers in this scenario: when a STA associates for the first time, the controller creates an LVAP for it, which is assigned to the physical AP that first detected it. The LVAP is a tuple including some parameters that will only be used to communicate with the STA. A physical AP hosts a number of LVAPs (one per STA), and sends the frames with the source MAC (Media Access Control) associated to each STA. Therefore, the AP will send frames with different source MAC addresses.

The LVAP can be moved between physical APs, corresponding to the movement of the STA, and also because of resource management decisions. It can be said that the LVAP *travels* with its STA. From the point of view of the STA, a single AP is always *seen* in spite of moving, which avoids the need to use any mechanism for associating to a new AP (as long as the network is able to provide good coverage).

A distributed solution using LVAPs was introduced back in 2011 [16], where a protocol for the direct exchange of information between APs was also proposed. One limitation of this proposal is that, due to the absence of a central controller, each AP has to build a list of neighboring APs by itself.

An LVAP-based solution including a central controller and a set of low-cost OpenWrt APs was presented in [17], using two southbound protocols that facilitate communication between the controller and the APs: OpenFlow, in charge of controlling the internal switch of the AP, and a new protocol called Odin that takes care of the wireless part. The solution was extended to support more than a channel in [18], and later in [1]. It was also extended in [7], where wireless management was incorporated to OpenFlow protocol.

In [6] a scheme called BIGAP was presented, which is based on the use of a mechanism below the MAC layer for handover, exploiting the Dynamic Frequency Selection (DFS) capability in 802.11. It does not require any modifications to the STAs, but requires the support of IEEE 802.11h [19].

Aeroflux [20] was also built upon the Odin framework, proposing a two-layer architecture on the control plane: an element that controls frequent events near the point where they occur, and another one in charge of general events. It makes use of the extended OpenFlow Wireless Datapath Transmission rules (WDTX) which define per-flow 802.11 properties.

In [5], EmPOWER was proposed, integrating different Radio Access Technologies (RAT). A set of programming abstractions was proposed so as to model important aspects of wireless networks. It was also used in [21], proposing a joint algorithm for mobility management and rate adaptation for multicast communications.

There is a commercial solution that makes use of a similar concept: Accton [22] has introduced the concept of Personal Virtual Access Point (PVAP). It is located in a control element, so the Wi-Fi network is transformed into an SDN-like structure without changing any hardware or adding an OpenFlow controller. The PVAP moves between the APs as the client station moves across the network. Accton reports handover times of around 150 ms.

Finally, a detailed review including implementation details of SDN for WLANs (SDWN) solutions, along with the most relevant recent research efforts and contributions can be found in [8]. In the survey, the authors discuss the benefits that WLANs can achieve by adopting SDN, and they provide a table with the main characteristics of each experimental SDWN setup.

D. SECURITY IN COORDINATED WLANs

In [7] security was added in a LVAP scheme based in Odin, by means of the separation of encryption and decryption functions from the AP, *i.e.* the authentication was performed by a RADIUS (Remote Authentication Dial-In User Service) server, so an embedded encryption component for centralized end-to-end data encryption was employed within the SDN network. Another element called EnDeC (Encryption and Decryption Component), in charge of encryption and decryption of all the traffic to/from the Internet, offloads security tasks from the APs.

One Big AP [6] also included security by means of several encryption / decryption appliances deployed around the wired network.

Proprietary coordinated solutions include security, managed in a central way: CAPWAP is employed as a way to enforce authentication and policies in the network. Encrypted CAPWAP mobility tunnels are also employed for roaming and the security context of each STA is centrally stored.

In the present paper we have opted for managing security on each AP. The main reason is that it is the most usual way in which authentication and ciphering is performed in our main target scenario: home networks. The addition of new components in these networks has to be very limited, considering that operators usually provide the equipment when the user contracts the service. Therefore, the operators usually make large orders from a single supplier, in order to reduce the costs. In our case, we already have the controller as an additional element. As we will see, it can run in a single-board computer (a Raspberry Pi in our tests), and in the future it could be integrated into the router provided by the telecom operator. However, if we loaded it with more functionalities, this would be impossible. State-of-the-art APs are able to encrypt / decrypt their traffic, so we see no reason for moving this function to another component, which would be a less scalable solution.

E. MANAGING HETEROGENEOUS 802.11 CLIENTS

Some papers have specifically addressed the problem of associating heterogeneous clients to APs. For example, back in 2012, the AP association for 802.11n with heterogeneous clients (802.11a/b/g/n) was explored in [23], [24].

The proposed algorithms were able to significantly improve the overall throughput.

In [25], the ability of dual band access points (APs) to support heterogeneous client adapters and applications was studied. After real experimentation, the authors found that dual band routers can be useful as a way to reduce the negative effects of the heterogeneity in the network adapters of the clients.

The problem of channel assignment in 802.11n WLANs with heterogeneous clients was studied in [26], considering that channel assignment becomes more complex in 802.11n WLANs, as the standard allowed two adjacent, non-overlapping 20 MHz channels to be combined.

All these studies have addressed the heterogeneity of 802.11 STAs. However, to the best of our knowledge, none of them has specifically put the focus on the heterogeneity of APs. Therefore, it can be said that the specific contribution of the present paper is the proposal of mechanisms that allow the network to jointly consider AP's and STA's characteristics, as a way to improve the resource management. It should be noted that, even though big enterprise network deployments are usually built from identical APs, many households throughout the world have small networks (2-4 APs) with heterogeneous hardware, which may benefit from the improvements proposed in the present study.

III. MANAGEMENT OF HETEROGENEOUS APs

If the information about the capabilities of each STA and AP can be transmitted to the controller and stored there, it can be useful in order to make smarter decisions about which STA can be associated to each AP. In this section we present three use cases: two of them showcase the potential advantages that can be provided by the consideration of the heterogeneous characteristics of the APs and STAs, and another one illustrates the advantages for security.

A. USE CASE 1: HANDOFF CAUSED BY USER MOBILITY

In this case, we have a STA connected to an AP (AP1) with certain capabilities (cap_1). For example, in Fig. 1 a), we see that an 802.11ac STA able to use 160 MHz channels, is first connected to an AP that only supports 80 MHz channels (cap_1).

In regular Wi-Fi, if the STA moves and re-associates, it will use the capabilities of AP2 automatically.

However, if a solution implementing fast handoffs [16]–[18] is employed, when the STA moves, a handoff will be ordered by the mobility management application running in the controller, and the STA will keep on using an 80 MHz channel, even when connected to the destination AP (AP2) with better capabilities (cap_2), 160 MHz in this case.

- In case cap_2 are better than cap_1, as the STA has initially been associated to AP1, it will keep on using cap_1, even if its capabilities match cap_2, because the handoff is unnoticeable to it (a virtual AP is used). As a result, it may happen that the STA keeps on using cap_1, even when associated with AP2.

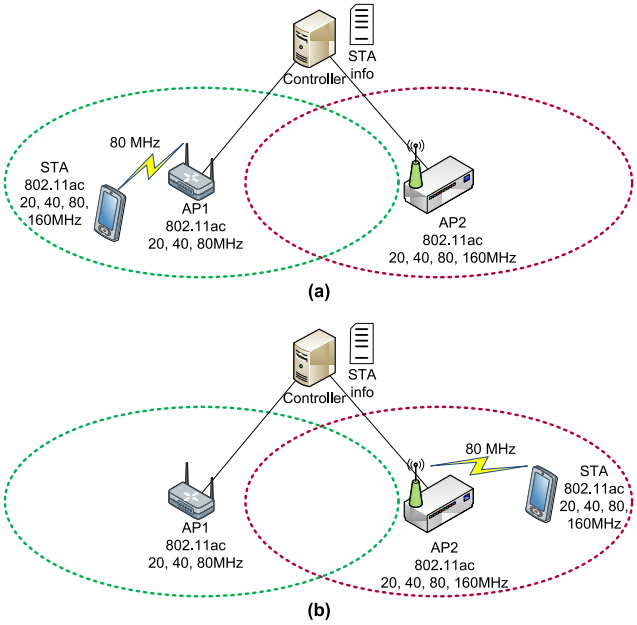

FIGURE 1. Use case 1: A STA moves from an AP to another one with different characteristics: a) initial situation; b) final situation.

- However, if the STA has moved from AP2 to AP1, it may have problems (AP1 does not implement the required capabilities) and even get disconnected when handed off by the controller. If it got disconnected, it may associate again with AP1, but then the handoff would not be seamless at all.

If the controller was aware of the capabilities of each AP and STA, it would know that the capabilities of the STA are similar to cap_2, so it would be able to solve these potential problems making the corresponding adjustments. For that aim, the Extended Channel Switch Announcement element can be used. This element can be included by the AP in beacon and *Probe Response* frames. It indicates the STA that it is moving to a new channel and/or changing operating channel width.

One interesting consequence of this use case is that the solutions proposed in the literature, able to provide fast handoffs by means of lightweight virtual APs [16]–[18], will fail if the APs do not have the very same characteristics (802.11 version, capabilities, etc.): when a STA is handed off, it may get disconnected if the destination AP does not implement any of the capabilities of the source AP, provided that the STA was using it.

B. USE CASE 2: SMARTER LOAD BALANCING IN THE CONTROLLER INCLUDING HANDOFF BETWEEN BANDS

In this case (see Fig. 2), we have 2 APs (one implements 11n in 2.4 GHz and the other one is dual: it includes 11n in 2.4 GHz and 11ac in 5 GHz) and 2 STAs (one implements 11n in 2.4 GHz and the other one is dual: 11n in 2.4 GHz and 11ac in 5 GHz). The controller implements a simple load balancing algorithm that tries to keep a homogeneous

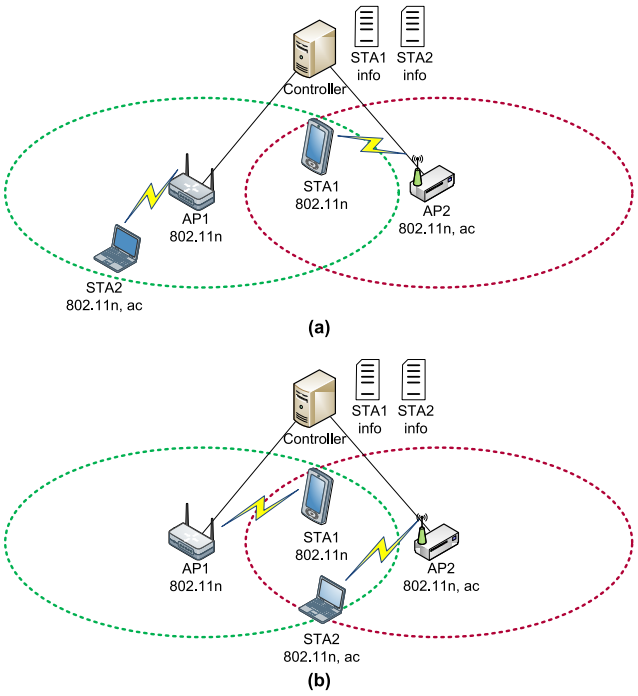

FIGURE 2. Use case 2: Optimal load balancing using the info about the capabilities of each STA: a) initial situation; b) final situation.

