Wi-5

What to do With the Wi-Fi Wild West
Funding scheme: H2020-ICT-2014-1
Grant number: 644262

Horizon 2020
European Union Funding
for Research & Innovation

Deliverable	D3.2
Title	Specification of Smart AP solutions version 1
Date	31/12/2015
Milestone	MS2
Editor	Jose Saldana (Unizar)
Reviewers	Ali Arsal (AirTies), Michael Mackay (LJMU)
Approved by	General Assembly
Dissemination	Public

Abstract

The *What to do With the Wi-Fi Wild West* H2020 project (Wi-5) combines research and innovation to propose an architecture based on an integrated and coordinated set of smart Wi-Fi networking solutions. The resulting system will be able to efficiently reduce interference between neighbouring Access Points (APs) and provide optimised connectivity for new and emerging services. The project approach will develop and incorporate a variety of different solutions, which will be made available in academic publications, in addition to other dissemination channels.

This document includes the specification of the first version of the Smart Access Point Solutions, which are being deployed within WP3 of the Wi-5 project. After the Executive Summary and the Literature Review, a Global View of the Wi-5 architecture is presented. This includes not only the Smart AP Solutions, but also the Cooperative Functionalities, being developed in WP4.

Next, the first definition of the Smart AP Solutions is presented, including the functionalities enabling Performance Monitoring tools and Radio Resource Management (i.e. Dynamic Channel Allocation, Load Balancing and Power Control). Next, the specification of the Packet Grouping features is included, also presenting the results of some tests performed in a laboratory environment. The current status of the implementation of the solutions is also included. The implementation is based on Light Virtual APs, which allow seamless handovers between APs.

After summarising the future objectives, the document ends with the Conclusions. Two annexes are also included: one about Simplemux, a Layer-3 packet grouping proposal which has been presented to the IETF; and another one explaining in detail how to adapt a commercial AP in order to be used for implementing the proposed solutions.

The Smart AP Solutions are based on the concept of Light Virtual Access Points (LVAPs) which are created for each terminal. Therefore, the AP will use a different LVAP for communicating with each terminal and the terminal will only "see" a single AP, even if it is actually moving between a number of APs. One of the main innovations proposed by Wi-5 is to combine the use of LVAPs with multi-channel APs, thus allowing two key features at the same time: seamless handovers, and radio resource management.

Wi-5 Consortium

Liverpool John Moores University

2 Rodney Street
Egerton Court
Liverpool, L3 5UK
United Kingdom

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek

Anna van Buerenplein 1
2595 DA Den Haag
Netherlands

Universidad de Zaragoza

Calle Pedro Cerbuna 12
Zaragoza
50009
Spain

Telefonica Investigación y Desarrollo SAU

Ronda de la Comunicacion S/N
Distrito C Edificio Oeste 1
Madrid 28050
Spain

AirTies Kablosuz İletişim San ve Dış. Tic. A.Ş

Gulbahar Mah. Avni Dilligil Sok. No:5 Çelik İş Merkezi
Mecidiyeköy
Istanbul 34394
Turkey

Contents

List of Figures

Glossary

AP	Access Point
CAIDA	Center for Applied Internet Data Analysis
CPU	Central Processing Unit
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DFS	Dynamic Frequency Selection
D-ITG	Distributed Internet Traffic Generator
Diffuse	DIstributed Firewall and Flow-shaper Using Statistical Evidence
DOI	Digital Object Identifier
DPI	Deep Packet Inspection
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
FF	Fittingness Factor
FPS	First Person Shooter
GSM	Global System for Mobile Communications
IANA	Internet Assigned Numbers Authority
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
L2TP	Layer 2 Tunnelling Protocol
LTE	Long Term Evolution
LVAP	Light Vırtual Access Point
MAC	Media Access Control
MMORPG	Massively Multiplayer Online Role Playing Game
MPDU	MAC Protocol Data Unit aggregation
MSDU	MAC Service Data Unit aggregation

MTU	Maximum Transmission Unit
PPP	Point to Point Protocol
QoE	Quality of Experience
QoS	Quality of Service
RFC	Request For Comments
ROHC	RObust Header Compression
RTP	Real Time Protocol
SDN	Software-Defined Network
SDWN	Software-Defined Wireless Network
STA	Wi-Fi Station
TCP	Transmission Control Protocol
TCRTP	Tunnelling Compressed RTP
TPC	Transmit Power Control
UDP	User Datagram Protocol
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
WEKA	Waikato Environment for Knowledge Analysis
WLAN	Wireless Local Area Network

Executive Summary

According to the Description of Work, the present document includes *“a first definition of the mechanisms to be included in the Wi-5 APs to perform dynamic channel allocation, load balancing and power control. It will also include a definition of the policies to be employed when using packet grouping between the AP and the end device, as defined in 802.11n and 802.11ac. The integration with the coordination entities of Wi-5 architecture, and the interface with performance monitoring mechanisms will also be defined.”*

The document first presents a Literature Review covering the use of Virtual Access Points in Wi-Fi environments, and the need to monitor the wireless environment. Automatic service detection is also discussed, in addition to different radio resource management algorithms for wireless networks. The literature about packet grouping is finally surveyed.

A global view of the Wi-5 architecture is provided next, including the Cooperative Functionalities, in addition to the Smart AP Solutions presented here.

The main section of the Deliverable is about the Smart AP Solutions themselves, including:

- Summary of the approach taken by Wi-5, which relies on Light Virtual APs.
- Performance monitoring, including two different aspects: firstly, an automatic detection feature in order to identify those flows with real-time requirements. Secondly, the radio environment that has to be scanned in order to have accurate information about the interference level on each channel, the power being sent by the STA, etc.
- Radio Resource Management. This includes (i) Dynamic Channel Allocation, looking for an optimal distribution of the channels of the APs, in order to reduce the interference; (ii) Load Balancing, looking for an optimal distribution of the users between the APs; (iii) Power Control, trying to keep the signal level as low as possible, in order to save energy and to reduce the interference.
- Packet grouping, considering smart scheduling policies enabling a better use of the aggregation policies already included in 802.11n and subsequent versions. This would alleviate the airtime inefficiency caused by the STAs requesting the shared channel before being able to send actual data. For legacy devices not including aggregation at Layer 2, multiplexing packets at Layer 3 can also be a solution.

A Conclusions section finishes the document, and surveys the features that should be included in the next versions of the Wi-5 solutions.

The document also includes two Annexes: first, a summary of a Layer-3 aggregation mechanism which has been proposed to the IETF, and then a practical document with detailed instructions about how to adapt a commercial AP in order to use it as a Wi-5 AP.

One of the main proposed innovations is to combine the use of LVAPs with multi-channel APs, thus allowing two key features at the same time: seamless handovers, and radio resource management. Another innovation presented is the use of packet grouping and aggregation at Layer 3, which can be convenient in certain scenarios for saving bandwidth and reducing the number of small packets per second.

1 Introduction

1.1 Background to project

The last few years have witnessed a significant increase in the use of portable devices, especially smartphones and tablets which, thanks to their functionality, user-friendly interfaces and affordable prices, have become ubiquitous worldwide. Most of these devices make use of IEEE 802.11 wireless standards, commonly known as Wi-Fi.

Given this increasing demand, Wi-Fi is facing mounting issues of spectrum efficiency due to its utilisation of non-licensed frequency bands, so improvements continue to be added in order to enhance its performance. For example, as Wi-Fi saturation increases in congested scenarios such as business centres, malls, campuses or even whole European cities, interference between these competing Access Points (APs) can negatively impact a user's experience.

At the same time, real-time services with tight latency constraints are becoming ubiquitous. For example, VoIP services such as Skype are now very popular. Furthermore, some instant messaging applications (e.g. *WhatsApp*) also include VoIP features. Finally, online games are no longer exclusive of high-end PCs, but many have been ported to tablets or even smartphones. These real-time services share the same connection with "traditional" applications, such as e-mail and Web browsing, but have different requirements in order to meet the Quality of Experience demands.

In addition, the availability of these services in mobile devices has a consequence: whereas the mobility of a user with a laptop can be considered as nomadic (i.e. the user may move, but he/she will stay for a long time in the same place), smartphone and tablet users may walk while using these real-time services.

The *What to do With the Wi-Fi Wild West* H2020 project (Wi-5) combines research and innovation to propose an architecture based on an integrated and coordinated set of smart solutions able to efficiently reduce interference between neighbouring APs and provide optimised connectivity for new and emerging services. Cooperating mechanisms will be integrated at different layers of the protocol stack with the aim of meeting a demanding set of goals such as seamless hand-over, reduced congestion, increased throughput and energy efficiencies. The project is developing a variety of different solutions, which are being made available in academic publications, in addition to other potential dissemination channels for industrial exploitation and standardisation.

1.2 Scope and structure of the deliverable

The aim of the present deliverable is to provide a first definition of the Wi-5 mechanisms enabling resource management (i.e. dynamic channel allocation, load balancing and power control) in Wi-Fi WLANs. The use of packet grouping for improving the efficiency and the global throughput is also considered. Finally, the use of monitoring mechanisms is required in order to permit a correct performance of the resource management algorithms. So the work performed with these mechanisms is also reported.

Beyond the introduction, the rest of the document is structured as follows. A Literature Review is first provided in section 2, related to the topics covered here. Next, a global view of the Wi-5 architecture is presented, including Smart Access Point Solutions, and also Cooperative Functionalities. Section 4 is devoted to explaining the functionalities enabling all the Wi-5 features, with additional information about the implementation status of each of them. The approach selected, based on Light Virtual Access

Points, is explained in detail, also reporting its limitations for accomplishing the Wi-5 objectives. Next, information regarding the monitoring solutions is provided, including the study of the tools that can provide a timely detection of real-time services. The tools enabling radio resource management are then reported, including the functionalities added (as long as those to be added in the future) in order to support the desired functionalities in a WLAN. Finally, a study about the savings that can be achieved by means of packet grouping is provided, including the comparison between Layer 2 and Layer 3 aggregation. This includes an analytical and a real-traffic test performed in Unizar labs. The document ends with a Conclusion in section 5.

1.3 Relationship to other deliverables

The five use cases and their requirements are reported in **Deliverable 2.3**, including the different scenarios, the applications and the services considered. The functionalities included in the present document will be in charge of enabling the accomplishment of these requirements.

The initial Wi-5 architecture is presented in **Deliverable 2.4**, which provides a global view of the whole set of solutions being deployed, including the Smart AP Solutions explained in the present deliverable. The architecture is described according to the ISO-IEC-IEEE 42010 standard, and the requirements are presented in the context of the business and stakeholders' requirements.

The Cooperative Functionalities, being deployed in WP4, are explained in detail in **Deliverable 4.1 "Specification of Cooperative Access Points Functionalities".** These functionalities are tightly related with the Smart AP Solutions, since they have to run in an integrated and seamless way, in order to provide the desired performance.

2 Literature Review

2.1 Use of Virtual Wi-Fi APs in Software-Defined Wireless Networks (SDWNs)

The SDN (Software-Defined Networking) concept aims to separate the network control and data plane, allowing an abstraction of the underlying technology for applications and services. It is becoming more and more popular, since it provides a coordinated programmable interface for network managers. In combination with NFV (Network Function Virtualisation), this concept is gaining acceptance not only in wired networks, but also in wireless environments [1].

Different high-level languages have been proposed for SDNs [2], [3], but they are mainly designed for wired networks based on the OpenFlow protocol [4] for data plane control. However, [5] surveyed a set of abstractions for wireless networks, as OpenFlow does not itself capture all the issues appearing in wireless scenarios. For example, the "flow" abstraction proposed by OpenFlow does not reflect the stochastic nature of wireless links (which are very different from an Ethernet connection), so it does not suffice for network management in wireless environments.

One of these abstractions is the concept of the *Light Virtual Access Point* (LVAP), which was first proposed in [6]. It assumes that there is a central controller, to which all the APs are connected. The controller creates an LVAP for each terminal, which is dynamically assigned to the physical AP where the terminal is located at each moment. Therefore, the AP will use a different LVAP (which includes a specific MAC) for communicating with each terminal. So the terminal will only "see" a single AP, even if it is actually moving between them, thus avoiding the need for re-association (see Figure 1). In [7], a solution also based on LVAPs was presented, which is able to perform very fast handoffs between different APs controlled by a single entity. An open-source implementation (called *Odin)* was also developed.

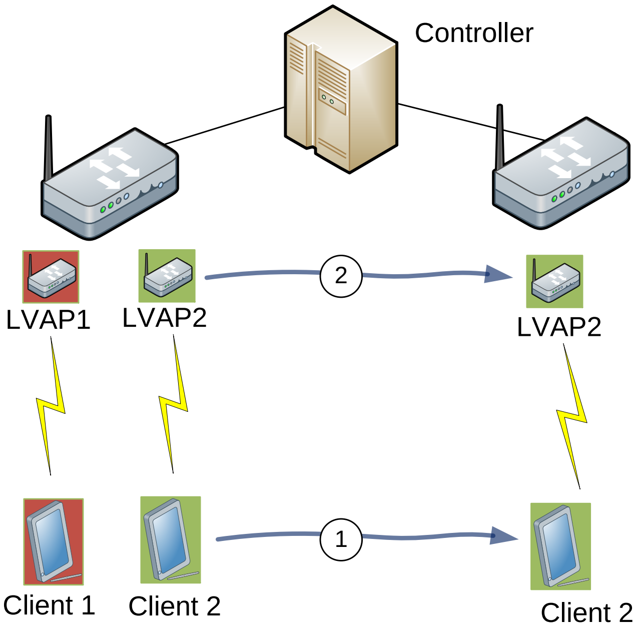


Figure 1: Scheme of a Wi-Fi network using LVAPs

In [8] the concept of *Multichannel Virtual Access Point* was introduced, adding to the LVAP the possibility of using different channels. This allows a STA to change its AP and channel at the same time, synchronising both events. The article proposed a protocol for the exchange of information between APs. For that aim, they used the *CSA (Channel Switch Announcement)* element in an 802.11 beacon. This message makes all the STAs associated to an AP move to a specific channel.

2.2 Monitoring the Wireless Environment in SDWNs

The 802.11 standard establishes some time intervals and approaches for a client to scan nearby APs. A passive scan can be used, in which the station just sets the desired channel, and waits for the reception of beacons from APs. In contrast, active scanning consists of sending a probe request, and waiting for a probe response from an AP [9].

In wireless scenarios where APs are distributed in different channels according to a central planning approach (e.g. airport, business centre), if an STA moves away from the AP it is associated with, it will not be detected by APs in the neighbourhood, since they will be on other channels. Therefore, periodic scanning should be performed for detecting STAs approaching. The use of multichannel LVAPs in SDWNs also makes it necessary to establish some periods for scanning on other channels in order to detect new clients. In [10] an optimisation method of the scanning period was proposed by making an active scanning only when needed, instead of using PBS (Periodic Background Scan) which results in a significant overhead.

2.3 Service Detection

Considerable research effort has been put on automated and real-time classification of IP traffic in recent years. This enables the seamless integration of QoS, since the detection of a service allows operators to more easily associate it with some quality requirements. For example, in [11], an automated system for QoS control was proposed for an application with tight real-time requirements (e.g. an online game). Another use of automatic detection is the prevention of intrusions, which was first proposed in [12].

Detection of flows can be made on a high level based on UDP or TCP port numbers, but this can present some problems: for example, some applications may employ different ports, and some regulations may even prohibit the inspection of the content of the packets. Statistical classification is also being used based on features of the flows, such as packet size or inter-packet time patterns. Combined with machine-learning techniques, this can present many advantages. The approach here include two stages: first, the algorithm has to be trained and then the devised rules can be employed for performing the classification. A number of proposals based on different algorithms have been presented for this. In [13], traffic with similar observable properties was clustered into different application types. The algorithm was therefore able to separate traffic into a small number of basic classes. In [14], the nearest neighbours were used, and Linear/Quadratic Discriminant Analysis ML algorithms were employed to map different network applications to predetermined QoS traffic classes. [15] used an unsupervised Bayesian classifier to find the best cluster set from the training data and a number of applications were studied, showing that some separation between them could be achieved.

In [16] a tool able to identify real-time traffic patterns was presented. It was employed for the unsupervised detection of real-time services with tight delay requirements (online games), obtaining a high accuracy of about 90%. It used the concepts of *recall* (percentage of members of a class correctly classified as belonging to that class among all members of the class) and *precision* (percentage of those instances that truly belong to a class among all those classified as belonging to that class).

2.4 Resource Management in Wi-Fi WLANs

Radio resource management (RRM) approaches aim to design the appropriate strategies and algorithms for configuring wireless transmission parameters in order to efficiently utilize the limited radio resources. In the context of Wi-Fi networks, RRM techniques, as identified by the Wi-5 project, should focus on configuring an appropriate channel selection, performing dynamic transmit power adjustment and providing load balancing strategies.

In order to tackle these issues, RRM usually requires the deployment of new functionalities in both the operators' and the users' equipment. In contrast, the radio resource management features proposed in the Wi-5 project are to be implemented on the operator's Access Point equipment only, and on top of the existing PHY and MAC Wi-Fi layers (802.11ac [17] in the 5 GHz band and 802.11n [18] in the 2.4 GHz band). For this purpose, the features of the 802.11h [19] and 802.11k [20] amendments to the standard can be leveraged. In order to comply with the ETSI regulations [21] and limitations on transmitted power in a given region, IEEE 802.11h defines two mechanisms on top of 802.11 MAC and 802.11a PHY layers, namely Dynamic Frequency Selection (DFS), and Transmit Power Control (TPC). The original purpose of these two mechanisms was to extend 802.11 operation in the 5 GHz band to support coexistence with the band's primary users, radar and satellite systems. However, both of them have numerous other applications in the context of more efficient radio resource management [22], which aligns well with Wi-5 interests. Some useful mechanisms to achieve this, such as a transmit power reporting mechanism between an AP and the associated stations or a channel switch announcement frame to advertise a channel switch to the associated station, are defined in the amendment. In addition, the radio resource measurement procedures described in 802.11k complement these functionalities with the required radio monitoring interface.

Nevertheless, although 802.11h defines protocols for DFS and TPC, it does not cover the implementations themselves. The defined rules and functions leave the way open for free implementations of both power control and dynamic channel selection mechanisms in WLAN devices.

As stated above, the RRM solutions in Wi-5 focus on three main issues: smart channel selection, dynamic transmit power control and load balancing. A literature review of these functionalities is provided hereafter. In the Wi-5 project, these functionalities aim at operating in scenarios where a large number of uncoordinated APs operate simultaneously to ensure more efficient resource reuse for the communication between APs and terminals. The aim of the proposed Wi-5 architecture is to present an over-the-top implementation to interact with neighbouring APs, which jointly performs these three features, to find the best overall configuration, thus minimising interference in a heterogeneous environment. SDN approaches are becoming popular in wireless environments. In [23] the authors used SDN and cloud computing to manage interference in Cognitive Radio Network deployments in residential areas. Wi-5 will also rely on the use of SDNs in order to achieve its goals.

2.4.1 Smart channel selection

Due to the limited number of orthogonal channels the 802.11 standard supports, high levels of interference are expected, which in the end will lead to a reduction in network efficiency and therefore in the Quality of Experience (QoE). In this context, in recent years several channel assignment schemes for infrastructure-based WLANs have been proposed. A comprehensive survey can be found in Chieochan *et al*. [24]. Most of these works propose centralised algorithms that assume there is a network that belongs to one administrative domain [25], [26], [27], [28], [29]. However, in most situations this is not the case for WLANs, which continuously evolve, generating heterogeneous scenarios where multiple WLANs are deployed by different owners and Wi-Fi access providers. In this scenario, channel assignment algorithms, where APs can be configured to manage their operating channels and their transmitted power level to minimise interference with adjacent APs, would be required. In this context, Least Congested Channel Search (LCCS) is a common feature provided by commercial APs [30] for channel auto-configuration. With LCCS each AP scans all available channels, listens to the beacons transmitted by neighbouring APs and chooses the channel used by the least number of associated devices as its operating channel. This basic mechanism suffers from the hidden interference problem (an AP not listening to another AP, but suffering interference from a client associated with that AP) and it does not take into account the traffic patterns of the devices, but only the quantity of devices. Other mechanisms trying to improve the performance of LCCS in an uncoordinated scenario have been proposed and evaluated through simulation [31], [32], [33]. In [34], a game-theoretic framework was utilised to construct a joint transmission power control and dynamic channel assignment scheme which reduces the total overlap area, thus reducing interference.

In [35] the authors introduce a channel assignment solution that exploits the gain of using partially overlapping channels relying on the Signal to Interference plus Noise Ratio (SINR) interference model, which considers the accumulative interference of the environment from the receiver point of view. They first analyse the relationship between network throughput and channel assignment by using partially overlapping channels in SINR interference model. Then, they propose a heuristic algorithm in order to assign overlapping channels to the APs in the system such that the network throughput can be maximized. The aforementioned studies exemplify the solutions with an overall network interference indicator set to be tracked that guides the assignment of the channels. The channels are also assumed to have predefined characteristics. In some other approaches the channel characteristics are considered to be dynamic. They are set to be adjusted locally to gain a desired impact on the network as well as meeting their local service quality [36]. Although the channel assignment solutions are proposed specifically for WLAN and Wi-Fi networks, they are not necessarily suitable for all new emerging and diverse use cases of these networks. Subsequently, more recent studies tend to provide solutions explicitly proposed for specific use cases such as high density networks [37] and areas with uncoordinated interfering network elements [38] which are among the most challenging contemporary deployments of Wi-Fi networks.

2.4.2 Dynamic transmit power control

In addition to channel selection, transmission power control algorithms are also critically important in any wireless system. These mechanisms are commonly applied in cellular systems (GSM, IS-95 CDMA, 3G-W-CDMA, LTE) in order to ameliorate the near-far problem and minimise the interference to/from other cells and therefore improve the wireless systems' performance. However, in the context of WLAN networks, devices typically transmit at their highest RF output power. This generates high levels of interference on the same channel, increasing the probability of packet collisions, and makes more neighbouring transmitters defer their frames, thus reducing the overall throughput of the network. Because of these drawbacks, in recent years adaptive transmit power control methods have been proposed for 802.11 trying to reduce interference and improve spatial reuse in order to increase network capacity.

One of these methods is MiSer (Minimum-energy transmission Strategy) [39], an algorithm based on the link-quality estimation scheme defined for TPC in IEEE 802.11h. The WLAN station (STA) estimates the path loss between itself and the transmitter, updates the data transmission status, and then selects the proper transmission rate and transmit power for the current data transmission attempt using a simple table look-up. The lower the transmit power or the higher the PHY rate (hence, the shorter the transmission time), the less energy is consumed in one single transmission attempt. However, this also increases the likelihood of transmission failures, thus causing re-transmissions and eventually consuming more energy. The key point of MiSer is to combine TPC with PHY rate adaptation and pre-establish a rate-power combination table. At runtime, a wireless station determines the best transmit power as well as the PHY rate for each data transmission attempt based on the rate-power combination table. MiSer relies on communication between the clients and AP in order to complete the table data, and hence the appropriate software must be running on both the AP and client stations in order for the technique to be used.

Another option is to use Contour-Slotted power control management [40]. Its main goal is the minimisation of the interference level when different APs and WLANs are working in the same area. The algorithm defines a controlled WLAN communication scheme where APs on different WLANs are synchronised in order to avoid asymmetric links. At any instant of time, all APs in the network operate at the same power level to avoid link asymmetry. Over time, by using different power levels, the system achieves per-client power control to maximise spatial reuse. Each AP can transmit to each of its clients at the lowest power level that minimises the interference to other APs' communications, while not affecting the performance perceived by the client. However Contour also needs GPS synchronisation, which is an important weakness for indoor deployments.

Symphony [41] considers a combination of power level control and rate adjustment for meeting the link quality requirements. Rate selection in WLANs is determined by an estimation of the channel conditions including packet loss, delivery ratio, throughput, or SINR estimation. Rate selection and transmit power control are tied together, since power control without considering the rate can reduce the SINR, leading to a reduction in the rate and hence the link and network throughput. Symphony considers the above problem and does not compromise the required rate.

2.4.3 Load balancing

Since STAs independently select the APs to connect to, the traffic in WLAN networks can be unevenly distributed, which leads to inefficient use of the available resources. Load balancing techniques try to solve this problem by better distributing the traffic load in the network. In [42] a survey of both network- and wireless-station-based solutions is presented. For example, Papanikos and Logothetis [43] apply a combined metric consisting of the number of stations associated, and mean and instantaneous RSSI for each of the clients associated with this AP. A similar AP-assisted approach has been proposed by Cisco [44], to give associated client information about the load through beacons. Both these solutions require modifications on the client side. Murty *et al*. [45], and Chandra and Bahl [46], achieve fair load balancing between APs through a centralised management approach that aggregates AP workload, which requires changes in the wireless network infrastructure.

2.5 Packet/Frame Grouping at Different Layers

An inherent characteristic of packet-switched networks is the need for a number of headers, which are added to the payload in order to make it possible to transport the data from the source to the destination. This overhead is not a problem when the payload is big, but the inefficiency caused by payloads in the order of tens of bytes may become excessive in certain scenarios with limited resources.

However, small packets are ubiquitous in nowadays' networks. The first example, and perhaps the most evident one, are TCP Acknowledgements, which are required by the traffic control mechanisms inherent to this protocol at Layer 4. These packets do not usually carry any payload, so they can be considered as 100% overhead packets. However, they are carried by the network in the same way as any other packet. In addition, emerging real-time services (e.g. VoIP, online games) also send high rates of small packets, required to enable the interactivity level demanded by the end users. Finally, small packets may also be present in Machine to Machine and IoT scenarios with limited network and energy resources.

In order to illustrate the problem of small packets, Figure 2 presents the packet-size histogram of a real traffic trace from The *CAIDA Anonymized Internet Traces* 2015 Dataset [47] (only the first 200,000 packets have been used). This trace was captured at a backbone link (10 GigE) of a Tier1 ISP between Chicago and Seattle. As can be observed, 44% of the packets are big, i.e. their size is near 1500 bytes, which corresponds to the Maximum Transmission Unit (MTU). At the same time, a high number of small packets are also present: 33.4% of packets are 60 bytes or smaller, and 41.4% overall are 200 bytes or smaller.

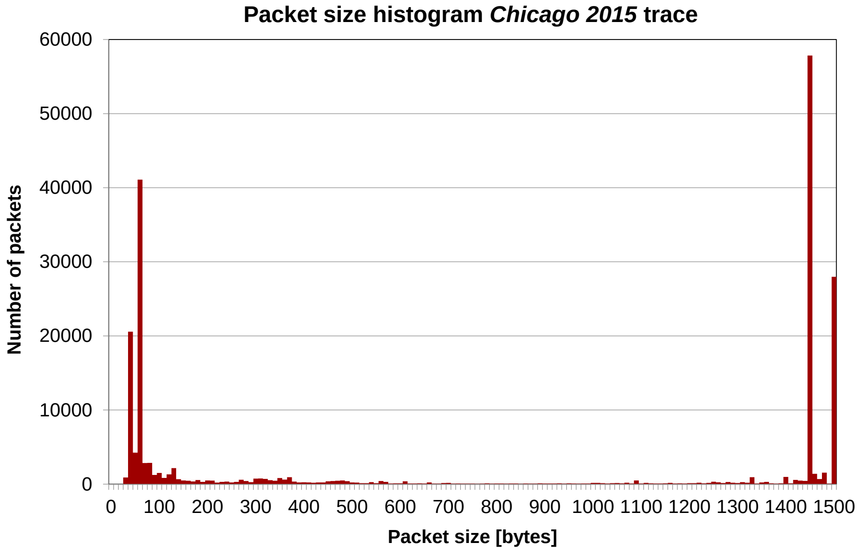


Figure 2: Packet size histogram of a traffic trace obtained in a backbone link

The presence of these amounts of small packets has some drawbacks: first, the overhead drawback, i.e. the amount of header bytes required for sending a small payload is high. For example, a VoIP packet carrying 20 bytes requires at least 40 bytes corresponding to IP, UDP and RTP headers. Second, when a small packet is passed to Layer 2, the Media Access Control (MAC) mechanisms make it necessary to define a number of waiting intervals until a host gets the channel (see Figure 3, where the 802.11 MAC mechanism is illustrated). CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is the mechanism employed in 802.11. This delay may be negligible in Ethernet (a preamble, a header and an inter-packet gap are required), but it may become significant when packets are using a wireless technology such as 802.11.

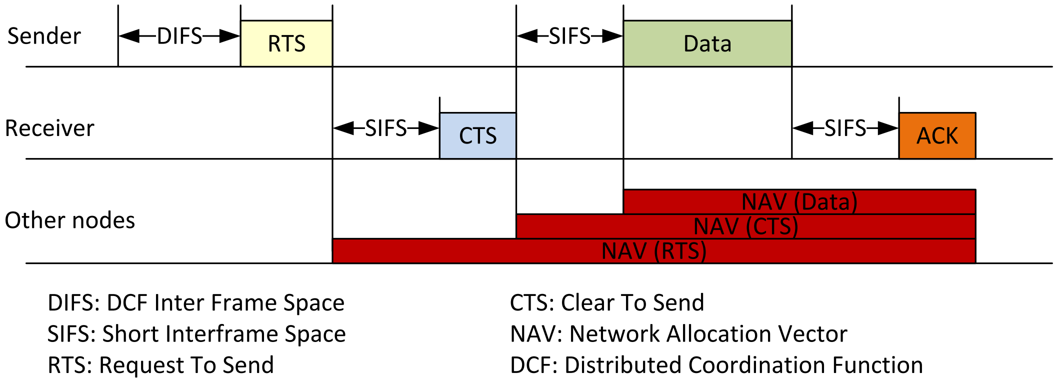

Sender
DIFS
RTS
SIFS
Data
Receiver
SIFS
CTS
SIFS
ACK
Other nodes
NAV (Data)
NAV (CTS)
NAV (RTS)
DIFS: DCF Inter Frame Space
SIFS: Short Interframe Space
RTS: Request To Send
CTS: Clear To Send
NAV: Network Allocation Vector
DCF: Distributed Coordination Function

Figure 3: Scheme of the Wi-Fi CSMA/CA procedure

In wireless networks MAC mechanisms also reduce efficiency, which is exacerbated for small packets. In Figure 4, we have used the model developed in [48] in order to build the graphs of the efficiency (defined as the quotient of data rate and PHY rate), when UDP and TCP packets of different sizes are sent following the 802.11 standard. It can be observed that the efficiency is lowest when small packets (some tens of bytes) are sent, since the time required for medium access is in the same order of magnitude as the time required for the actual transmission of the data.

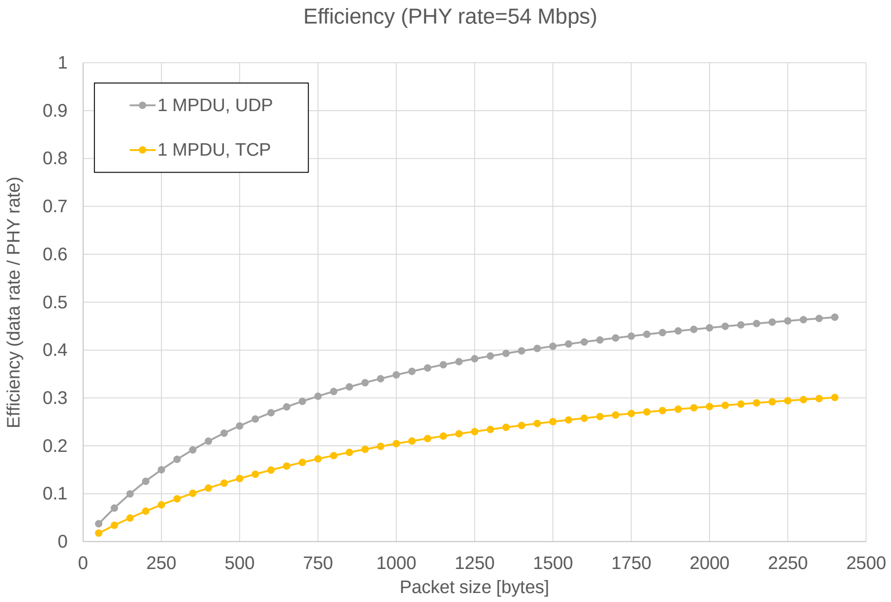


Figure 4: Efficiency of 802.11 for UDP and TCP, as a function of packet size

There is another drawback related to the limited processing capacity of the machines managing the packets. Datasheets of commercial devices often report the performance both in terms of bandwidth and packets per second. For example, a commercial 50-Port switch [49] has *"13.6 Gbps switching capacity, 10.1 million pps".* This means that, for 100-byte packets, the throughput of the switch would in fact be limited to 8.08 Gbps. Something similar happens with Layer 3 packet routing: the so-called "64 Byte Throughput" has become a figure of merit, and specific features are being added to processors and network interfaces in order to improve the way they manage these small packets [50]. This would reflect the processing drawback of small packets.

Other hardware drawbacks may also appear: for example, the energy consumed by a router is expected to rise not only with the generated and received throughput, but also with the amount of packets per second it is managing. According to [51], internal packet processing engines and switching fabric require 60% and 18% of the power consumption of high-end routers respectively.

In this context, the aggregation (multiplexing) of a number of small packets to form a single and bigger one can be seen as a means to jointly overcome these drawbacks. Some initiatives aimed to increase the average size of the Internet packets are already in place. For example, Ethernet Jumbo Frames, with an MTU of 9000 bytes instead of 1500, present some advantages in terms of throughput, and even in the TCP window growth speed [52]. Furthermore, in Wi-Fi networks, frame aggregation was added as an option to 802.11n, and it is compulsory in 802.11ac. We will now explore these in more detail.

2.5.1 Packet/Frame grouping standards

The aim of multiplexing is to save bandwidth (i.e. minimizing the overhead drawback) and to reduce the amount of packets per second (i.e. improving the airtime efficiency in wireless networks). Although it can be deployed in Layer 2 or in upper layers, there are some differences between these two possibilities. If frames are multiplexed at Layer 2, they will traverse a single link together, and then they will be de-aggregated. If the common path includes a number of links, a demux-mux process will be required at each node. However, if multiplexing is deployed at the upper levels, packets can travel together during the whole path, thus reducing the processing drawback, at the cost of adding a tunnelling header which allows end-to-end delivery.

a) Layer 2 Aggregation Standards

Regarding Layer 2, two frame multiplexing policies are included in 802.11n (and subsequent versions), namely MAC Service Data Unit aggregation (A-MSDU) and MAC Protocol Data Unit aggregation (A-MPDU). Aggregation has become even more important in 802.11ac, where all the frames must have an A-MPDU format, even if they include a single sub-frame. The former allows multiple MSDUs to be sent to the same receiver, as a single MPDU. The latter is able to join a number of MPDU sub frames sharing a single leading PHY header. The main difference is that A-MPDU works after the MAC header encapsulation. This has two advantages: a higher bandwidth reduction, and the fact that each sub-frame includes its own CRC, which avoids the need for discarding the whole frame because of an error in a single sub-frame: if a sub-frame is wrong, only that one will be retransmitted.

A number of research works have studied the achievable savings when using 802.11 aggregation. In [48], the authors presented an analytic model for estimating the improvements of A-MPDU and A-MSDU. Their findings showed a significant efficiency increase, and a better performance of A-MPDU, which was stressed when packet-error rate was high. In [53] a scheduler for selecting the packets to be multiplexed together was proposed, taking into account that the 802.11 standard only specifies the frame format, but scheduling schemes are left as the vendor’s choice. An optimal frame size was calculated, and packets were grouped trying to fit this size. In [54], the number of aggregated sub-MAC protocol data units is optimised and adjusted dynamically according to the sub-frame size, the maximum aggregation level allowed and the real-time channel bit-error-rate, thus increasing the throughput.

b) Layer 3 Aggregation Standards

Different standard protocols for multiplexing packets at higher layers do exist. First, TMux [55] was approved as RFC1692 in 1994 to include a number of transport-level payloads (mainly TCP) into a single packet. This protocol is therefore limited to multiplexing packets traveling between the same pair of machines. Here, mini-headers of 4 bytes are inserted before each of the multiplexed headers.