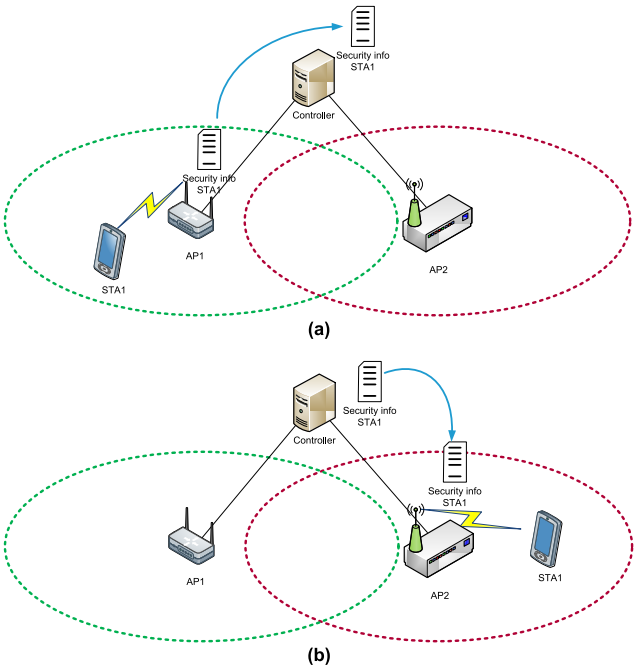

FIGURE 3. Exchange of security information: a) STA1 associates to AP1, and the security information is sent to the controller; b) the information is transmitted by the controller to AP2 during a handoff.

number of STAs per AP (see *e.g.* the load balancing algorithm presented in [17]).

At the beginning (Fig. 2 a) STA1 (802.11n, 2.4 GHz) is in the zone where the coverage of both APs overlaps, and STA2 (802.11n, 11ac) only has coverage from AP1 (802.11n, 2.4 GHz). As a consequence, the load balancing algorithm will associate STA2 to AP1, and STA1 to AP2, as it is the only possibility of having one STA per AP.

If STA2 moves to the overlapping zone (Fig. 2 b), the load balancing algorithm has two options: if it is not aware of the capabilities of each STA, it may do nothing and keep STA1 with AP2 and STA2 with AP1. However, if the controller has the information about the capabilities, a smarter decision will be to assign STA1 to AP1 (both using 802.11n in 2.4 GHz) and STA2 to AP2 (both using 802.11ac in 5 GHz).

In regular Wi-Fi, a re-association would be required. In solutions based on SDWN, the re-association would require a notification to STA2 in order to switch to the new channel (in another band), and to notify the new capabilities using the Extended Channel Switch Announcement.

C. USE CASE 3: HANDOFF WITH SECURITY

Since we have the possibility of storing information about each STA in the controller, a new possibility opens: to include the information associated to the security association, as a part of the stored information. If this is achieved, a STA that successfully completes the 4-way handshake (the security association used in most IEEE 802.11 networks), can be handed off to another AP without performing a new security association, since the associated security information (keys, serial numbers, cipher suites included, etc.) can be sent by the controller to the destination AP during a handoff (see Fig. 3).

And another consideration is that heterogeneity may also appear regarding security features: each AP includes its security features in the RSN (Robust Security Network) Information Element of the *Probe Response*, and the STA includes them in the *Association Request*. Although in the present paper we have always used the same value for this Information Element, it would be possible that different APs implement *e.g.* different cipher suites, and this could also be considered as a relevant input for load balancing.

D. EXAMPLE OF THE ACHIEVABLE BENEFITS

In this subsection we present an example that illustrates the benefits of use case 1. For that aim, a network simulation tool (ns3) has been employed. The parameters of the simulation are detailed in Section VI, and also in the Appendix.

A scenario including two APs with different characteristics has been built: the first AP runs 802.11n, and the second one is a dual-band AP with 802.11n, and 802.11ac (with a channel bandwidth of 40 MHz). A dual-band STAs moves linearly from the first to the second AP, while performing a TCP download.

Two situations can be compared: if the STA stays in the 2.4 GHz band (Fig. 4), its throughput will be limited to the one provided by 802.11n. However, if the STA is able to switch to the 5 GHz band (802.11ac), the achievable throughput will be much higher (see Fig. 5). Another interesting question can be observed from the graphs: 802.11n in 2.4 GHz has a wider coverage than 802.11ac in 5 GHz, due to the different fading level.

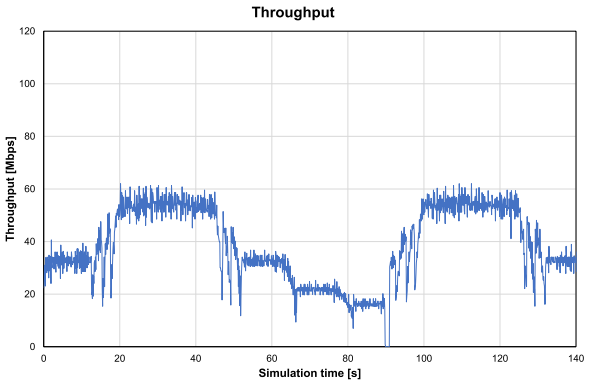

FIGURE 4. Throughput achieved by the STA when two 802.11n APs are present.

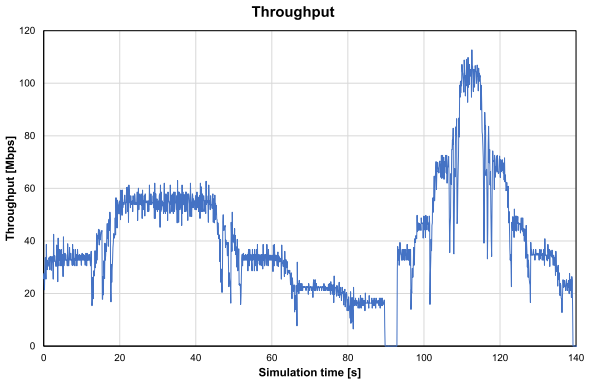

FIGURE 5. Throughput achieved by the dual STA when an 802.11n and an 802.11ac APs are present.

More simulation results will be presented in Section VI, using an algorithm that tries to use the best suited AP for each STA, considering their characteristics. It should be noted that the ns3 simulation does not implement fast handoffs.

E. OVERALL ADVANTAGES AND CONTRIBUTION

Once the use cases have been explained, it can be observed that, if the controller keeps the information about the *bare* capabilities of each STA (in spite of the AP where it is connected), it can run better algorithms, resulting in a better management of the resources.

This can be done if the capabilities' info included by the STA in its initial *Probe Request* is first stored by the AP, and then forwarded to the controller. It should be noted that the capabilities sent in the *Probe Request* can be different from those in the *Association Request*, because the STA may remove those not supported by the AP.

The same happens with the security features supported by each STA: if they are sent to the controller, they can later be used for running smarter algorithms.

Once a detailed view of the potential advantages of this approach has been provided, we are in the position to summarize the main contributions of this paper:

1) The consideration of AP's and STA's capabilities as input parameters for a better resource management (mobility management, load balancing) of WLANs including heterogeneous APs. This requires the system to store and make use of the information sent by STAs in their first *Probe Request* message.
2) The addition of WPA2 PSK security to the same solution, by the inclusion of the security information as an extension of the LVAP, *i.e.* the security information becomes a part of the LVAP and *travels* with the STA. avoiding the need of using a RADIUS server.
3) The design of a handoff scheme that *a*) keeps track of the capabilities of each AP and STA; *b*) can be performed between the 2.4 and 5 GHz bands; and *c*) maintains the security association. From the point of view of the STA, the handoff is just seen as a channel switch of the AP where it is associated. Therefore, there is no need to perform a new 4-way handshake.
4) The implementation of a proof-of-concept system, which includes the previous proposals. It has been implemented as an enhancement to an existing solution based on Lightweight Virtual APs. The proof-of-concept has been used in order to carry different tests with real hardware, including three different chipsets working in the 2.4 and the 5 GHz bands. The tests run show that secure handoffs between different bands are possible and fast.

The main approach followed in this paper is practical and implementation-oriented, as required to confirm that our proposals are possible in real scenarios. However, in order to complement the practical and qualitative approach, a ns3 simulation environment has been employed (see Section VI) to mimic the scenarios of interest, which has allowed us to showcase and quantify the benefits that can be achieved if the specific characteristics of each AP are considered. Although this is not the main objective of the paper, it can be considered as an additional contribution.

IV. ARCHITECTURE OF THE SYSTEM

This section provides a detailed description of the system architecture. It has been implemented as an evolution of the system initially developed in [17] (with all the APs in a single channel), and later extended during the H2020 Wi-5 project [4] to support multi-channel handoffs [18].

A. REQUIREMENTS

The next 802.11 features should be supported by the system:

- Wi-Fi variants:
  - 2.4 GHz: 802.11g, 802.11n
  - 5 GHz: 802.11a, 802.11ac.
- Seamless handoffs between Wi-Fi bands (2.4 and 5 GHz must be possible.
- Capabilities (if supported by the wireless card):
  - Short and long Guard Interval.
  - 20, 40, 80, 160 MHz channels.
  - 1 to 4 spatial streams.

- Any rate or MCS that is supported by the wireless card.
- Data and QoS frames.

And these were the security requirements to be supported by the system:

- The need of any security server should be avoided, *i.e.* the security association must be established between the STA and the first physical AP to which it associates. This happens through the 4-way handshake [27].
- WPA2-PSK should be supported. It uses Counter Mode CBC-MAC Protocol (CCMP) for ciphering, which is the mechanism that substituted Temporal Key Integrity Protocol (TKIP) as the standard for WPA2.
- The handoff between physical APs should not require any security re-association, *i.e.* it should be transparent to the STA, in the same way the handoff is already transparent to it.

Finally, the system should be able to run it in low-cost elements, as the ones that can be found in home networks. As explained in Section II, this is because we are targeting home networks, in which the inclusion of expensive elements is not possible because of the current business model followed by the operators.

B. ENHANCED ARCHITECTURE

A preliminary SDWN architecture, presented in [1], provided some features as LVAPs, multi-channel handoffs and the possibility of running different applications for resource management. However, it presented some limitations, being the main one that it was limited to 802.11g, and it also assumed that all the APs had exactly the same characteristics.

The enhanced architecture is able to consider the different features that are being included in the last versions of 802.11. In addition, these features are treated individually, so the system will look for the best achievable results considering the specific capabilities of each of its APs and connected STAs.

The architecture includes a controller and a number of APs, also known as *agents* (see Fig. 6). Following the SDN approach, *control* and *data* planes are separated. In the next subsections we will explain each of the elements in detail.

1) LIGHTWEIGHT VIRTUAL AP (LVAP)

In order to enable fast and seamless handoffs, our solution makes use of LVAPs, which have been explained in Section II. In our case, the LVAP structure has been extended. Initially, it was a tuple including four fields, namely the real MAC of the STA, its IP address, and also a MAC and an SSID that will only be used to communicate with the STA.

The new fields of the extended LVAP structure are also sent to the destination AP whenever a handover is performed. These are the new parameters of the LVAP:

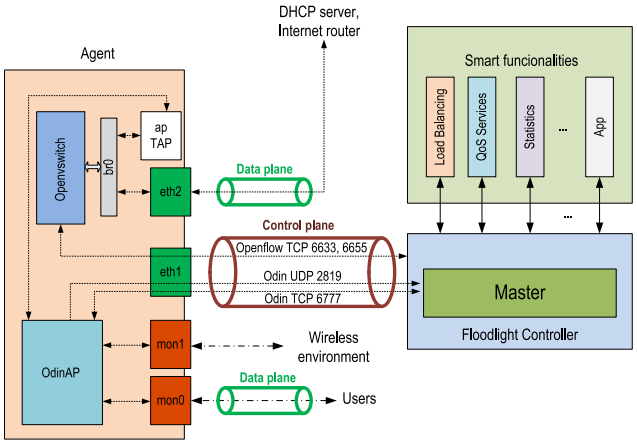

FIGURE 6. Scheme of the system, including one AP and the controller.

- Capabilities of the STA, including HT (802.11n) and VHT (802.11ax),[3] sent by the STA in both the *Probe Request* and the *Association Request*.
- Security information, including the three keys, the RSN Information Element, and the Tx and Rx packet numbers used by the CCMP ciphering mechanism.
- Status, *i.e.* the *Sequence Number* of the last frame sent / received. This allows the destination AP to maintain the sequence that was being sent by the origin AP.

A more detailed version of the extended structure is presented in Fig. 7. Note that the legacy structure just included the *Key* and the *main* parameters.

2) CONTROLLER

The controller (developed in Java) is built on top of the Floodlight OpenFlow controller,[4] and the resource management algorithms (also known as *applications* or *smart functionalities)* make use of an API provided by it. A number of APs are managed by a controller. Each of them runs *Open vSwitch*[5] that makes its internal switch behave as an OpenFlow switch.

The controller has been extended by the addition of the new parameters of the LVAP to the structure that stores it. In addition, some of the messages have been modified in order to send more information during a handoff (this will be explained in detail in the next subsections).

3) AGENT

As it happened in [1], an extra wireless interface is added to each of the APs for monitoring purposes. This avoids the need to periodically use the main interface for that aim, which would interrupt the service to the associated STAs.

The previous version made use of Click Modular Router, that allowed the implementation of the main module of the

[3]The meaning of 'HT' is *High Throughput*, which refers to the capabilities included in 802.11n. In a similar way, 'VHT' means *Very High Throughput*, *i.e.* the capabilities of 802.11ac.

[4]Floodlight SDN Controller, http://www.projectfloodlight.org/floodlight

[5]Open vSwitch, http://openvswitch.org

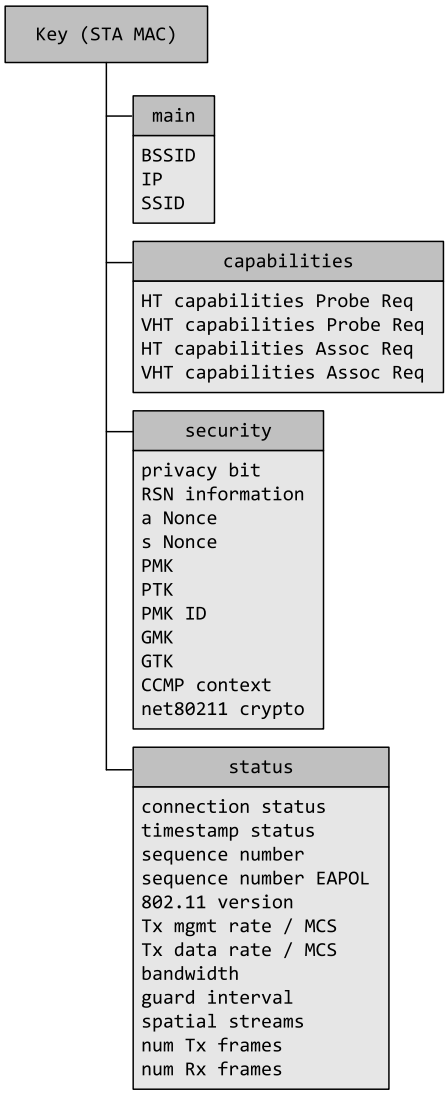

FIGURE 7. Structure of the LVAP.

agent. In the current version, the Click module has been substituted by a standalone user-space application called *OdinAP,* programmed in C. The rest of the elements of the system have been maintained, including the ports for communicating with the controller, the wireless interfaces, etc. The main reason for avoiding Click Modular Router is that it has its own 802.11 elements, which do not incorporate the latest capabilities of the standard.

The developed application includes five debug levels (in addition to level *0*, *i.e.* no debug). It allows the dump of the frames. In the current version only IPv4 is supported.

4) ODIN PROTOCOL

In addition to OpenFlow, the Odin protocol is employed between the controller and each of the APs. The protocol was first defined in [17]. It is in charge of communicating all the management information between the controller and the AP. It includes a TCP and a UDP connection. The former is employed in order to transmit information regarding associations, etc. The latter transmits other information as periodic reports, and other notifications.

As we will see in the next subsection, Odin has been enhanced by the inclusion of new messages, and also by the addition of new parameters to already existing ones.

C. EXTENSIONS ADDED

This subsection summarizes the extensions that have been added, with respect to the system presented in [1].

First, the use of a standalone application, instead of Click Modular Router, has allowed us to directly use Radiotap,[6] the de-facto standard for wireless injection and reception in 802.11. The developer has to define the Radiotap structure preceding the data itself. This structure defines all the radio characteristics of the frame to be injected. Once passed to the driver, it reads them and sends the frame to the air. The same happens when a frame arrives: the driver fills a Radiotap structure where the parameters of the received frame can be found. Currently, Radiotap supports all the 802.11n and 11ac features, and it is in constant evolution to support new ones (*e.g.* those included in 802.11ax).

As a consequence, the enhanced system is not limited to 802.11g (as it happened in [1]), but we can now use 802.11n (in addition to 11g) in the 2.4 GHz band, and also and 802.11ac (and 11a) in the 5 GHz band.

The extensions added to the system permit the exchange of the capabilities and the security information. For that aim, new messages have been defined, and new parameters have been added to already existing ones. We will present them in the next subsections, by means of a detailed explaining the new association and handoff schemes.

1) ASSOCIATION PROCESS

The association process is shown in Fig. 8 (the new features added are in blue letters). The process is started by the sending of a *Probe Request* by the STA. The AP provisionally stores the capabilities announced in that message, and sends a *Probe Request Notification* message to the controller. The controller creates a new LVAP for that STA, and sends an *Add LVAP* message to the AP. The value of the capabilities, security and status are null in this *Add LVAP* message.

The arrival of this message to the AP makes it add a new register in the STA *mapping table, i.e.* the table that stores all the associated STAs, and sends the *Probe Response* to the STA. The process is continued by the exchange of the *Authentication Request* and *Response,* and the *Association Request* and *Response.* If security is active, the *Association Request* will include the RSN Information Element of the STA.

Once the *Association Response* has been sent, the AP also sends to the controller a *Complete Association Notification* message, in which the HT and VHT capabilities of the associated STA are included. The controller stores them in the corresponding register of its table of LVAPs. Note that storing

[6]Radiotap, see https://www.radiotap.org/

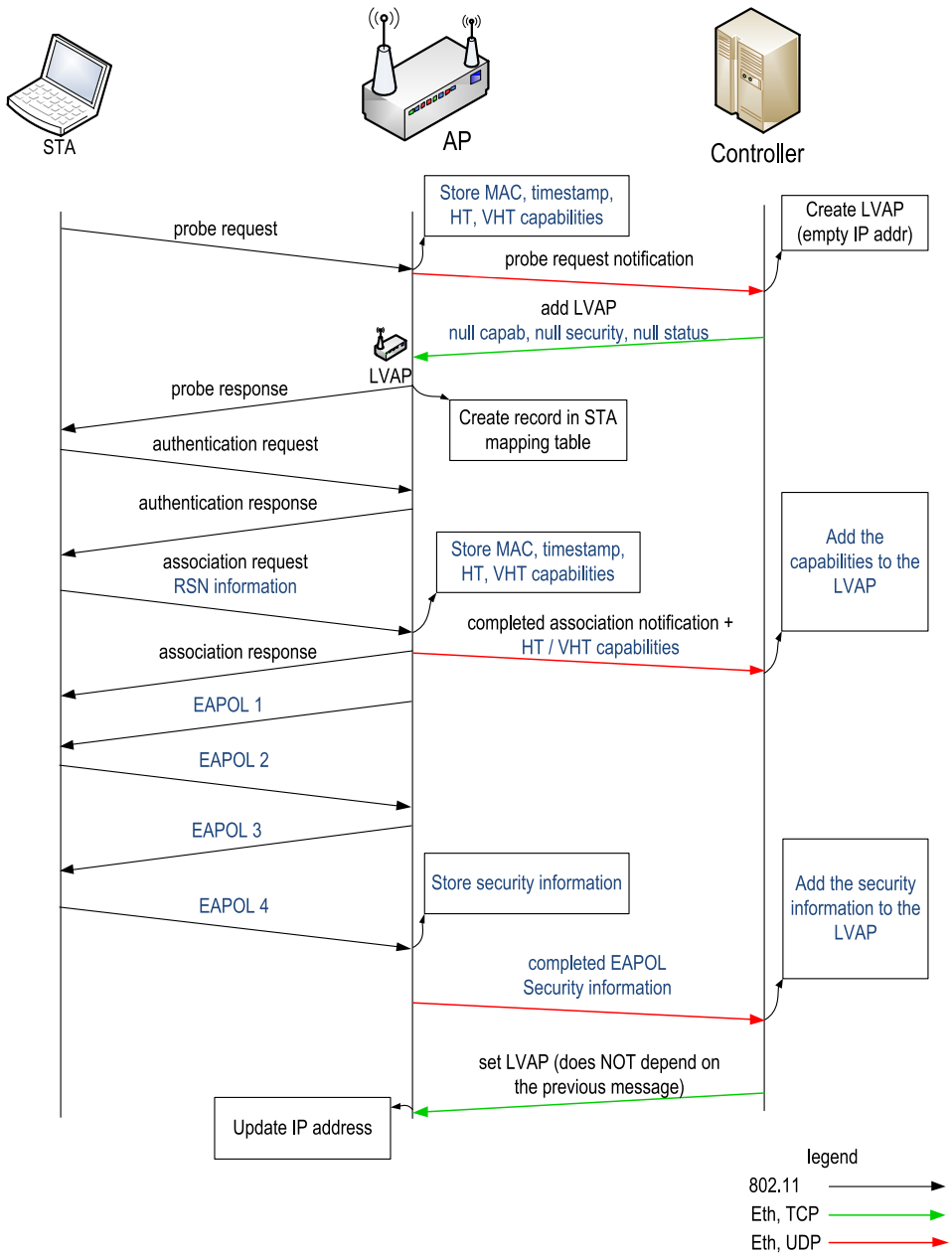

FIGURE 8. LVAP association process with security and capabilities exchange.