Another IETF multiplexing protocol is PPPMux [56], an extension of PPP (Point to Point Protocol) allowing the inclusion of a number of packets into a single frame. This protocol permits hosts to multiplex whole packets. However, when packets have to travel over an IP network, the use of L2TP (Layer 2 Tunnelling Protocol) is necessary, as it happened in TCRTP (Tunnelling Compressed RTP) [57], which combined header compression with multiplexing and tunnelling, in order to optimize VoIP RTP flows.

Multiplexing at higher layers has been studied in some works: [58] and [59] presented different proposals for VoIP optimisation, trying to keep a good voice quality. The adaptation of TCRTP for other real-time services such as online games has also been proposed [60].

Aggregation has also been proposed in SDNs: relying on the flow identifier of OpenFlow, many of the fields that are repeated in all the packets of a flow can be avoided, and a number of packets can also be aggregated [61].

2.6 Wi-5 innovation objectives

In summary, we have identified a number of gaps in the existing work that can be addressed by the Wi-5 objectives. For example, a good integration of LVAPs with multichannel in a centralised scheme would be convenient, since the solutions here consider that all the APs are in the same channel, which is not compatible with frequency planning.

Another field where Wi-5 has to present innovative results is the scanning of the wireless environment, with the aim of finding potential STAs approaching the AP. A trade-off appears: if the scanning time is high, a better precision will be achieved, but the time devoted to transmitting information of the STAs already associated will be reduced.

Regarding packet grouping, new research will be required in order to match the frame aggregation policy (mainly in terms of added delay) with the requirements of each of the applications present in the WLAN. The special focus of Wi-5 on real-time services, with very tight real-time requirements, will make it convenient to develop scheduling policies which respect these latency limits, but at the same time maximise the throughput of non real-time flows (e.g. file downloads). In addition, these scheduling policies have to be centrally coordinated between all the APs.

Finally, we have seen that scalability issues may appear when running resource management algorithms, taking into account that the decisions will be made by a central controller and that signalling traffic (e.g. monitoring, power control) in the wireless network has to be limited. Something similar will happen in the wired network connecting the APs and the controller, where the signalling traffic should not interfere with data traffic generated by the clients. The required processing capacity will also have to be taken into account, as low-cost APs with limited capabilities are being used. This could also be a limitation in the central controller, depending on the number of APs it is managing.

3 Global view of the Wi-5 Architecture

In this section we provide a global view of the Wi-5 architecture. A more detailed view of this has been presented in **Deliverable 2.4** ***"Wi-5 Initial Architecture".***

The initial design of the Wi-5 architecture relies on the separation of control and data planes in Wi-Fi APs based on the SDN approach. We have followed this approach in order to have a single point where all the control operations can be integrated. The most important entity is the Wi-5 controller, having a global view of the network, and being able to run different algorithms for optimising the network traffic.

A Software Defined Network approach, relying on OpenFlow [4] protocol is being used, so the Wi-5 controller runs within an OpenFlow controller. Therefore, certain functionalities (e.g. load balancing, channel selection) can run as applications on top of the controller (see Figure 5).

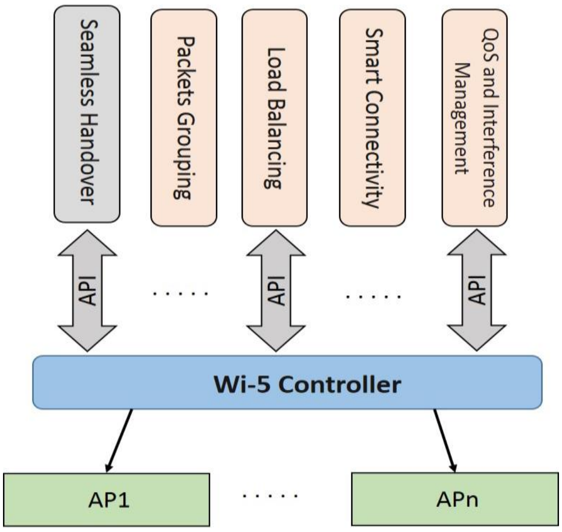


Figure 5: Scheme of the Wi-5 architecture design

In order to make it possible for the controller to manage all the APs, new functionalities have to be included on each of them, i.e. their internal switch must become an OpenFlow switch, and a Wi-5 agent will be added in order to interact with the Wi-5 controller. Something similar also has to be done with the OpenFlow controller, where new functionalities must be added in order to interface with the Wi-5 functionalities. In Figure 6 a scheme of the Wi-5 entities is shown, including the solutions, the controller and the APs.

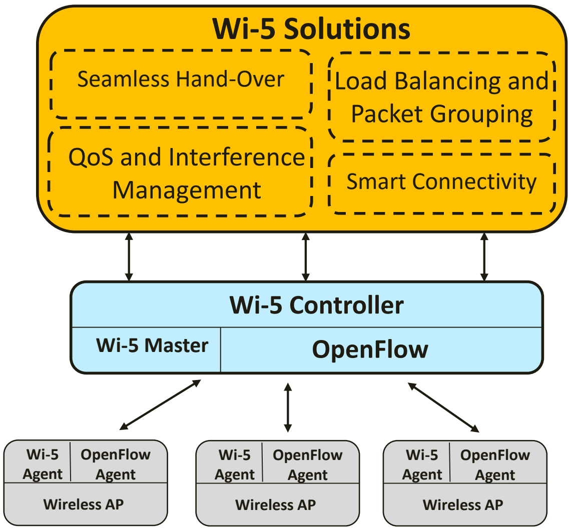


Figure 6: Scheme of the Wi-5 entities

One of the aims of the Wi-5 Project is to make it possible for a set of APs to support real-time applications (e.g. VoIP, online games) with quality. This includes resource management algorithms that take into account the nature of each flow, and its coexistence with other services. In addition, seamless handovers between APs are not only required for supporting user mobility, but also for the optimisation of radio resources. The use of Light Virtual APs (LVAPs) implementing a virtual Wi-Fi network (see Figure 7) enables seamless handovers [48], which may be acceptable even for users of real-time applications.

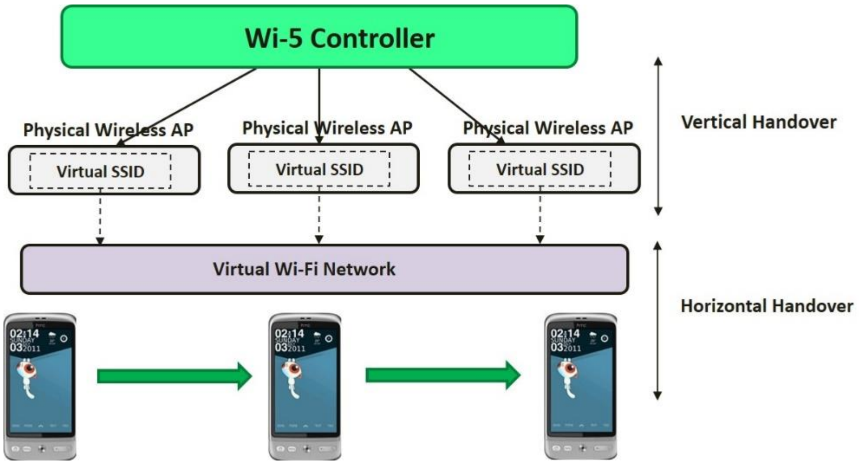


Figure 7: Seamless Handover using Wi-5 Architecture

The Wi-5 functionalities can be divided into two categories:

- Smart Access Point Solutions, aimed to enable the improvement of Wi-Fi networks by means of radio configuration capabilities and resource management algorithms, including dynamic channel allocation, load balancing and power control. The use of packet grouping is also considered here. These functionalities consider a scenario where all the APs are managed by a controller.

- Cooperative Access Point Functionalities will enable cooperation between Wi-Fi networks under different management authorities, in cooperation with the smart access point solutions. These functionalities improve interference management in *Wi-Fi jungle* scenarios (i.e. including a high number of devices in the same zone), and the realisation of seamless soft and hard handover.

3.1 Smart Access Point Solutions

This subsection provides a brief summary of the solutions which will be explained in more detail in Section 4. The Wi-5 Smart Access Point Solutions are a set of improvements being developed in WP3 considering a centralised cooperation between APs. As shown in Figure 8, a number of APs are connected to a central controller using a wired network as a backhaul. This controller is able to manage the radio parameters of the APs, and perform load balancing of users. The power of the signal can also be controlled by the AP, in order to reduce the interference level and to save energy. Monitoring elements are also placed in every AP, which will report the status of the network to the controller.

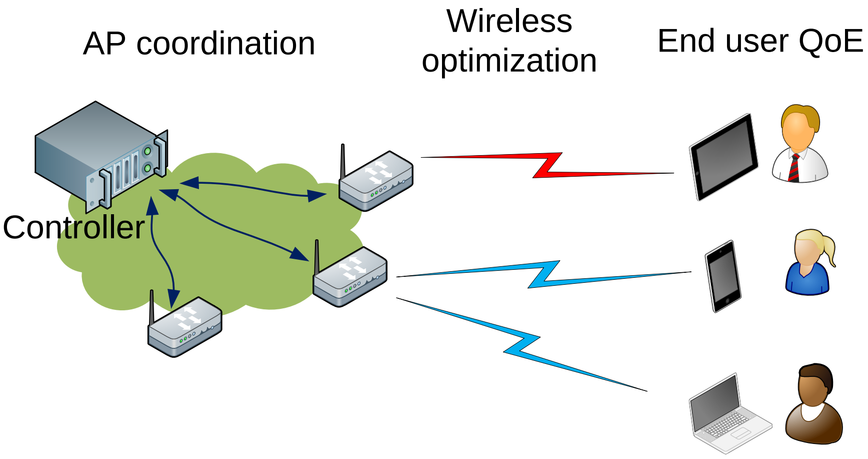


Figure 8: Basic scheme of the smart APs architecture

The functionalities can be summarised as:

- Performance monitoring, including two different things: firstly, an automatic detection feature has to be added in order to identify those flows with real-time requirements. Secondly, the radio environment has to be scanned in order to have accurate information about the interference level on each channel, the power being sent by the STA, etc.
- Radio Resource Management. This includes mechanisms allowing a good performance of the algorithms being deployed in the Wi-5 architecture: (i) Dynamic Channel Allocation, looking for an optimal distribution of the channels of the APs, in order to reduce the interference; (ii) Load Balancing, looking for an optimal distribution of the users between the APs; (iii) Power Control, trying to keep the level signal as low as possible, in order to save energy and to reduce the interference.
- Packet grouping, considering smart scheduling policies enabling a better use of the aggregation policies already included in 802.11n and subsequent versions. This would alleviate the airtime inefficiency caused by the STAs requesting the shared channel before being able to send actual data. For legacy devices not including aggregation at Layer 2, multiplexing packets at Layer 3 can also be a solution.

3.2 Cooperative Functionalities

This section introduces the first version of the algorithms designed to efficiently exploit the use of the radio resource, reducing interference between neighbouring APs and providing optimised connectivity for each user/flow that is served by an AP in the considered scenarios. A more detailed explanation of the developed algorithms has been included in **Deliverable 4.1** ***"Specification of Cooperative Access Points Functionalities version 1".*** Specifically, different algorithms have been designed with the aim of achieving the following purposes:

- Defining an optimised channel assignment procedure which will reduce the radio interference throughout the WiFi network.
- Defining a transmit power control mechanism which will help achieving the user's required quality, maintaining the acceptable level of interference in the network and providing a tool for energy saving.
- Defining a smart allocation procedure that will assist users/flows in selecting the most suitable AP according to the application running on the station in terms of Quality of Service (QoS) requirements. Moreover, the allocation of the APs will aim at providing satisfactory performance to both, an individual user/flow and the overall Wi-Fi network.

3.2.1 Access Point Channel Assignment Algorithm

The AP channel assignment algorithm allows the controller to select the channels for the different APs in a network based on the Wi-Fi properties (e.g. IEEE 802.11's standard channel characteristics), the actual network topology (i.e. AP distribution throughout the network) and the desired resource management criteria (e.g. the assigned channels, interference related QoS or handover requirements). This solution will be implemented in the Wi-5 controller; therefore, it is assumed that the configuration management is provided through a central control entity with the capability of monitoring and acquiring the status of the network. The configuration adjustments per user/flow or group of users/flows will be processed and applied in a network of APs.

3.2.2 Smart Connectivity Algorithm based on the Fittingness Factor

The Smart Connectivity algorithm based on the Fittingness Factor (FF) is a solution that will be implemented in the Wi-5 controller in charge of associating an AP to each new user/flow taking into consideration the bit rate requirements. It relies on the *reward* concept that inherently considers heterogeneity of the requirements for the different stations accessing the network, so that not all the APs are equally appropriate for all the users/flows depending on the application needs. Several possible definitions of the reward metric may exist, such as sigmoid[1] functions, linear functions, and FF. In our case, the reward function will be based on the FF concept developed starting from the formulation defined in [62].

3.2.3 Monitoring Tools and Radio Configuration

The functional blocks defined in the Wi-5 architecture which will implement the AP channel assignment and the Smart Connectivity algorithm are illustrated in Figure 9. These are: (i) *QoS and Interference Management* block, which will be in charge of implementing the AP channel assignment algorithm; (ii)

[1] A sigmoid function is a bounded differentiable real function that is defined for all real input values and has a positive derivative at each point.

Smart Connectivity block, which will be in charge of executing the Smart Connectivity algorithm based on the FF when required.

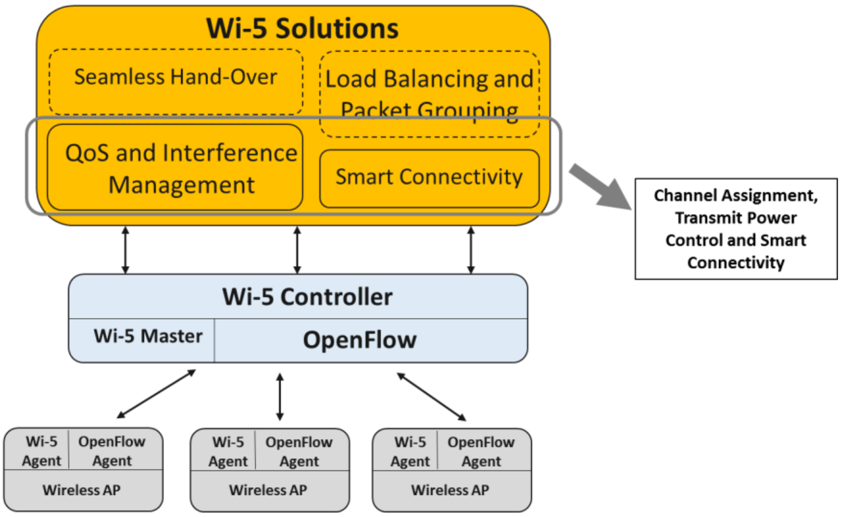


Figure 9: Entities in charge of AP channel assignment and FF-based reward algorithms

In order to allow the correct deployment of the *QoS and Interference Management* and *Smart Connectivity* functionalities, a set of monitoring tools has to be included on the Wi-5 APs and on the Wi-5 controller. The role of these tools is to provide information on: (i) the interference level sensed from each AP at the available channels in the considered frequency bands; (ii) the number of users/flows associated with each AP; (iii) automatic identification of different kinds of user services in terms of bit rate requirements (e.g. a combined PHY and MAC layers process at the APs). These monitoring mechanisms will be helpful during the decision-making process at the Wi-5 controller. They also contribute to the optimal AP channel assignment and the smart AP allocation to each new user/flow joining the network.

Monitoring of the interference levels will support the *QoS and Interference Management* block during the initialisation of the Wi-Fi network or during a possible reassignment of the channels due to a change of status in the network. This algorithm will provide the Wi-5 agents with the channel allocated to each AP. Moreover, this block will share information on the interference levels with the *Smart Connectivity* block during the AP allocation procedure to support smart AP allocation when a new user/flow tries to join the network. The result of this algorithm may trigger a reconfiguration of a certain AP's transmit power, and it will again provide the Wi-5 agent in the allocated AP with the appropriate radio configuration parameters, as illustrated in Figure 10.

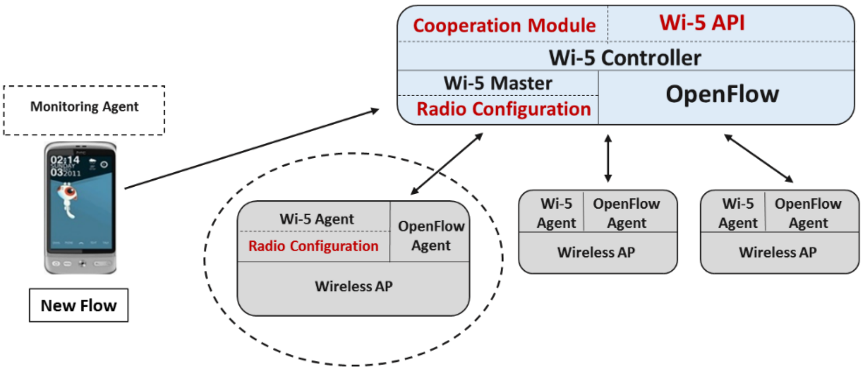


Figure 10: Radio configuration procedures

4 First definition of the Wi-5 Smart Access Point Solutions

The Wi-5 architecture includes a series of improvements for AP cooperation (be it intra or inter-operator). Therefore, a number of functionalities and procedures have to be defined in WP3 in order to enable the different optimisations considered to be enforced. These functionalities will be exploited by the radio resource management algorithms, and also in the cooperative functionalities summarized earlier and detailed in **Deliverable 4.1** ***"Specification of Cooperative Access Points Functionalities version 1***."

The existence of an entity accessible to all the APs, and the monitoring of the traffic being managed by each of them, allows a centralised coordination of the Wi-Fi channel used by each AP, and to perform load balancing and power control between adjacent APs. Finally, the possibility of grouping packets between the AP and the end device, according to the type of service reported by the monitoring element, is being developed here.

This section details the current design and definition of these features. As outlined in the literature review, the use of Light Virtual APs (LVAPs) is seen as an interesting way of supporting seamless handovers and is therefore a good option when implementing resource management in Wi-Fi WLANs. This is the reason why we have decided to follow this approach. In addition, a lab implementation is being built from the beginning of the Project, integrating this concept as a proof of concept, thus allowing us to test if the solution is adequate and enables all the desired functionalities.