the capabilities set by the STA in the *Probe Request* is useful: if a STA has better capabilities than the AP, the capabilities in the *Association Request* will be *lower* than those in the *Probe Request*. In the case of having a heterogeneous network with different APs, having this information about the real capabilities of the STA may be interesting, since it can be used in order to match the STA with a better AP also present in the network.

If security is active, the 4-way handshake takes place, which consists of four EAPOL (Extensible Authentication Protocol over LAN, also known as 802.1X [28]) frames in which the security information required for the secure generation of the keys is exchanged. If the handshake ends successfully, then the security information is stored in the AP, and forwarded to the controller in a new message called *completed EAPOL*. It includes:

- KCK: EAPOL Key Confirmation Key.
- KEK: EAPOL Key Encryption Key.
- TK: Temporal Key used for frame encryption / decryption.
- RSN Information Element of the STA.

The controller stores this information in its table of LVAPs.

Finally, once an IP address has been obtained by the STA from the DHCP server, the controller reports it to the AP.

As a result of this process, the HT and VHT information, jointly with the security keys, is stored in the AP, but also in

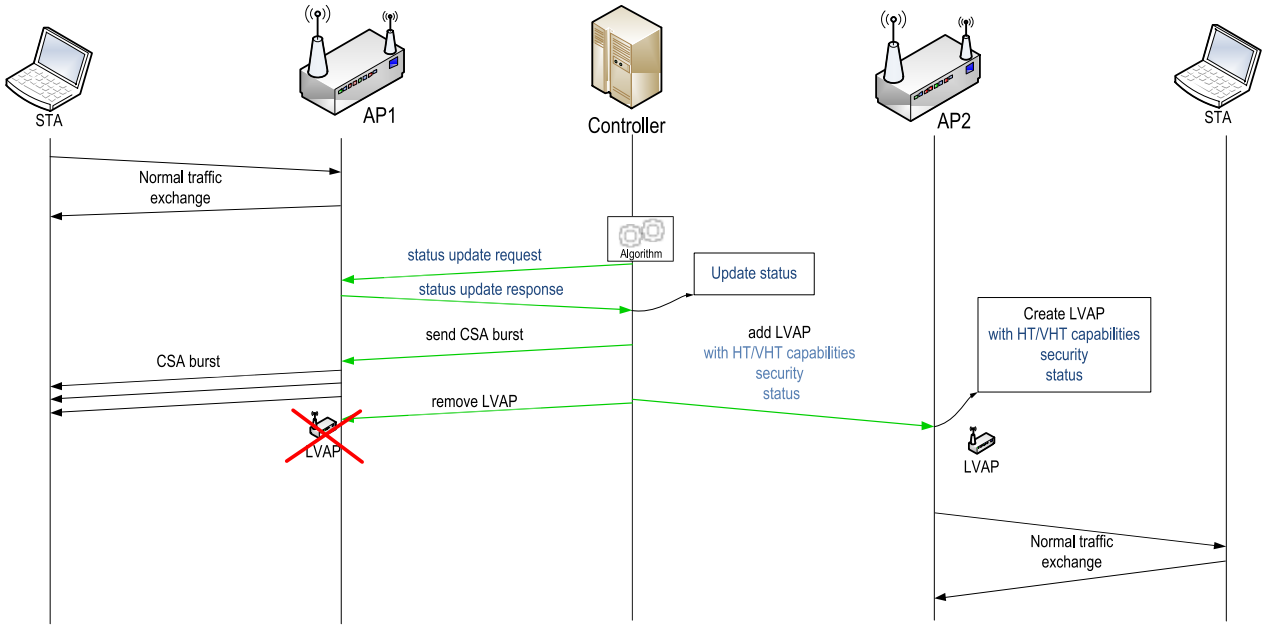

FIGURE 9. Handoff process with capabilities and security exchange.

the controller, which can use it to run resource management algorithms.

2) HANDOFF PROCESS

The handoff process with capabilities and security exchange is illustrated in Fig. 9. As it can be observed, it makes use of the new *Status Update* messages, and also of the extended *Add LVAP* one, with a significant number of new parameters, as we will next see.

First, the STA is associated to AP1 and is exchanging frames normally. In a certain moment, the algorithm running in the controller decides that this STA must be handed off to AP2 (because of mobility or maybe because of a load balancing decision).

Before starting the handoff itself, the controller requests an update of the status of the STA from AP1. The *Status Update Response* includes information about the value of three counters: the *Sequence Number* (a field of the 802.11 header) of the last frame sent by AP1; and the values of the two counters used by CCMP cipher: CCMP Tx and CCMP Rx. This information will later be sent to AP2, which will be able to send (and receive) its frames using the correct values of the counters.

One remark should be done with respect to the status: a requirement of CCMP is that the value of the CCMP Tx and Rx increase monotonically. However, it could happen that some frames are sent by the STA to the AP, in the time period between the arrival of the *Status Update Request* and the handoff itself (at the end of the CSA burst). Therefore, in order to avoid the sending of a frame with a decreasing value of CCMP Tx, a fixed value (empirically set as 100) is added by the controller, so the value of CCMP Tx sent to AP2 is higher than the one received from AP1.

As it was done in [18], a burst of beacons with the CSA element (or the Extended CSA if accommodation of new capabilities is required) is then sent to the STA which will move to the new channel (that of AP2) afterwards. In that moment, the controller makes two simultaneous actions (using different threads): it removes the LVAP from AP1 and sends an *Add LVAP* message to AP2. In this case, the *Add LVAP* message includes the value of the capabilities, security and the status of the STA (see Appendix, A for a more detailed explanation of the message).

Finally, it should be noted that the only added messages, with respect to the previous work [1], are the *Status Update Request* and *Response*. As they happen before the starting of the handoff itself, they do not add new delays to the handoff. Therefore, the delays reported in that work are also valid for this handoff scheme (apart from some processing delays required for storing the new parameters included in the enhanced *Add LVAP* message, which can be considered as negligible if compared to the time required by the wireless card to switch its channel).

3) OBTENTION OF THE CHARACTERISTICS OF THE AP

Another additional feature that has been added is a mechanism that the controller uses in order to request the characteristics of each AP. This is important, since detailed information is needed in the controller in order to run resource management algorithms that use as an input the heterogeneous characteristics of the APs. It should be noted that the capabilities of the STAs are also available for the controller, since they are sent during the association process (in the *Completed Association Notification*), as we have just explained.

TABLE 1. Extensions added to odin protocol.

Message	Arguments	Description
Add LVAP (TCP)	MAC and IP of the STA MAC and SSID of the LVAP HT params in *Probe Req* HT params in *Assoc Req* VHT params in *Probe Req* VHT params in *Assoc Req* KCK, KEK, TK RSN Information Element *Sequence Number* CCMP Tx, CCMP Rx	The controller tells the agent to add a new LVAP and (optionally) sends its LVAP, capabilities, security information and status
Completed Association Notification (UDP)	MAC of the STA HT params in *Probe Req* HT params in *Assoc Req* VHT params in *Probe Req* VHT params in *Assoc Req*	The AP tells the controller that the association has been completed, and transmits the HT and VHT parameters of the STA
Completed EAPOL (UDP)	MAC of the STA KCK, KEK, TK RSN Information Element	The AP tells the controller that the 4-way handshake has been completed, and transmits the generated keys to be used with that STA.
Status Update Request (TCP)	MAC of the STA	The controller requests the status of a STA
Status Update Response (TCP)	MAC of the STA Sequence Number CCMP Tx, CCMP Rx	The AP tells the controller the current status of the STA

A table with the original messages can be found in [29], §5.2. We include in the Appendix, B some examples of the messages.

These are the characteristics that the controller gathers from each AP:

- Version of 802.11.
- HT capabilities info.
- VHT capabilities info.

4) SUMMARY OF THE IMPROVEMENTS ADDED TO ODIN PROTOCOL

As a summary we provide Table 1, in which the extensions to the Odin protocol are detailed.

5) SECURITY CONSIDERATION

It should be noted that security information (including temporal keys) is exchanged between the controller and the APs. This increases the attack surface, since the wired connections between the controller and the APs must also be secured now, and the same happens with the database of the controller. We consider that the protection of the information in the wired network is out of the scope of the present work, assuming that the exchange can be protected by means of proper protocols (*e.g.* TLS for TCP flows and DTLS for UDP ones), and the database can be protected by normal procedures.

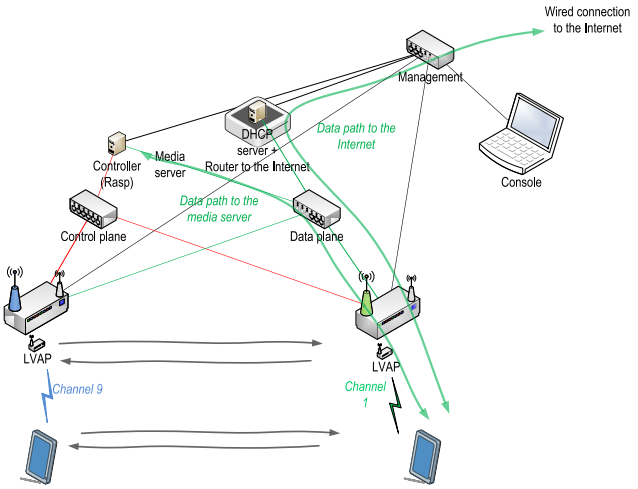

FIGURE 10. Lab setup used for the tests.