The content of this section can be summarised as the definition and first results of the lab implementation of:

- The description of the **approach taken for the implementation**: It is based on an SDN approach, and it relies on LVAPs including an OpenFlow switch on each of the Wi-Fi APs. We have selected Odin [7], as it is a LVAP solution based on common and open platforms (OpenFlow, OpenWRT, etc.) and therefore it is broadly applicable.
- **Monitoring**: This functionality will allow Wi-5 to gather information about the state of the Wi-Fi network, its environment, operational parameters, and performance.
- **Dynamic Channel Selection and Transmit Power Control**: This functionality will enable Wi-Fi networks to dynamically adjust the radio configuration, including changing the transmission channel within the network and the transmit power between an AP and a wireless device.
- **Load Balancing**: This functionality will enable Wi-Fi networks to make decisions on when not to accept new association requests, and to decide the AP to which each STA is associated, with the aim of maximising the aggregate data rate of these networks.
- **Packet Grouping**: This functionality will enable packet grouping between the Wi-Fi AP and the wireless device which should result in a significant overhead reduction and bandwidth and energy savings.

Figure 11 where the Wi-5 entities are implemented and how they interact with the rest of the architecture. As we will see, monitoring functionalities will in principle run in the Wi-5 Agent included in each AP, but a centralised approach is also being considered for detecting the kind of application. Decisions about resource management (channel selection, power control and load balancing) and packet grouping will also be done in the central controller and applied in the AP.

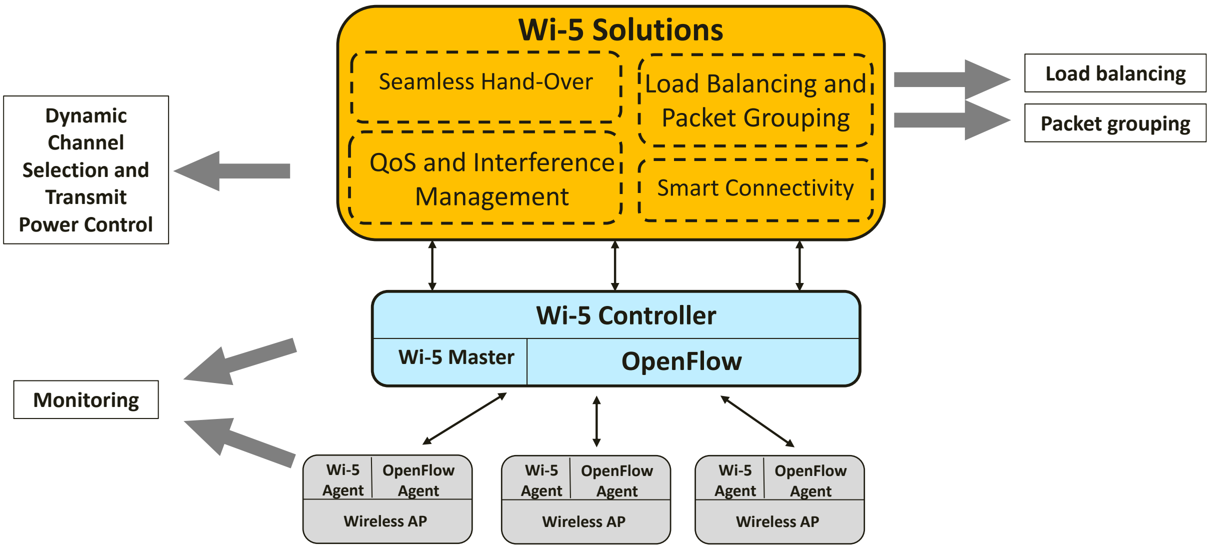


Figure 11: Scheme of the Wi-5 entities

4.1 Approach taken: Light Virtual APs for Wi-Fi coordination

Odin [7] has been selected for the implementation of the Wi-5 functionalities, as summarised above as discussed in **Deliverable 2.4 *"Wi-5 initial architecture."*** The main reason for this selection is that it is based on LVAPs, so it is suitable for supporting load balancing, dynamic channel and power configuration and other interesting features in multi-channel WLANs. There is an additional advantage: in regular Wi-Fi, the handover is usually triggered by the user device so it is not controlled by the network and it may require 1 or 2 seconds to perform [5]. In contrast, the SDWN solution allows the network to control the mobility and to select the best moment for the handover, which is very fast.

Some tests have been performed with the aim of testing the Odin handover. They were published in [63] and presented as a demonstration paper in Netgames 2015[2], a conference about network support for online games. An online game with very strict delay limits was selected because it is a good example of a real-time application with tight latency constraints. The tests showed that the handover can be really fast, to the extent that a player cannot detect if his/her device is being switched from a Wi-Fi AP to another.

This subsection includes some details of the implementation of the Wi-5 Smart AP Solutions based on Odin.

4.1.1 Basic Description of Odin and Limitations

As explained in the Literature Review, Odin proposed and implemented an LVAP-based wireless LAN solution. It includes a central *controller*, and a set of *agents* (i.e. the APs). The system is based on commodity OpenWrt APs with a single radio.

OpenWrt is a Linux distribution for embedded devices. It does not create a single, static firmware, but it provides a fully writable filesystem with package management. This enables application selection and

[2] NetGames 2015, The 14th International Workshop on Network and Systems Support for Games (In co-operation with ACM SIGCOMM and ACM SIGMM, Technically co-sponsored by IEEE Communications Society), http://netgames2015.fer.hr/

configuration. As said in the project web page[3]: *"For developer, OpenWrt is the framework to build an application without having to build a complete firmware around it; for users this means the ability for full customization, to use the device in ways never envisioned."* More than 1000 Wi-Fi devices are currently supported by OpenWrt (see http://wiki.openwrt.org/toh/start). Many of these devices are low-cost APs, typical of SOHO (Small Office / Home Office) wireless scenarios.

The authors used OpenFlow in order to control the internal switch of each of the wireless APs in a network. In addition, they installed *Click Modular Router* [64] in the AP, adding a specific Odin module, which interacted with the Odin controller when required. The use of *Click* enables the possibility of directly managing the traffic. In addition, *Open vSwitch*[4] is installed, thus making the internal switch of each AP behave as an OpenFlow switch. The controller runs a Floodlight Openflow Controller[5] in order to manage all the switches of the APs. The resource management algorithms are added as applications on top of the controller. A scheme of Odin entities and interactions is shown in Figure 12.

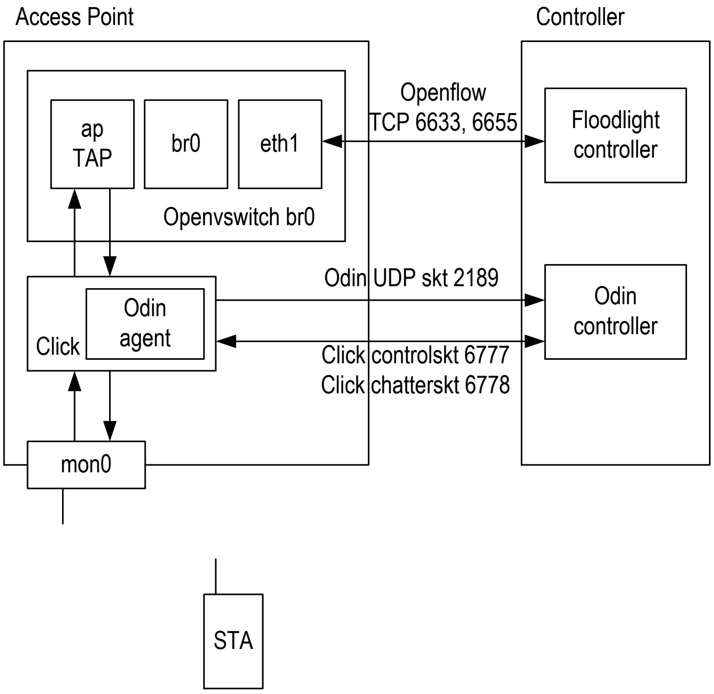


Figure 12: Entities and communications in Odin

As can be seen from figure 11, the controller and the AP exchange signalling information which is used for the implementation of the resource management. This includes:

- OpenFlow: uses TCP ports 6633 and 6655 to control the internal switch of the AP, as it is an OpenFlow switch using *Open vSwitch*.
- *Click control socket* and *Click chatter socket*: uses TCP ports 6777 and 6778.
- Odin agent: uses UDP port 2189 in order to transmit messages to the controller.

[3] OpenWrt, Wireless freedom, https://openwrt.org/

[4] Open v Switch, http://openvswitch.org/

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

A summary of the implementation-specific details follows. A virtual Linux *tap* [6] interface called *ap* is added to the internal switch of the controller (called *br0)*, and it is this that communicates with the *Click* Odin module. The *Click* module includes a new entity called *Odin Agent*, which is in charge of communicating with the controller and performing all the functionalities implementing the LVAPs. A patch has to be added to the 802.11 driver (Atheros *ath9k*) of the AP in order to support different virtual MAC addresses in a single real interface. The wireless network interface is set to *monitor* status, so its name is no longer *wlan0*, but *mon0.* In Annex B we present the full scheme for the adaptation of a commercial AP (TP-Link1043ND) for its use with Odin.

A mobility manager was initially defined as an Odin application running on top of the Floodlight OpenFlow controller[7]. This is a reactive application that manages the handover of a STA, when the user is moving towards a new AP. The scheme is shown in Figure 13: first, the controller adds a `SUBSCRIPTION` to each AP (1). As a consequence, if the STA moves (2) and an AP detects it with a signal strength higher than a threshold, it reports the event (3) to the controller (`PUBLISH` message). The controller makes a decision, and it may move the LVAP corresponding to the STA from the origin to the destination AP (4).

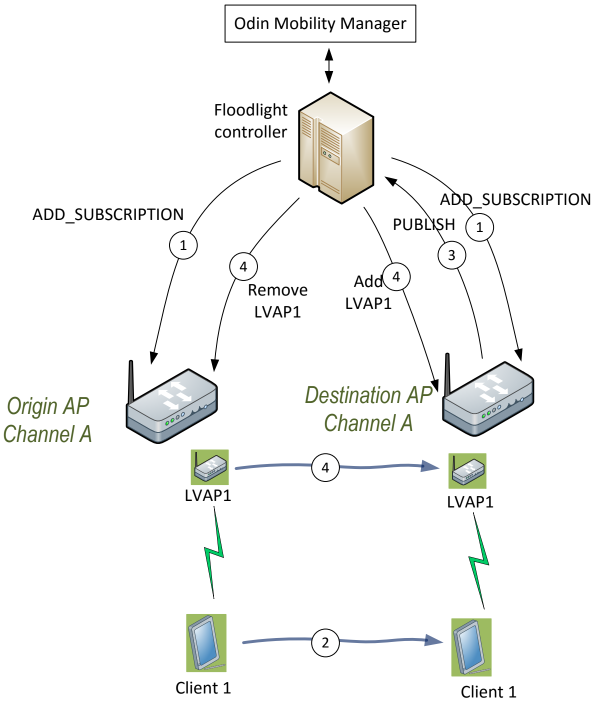


Figure 13: Scheme of Odin Mobility Manager application

This is the (simplified) algorithm running in the Mobility Manager:

```
//Performed once at the beginning
For every Agent
{
     register subscription (if client_strength > threshold, call event handler)
}

----------------
//Event handler (triggered by a PUBLISH message from the AP)
```

[6] TAP enables layer 2 frame reception and transmission for user space programs in Linux.
[7] The Floodlight Open SDN Controller, http://www.projectfloodlight.org/floodlight/

```
{
    if the client is already in the AP {
        update statistics
    } else {
        if (hysteresis_period is finished) {
            if (compare_signal_strength == true) {
                handoff the client
            }
        }
    }
}
```

4.1.2 Limitations of Odin for performing radio resource management

Although Odin represents a good starting point, it has many limitations for the aims of the Wi-5 project. The first limitation is that Odin assumes that all the APs are using the same channel, as this makes it possible for an AP to hear all clients in the vicinity, even if they are associated to other APs. Although this enables relatively simple mobility management, it also represents a severe limitation, since channel planning for the different APs would not be possible.

In addition, the available applications (a mobility manager and a load balancer) are just at proof-of-concept level and the algorithms they implement are rather simple. For example, the load balancing only consists of a round robin algorithm that does not take into account any signal power parameters.

Therefore, we concluded that Odin was potentially a good option, but many features should be added in order to build solutions for resource management in real scenarios. Different functionalities are being added to Odin, in order to make it capable of supporting the requirements of Wi-5. The new code is being shared in the Wi-5 GitHub repository[8], including the Odin controller (written in Java) and the Odin agent (written in C++).

4.1.3 Functionalities to be added

Our plan is to first integrate the seamless handover with the channel switching. For that aim, the channel switching and the handover have to be synchronised. This would allow the use of different channels in the WLAN, thus reducing the interference level.

Another objective is to tune the handover procedure in order to adapt it to the services currently running in the client. For example, the current implementation first adds the LVAP to the destination AP, and then removes it from the origin, so this may produce a number of duplicated packets. Depending on the service, it may be preferable to do the opposite (removing the LVAP first), taking into account that some services have a good tolerance to packet loss. For example, in [65] it was shown that players of *Quake 4* did not notice packet loss up to 35%.

New functionalities and control messages will also have to be added to Odin in order to enable the Wi-5 resource management algorithms:

- New procedures able to measure the interference (scanning). This is required for the Monitoring functionalities.
- Procedures for the controller to manage the power that an AP sends to each STA, and to request the signal power information from the STAs.

[8] Wi-5 GitHub code repository, https://github.com/Wi5

- The integration of packet grouping in the implementation is also necessary. First, we will explore the possibility of integrating it within the *Click Modular Router*. Another option is to leverage the *moepi* library [66], which allows frame injection via the *mac80211* stack of Linux, and is publicly available[9].

4.2 Monitoring

The role of the monitoring tools is to measure the interference level and the channel load seen at each available channel in the relevant frequency bands (i.e. 2.4 and 5 GHz). In addition, the number of clients associated with an AP and the amount of data passing through each AP will be considered. Finally, automatic detection tools, based on machine-learning [16], are being explored in order to detect and identify different kinds of real-time services (mainly VoIP and online games).

The information gathered by the performance monitoring elements will be combined and used to perform the coordination features and the packet grouping. One of the first objectives is to associate a flow with a type of service in order to know its requirements (e.g. latency in delay-sensitive services).

4.2.1 Detecting the Service

In [16], an automatic tool for traffic detection without human intervention was proposed. The objective is to make it possible for a machine to identify a kind of traffic, just based on packet size and inter-packet time. This avoids the need for using Deep Packet Inspection (DPI), thus providing better guarantees over user privacy and network neutrality. It should be noted that one of the aims of the Wi-5 architecture is to provide a good quality to real-time services with very tight latency constraints. A first step for this is to detect these traffic flows and the APs where they are present.

In the paper above, a solution called *Diffuse* (DIstributed Firewall and Flow-shaper Using Statistical Evidence) was explained in detail. This software was developed by the Swinburne University of Technology, and its source code is open and downloadable[10]. Diffuse was designed to run inside an Access Point, e.g. those based on OpenWrt, but it can be executed elsewhere. It performs both traffic classification (in classification nodes) and traffic prioritisation (in activation nodes). These nodes could actually be the same device, but experiments have proven that, due to CPU consumption, it is better to have one device for each purpose, when the throughput of the traffic analysed is higher than common DSL speeds. Diffuse uses *ipfw*, “the user interface for controlling the *ipfw* firewall, the *dummynet* traffic shaper/ packet scheduler, and the in-kernel NAT services[11].”

In order to implement the prioritisation of traffic and to establish different queues, tagging IP packets is based on a statistical analysis made using the data mining software *WEKA* (Waikato Environment for Knowledge Analysis)[12], developed in Java by the University of Waikato, NZ [67]. This means that each different application traffic you want to detect has to be first analysed with *WEKA*, in order to create the statistical data for it. It can then detect and serve different queues for different applications, or it can also group them together.

The WEKA data categorisation application does not have to be executed in real-time along with Diffuse for traffic detection. It only has to analyse each application one time offline in order to be able to detect

[9] Moepi library, http://moepi.net/

[10] DIFFUSE – Downloads, http://caia.swin.edu.au/urp/diffuse/downloads.html

[11] FreeBSD Man Pages, ipfw, https://www.freebsd.org/cgi/man.cgi?ipfw(8)

[12] Weka 3: Data Mining Software in Java, http://www.cs.waikato.ac.nz/ml/weka/

its patterns thereafter. Its description traffic files are then used as a parameter to execute Diffuse. *WEKA* can be configured so it can make faster decisions with lower CPU usage (losing accuracy) or optimize accuracy (with a higher decision tree). Its goal is to provide an easy-to-use interface for applying machine learning techniques and it relies on the statistical C4.5 algorithm to create the different categories.

We are considering the possibility of adding new traffic patterns to *Diffuse,* for example to detect online games based on TCP [68], [69]. Some games, especially those called MMORPG (Massively Multiplayer Online Role Playing Games) are usually based on TCP, although they have real-time requirements [70]. So, although in a first approach, a TCP flow will not currently be considered as a candidate to be marked as real-time, it could be interesting to add this feature. It should be taken into account that these games are becoming increasingly popular in the recent years [71] [72].

Regarding the place where traffic detection will be performed in the Wi-5 architecture, two options are possible (see Figure 14): *a)* it can be done in a distributed manner, i.e. running on each AP (1), which would in turn send a report to the controller every time a real-time traffic is detected; *b)* a centralised approach can also be taken, using the router (2), or even a specific traffic-detection machine (3).

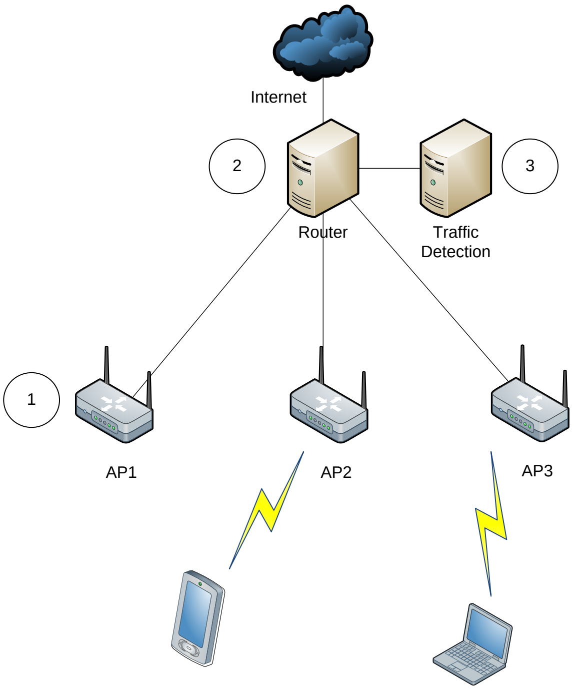


Figure 14: Possible locations of the traffic detection functionality

The advantage of the first option is that it is distributed, but it should be taken into account that the APs have a very limited processing capacity. If the centralised option is taken, a more capable machine can be used (e.g. the router or a machine next to it), and traffic detection can be made there.

We have also explored the possibility of using tools for this, e.g. *Bro IDS* (Intrusion Detection System)[13]: Bro is a network analysis framework, which provides a powerful abstraction layer. Using top-level-functions in a C-like syntax, *Bro* supports the development of configuration scripts that enclose low level capabilities. It can be executed in the same network elements that route traffic but it

[13] The Bro Network Security Monitor, https://www.bro.org/

can also be attached to the network in a mirror link as an independent monitoring tool. It also includes the possibility of using DPI.

We are currently studying the possibility of integrating *Diffuse* statistical analysis into *Bro IDS*, in order to be able to apply complex classification rules based on statistical analysis techniques, aiming to achieve better accuracy in IP traffic classification without increasing the process time significantly.

4.2.2 Monitoring the Power of the STA

The Wi-5 architecture also considers the optimisation of the radio power to be transmitted by the APs. This is required for interference reduction, and also for energy savings. The power transmitted by the AP (downlink) can be defined and tuned by the Wi-5 controller, so it is not necessary to monitor it. However, in a first approach, the power being transmitted by the STA (uplink) is not known. Indeed, the AP only knows the power of the signal received, but this not only depends on the power transmitted, but also on the channel.

For monitoring this parameter, the features defined in IEEE 802.11h can be exploited: the *TPC request / report* elements enable the estimation of the channel gain between the serving AP and the STA. Taking into account that this standard is from 2003, the vast majority of current STAs support them.

These features were extended in IEEE 802.11k (2008) [73], with improved capabilities to support measurements of APs different from the serving AP. These APs may even be in a different channel. There are certain devices in the market that support 802.11h but not 802.11k. In contrast, some others (e.g. Apple devices) support both of them.

All these features were included in 802.11-2012 [74] and they define mechanisms for APs and STAs to dynamically measure the available radio resources. Using them, APs and STAs can send reports to their neighbours, beacon reports, and link measurement reports to each other. This includes a series of request and report messages which can be used for getting these data from the station:

- The power the STA is transmitting.
- The link margin: the difference between the receiver's sensitivity for the current transmission rate and the actual received power.

In Section **8.4.2.18 *TPC Request* element**, the standard defines a “request for a STA to report transmit power and link margin,” which should be answered by the station with a *TPC Report* element including this information. As a complement to the TPC Request, Section **8.4.2.19 *TPC Report* element** defines the element that contains “transmit power and link margin information sent in response to a TPC Request element or a Link Measurement Request frame. A TPC Report element is included in a Beacon frame or Probe Response frame without a corresponding request.”. Sections **10.11.5 Station responsibility for conducting measurements** and **10.11.6 Requesting and reporting of measurements** of the 802.11-2012 standard specify the behaviour of a STA when receiving a measurement request.

Periodical requests will be included in subsequent versions of the Wi-5 architecture in order to get this information from the STAs. New functionalities will be added to the current Odin implementation in order to provide these functions, enabling the resource management algorithms to use them.

4.2.3 Monitoring the Radio Environment

Wi-5 APs must incorporate scanning features, with the objective of gathering information of the occupancy of the radio channels in their neighbourhood. This information will then be forwarded to the controller, to be used as an input for the radio resource management algorithms. The objective is twofold:

- The interference caused by the different APs in the network (both under and outside the Wi-5 administrative domain) has to be detected. Those in the same Wi-5 administrative domain will be properly allocated to minimize the interference in the radio resource management algorithms.
- Other Wi-5 STAs approaching have to be detected, taking into account that we are considering users that walk while using the service. In a network initiated handover between Wi-5 APs, as we proposed, the capability of detecting a new user is necessary in order to trigger the procedure in a timely manner.

As illustrated in Figure 15, we are considering a client moving from AP_1 to AP_2. Logically, it can be expected that adjacent APs are in different (and non-overlapping) Wi-Fi channels. Therefore, AP_2 will not receive frames from a client associated with AP_1. Since an event is required to trigger the handover, it is seen as necessary to establish some scanning periods in AP_2 in order to look for Wi-5 users in the vicinity. If a user is detected, it can be reported to the controller, which, according to its load balancing algorithm, will make a decision about handing off the client or not.

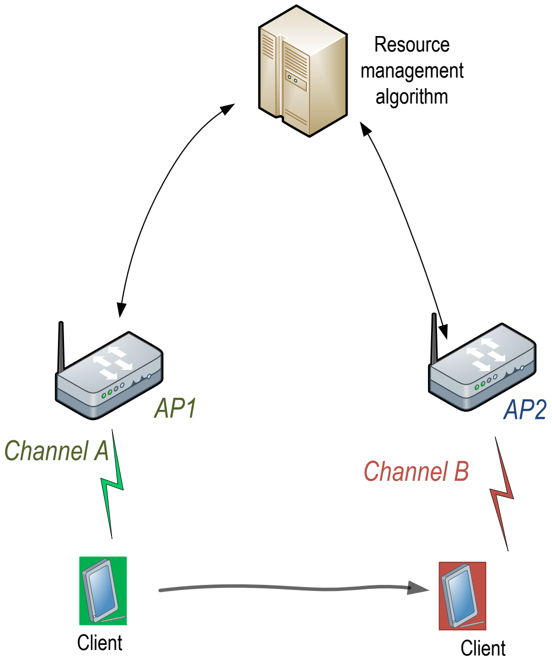


Figure 15: Need for scanning in other channels to trigger hand-offs

As discussed in the Literature Review section, the use of Multichannel Light Virtual APs was proposed in [8], allowing a STA to change the AP and the channel at the same time. The solution was based on the communication between the involved APs. Wi-5 solutions will follow this approach but, instead of using an AP-AP protocol, the handoff will be governed by the controller.

Therefore, a trade-off appears: on the one hand, scanning in other channels is necessary, but on the other hand, the AP will not be able to manage its own clients while scanning [10]. This trade-off has to be studied and explored in order to arrive to an optimum solution.

However, this trade-off can be solved in another way: if an additional 802.11 interface is added to each AP, it can be used only for scanning purposes, relieving the main interface from this task. Taking into account the low cost of an additional 802.11 interface, this option will be explored as another way for solving this trade-off.

New Monitoring Message

A new method has been added to Odin with the objective of asking an AP its current channel number:

```
getChannelFromAgent(agentAddr)
```

This method reads the variable `_channel` from a specific AP and returns the corresponding value.

The corresponding functionalities have been added in the Odin agent entity[14] of the *Click Modular Router*, in order to respond to the messages received from the Odin controller.

4.3 Dynamic Channel Allocation and Power Control

The scenario we are assuming consists of a number of APs covering an area, under a single controller. However, it is possible that other 802.11 devices (APs and STAs), not managed by the controller, may operate in the same area, thus producing a certain degree of interference. The monitoring capabilities included on each AP provide detailed information about the state of the AP and its environment, and this is used to perform coordinated resource allocation. According to the proposed centralised architecture, all these algorithms will run in the Wi-5 controller.

The resource management algorithms will pose different optimisation problems, trying to manage channel allocation and power control, to fulfil the requirements of the different applications, and at the same time to maximise the use of the available resources. The complexity of the resulting problem can lead to the use of suboptimal algorithms.

We assume a dense scenario where there are several APs working in different channels, and typically most of the zones will be covered by more than a single AP. This will make it possible that a STA is attended by more than a single AP in different channels. Therefore, the Wi-5 controller will also be able to make the decisions on which STA and which channel is assigned to which AP, as defined in the Wi-5 architecture. Both 5 GHz and 2.4 GHz bands will be considered to perform the channel allocation.

Support of Different Channels

As identified above, the original design of Odin in which all the APs are located in the same channel is not suitable to build deployments in big scenarios, since the interference level would be very high. Therefore, new functionalities for managing APs in different channels are required. First, inter-channel handover should be enabled. In Figure 16 the scheme of an inter-channel handover is presented.

[14] https://github.com/Wi5/odin-agent/tree/devel_unizar

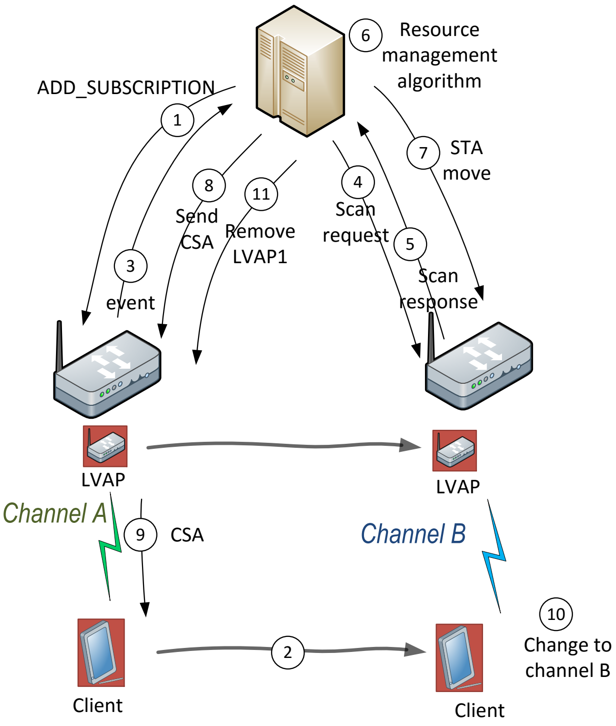


Figure 16: Scheme of a handover between APs in different channels

These would be the steps of the new algorithm implementing inter-channel handover:

1. Subscription: The manager sends packets with different “events” that will trigger when a threshold is reached (noise, power, etc).
2. The STA moves
3. The Origin AP detects that the signal of the STA is less than a threshold and sends an *event* to the Controller
4. The Controller sends to neighbor APs a *Scan Request* message
5. For a short period of time, all neighbor APs switch to channel A and listen to STA packets. If an AP successfully listens to STA packets, it sends a *Scan Response* message to the controller.
6. The Controller receives all the *Scan Response* messages and chooses the AP with the best signal, according to its resource management algorithms. Decision is: *move STA to Destination AP*
7. The Controller sends a *Station Move (*including *Add LVAP)* to AP2, and AP2 starts sending beacons to STA in channel B
8. The controller tells the AP1 to send the *Channel Switch Announcement* to the STA
9. AP1 sends beacons to the STA with the *Channel Switch Announcement* element to force the STA to switch to channel B
10. STA receives the beacons with the CSA element and switches to channel B
11. When the controller watches the traffic of the mobile from the destination AP, it sends a *remove LVAP* to AP1

In order to implement this handover, new functions have been added to Odin, and these are available at the Wi-5 GitHub repository:

`setChannelToAgent(agentAddr, channel)`

This method writes the variable `_channel` in the AP, and consequently changes the physical channel of the corresponding agent.

`sendChannelSwitch(MACAddress clientHwAddr, MACAddress bssid, Set<String> ssidList, int channel)` [15]

> This method tells the AP to send a *Channel Switch Announcement* (CSA) to a certain STA. The parameters are the hardware address of the agent and the STA, the SSID, and the new channel. After receiving this message, the AP will send a series of beacons (10 by default) including the CSA element, which makes the STA switch to the new channel.

Finally, a simple application named `TestingChannelOnly.java`[16] has been added to Odin, in order to run the first tests with the multi-channel handover.

Power control

The measurements reporting the interference level caused by both Wi-5 and non-Wi-5 devices will have a special importance for these algorithms. As for the Wi-5 APs, information about which APs can potentially interfere among them if they use the same channel and the current load of those interfering APs will be required to properly assign both channels and users. This information can be estimated by the Wi-5 APs themselves and reported to the Wi-5 controller. In addition, reports about the interference level caused by non-Wi-5 devices will be important to avoid those channels presenting a high level of activity. For that aim, the scanning tools defined in 4.2.3 will be leveraged.

Power control will be performed in order to jointly reduce the overall interference (therefore increasing the radio resource reuse) and the energy consumption. The idea is to take advantage of the *TPC request / report* elements, defined in IEEE 802.11h and supported by most current 802.11 devices, to adjust the transmission power of each AP towards each STA. Due to the operation mode of 802.11 devices, the link margin in the STA is mainly related to the channel conditions and the transmission power in the APs, regardless of the interference of other 802.11 devices, due to the *Clear Channel Assessment* (CCA) functions, which prevents them from accessing the channel when it is busy. In this scenario, each *TPC report element* contains the link margin, which directly reflects the difference between the receiver's sensitivity for the current transmission rate following the defined notation, and the actual received power. Therefore, the transmit power in the AP could be theoretically reduced by this link margin while keeping the same transmission rate. Finally, a security margin should be included (i.e., the power reduction should be slightly lower than the one allowed by the link margin) in order to avoid instabilities in the transmission rate due to channel fluctuations.

This power control mechanism can be performed dynamically and more frequently than the joint channel assignment and user association mechanism. It will indirectly impact on that optimization problem by modifying the interfering load among APs (i.e., flows transmitted from an AP at a lower power may not interfere to another AP which would be interfered at maximum transmitted power). In addition, the periodicity in the use of TPC messages is an important parameter to find a balance between quick updates and the related overhead. All these issues will be further analysed in upcoming work.

[15] This functionality has been added in the function https://github.com/Wi5/odin-controller/blob/devel_unizar/src/main/java/net/floodlightcontroller/odin/master/OdinAgent.java

[16] https://github.com/Wi5/odin-controller/blob/devel_unizar /src/main/java/net/floodlightcontroller/odin/applications/TestingChannelOnly.java

4.4 Load Balancing

This functionality will enable Wi-5 networks to make decisions on when not to accept new association requests, with the aim of maximising the aggregate data rate of these networks. The centralised approach will make this relatively straightforward, since all the association requests have to be approved by the central controller.

Taking into account that we have opted for a solution based on LVAPs, the controller has the freedom to assign a STA to any Wi-5 AP, and to move it seamlessly from one Wi-5 AP to another, even if they are working on different channels. Therefore, moving a STA to a new Wi-5 AP or changing the operating channel in the Wi-5 APs does not require a Layer 3 re-association, so the algorithms can consider a relatively high level of movement between Wi-5 APs.

SimpleLoadBalancer

A proactive load balancing application is included in the original release of Odin as an example, which runs periodically (every 60 seconds by default). The scheme is shown in Figure 17: the controller first queries every AP (1) in order to know all the STAs they are able to *hear*. Once the statistics have been gathered (2), a simple round robin algorithm is run, and the STAs are re-assigned to the APs. Those STAs having to switch from an AP to another are handed-off by moving their LVAPs (3).

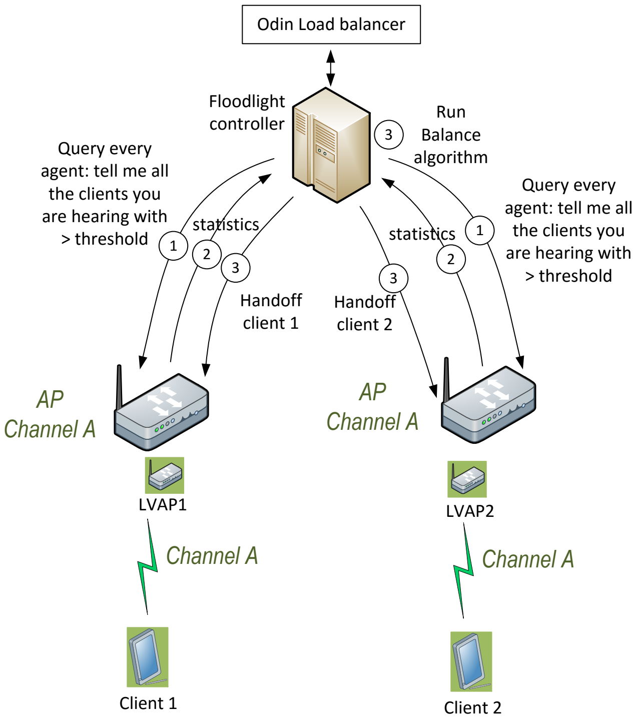


Figure 17: Scheme of Odin Load Balancer application

This is the scheme of the Load Balancer algorithm:

```
Every 60 seconds
{
     // build the “hearing table”
     For every agent
     {
            obtain the IPs and MACs heard above a threshold
     }
     // result: updated map of agents and clients they hear

     // run balance() function
     For every client
     {
            find the most suitable AP
            handoff the client if necessary
     }
}
```

New load balancing functions will be added to the Wi-5 controller in order to allow for a more intelligent distribution of the network load, also in cooperation with the rest of functionalities. This will be addressed in future work.

4.5 Packet Grouping

The objective of this functionality is to define and implement the mechanisms for packet grouping between the AP and the end device as specified in the IEEE 802.11n [18] and 802.11ac [17] standards. Two forms of frame aggregation are explored: Aggregated Mac Service Data Unit (A-MSDU), and Aggregated Mac Protocol Data Unit (A-MPDU). In addition, Layer 3 optimisation has also been explored: in certain scenarios, legacy 802.11 devices (prior to 802.11n) exist, so this optimisation is not possible at Layer 2.

The achievable gain when intelligently using these grouping mechanisms is also being explored. But at the same time, we should consider how this gain maps to user experience in real-time applications. This will also interact with monitoring mechanisms (identifying the service according to traffic patterns, as proposed in subsection 4.2.1) in order to determine which flows can be grouped and which cannot, based on the technical characteristics of the applications supported, such as the delay sensitivity. In addition, the number of packets grouped may be determined in order to guarantee that the medium will be available at a given point in time.