V. TESTS IN A REAL SETUP

This section details a battery of tests that have been performed with real equipment, which show the implementation details of the proposed solutions.

A. TESTBED SETUP

The setup (Fig. 10) for testing the enhanced system includes different elements: a number of APs (mini PCs, single board computers and commodity APs), three switches (control plane, data plane, management), a controller (Raspberry Pi), a machine that acts as DHCP server and router (it is a virtual machine running inside an Intel Nuc), and a console. All the elements are connected to the management network, where the traffic can be monitored.

1) EQUIPMENT USED AS APS

Three kinds of hardware platforms with very different capabilities have been used as APs (see Fig. 11):

- Mini PCs (ASRock Core 100HT) with Debian (kernel 4.19.28). The processor is an Intel Core i3 370M. They have 4GB of RAM. The internal wireless card is a Qualcomm Atheros AR9287 802.11n.
- Single board computers: PC Engines APU 2d4. The CPU is an AMD Embedded G series GX-412TC, 1 GHz quad Jaguar core with 64 bit and AES-NI support. 4 GB of RAM. The internal wireless card is a WLE600VX–COMPEX 802.11ac with chipset Qualcomm Atheros QCA9882.
- Commodity APs: Netgear R6100 with OpenWrt 15.05, commodity Dual Band WiFi routers with Atheros AR9344, 560 MHz CP, 128 MB RAM. They have an Atheros QCA9882-2R4E, 802.11b/g/n in 2.4GHz, and 802.11a/n/ac in 5GHz.

A TP-LINK TL-WN722N v1.10 USB card (chipset Atheros AR9002U) is used as the auxiliary interface in all cases for the 2.4GHz band.

For injection and monitoring in 5 GHz, each mini PC and PC Engines APU is equipped with two Alfa AWUS036 ACH

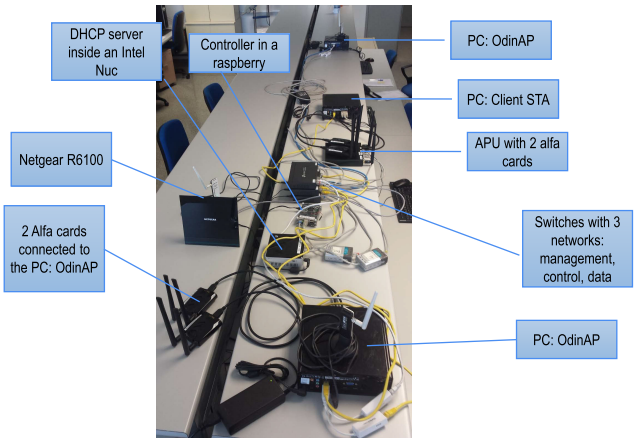

FIGURE 11. Equipment used for the tests.

USB cards, with chipset Realtek RTL8812AU. This model has been chosen because of its advanced injection and monitoring capabilities. The used driver is RTL 8812 au, version 5.2.20.

The use of a number of LVAPs in the same physical AP requires some tweaks in order to send the Layer-2 ACKs correctly [17]. The way in which we have managed this issue is summarized in the Appendix, B.

2) EQUIPMENT USED AS STAS

The next devices have been used as STAs:

- One Mini PC with Kali Linux, running *wpa_supplicant*,[7] which implements WPA key negotiation with a WPA Authenticator and EAP authentication with an Authentication Server. In addition, it controls the roaming and IEEE 802.11 authentication / association of the wireless LAN driver.
- An unmodified Samsung Galaxy GT-i9505, with Wi-Fi 802.11 a/b/g/n/ac, dual-band, has also been employed in some tests.

3) CONTROLLER

The controller runs in a Raspberry Pi 3 Model B v1.2, with Quad Core 1.2GHz Broadcom BCM2837 64bit CPU, 1GB RAM and 100 Base Ethernet cards.

B. TESTBED RESULTS

This section includes some tests that illustrate how the requirements are accomplished (see Section IV.A). It should be noted that the presented results are more qualitative than quantitative: considering that our aim is to show the feasibility of these functionalities in real scenarios, the paper is mainly focused on testing their correct work. However, a different approach should be followed in order to quantitatively estimate the achievable benefits of this proposal: simulation of long time periods, or tests in environments with controlled interference sources should be required.

[7]WPA supplicant, https://linux.die.net/man/8/wpa_supplicant

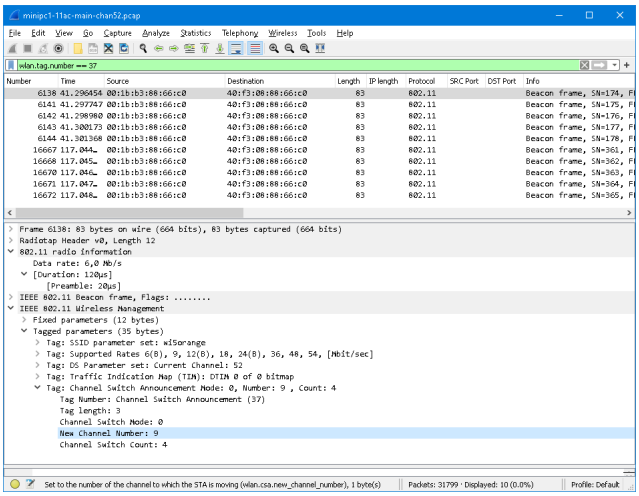

FIGURE 12. Beacon including a Channel Switch Announcement from channel 52 to channel 9.

1) HANDOFF IN A MIXED SCENARIO (2.4 AND 5GHZ)

One of the requirements was that the mobility should also be possible among Wi-Fi bands (2.4 GHz and 5 GHz). In this section we show a capture illustrating that this is possible.

Two mini PCs are used as APs: mini PC 1 is in channel 52, using 802.11ac. It uses two Alfa wireless cards. mini PC 2 uses 802.11n in channel 9. Its main interface is an internal ath9k card, and it also has an auxiliary Alfa card, able to scan in both bands. The controller is a Raspberry Pi running the controller with a mobility management and load balancing application called *SmartAPSelection*.[8] The STA is a Samsung mobile phone.

When the application orders a handoff from channel 52 to channel 9, beacons with the Channel Switch Announcement element appear in both cases (see the Wireshark captures in the corresponding figures):

1) Mini PC 1 sends CSAs in the 5 GHz band (channel 52), ordering the STA to switch to channel 9 (Fig. 12).
2) Mini PC 2 sends CSAs in the 2.4 GHz band (channel 9), ordering the STA to switch to channel 52 (Fig. 13).

At the end of the last beacon with the CSA element, the STA switches from one channel to the other. It should be noted that, from a point of view of the system, the mechanism of this handoff is not at all different from the ones between channels in the same band: the only thing that changes is the channel number.

2) ENCRYPTION/DECRYPTION PROCESSING DELAY

In this subsection we estimate the processing delay required for encryption and decryption of frames. The delay has been measured in the three considered hardware platforms. It is defined as:

- The time between the arrival of an Ethernet frame from the router, and the departure of the corresponding Wi-Fi frame (maybe encrypted) to the STA.

[8]See https://github.com/Wi5/odin-wi5/wiki/Application-SmartAp Selection

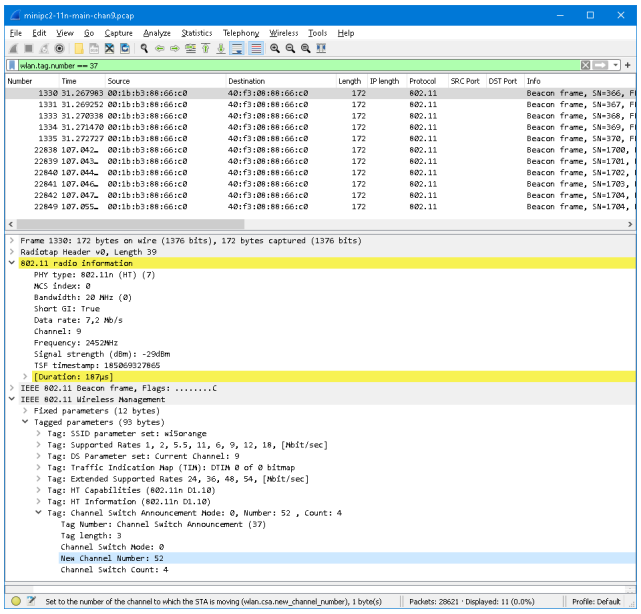

FIGURE 13. Beacon including a Channel Switch Announcement from channel 9 to channel 52.

- The time between the arrival of a Wi-Fi frame (maybe encrypted) from the STA, and the departure of the corresponding Ethernet frame to the router.

The next methodology is used for the tests: a single AP runs the program, using debug level 3, and activating the timestamp for the debug information. 802.11n is used, although this is not relevant for testing the processing delays associated to the security. The controller runs without any application (this is to avoid any handoff happening during the tests).

A STA (a mini PC) is connected to the wireless network. Once it gets the IP address using DHCP, a set of 'ping' messages are sent to the IP address of the router. This is repeated with and without security. The debug information generated by the AP is stored in a file, and the processing delay is obtained as the difference between the no security and the security cases.

The results using the three hardware platforms are presented in Table 2. Each value is the average of 10 packets.

In the Mini PC, the delay attributable to encryption or decryption of a frame is quite similar (it should be considered that AES algorithm is symmetric), roughly 120 μsec.

The PC Engines APU presents a higher delay, between 164 and 192 μsec, and this delay is much higher for the Netgear R6100 router, in which it requires some milliseconds. The delay attributable to encryption / decryption is also significant.

Although these values may seem very high, it should be considered that our program is a proof-of-concept that runs in user space. If encryption was performed at lower levels, these delays could be significantly reduced, in a similar way to what usually happens when a commodity AP encrypts / decrypts traffic.

TABLE 2. Processing delay (μsec).

	Mini PC	PC Engines APU	Netgear R6100
WiFi frame to Ethernet management delay without decryption (1)	103.2	297.7	3458.1
WiFi frame to Ethernet management delay with decryption (2)	222.6	490.4	6295.2
Delay attributable to decryption (2) – (1)	119.4	192.7	2837.1
Eth frame to Wi-Fi management delay without encryption (3)	247.3	548.3	3034.5
Eth frame to Wi-Fi management delay with encryption (4)	368.7	713	8986.5
Delay attributable to encryption (4) – (3)	121.4	164.7	5952

TABLE 3. Round-trip time between an associated STA and the router (msec).

	Mini PC	PC Engines APU	Netgear R6100
RTT without security	5.64	6.36	11.28
RTT with security	5.40	6.17	14.35

3) ROUND TRIP DELAY

In this experiment we want to estimate the delay introduced by the LVAP solution. For that aim, a number of ping messages are sent from a connected STA, to a computer in the wired network (which is in fact the router/DHCP server, see Fig. 10). The contribution of the wired segment to the delay is considered as very small.

The STA that connects is a mini PC with Kali Linux, running *wpa_supplicant*. The experiment consists of starting the AP, starting the controller, connecting a STA and sending a number of pings to the router / DHCP server. The Round-Trip Time is estimated as the average of a number of ping messages (40 by default).

In Table 3 we present the results using different equipment for running the AP: a mini PC, a PC Engines APU and a Netgear R6100, with and without security.

It can be seen that the processing delay, which strongly depends on the hardware platform, has some influence on the overall delay. If we observe the results reported in the previous subsection, we confirm that the mini PC is faster than the PC Engines, and both are much faster than the Netgear R6100.

4) HANDOFF DELAY

The tests presented in this subsection are aimed at getting an estimation of the handoff delay. The scheme is also the one illustrated in Fig. 10. In this case we have:

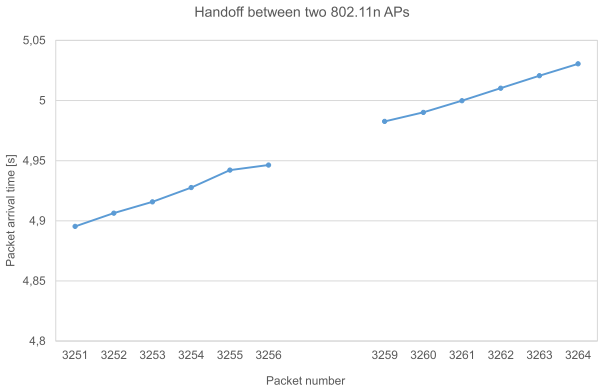

FIGURE 14. Measurement of a handoff.

TABLE 4. Estimated handoff delay (msec).

	802.11g	802.11n
Handoff delay without security	10 - 40 ms	20 - 30 ms
Handoff delay with security	10 - 50 ms	20 - 30 ms

- An 802.11 Wi-Fi network with 2 APs is created. The 2 APs are mini PCs. One is in channel 1, and the other one is in channel 11.
- The controller application *MobilityManager*[9] is run, with the parameters set in order to have periodical handoffs.
- D-ITG traffic generator [30] is set in the STA, and 1000 UDP packets of 60 bytes of payload are sent at a rate of 100 pps (this allows a granularity of 10 ms) during 100 sec.
- D-ITG receiver is set in the router / DHCP server. The log file received is decoded in order to get the list of arrived packets, and also their arrival times. With this information, the handoff delay can be estimating according to the number of lost packets (see Fig. 14, where an example with 2 lost packets is shown).

The obtained results are presented in Table 4. It can be observed that the delays are small enough in order to avoid any significant service disruption. In addition, what is more interesting is to observe that the addition of security has a negligible impact on the handoff delay. This could be expected, considering the way in which the handoff scheme has been designed (see Section IV.C). Therefore, the handoff delays reported in [1] are still valid (they were in the order of the tens of milliseconds, depending on the hardware).

VI. TESTS IN SIMULATED SCENARIOS

As a complement to the tests with real equipment, a simulation environment that illustrates the achievable benefits with a higher number of devices.

[9]See https://github.com/Wi5/odin-wi5/wiki/Application-Mobility Manager

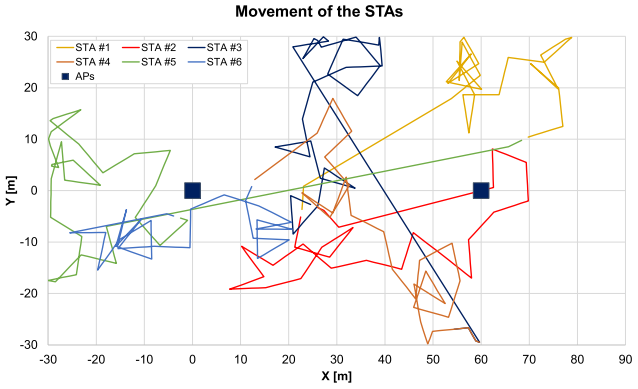

FIGURE 15. Scenario with 2 APs, showing the trajectories of six STAs.

A. SIMULATION SETUP

The simulation environment has been built in ns3.[10] It includes dual APs and STAs, which have been implemented as two nodes (one with an 802.11n device and another one with an 802.11ac one) that are always in the same place: in the case of the STAs, both nodes follow the same random mobility pattern, and only one of them can be active in a certain moment. As it happens in commercial devices, they can only be connected in one band at a time.

The STAs move in a rectangular scenario (see Fig. 15) with a number of APs (2 or 3), following the ns3 random waypoint model (1.5 m/s and 2 s of pause). The distance between APs is 60 or 80 meters. The blue squares represent the APs.

In order to mimic the home scenarios that we are considering in our study, the setup includes both dual APs (802.11n and 802.11ac), coexisting with APs that only implement 802.11n in 2.4 GHz.

Two situations have been compared: *a*) as a baseline, each STA connects to the first AP it sees. In the case of dual APs, it may happen that the STA connects to the 802.11n or the 11ac one. This situation corresponds to a typical home setup where there is no coordination between APs, so each device connects randomly to the first AP it sees. *b*) A situation in which two algorithms run simultaneously:

- If a STA is connected to an 11n AP, but it is very close (an "optimal zone" of 20 meters around the AP has been defined) to an 11ac AP, the STA is switched to the 11ac AP.
- If a STA is connected to an 11ac AP, but it is far from it, it may be switched to an 11n AP that is closer and can provide a better signal level.

These algorithms do not introduce any additional limit regarding the number of STAs that can connect to the wireless network.

B. SIMULATION RESULTS

Simulations with 2 and 3 APs, and 1 to 6 users in the scenario have been run. Each STA runs a TCP bulk download, and the aggregate achieved throughput is used as the main KPI

[10]The code is available here: https://github.com/wifi-diversity/ns3

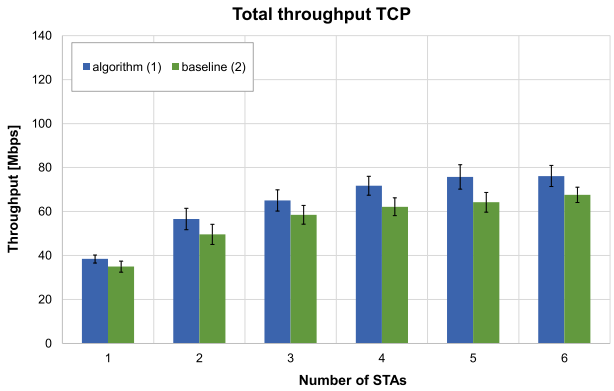

FIGURE 16. Aggregate throughput with 2 APs separated by 80 m.

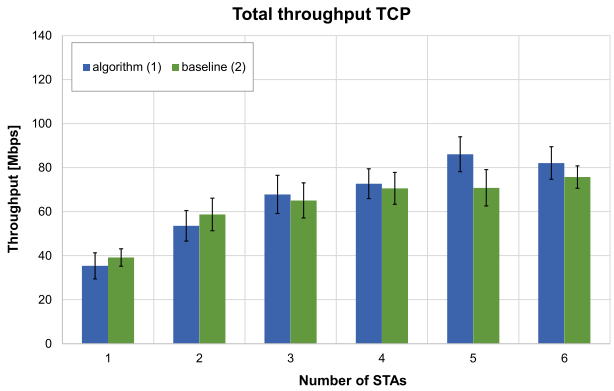

FIGURE 17. Aggregate throughput with 2 APs separated by 60 m.

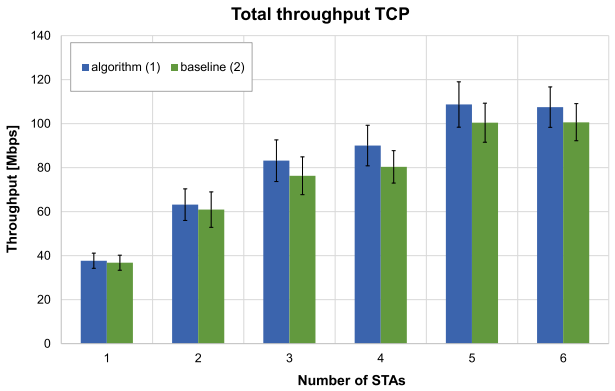

FIGURE 18. Aggregate throughput with 3 APs separated by 80 m.

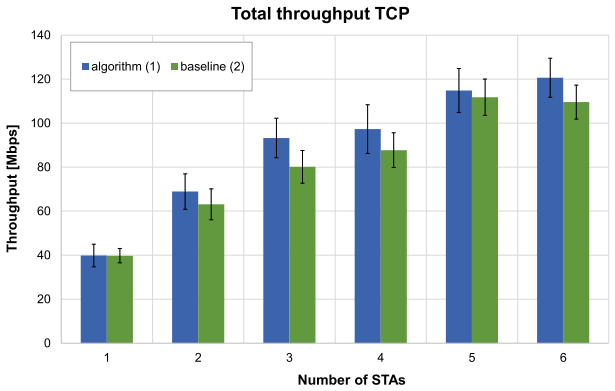

FIGURE 19. Aggregate throughput with 3 APs separated by 60 m.

(Key Performance Indicator). The 95% confidence intervals are presented.

Fig. 16 shows the results with 2 APs separated by 80 m (one is dual and another one is an only 802.11n one), and Fig. 17 the ones if the APs are separated by 60 m. A 3 AP scenario is also simulated: the AP in the middle is dual, and the two others are 802.11n APs. The results are presented in Fig. 18 (80 m between APs) and Fig. 19 (60 m between APs). The results are the average of 60 (Fig. 16) or 30 (Fig. 17-19) simulations.

It can be observed that significant throughput increases can be obtained if the algorithm is employed: in the case of 2 APs, the throughput can be increased up to 22% with respect to the baseline case (see Fig. 16 and 17). If the distance between APs is higher (80 m), benefits are obtained even for a single user. If it is smaller (60 m), benefits are only obtained for 3 or more users. The cause is that the 11ac "optimal zone" is always the same (20 m around the AP). Therefore, if the scenario becomes smaller, the achievable throughput with 11n outside of the 11ac "optimal zone," will become better (as we are closer to the 11n AP). This is why the algorithm is not so beneficial in these cases. In contrast, if the number of users is higher (3 or more), the algorithm only assigns them to the 11ac AP if they are really close and they can obtain significant throughput.