The policies proposed do not contemplate discarding packets or reducing bit rates.

4.5.1 Layer-2 vs Layer-3 optimisation in 802.11

a) Layer-2 optimisation

New versions of Wi-Fi (from 802.11n) include mechanisms for frame grouping: A-MPDU and A-MSDU (see Figure 18):

- A-MPDU: a number of MPDU delimiters each followed by an MPDU.
- A-MSDU: multiple payload frames share not just the same PHY, but also the same MAC header.

It should be noted that frame aggregation is becoming a common feature. In fact, in 802.11ac all the frames must have an A-MPDU format, even when a single sub-frame is transported.

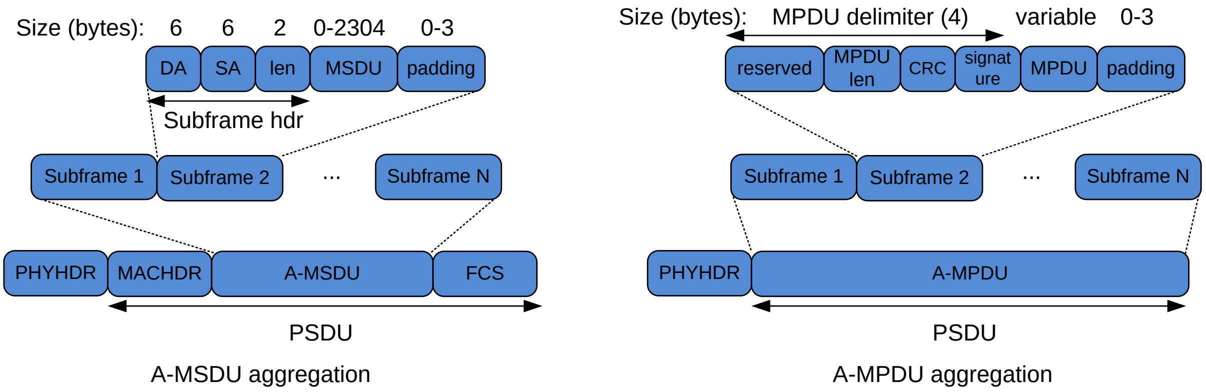


Figure 18: Frame aggregation schemes in 802.11n: a) A-MSDU; b) A-MPDU

The increase in efficiency achievable when aggregating frames is significant. Figure 19 shows an example: we have used the model developed in [48] in order to represent the efficiency increase when these two aggregation mechanisms are used. It should be noted that A-MPDU allows a higher number of frames to be aggregated. The efficiency can increase up to 90% for UDP packets, and 80% for TCP. The packet size considered is 1500 bytes. However, it can also be seen that this has a counterpart: if 50 frames are to be aggregated, some additional delay will appear.

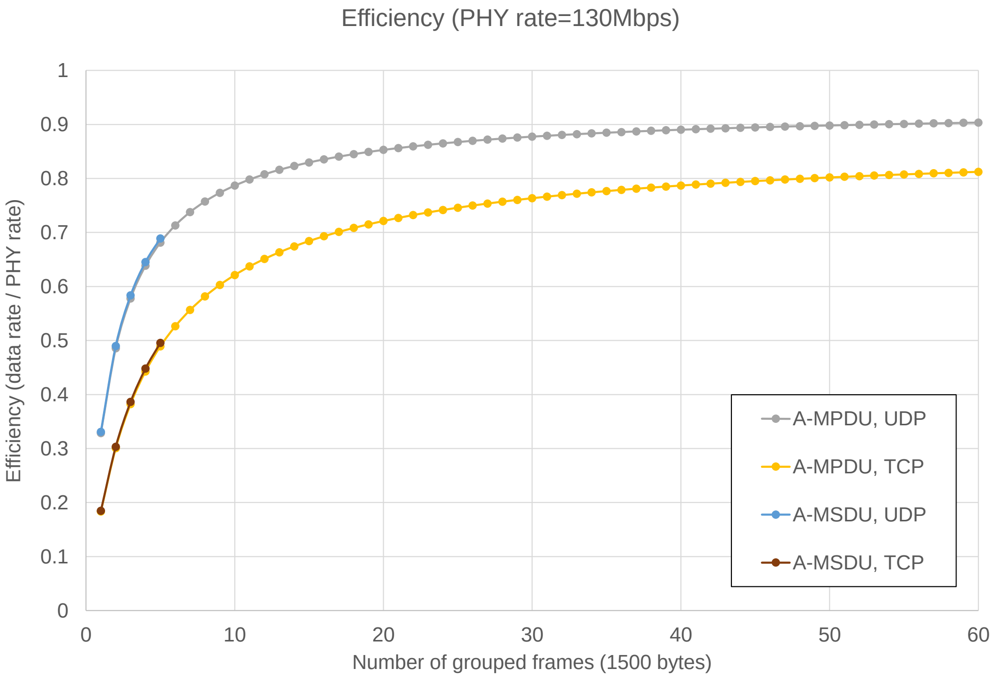


Figure 19: Efficiency improvement in 802.11 when using aggregation schemes

The frame aggregation will follow the approach of Wi-Fi Multimedia (WMM) [75]), a subset of the IEEE 802.11e specification [76] that adds quality of service (QoS) functionalities by prioritizing data packets according to four categories using the flow analysis feedback provided by the monitoring tools. WMM defines four queues (see Figure 20), for *Voice*, *video*, *best-effort* and *background* packets, and different values for the *interframe space*, CW_{min}, and CW_{max} values. This system is called enhanced distributed coordination function (EDCF). If two frames from different access categories collide internally, the frame with the highest priority is sent, and the lower priority frame adjusts its backoff parameters as if it had collided with a frame external to the queuing mechanism.

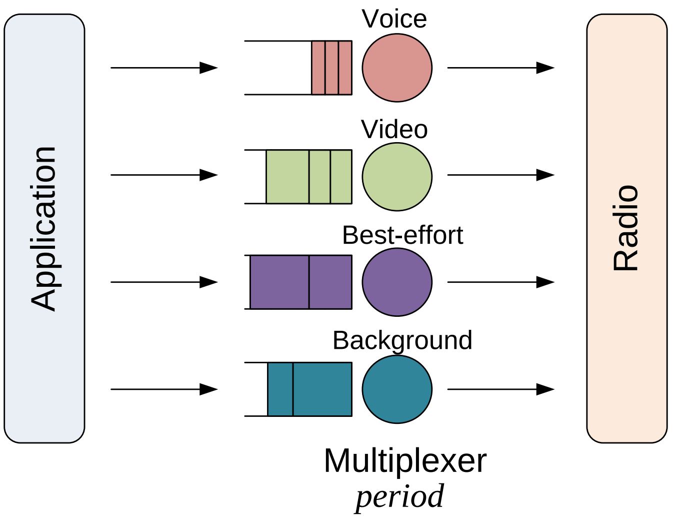


Figure 20: Scheme of the four queues included in Wi-Fi Multimedia

The solutions to be developed in Wi-5 will consider these four queues, and the optimisation of the aggregation parameters globally. The following restrictions apply:

- Only packets from the same queue, and destined to a single user, will be aggregated together.
- The delay restrictions of each service will be respected, i.e. voice packets will not be stopped at the queue if this would add unacceptable delays.

The Wi-5 controller will therefore be able to enable/disable aggregation in a certain AP in a centralised manner. Therefore, it may be expected that some APs will have aggregation enabled, and the controller will assign users with no real-time requirements to them.

b) Layer-3 optimisation

Simplemux is a generic and lightweight multiplexing protocol aimed to enable the multiplexing of a number of packets belonging to a protocol (the “multiplexed packets”), into another protocol (i.e. the “tunnelling protocol”), as shown in Figure 21. Small separators are inserted between the packets, including the length and an identifier of the protocol of the multiplexed packets. Thus, any tunnelling protocol may be virtually able to carry a number of packets of any other protocol.

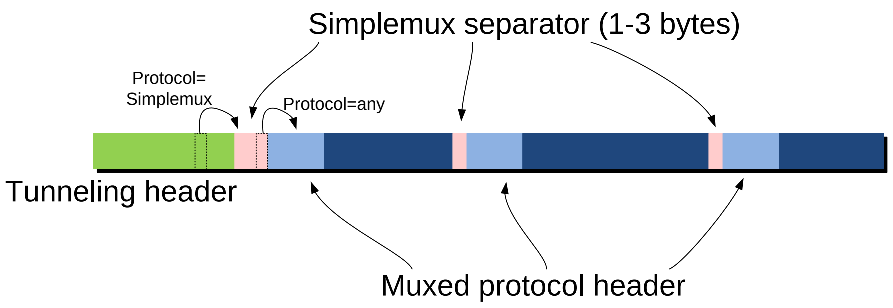


Figure 21: Scheme of a Simplemux packet

Simplemux may work as an alternative for 802.11 aggregation with the additional benefit of end-to-end optimisation including a number of hops. It may also be useful in legacy systems not implementing the aggregation mechanisms defined by 802.11n and subsequent versions.

Simplemux can also be seen as an improvement with respect to existing Layer 3 optimisation mechanisms such as TCRTP, as standardised by the IETF in RFC 4170 [77]. In fact, Simplemux is able to accomplish the same tasks with reduced management. It can also substitute PPPMux, mainly aimed for point-to-point links. In fact, the L2TP and the PPP sessions required by TCRTP could be avoided.

A more detailed explanation of Simplemux can be found in *Annex A. Simplemux Proposal for Packet grouping at Layer 3*. More information is also available in the article [79], and the detailed definition is provided in an IETF draft [78].

A research paper proposing a Layer 3 aggregation mechanism, and comparing it with the Layer 2 mechanisms included in 802.11 has been published and presented in a conference by the Wi-5 Unizar team [79].

c) Discussion

Layer 3 aggregation may work as an alternative for 802.11 aggregation, with the additional benefit of end-to-end optimisation including a number of hops (in 802.11 it covers only one). It may also be useful in legacy systems not implementing the aggregation mechanisms defined by 802.11n and subsequent versions.

In [80] some scenarios of interest where multiplexing can provide benefits were identified:

- The aggregation network of an operator. Multiplexing can be deployed between different devices in residential scenarios. Traffic can be grouped at different levels as e.g. at gateway level in LTE or ISP edge routers.
- In corporate environments, a number of simultaneous small-packet flows (as e.g. VoIP calls or remote desktop sessions) between two central offices of a company can be multiplexed.
- In Machine-to-Machine and IoT scenarios with bandwidth and processing constraints, small packets generated by e.g. a sensor can be aggregated.

In addition to these scenarios, a new one has been identified, namely Community Networks or other network deployments alternative to traditional ones [81], which are becoming popular in the last years, with a special relevance in developing countries. In these networks, users create, own and manage the network infrastructure, which serves as a backhaul for providing Internet access. They are not only deployed in remote villages, but also in urban environments [82].

In this kind of scenario, Simplemux can be used for traffic optimisation, taking into account some special questions: first, these networks are mainly based on wireless (Wi-Fi) links, so the packets traverse a series of hops before reaching their destination. In that case, an end-to-end optimisation can reduce the amount of packets (*airtime* drawback) with an advantage over Layer-2 optimisation, which would be applied at each intermediate router (*processing* drawback). In Figure 22, thick blue lines represent the paths where Simplemux could be employed to optimise the traffic. In these scenarios, especially in developing countries, new versions of 802.11 including frame aggregation may not be widely deployed.

In some cases, a network operator and the owners of the infrastructure may sign an agreement, so the operator deploys a 3G femtocell in a remote village (see the figure), using the community network as a backhaul for connecting to the Internet. This constitutes a win-win scenario, since the operator avoids the costs of extending the network to that village, which can get connected with the mobile network [83].

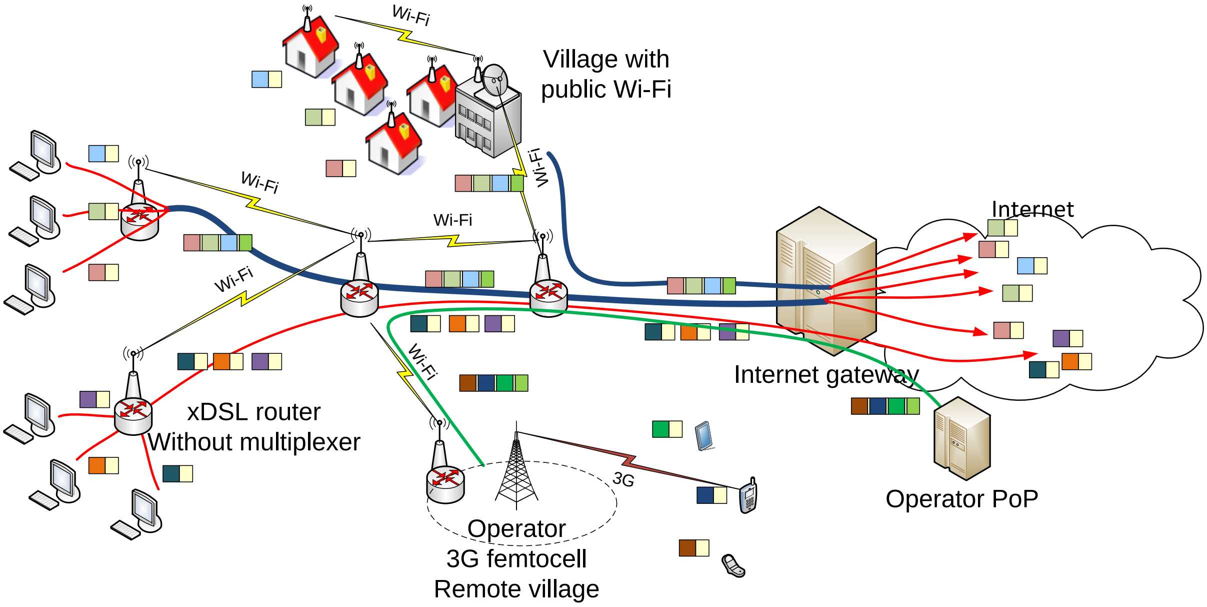


Figure 22: Simplemux optimisation in an *alternative network* scenario

d) Delay limits

Real-time applications can be defined as those having strict latency limits. The Internet Society organised a workshop in 2013 titled *"Speeding Up the Internet - Reducing Latency,"*[17] with the objective of discussing the sources of latency in the modern Internet. One of the conclusions, summarised that *"(…) if you care about latency, you have to be very careful and look in a lot of places for potential optimisations, and potential conflicts of those optimisations."*. This conclusion fits clearly with what we are proposing: a traffic optimisation based on aggregating packets. However, this aggregation must be carefully done, taking into account that it may add a new delay, required for gathering a number of packets to be sent together.

In addition, the Internet Society workshop proposed the concept of "latency budget," meaning the maximum latency tolerated by a service [84]. A latency budget is assigned to each application and it is *consumed* by *sources* of latency. In that sense, every additional network process is seen as a *consumer* of latency, i.e. it requires a certain delay to be applied. Frame aggregation adds no delay if a number of packets are already waiting in the buffer (this may occur in congested links). However, if aggregation is forced in a device (e.g. a router or an AP), an aggregating period can be defined, in order to set an upper bound on the maximum additional delay. This means that an aggregated frame/packet will be sent at the end of each period (see Figure 23), so the average delay will be half the period, and the jitter (standard deviation of the additional delay) will be $period/\sqrt{12}$, as shown in [85].

[17] Available at http://www.internetsociety.org/blog/2013/12/speeding-internet-reducing-latency

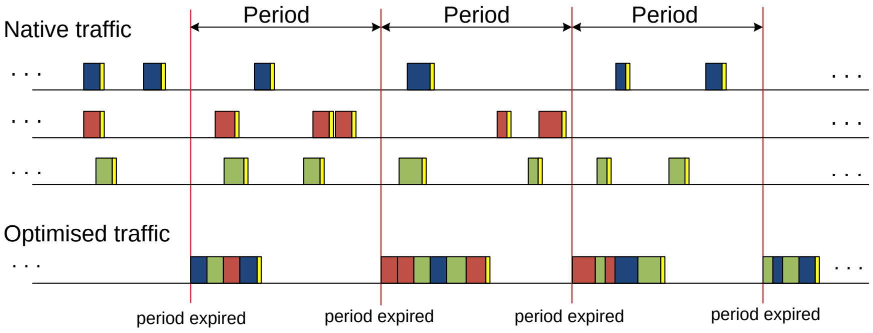


Figure 23: Aggregation period

An Internet Draft surveying these limits has been written [86], and these are some of the delay limits it includes (additional references can be found in the draft):

- VoIP: 150 ms.
- Online games: It may vary depending on the game genre: from 100 ms (First Person Shooters) to 1000 ms (Real-Time Strategy).
- Remote desktop: 200 ms.
- IoT samples in constrained network scenarios may tolerate delays up to some seconds.

4.5.2 Analytical Calculation of the Expected Savings Achievable by Aggregation

This subsection has three parts: first, the savings in terms of packets per second are obtained. Next, the calculation of the bandwidth reduction is presented. Finally, the last subsection presents a comparison between the savings obtained by Simplemux (Layer-3) and 802.11 (Layer-2) aggregation mechanisms.

a) Packets per second savings

The scenario we are considering is a network node where packets of different sizes arrive. They are classified according to their size, and only small ones are sent to a multiplexer (Figure 24). A period *PE* is defined at the multiplexer and every time the period expires, a packet is sent including all the arrived packets. However, if a number of packets *N* have arrived before the end of *PE*, a multiplexed packet is sent and a new period begins.

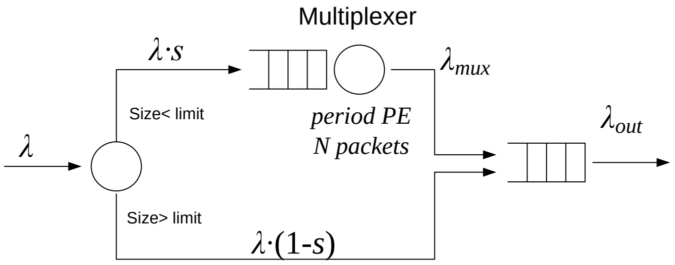


Figure 24: Scheme of a node classifying and multiplexing traffic

Let λ be the packet arrival rate. If we set a size limit at the classifier, we have:

$$s = \Pr\,[size \leq limit] \qquad (1)$$

$$1 - s = \Pr\,[size > limit] \qquad (2)$$

We want to find λ_{out} and BW_{out}, i.e. the packet rate and the bandwidth at the output. In the following, we are assuming that no packets are lost in the queues.

Let *k* be the number of packets arriving as the multiplexer in a period. Three cases can be distinguished: *a)* no packets arrived; *b) k* packets arrived ($k \in [1, N\text{-}1]$); and *c) N* packets arrived. Therefore, we can express the value of λ_{mux} as:

$$\lambda_{mux} = \lambda_{mux|k=0} \cdot \Pr(k = 0) + \lambda_{mux|1 \leq k \leq N\text{-}1} \cdot \Pr(1 \leq k \leq N\text{-}1) + \lambda_{mux|k=N} \cdot \Pr(k = N) \quad (3)$$

In order to simplify this expression, we must take into account that:

- If no packets have arrived, we have $\lambda_{mux|k=0} = 0$.
- If $k \in [1, N\text{-}1]$, then a multiplexed packet will be sent at the end of the period, so $\lambda_{mux|1 \leq k \leq N\text{-}1} = 1/PE$.
- If *N* packets have arrived, we have $\lambda_{mux|k=N} = \lambda \cdot s/N$.

So we can express λ_{mux} as:

$$\lambda_{mux} = \frac{1}{PE} \Pr(1 \leq k \leq N\text{-}1) + \frac{\lambda \cdot s}{N} \cdot \Pr(k = N) \quad (4)$$

From (4), we can see that, if the amount of packets per second arriving at the multiplexer is high, then *N* packets will always be multiplexed together, and the end of the period will never be reached, so $\Pr(k = N) \approx 1$, and in that case:

$$\lambda_{mux} \approx \frac{\lambda \cdot s}{N} \quad (5)$$

$$\lambda_{out} \approx \frac{\lambda \cdot s}{N} + \lambda \cdot (1 - s) = \lambda \left[\frac{s}{N} + (1 - s) \right] \quad (6)$$

This simplified expression (only valid for high amounts of traffic) is ruled by two parameters, namely the number of packets that can be multiplexed *N*, and the probability of having a small packet *s*. So the reduction in terms of packets per second will depend on the packet size distribution, but it will also depend on the MTU of the underlying technology employed, since *N* is related to both parameters.

Finally, if a header compression algorithm such as ROHC [87] is employed, the compression ratio will also have an influence on the maximum number of native packets to be included in a multiplexed bundle. However, if the traffic only consists of small packets (e.g. VoIP packets between two offices), we will have s=1, so the amount of packets is directly reduced by a factor of *N*.

In Figure 25, the relationship between the amount of packets per second at the input and at the output (λ_{out}/λ) is presented. The graph "Uniform size distribution" has been obtained considering a uniform packet size distribution (between 40 and 1500 bytes). In this case, the reduction in terms of packets per second could theoretically be about 50%. The graph decreases monotonically, so in a first approach it would seem that the best choice is to send all the packets to the multiplexer.

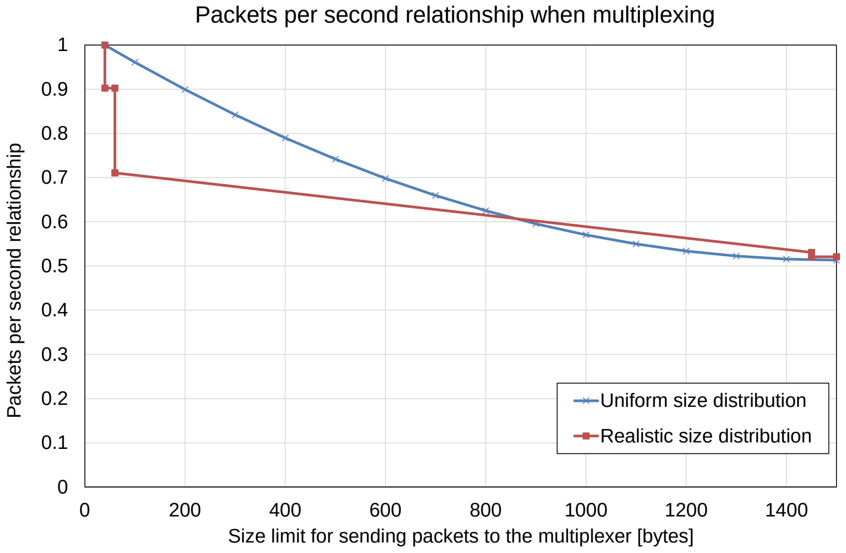


Figure 25: Theoretical reduction of the packets per second when multiplexing 1000 packets per second

However, as shown in Figure 2, real Internet traffic does not have a uniform size distribution; in fact, a clear division between *small* and *near-to-MTU* packets can be observed. Thus, the graph "Realistic size distribution" represents the relationship, when the traffic is modelled this way: a peak of 40-byte packets (10%); a peak of 60-byte packets (20%); a peak of 1450-byte packets (29%); a peak of 1500 bytes (14%); the other 27% of the packets are uniformly distributed between 61 and 1449 bytes. In this case, it can be observed that a significant decrease in terms of packets per second is achieved even if only small packets are sent to the multiplexer. If bigger packets are also multiplexed, the curve decreases slowly. So it would make sense to send to the multiplexer only the small ones, thus avoiding additional processing, delays, etc. to affect the big packets. In the test section below we will present some results obtained with a real Internet trace.

b) Bandwidth savings at Layer 3

In order to obtain the bandwidth at the output here, we need the average size of the multiplexed packets, E[*size*]. The bandwidth will be:

$$BW_{out\,=}\,\lambda_{mux}\cdot \mathrm{E}[size_{muxed\_packets}] + \lambda\cdot(1-s)\cdot \mathrm{E}[size_{big\_packets}] \qquad (7)$$

Since the expected size of big packets will normally be about one order of magnitude over that of small ones (i.e. 1500 with respect to 150 bytes), the savings in terms of bandwidth will only be significant if $\lambda_{mux} >> \lambda\cdot(1-s)$. Otherwise, the savings will mainly be achieved in terms of packets per second reduction (*airtime* and *processing* improvement).

Let *CO (Common Overhead)* be the size of the common tunnelling header of the multiplexed packet; *SO (Single Overhead)* be the size of the multiplexing separator added to each packet; and *CR* the *Compression Ratio* of a hypothetical header compression mechanism employed in combination with multiplexing. The size of a multiplexed packet is a function of *k*, the number of packets arrived to the multiplexer in a period:

$$\mathrm{E}[size_{muxed\_packets}]=CO + \mathrm{E}[k]\cdot(SO + CR\cdot \mathrm{E}[size_{small\_packets}]) \qquad (8)$$

Where $\mathrm{E}[k] = \lambda\cdot s / \lambda_{mux}$ ($\mathrm{E}[k] \approx N$ when the traffic load is high), *CO* and *SO* depend on the multiplexing method (e.g. if IPv4 is used, *CO*=20 bytes). For Simplemux, *SO* will be the average size of the separators (between 1 and 3 bytes), *CR* depends on the header compression algorithm. Finally, E[$size_{small\_packets}$] and E[$size_{big\_packets}$] will depend on the statistical distribution of the packet size.

c) Efficiency Improvement with Aggregation

The analytical method proposed in [48] for calculating the savings of 802.11 aggregation mechanisms, has been adapted in order to include the possibility of multiplexing at higher layers. As a result, we have obtained Figure 26, where the efficiency *(data rate /PHY rate)* is presented for small 200-byte frames, for both UDP and TCP traffic. It can be observed that Simplemux behaves very similar to both 802.11 frame grouping options. The number of frames that can be optimised with A-MPDU is significantly higher, because of the different MTU allowed by 802.11n standard.

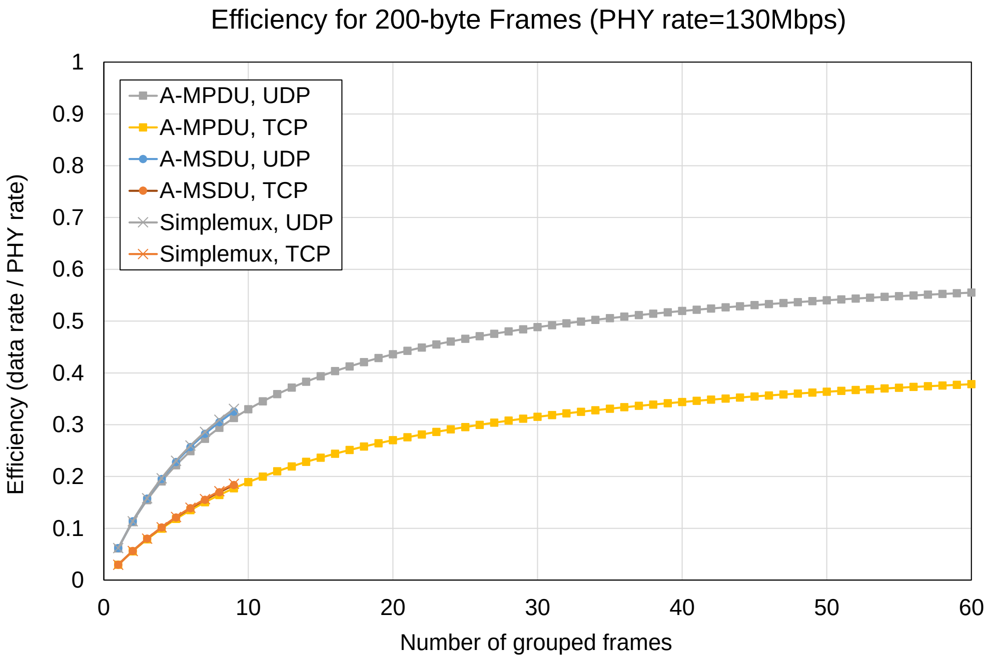


Figure 26: Network efficiency when grouping 200-byte packets at Layer 2 or Layer 3

4.5.3 Lab tests performed for measuring savings

An implementation of Simplemux has been developed in C, mainly for testing and demonstration purposes. Its source code has been made publicly available in GitHub[18]. The default tunnelling protocol is IPv4, using *Protocol Number* 253, which is reserved by IANA (Internet Assigned Numbers Authority) *"for experimentation and testing"* [88]. In addition, in order to avoid firewalls dropping packets belonging to an unknown protocol, the option of using UDP has been added, at the cost of 8 additional bytes per multiplexed bundle.

The multiplexed packets are native IP, but the implementation also relies on an open-source ROHC implementation[19] for compressing headers before multiplexing the packets. This combination of Tunnelling, Compressing and Multiplexing (TCM) makes it possible to send header-compressed packets end-to-end, being the common tunnelling overhead shared by a number of packets.

[18] Simplemux in Github, https://github.com/TCM-TF/simplemux

[19] The OpenSource ROHC library, https://rohc-lib.org/

The program runs in user space. A Linux *tun* device[20] is created, and the multiplexer captures all the packets that are forwarded to this device. Therefore, the decision about what packets are sent to the multiplexer can be implemented this way: packets are first marked with *iptables*, according to the desired policies (defined by IP, port, packet length, etc.); then *iproute* is used to forward the marked flows to the *tun* device.

The implementation includes the following features:

- Two ROHC compression modes are included: *Unidirectional* and *Bidirectional Optimistic*. A feedback channel can be created from the decompressor to the compressor. ROHC profiles included: IP/UDP/RTP, IP/UDP, IP/TCP, IP/ESP and IP/UDP-Lite.
- Four different multiplexing policies can be combined: a) sending a fixed number of native packets; b) filling a packet size; c) sending if a packet arrives after a timeout expiration; and d) sending in a periodic way.

The implementation has 2,700 lines of code (ROHC library not included). The processing delay in a commodity PC (Intel Core i3) has been measured at roughly 0.25ms. In a low-cost OpenWrt Access Point (TP-Link TL1043ND) it is about 3.5ms.

a) Test Setup

a) Test scenario: Four machines are used for the tests: *generator*, *receiver*, *multiplexer* and *demultiplexer*, the bottleneck is introduced in the link between these two (Figure 27). The bottleneck can either be wired or wireless. These are the tools employed in the tests:

- The machines are commodity PCs with Core i3 processors, running Debian 6.
- In the tests with wired connections, 3Com Ethernet switches (100Mbps) are used.
- For the wireless tests, 802.11 USB devices (TP-Link AC600, Archer T2U) are used. The tests are carried out at 5.56 GHz in order to reduce the potential interference with other devices operating in the 2.4 GHz band. The MTU is set to 2304 bytes, which allows a higher amount of packets to be multiplexed.
- D-ITG traffic generator [89] is employed in the *generator* and the *receiver*.

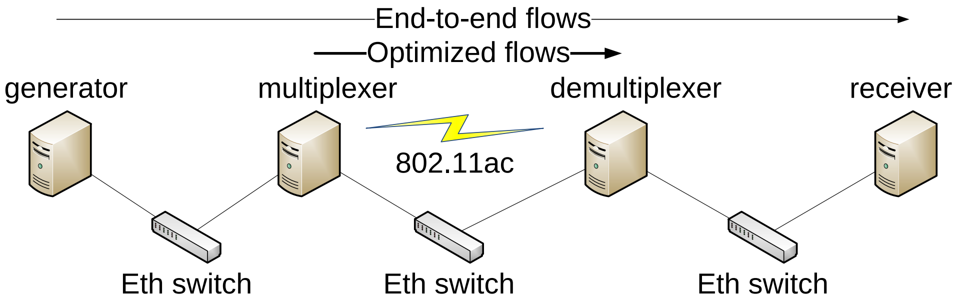


Figure 27: Test scenario

b) Traffic traces: Two kind of traffic traces have been generated with D-ITG: in tests requiring a fixed size (e.g. small UDP packets, RTP flows), the standard options of the traffic generator are used. For generating variable size traffic, we have extracted the packet size and inter-packet time distributions

[20] TUN enables packet reception and transmission at layer 3 for user space programs in Linux.

from the trace in [47], so as to preserve the packet size distribution of real Internet traffic. When required, the inter-packet time has been scaled in order to reduce the bandwidth to a target amount.

b) Modification of the Traffic Profile with Multiplexing

As explained in the *a) Packets per* second savings Section of 4.5.2, multiplexing can achieve significant reductions in terms of packets per second. In this subsection we have used the Internet trace [47], scaled down to 8 Mbps, and sent it through the multiplexer, using different values for the size limit of the multiplexed packets.

Figure 28 presents the packet size of 15 sec. of the Internet trace. It can be seen that a thick line corresponding to small packets (40-60 bytes), and two lines of big packets (1450 and 1500) are present, which correspond to the peaks in Figure 2. If we multiplex the small packets (using 200 bytes as the size limit), we obtain the traffic distribution shown in Figure 29, where red “x” dots correspond to the multiplexed packets. It can be observed that small packets are multiplexed into bigger ones. In this case, 7,908 packets travel into 395 multiplexed bundles. The rest of the packets (10,932) are not multiplexed.

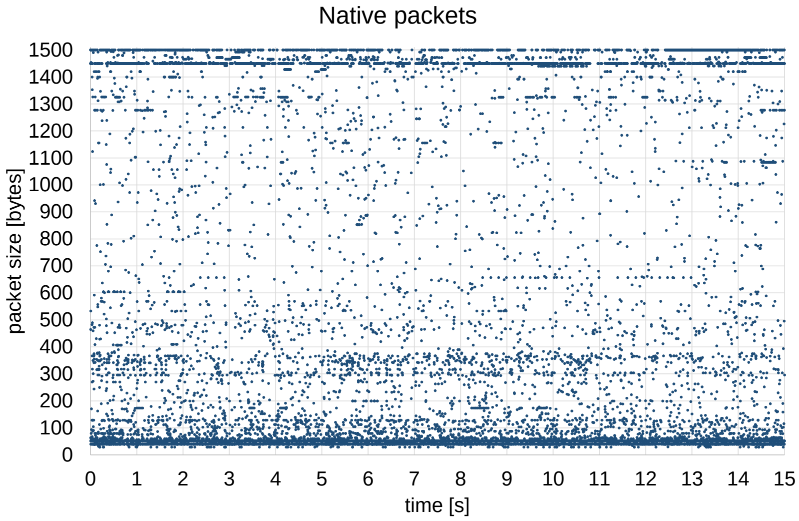


Figure 28: Packet size distribution of the original Internet traffic trace [47]

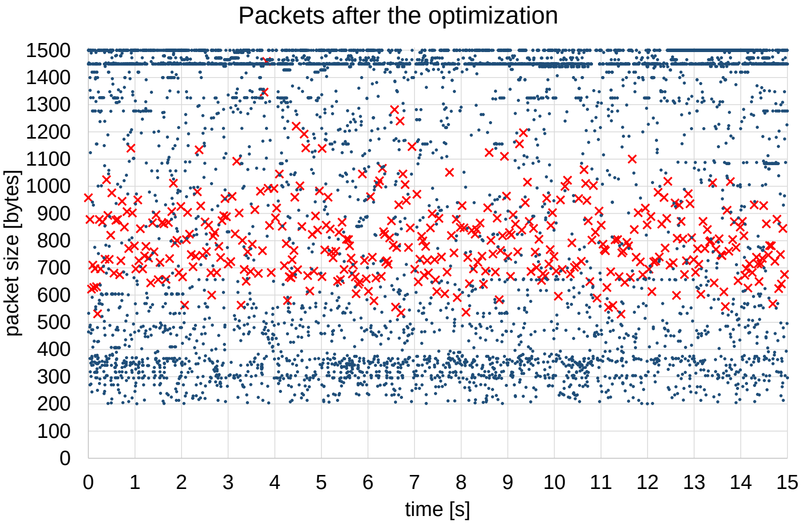


Figure 29: Packet size distribution of the Internet traffic trace, once packets smaller than 200 bytes have been multiplexed

Obviously, if we increase the size limit, more packets will be sent to the multiplexer, so the amount of packets will be further reduced. The reduction in terms of packets per second can be up to 50 % if the size limit is higher. However, Figure 30 shows that the improvement is small, since the saving is mainly produced by the multiplexing of the very small packets. It can be observed here that the savings are similar to those predicted analytically (Figure 25).