If the scenario includes 3 APs (Fig. 18 and 19), the overall throughput becomes higher, and the benefits are up to 16 % if the algorithm is used.

Although the simulations are not exhaustive, they showcase the potential benefits that can be obtained by the coordination between APs in these scenarios, even in the case of having only 2 or 3, as it happens frequently in home networks. Future works may propose more complex algorithms for an optimal assignment of APs to STAs in heterogeneous scenarios. These algorithms should be aware of the distance between APs, which is an important parameter, considering the different attenuation between 2.4 and 5 GHz bands.

VII. CONCLUSION

This paper has been focused in Wi-Fi scenarios integrating a small number of APs (typically 2-4) with heterogeneous characteristics, including the last advances of 802.11n and 11ac, and security options. It has proposed the consideration of the specific capabilities and other characteristics in order to improve the management of the radio resources in the network.

A new user-space application has been built, that works in coordination with an existing controller, in order to constitute a SDWN solution based on LVAPs. This allows seamless handoffs and permits a smart management of the STAs. The application also manages security, avoiding the need of

```
WRITE odinagent.add_vap 74:F0:6D:20:DA:CF
192.168.137.205
00:1B:B3:20:DA:CF
wifiunizar
htpr ee111bffff000000000000000000001000000000000000000
htar ee111bffff000000000000000000001000000000000000000
vhtpr 00000000000000000000000
vhtar 00000000000000000000000
kck 67920d9e87f7bce7bcaf187bd8bc1493
kek 1067e252a39b26d8ff8a5c8e2c7c8200
tk 0a210178ac3b0f2a070a363cd655aca5
rsn 0100000fac040100000fac040100000fac020000
seqnum 470
ccmptx 45
ccmprx 25
```

FIGURE 20. Example of an *Add LVAP* message.

adding specific elements for authentication, encryption and decryption.

By means of three use cases, it has been shown that the consideration of the different characteristics of the APs is relevant, and can provide significant benefits for this kind of solutions, and also in any coordinated WLAN with heterogeneous APs.

The existing protocol for the communication between the AP and the controller has been extended, in order to communicate and store the specific characteristics of each AP and STA, including the capabilities, the security features and the status. This allows the use of these parameters by new resource management algorithms that can be developed in the future. A battery of tests has been run using different equipment, showing that handoffs between bands are possible, and estimating the processing delays, the RTT and the handoff delay, which is small enough in order not to produce any significant disruption to the user.

Finally, the considered scenarios have been replicated in a simulation environment. The quantitative results show that significant benefits can be achieved if the specific characteristics of each AP are considered.

As future work, simulation tools can be used in order to explore and measure the benefits achievable by means of the consideration of the heterogeneous characteristics of the APs, in order to assign each connected STA to the AP that best fits with its characteristics. Smart algorithms for resource optimization can be tested in these environments. In addition, the proposed solution could be compared (qualitatively and quantitatively, and also in terms of security) with *EasyMesh* by the Wi-Fi Alliance.

APPENDIX

A. EXAMPLES OF THE NEW ODIN MESSAGES

We include here some examples of the messages that have been created as an extension to the Odin protocol (see Table 1).

Fig. 20 shows an example of the *Add LVAP* message. In this case, it corresponds to a handoff between APs, so it includes the complete set of parameters that are transmitted to the destination AP. Additional linefeeds have been added after each parameter.

As it can be observed, the *Add LVAP* includes these parameters:

```
association 74:f0:6d:20:da:cf
htpr ee111bffff000000000000000000001000000000000000000
htar ee111bffff000000000000000000001000000000000000000
vhtpr 00000000000000000000000
vhtar 00000000000000000000000
```

FIGURE 21. Example of a *Completed Association Notification* message.

```
eapol 74:f0:6d:20:da:cf
kck 67920d9e87f7bce7bcaf187bd8bc1493
kek 1067e252a39b26d8ff8a5c8e2c7c8200
tk 0a210178ac3b0f2a070a363cd655aca5
rsn 0100000fac040100000fac040100000fac020000
```

FIGURE 22. Example of a *Completed EAPOL* message.

```
200 Read handler 'odinagent.status' OK
DATA 52
74:f0:6d:20:da:cf seqnum:741 ccmptx:57 ccmprx:38
```

FIGURE 23. Example of a *Status Update Response* message.

- The legacy 4-tuple with the MAC and IP of the STA, the MAC of the virtual AP and the SSID.
- Capabilities
  - HT capabilities, both in the *Probe Request* (*htpr*) and the *Association Request* (*htap*). The capabilities are expressed in the same way they are included in the messages, *i.e.* as a hexadecimal array.
  - VHT capabilities in the Probe Request (*vhtpr*) and the Association Request (*vhtar*).
- Security information
  - *kck*: EAPOL Key Confirmation Key.
  - *kek*: EAPOL Key Encryption Key.
  - *tk*: It is used for encryption / decryption of frames
  - *rsn*: RSN Information Element.
- Status
  - *seqnum*: sequence number of the last frame sent to the STA.
  - *ccmptx*: last value of the CCMP Tx Packet Number.
  - *ccmprx*: last value of the CCMP Rx Packet Number.

Fig. 21 shows an example of the *Completed Association Notification* message.

Fig. 22 shows an example of the *Completed EAPOL* message.

Fig. 23 shows an example of the *Status Update Response* message.

B. 802.11 TRAFFIC INJECTION AND ACKs

The LVAP solution requires that a single AP sends frames with different transmitter MAC addresses. This can be achieved by the injection of traffic in monitor mode, because the frame is constructed by the user-space application, including the MAC header with all the desired addresses.

In addition, 802.11 requires that an ACK is received just after the sending of a frame, in order to let the transmitter know that the frame has arrived correctly. Otherwise, the frame is retransmitted.

Therefore, when a STA sends a frame to the AP, an ACK with the MAC address of the STA has to be sent in response. The question is that this action has to be very fast, and it has to

TABLE 5. Parameters employed in the NS3 simulations.

ns3 version	ns-3.30.1
Mobility model	Random Waypoint. Walking speed 1.5 m/s with pause time 2 s
TCP pkt size	1,500 bytes
WiFi model	SpectrumWifiPhy with MultiModel SpectrumChannel
TCP variant	New Reno
Channels 5 GHz	36 to 128 (20 MHz channels)
Channels 2.4 GHz	1, 6 and 11
Simulation time	120 s
RTS/CTS	Disabled
WiFi rate control model	Idealwifi Manager
Inter-AP distance	60 – 80 m (30 – 40 m to the border)
Propagation loss model	FriisSpectrum
Short guard	Not enabled
Error rate model	Nist ErrorRateModel
EDCA priorities	Disabled

be done at driver level. For that aim, the driver has to find its own address in the *Receiver Address* field of the MAC header.

1) INJECTION AND ACKS IN 2.4GHZ

In [17] a patch to the ath9k driver was presented, using a mask that allowed a set of addresses to be acknowledged by the driver. In the present paper we have made use of this same solution in the tests performed in 2.4 GHz.

2) INJECTION AND ACKS IN 5GHZ

We initially included an option in the developed agent, which allowed the sending of ACKs by software. However, we observed that it was not fast enough, and caused many retransmissions.

As a solution, we discovered that certain wireless cards, when put in ''monitor active'' mode, do send ACKs if they receive a frame targeted for their physical MAC address. This gave us the idea of having an interface just focused on sending these ACKs. We built a setup in which the agent runs in a PC Engines APU with 2 interfaces (in addition to the one used for monitoring):

- Realtek Alfa: main wireless interface, in monitor mode. It is in charge of injection and capture of frames.
- Internal card using ath10k driver: it is only used for sending layer-2 ACKs.

The internal card is in ''monitor active'' mode. Whenever it receives a frame addressed to its physical MAC address, it sends a layer-2 ACK. An option has been included in the program that allows this: it modifies the value of the LVAP created by the controller, and substitutes it by the value of the MAC address of the interface that sends the ACKs. This introduces a limitation: a single LVAP can be used, which means that a single STA can be connected at the same time to the AP.

Although the limitation is severe, it allows the measurement of some parameters as *e.g.* handoff delays. Future versions of the driver may allow the sending of ACKs in 5 GHz, in the same way it is possible in the 2.4 GHz band. It should be considered that the maturity level of the ath9k driver is much higher than that of ath10k.

C. PARAMETERS OF THE ns3 SIMULATOR

Table 5 summarizes the parameters employed in the ns3 simulations.

REFERENCES

[1] J. Saldana, R. Munilla, S. Eryigit, O. Topal, J. Ruiz-Mas, J. Fernandez-Navajas, and L. Sequeira, ''Unsticking the Wi-Fi client: Smarter decisions using a software defined wireless solution,'' *IEEE Access*, vol. 6, pp. 30917–30931, 2018.

[2] (Dec. 2020). *Miercom, Cisco Catalyst 9800 Wireless Controller Detailed Report DR190220E. Competitive Test Data for HPE-Aruba, Ruckus Networks and Huawei Technologies*. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/wireless/nb-10-cat9800-miercom-2019-analyst-rpt-cte-en.pdf

[3] (Dec. 2020). *Wi-Fi EasyMesh-Specification Version 3.0*. [Online]. Available: https://www.wi-fi.org/discover-wi-fi/wi-fi-easymesh

[4] F. Bouhafs, M. Mackay, A. Raschella, Q. Shi, F. D. Hartog, J. Saldana, R. Munilla, J. Ruiz-Mas, J. Fernandez-Navajas, J. Almodovar, and N. V. Adrichem, ''Wi-5: A programming architecture for unlicensed frequency bands,'' *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 178–185, Dec. 2018.

[5] R. Riggio, M. K. Marina, J. Schulz-Zander, S. Kuklinski, and T. Rasheed, ''Programming abstractions for software-defined wireless networks,'' *IEEE Trans. Netw. Service Manage.*, vol. 12, no. 2, pp. 146–162, Jun. 2015.

[6] A. Zubow, S. Zehl, and A. Wolisz, ''BIGAP—Seamless handover in high performance enterprise IEEE 802.11 networks,'' in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, Istanbul, Turkey, Apr. 2016, pp. 445–453.

[7] K. Koál, R. Bencel, M. Ries, P. Tráchly, and I. Kotuliak, ''High performance SDN WLAN architecture,'' *Sensors*, vol. 19, no. 8, p. 1880, Apr. 2019.

[8] K. I. Qureshi, L. Wang, L. Sun, C. Zhu, and L. Shu, ''A review on design and implementation of software-defined WLANs,'' *IEEE Syst. J.*, vol. 14, no. 2, pp. 2601–2614, Jun. 2020.

[9] *IEEE Standard for Information Technology—Local and Metropolitan Area Networks–Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs*, Standard 802.11k-2008 Amendment to IEEE Std 802.11-2007, Jun. 2008.

[10] *IEEE Standard for Information Technology—Local and Metropolitan Area Networks– Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition*, Standard 802.11r-2008 Amendment to IEEE Std 802.11-2007, Jul. 2008.

[11] *IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: IEEE 802.11 Wireless Network Management*, Standard 802.11v-2011 802.11-2007 802.11k-2008 802.11r-2008 802.11y-2008 802.11w-2009 802.11n-2009, 802.11p-2010, 802.11z-2010, Feb. 2011.

[12] P. Calhoun, *RFC 5415, Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification*. [Online]. Available: https://tools.ietf.org/html/rfc5415

[13] Miercom knows: Cisco Catalyst 9800 Wireless Controllers are in a Class by Itself, May 7, 2019, available at. [Online]. Available: https://blogs.cisco.com/wireless/miercom-knows-cisco-catalyst-9800-wireless-controllers-a-class-by-itself

[14] PCMag, The Best Wi-Fi Mesh Network Systems for 2019, available at. [Online]. Available: https://www.pcmag.com/roundup/350795/the-best-wi-fi-mesh-network-systems

[15] Omnicore. (Dec. 2020). *8 Best Wi-Fi Mesh Network Systems for Insane Internet Speed*. [Online]. Available: https://www.omnicoreagency.com/best-wifi-mesh-network-systems/
[16] M. E. Berezin, F. Rousseau, and A. Duda, "Multichannel virtual access points for seamless handoffs in IEEE 802.11 wireless networks," in *Proc. IEEE 73rd Veh. Technol. Conf. (VTC Spring)*, May 2011, pp. 1–5.
[17] J. Schulz-Zander, P. L. Suresh, N. Sarrar, A. Feldmann, T. Hhn, and R. Merz, "Programmatic orchestration of WiFi networks," in *Proc. USENIX Annu. Tech. Conf.*, G. Gibson and N. Zel-Dovich, Eds., 2014, p. 347358.
[18] L. Sequeira, J. L. de la Cruz, J. Ruiz-Mas, J. Saldana, J. Fernandez-Navajas, and J. Almodovar, "Building an SDN enterprise WLAN based on virtual APs," *IEEE Commun. Lett.*, vol. 21, no. 2, pp. 374–377, Feb. 2017.
[19] *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe*, Standard IEEE 802.11h, 2011.
[20] J. Schulz-Zander, N. Sarrar, and S. S. Tu, "AeroFlux: A near-sighted controller architecture for software-defined wireless networks," in *Proc. Open Netw. Summit*, Santa Clara, CA, USA, Mar. 2014, pp. 1–2.
[21] E. Coronado, R. Riggio, J. Villalon, and A. Garrido, "Joint mobility management and multicast rate adaptation in software–defined enterprise WLANs," *IEEE Trans. Netw. Service Manage.*, vol. 15, no. 2, pp. 625–637, Jun. 2018.
[22] Accton. (Dec. 2020). *Software-Defined Networking for Wi-Fi White Paper*. [Online]. Available: https://docplayer.net/9190422-Software-defined-networking-for-wi-fi-white-paper.html
[23] D. Gong and Y. Yang, "AP association in 802.11n WLANs with heterogeneous clients," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 1440–1448.
[24] D. Gong and Y. Yang, "On-line AP association algorithms for 802.11n WLANs with heterogeneous clients," *IEEE Trans. Comput.*, vol. 63, no. 11, pp. 2772–2786, Nov. 2014.
[25] M. A. Abusubaih, S. Najem Eddin, and A. Khamayseh, "IEEE 802.11n dual band access points for boosting the performance of heterogeneous WiFi networks," in *Proc. 8th ACM Workshop Perform. Monitor. Meas. Heterogeneous wireless wired Netw.*, New York, NY, USA, 2013, pp. 1–4.
[26] D. Gong, M. Zhao, and Y. Yang, "Distributed channel assignment algorithms for 802.11n WLANs with heterogeneous clients," *J. Parallel Distrib. Comput.*, vol. 74, no. 5, pp. 2365–2379, May 2014.
[27] *IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements*, Standard 802.11i-2004, Jun. 2004.
[28] *IEEE Standard for Local and Metropolitan Area Networks–Port-Based Network Access Control*, Standard 802.1X-2010, 2011.
[29] L. Suresh Puthalath, "Programming the enterprise WLAN: An SDN approach," M.S. thesis, Dept. Elect. Comput. Eng., Instituto Superior, Técnico, Lisbon, 2012.
[30] A. Botta, A. Dainotti, and A. Pescapé, "A tool for the generation of realistic network workload for emerging networking scenarios," *Comput. Netw.*, vol. 56, no. 15, pp. 3531–3547, Oct. 2012.

JOSE SALDANA (Senior Member, IEEE) was born in San Sebastián, Spain, in 1974. He received the B.S. and M.S. degrees in telecommunications engineering in 1998 and 2008, respectively, and the Ph.D. degree in information technologies from the University of Zaragoza, in 2011.

He is currently a Senior Postdoctoral Researcher with the Department of Engineering and Communications. His research interests include quality of service in real-time multimedia services, as VoIP and networked online games, traffic optimization, and resource management in Wireless LANs. He is also a member of the Internet Society. He also serves as an Editor for IEEE Access, and as an Area Editor for *KSII Transactions on Internet and Information Services*. For several years, he has served in the Organization Committee for IEEE Consumer Communications and Networking Conference (CCNC), and in the technical program committee for many other conferences as, e.g., IEEE ICC and IEEE Globecom.

JOSÉ RUIZ-MAS was born in Lorca, Murcia, Spain, in 1965. He received the engineer of telecommunications degree from the Universitat Politècnica de Catalunya (UPC), Spain, in 1991, and the Ph.D. degree in telecommunications engineering from the University of Zaragoza (UZ), in 2001.

He worked as a Software Engineer with the company TAO Open Systems, from 1992 to 1994. In 1994, he joined the EINA as an Assistant Professor until 2003, when he became an Associate Professor. He was the Director of Telefonica Chair (University of Zaragoza) from June 2004 to June 2008 and the Coordinator of Master in Information Technology and Mobile Communications from December 2007 to 2009. He is currently with the Department of Electronics Engineering and Communications, Higher Engineering and Architecture School, UZ. He is also a member of the Aragón Institute of Engineering Research (I3A). He has been the co-investigator since 1995 of research grants from EU Research Projects, the Ministry of Science and Technology, the Sanitary Research Funds, and the Government of Aragon, Spain, in the areas of distributed multimedia system and wireless networks. Major industrial and mobile companies in the area of wireless communications also support his work. He is also the co-investigator of several research projects supported by companies as Telefónica and Teltronic. His current research interests include communication networks with special emphasis on wireless networks, distributed multimedia systems, quality of service (QoS), and quality of experience (QoE).

JULIÁN FERNÁNDEZ-NAVAJAS was born in Alfaro, La Rioja, Spain, in 1969. He received the engineer of telecommunications degree from the Universidad Politécnica de Valencia (UPV), Spain, in 1993, and the Ph.D. degree in telecommunications engineering from the University of Zaragoza (UZ), in 2000.

In 1994, he joined the EINA as an Assistant Professor until 2002, when he became an Associate Professor. He is currently with the Department of Electronics Engineering and Communications, Higher Engineering and Architecture School, UZ. He is also a member of the Aragón Institute of Engineering Research (I3A). He has been the co-investigator since 1995 of research grants from EU Research Projects, the Ministry of Science and Technology, the Sanitary Research Funds, and the Government of Aragón (Spain) in the areas of distributed multimedia system and wireless networks. Major industrial and mobile companies in the area of wireless communications also support his work. He is also the co-investigator of several research projects supported by companies as Telefónica. His currently research interests include communication networks with special emphasis on wireless networks, distributed multimedia systems, quality of service (QoS), and quality of experience (QoE).

JOSÉ LUIS SALAZAR RIAÑO received the mathematical sciences degree from the University of Zaragoza, in 1993. In June 1995, after working momentarily at the Public University of Navarra, he received the Ph.D. degree from the University of Zaragoza, in 1999.

That year, he joined the Department of Mathematics and Computing, University of La Rioja, for two academic years. That year, he joined the EINA, University of Zaragoza. As a Research activity, he has participated in numerous R + D + i projects financed in competitive calls from public or private administrations or entities, forming part of the research group ''Communications Technology Group (GTC),'' since 2014, in the group ''Communications Networks and Information Technologies for e-Health and Quality of Experience Group (CeNITEQ)'' and since 2017 ''Communications Networks and Information Technologies (CENIT).'' As a Consequence, he has published scientific-technical documents, several of them in journals and has participated in many presentations at national and international conferences. He is also a member of the University Institute of Engineering Research in Aragon I3A. His research interests include cryptology, computer security, and electronic commerce. He is dedicated to apply emerging cryptographic operations to protocols related to new services: ring signatures for electronic voting in e-cognocracy; and added signatures for RFID tagging. His current research interest includes the use of new trust schemes applied to secure routing in MANETs with strong resource constraints.

JEAN-PHILIPPE JAVAUDIN (Member, IEEE) was born in Rennes, France, in 1979. He received the M.S. degree in telecommunications engineering from Telecom Paris, in 2001. Since then, he had been working with Orange as a 3GPP standardisation delegate from 2002 to 2005. He coordinated several French and EU cooperative projects. He has been a Research Program Leader with Orange Labs since 2011 on radio connectivity for Local Networks.

JEAN-MICHEL BONNAMY was born in Saint-Brieuc, France, in 1972. He received the M.S. degree in telecom engineering in 1996. He is currently a Network Architect with Orange Labs. His research interest includes residential networks for several years. He has been contributing to standardization groups, such as Broadband Forum, Home Gateway Initiative, IEEE, and the WiFi Alliance. He initiated the first plugfest for residential gateways as a Group Chair.

MAËL LE DIZES was born in France, in 1990. He graduated from ENSSAT, Lannion. He received the M.S. degree in multimedia and telecommunication engineering from ENSSAT. He joined Orange Business Services then integrated Orange Labs as a LAN Designer and Developer. His research interests include LAN technologies, smart Wi-Fi, and E2E network diagnosis.