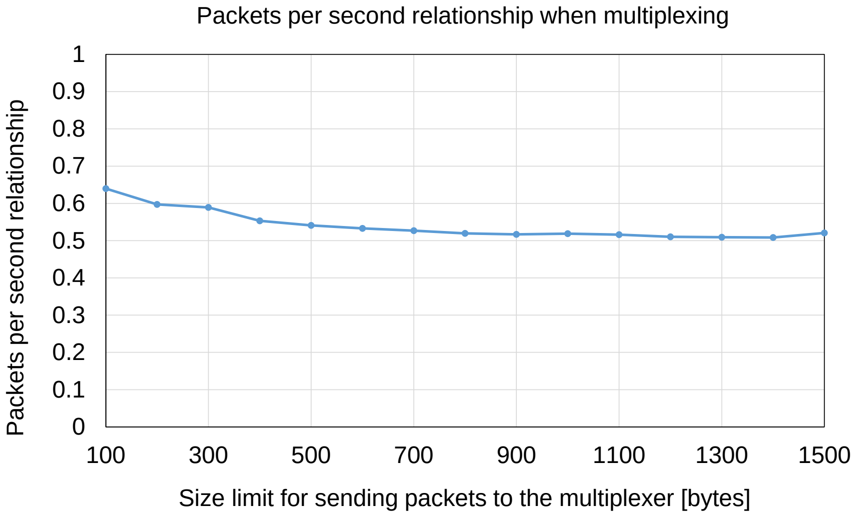


Figure 30: Relationship between the amount of packets per second in the original and the optimised traces

c) Bandwidth Savings

Two different cases have been tested in order to obtain the bandwidth savings:

a) RTP using the wired bottleneck: Five concurrent RTP sessions, using different codecs, are sent through the multiplexer (Figure 31) using the wired bottleneck. It can be observed that the maximum savings are obtained for the codecs with the highest header-to-payload ratio. In this case, the saving is mainly produced by header compression. Multiplexing allows the sending of compressed headers end-to-end, and maintains the tunnelling overhead low. The compression ratio can be up to 46% for certain codecs.

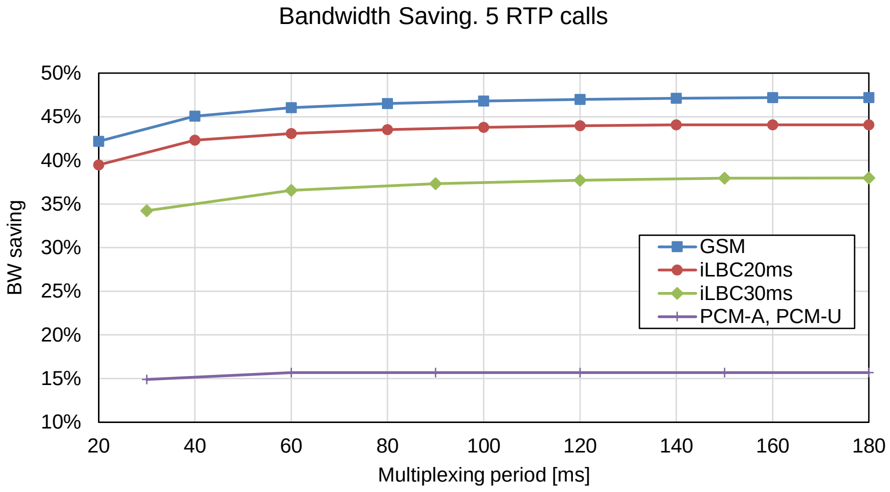


Figure 31: Bandwidth savings for VoIP RTP traffic in a wired connection

b) Small UDP traffic using the wireless bottleneck: A flow of 15,000 small packets per second (60 bytes) is sent through the multiplexer (7.2 Mbps at IP level). The bottleneck is an 802.11ac link at 9 Mbps, but the airtime drawback makes it impossible for the flow to traverse the link: in the first column of Figure 32 (native), it can be seen that when multiplexing is not activated, packet loss is very high. The cause is that the MAC protocol has to act before each packet is sent, so airtime efficiency is poor, taking into account that the packets are only 60 bytes long.

However, if packets are multiplexed (blue left columns in Figure 32), it can be observed that packet loss gets reduced dramatically (if the number of multiplexed packets is higher than 1). In this case, the improvement of the *airtime* drawback achievable with multiplexing is clear: significant savings are obtained because the number of times MAC mechanisms have to be employed is reduced, as a consequence of the packet per second reduction. In addition, if ROHC is activated (patterned right columns), the saving becomes significantly higher, but in this case the reason is the size reduction achieved by header compression of small packets.

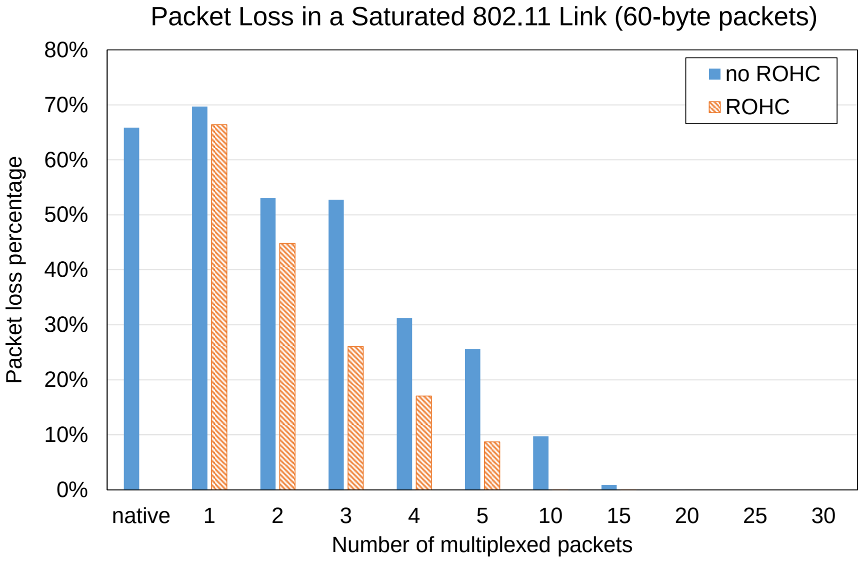


Figure 32: Packet loss reduction in a saturated wireless link

5 Conclusions

This document has presented the first version of the Smart Access Point Solutions being developed within WP3 of the Wi-5 Project. First, a Literature Review has been presented, including the different research fields such as monitoring of the wireless network, automatic service detection, resource management in Wi-Fi WLANs and packet/frame grouping for improving network efficiency.

A global view of the Wi-5 architecture has been provided, including the different entities and the basic description of the functionalities being considered. An approach based on the use of Software Defined Networking is being followed in order to implement the Wi-5 functionalities. The architecture considers a central controller, to which all the APs are connected. It also uses an abstraction called *Light Virtual Access Point*, which means that the controller creates an LVAP for each terminal, which is dynamically assigned to the physical AP where the terminal is located at each moment. Therefore, the AP will use a different LVAP (which includes a specific MAC) for communicating with each terminal. So the terminal will only “see” a single AP, even if it is moving between different APs, thus avoiding the need for re-association.

In addition to Smart AP Solutions, other Cooperative Functionalities have been described. A Fittingness Factor (FF)-based reward algorithm will be implemented in the Wi-5 controller in charge of associating an AP to each new user/flow, taking into consideration the specific bit rate requirements.

Then, a detailed description of the first definition of the Smart AP Solutions has been developed. Regarding performance monitoring, a tool able to automatically detect real-time services e.g. online games, has been presented. It has a first stage where the traffic of interest is used for training purposes, and thereafter it will be able to detect traffic patterns with good precision and accuracy. Different methods for monitoring the radio environment have also been summarised, including the possibility of using a secondary interface only for monitoring purposes.

A scheme of the current implementation of the proposed solutions has been presented, including a summary of the new functionalities added to the selected open-source solution *(Odin)*. The different approaches followed by Radio Resource Management Algorithms have been discussed, including different considerations about the possibility of implementing them using the LVAP approach. The Load Balancing algorithms can be easily implemented in a LVAP scenario, since the re-association of a STA to another AP can be done seamlessly.

Finally, packet grouping policies have been discussed. The potential savings when aggregating frames at Layer 2 have been calculated, and also compared with the possibility of aggregating at Layer 3, which is the only available possibility in legacy devices. This can be useful in certain scenarios as e.g. alternative networks in developing countries, where multi-hop networks based on Wi-Fi are being developed by communities. The Wi-5 controller will be able to enable or disable the packet grouping policies on a per AP basis and allocate users/flows to them based on their traffic requirements.

The main innovative aspects introduced here relate to the combination of LVAPs with multi-channel APs, which will supports seamless handovers, and radio resource management, and the use of packet grouping and aggregation at Layer 3, which can be convenient for saving bandwidth and reducing the amount of sent packets per second. This has also been proposed to the IETF for possible standardisation.

As future work, the seamless handover has to be correctly synchronised with the channel switching in order to work correctly. This would allow the use of different channels in the WLAN, thus reducing the interference level. Another objective is to tune this handover procedure in order to adapt it to the services currently running in the client. New functionalities and control messages will also have to be added to Odin in order to enable the Wi-5 resource management algorithms: a) new procedures able to measure the interference (scanning); b) procedures for the controller to manage the power that an AP sends to each STA, and to request the signal power information from the STAs; c) the integration of packet grouping in the implementation is also necessary.

References

[1] R. Riggio, T. Rasheed, R. Narayanan, “Virtual network functions orchestration in enterprise WLANs,” in Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on , pp.1220-1225, 11-15 May 2015.

[2] N. Foster, R. Harrison, M. J. Freedman, C. Monsanto, J. Rexford, A. Story, D. Walker, “Frenetic: A network programming language,” SIGPLAN Not., vol. 46, no. 9, pp. 279–291, Sep. 2011.

[3] A. Voellmy, H. Kim, N. Feamster, “Procera: A language for highlevel reactive network control,” in Proc. of ACM HotSDN, 2012.

[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner, “OpenFlow: enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review 38, no. 2 (2008): 69-74.

[5] R. Riggio, K.M. Gomez, T. Rasheed, J. Schulz-Zander, S. Kuklinski, M.K. Marina, “Programming Software-Defined wireless networks,” in Network and Service Management (CNSM), 2014 10th International Conference on, pp.118-126, Nov 2014.

[6] Y. Grunenberger, F. Rousseau, “Virtual Access Points for Transparent Mobility in Wireless LANs,” In Wireless Communications and Networking Conference (WCNC), 2010 IEEE (pp. 1-6).

[7] J. Schulz-Zander, L. Suresh, N. Sarrar, A. Feldmann, T. Hühn, R. Merz, “Programmatic orchestration of wifi networks,” in USENIX Annual Technical Conference (USENIX ATC 14), pp. 347-358, Jun 2014.

[8] M.E. Berezin, F. Rousseau, A. Duda, “Multichannel Virtual Access Points for Seamless Handoffs in IEEE 802.11 Wireless Networks,” in Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd , pp.1-5, May 2011.

[9] H. Wu, K. Tan, Y. Zhang, Q. Zhang, “Proactive Scan: Fast Handoff with Smart Triggers for 802.11 Wireless LAN,” in INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, pp.749-757, May 2007.

[10] S. Lee, M. Kim, S. Kang, K. Lee, I. Jung, “Smart scanning for mobile devices in WLANs,” Communications (ICC), IEEE International Conference on. IEEE, 2012.

[11] J. But, G. Armitage, L. Stewart, “Outsourcing automated QoS control of home routers for a better online game experience,” IEEE Commun. Mag., vol. 46, no. 12, pp. 64–70, Dec. 2008.

[12] J. Frank, “Machine learning and intrusion detection: Current and future directions,” in Proc. 17th Nat. Comput. Security Conf., Oct. 1994, pp. 22–33.

[13] A. McGregor, M. Hall, P. Lorier, and J. Brunskill, “Flow clustering using machine learning techniques,” in Proc. PAM, Apr. 2004, pp. 205–214.

[14] M. Roughan, S. Sen, O. Spatscheck, and N. Duffield, “Class-of-service mapping for QoS: A statistical signature-based approach to IP traffic classification,” in Proc. 4th ACM SIGCOMM IMC, Oct. 2004, pp. 135–148.

[15] S. Zander, T. Nguyen, and G. Armitage, “Automated traffic classification and application identification using machine learning,” in Proc. IEEE 30th LCN, Nov. 2005, pp. 250–257.

[16] T. T. T. Nguyen, G. Armitage, P. Branch, S. Zander, “Timely and Continuous Machine-Learning-Based Classification for Interactive IP Traffic,” in Networking, IEEE/ACM Transactions on, vol.20, no.6, pp.1880-1894, Dec. 2012.

[17] IEEE 802.11ac, 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 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz, 2013.

[18] IEEE 802.11n, 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 5: Enhancements for Higher Throughput, IEEE Std 802.11n-2009, 2009.

[19] IEEE 802.11h, 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.

[20] IEEE 802.11, 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 1: Radio Resource Measurement of Wireless LANs, IEEE Std 802.11k-2008, 2008.

[21] ETSI standard EN 301 893 V1.7.0, Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive, 2012.

[22] D. Qiao, S. Choi, “New 802.11h Mechanisms Can Reduce Power Consumption,” IT Professional, vol. 8, no.2, pp. 43-48, Mar-Apr. 2006.

[23] A. Zubow, M. Doring, M. Chwalisz, A. Wolisz, “A SDN approach to spectrum brokerage in infrastructure-based Cognitive Radio networks,” in Dynamic Spectrum Access Networks (DySPAN), 2015 IEEE International Symposium on , pp.375-384, Sept. 29 2015-Oct. 2 2015

[24] S. Chieochan, E. Hossain, J. Diamond, “Channel assignment schemes for infrastructure-based 802.11 WLANs: a survey,” IEEE Communications Surveys and Tutorials 2010; 12(1): 124–136.

[25] A. Hills, “Large-Scale Wireless Lan Design,” IEEE Comm. Magazine, vol. 39, no. 11, pp. 98-107, Nov. 2001.

[26] K.K. Leung, B.-J.J. Kim, “Frequency Assignment for IEEE 802.11 Wireless Networks,” Proc. IEEE Vehicular Technology Conf., Jeju, South Korea, 22-25 April 2003.

[27] Y. Lee, K. Kim, Y. Choi, “Optimization of AP Placement and Channel Assignment in Wireless LANs,” Proc. IEEE Conf. Local Computer Networks, Tampa, FL, USA, 6-8 November 2002.

[28] I. Broustis, K. Papagiannaki, S.V. Krishnamurthy, M. Faloutsos, V. Mhatre, “Mdg: Measurement-Driven Guidelines for 802.11 WLAN Design,” Proc. ACM MobiCom, Montreal, QC, Canada, 9-14 Sept. 2007.

[29] R. Murty, J. Padhye, R. Chandra, A. Wolman, B. Zill, "Designing High Performance Enterprise Wi-Fi Networks," Proc. Symp. Networked Systems Design and Implementation (NSDI), San Francisco, California, USA, 16-18 April 2008.

[30] M. Achanta, "Method and Apparatus for Least Congested Channel Scan for Wireless Access Points," US Patent No. 20060072602, Apr. 2006.

[31] A. Mishra, V. Shrivastava, D. Agrawal, S. Banerjee, S. Ganguly, "Distributed Channel Management in Uncoordinated Wireless Environments," Proc. ACM MobiCom, Los Angeles, CA, USA, 24-29 Sept. 2006.

[32] A. Mishra, S. Banerjee, W. Arbaugh, "Weighted Coloring Based Channel Assignment for WLANs," Proc. ACM SIGMOBILE Computing and Comm. Rev., vol. 9 issue 4, Oct. 2005

[33] X. Yue, C-F. M. Wong, S-H. Gary Chan, "CACAO: Distributed Client-Assisted Channel Assignment Optimization for Uncoordinated WLANs", IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 9, pp. 1433-1440, Sep. 2011.

[34] S. Kamiya, K. Nagashima, K. Yamamoto, T. Nishio, M. Takayuki, M. Morikura, T. Sugihara, "Joint range adjustment and channel assignment for overlap mitigation in dense WLANs," in Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015 IEEE 26th Annual International Symposium on , pp.1974-1979, Aug. 30 2015-Sept. 2 2015

[35] K. Zhou, X. Jia, L. Xie, Y. Chang, X. Tang, "Channel Assignment for WLAN by Considering Overlapping Channels in SINR Interference Model", International Conference on Computing, Networking and Communications (ICNC), Maui, Hawaii, USA 30 Jan.- 2 Feb., 2012.

[36] J. Herzen, et al., "Distributed spectrum assignment for home WLANs", International Conference on Computer Communications (INFOCOM), Turin, Italy, 14-19 Apr. 2013.

[37] W. Lingzhi, et al, "Online channel selection and user association in high-density WiFi networks", International Conference on Communications (ICC), London, UK, 8-12 Jun. 2015.

[38] S. Kajita, et al, "A channel selection strategy for WLAN in urban areas by regression analysis" International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Larnaca, Cyprus, 8-10 October 2014.

[39] D. Qiao, S. Choi, K.G. Shin, "Interference Analysis and Transmit Power Control in IEEE 802.11a/h Wireless LANs," IEEE/ACM Transactions on Networking, vol. 15, no.5, pp. 1007-1020, Oct. 2007.

[40] V. Navda, R. Kokku, S. Ganguly, S. Das, "Slotted Symmetric Power Control in managed WLANs," Technical Report, NEC Laboratories America, 2007.

[41] K. Ramachandran, R. Kokku, H. Zhang, M. Gruteser, "Symphony: Synchronous Two-Phase Rate and Power Control in 802.11 WLANs," IEEE/ACM Transactions on Networking, vol. 18, no. 4, 1289-1302, Aug. 2010.

[42] L.-H. Yen, T.-T. Yeh, K.-H. Chi, "Load Balancing in IEEE 802.11 Networks" , IEEE Internet Computing, Jan-Feb 2009, pp. 56-64

[43] I. Papanikos, M. Logothetis, "A study on dynamic load balance for IEEE 802.11 b wireless LAN," in Proc. 8th International Conference on Advances in Communication and Control (COMCON), Crete, 25-29 June 2001.

[44] Cisco Systems Inc., “Data sheet for Cisco Aironet 1200 series,” 2004, http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/product_data_sheet09186a00800937a6.pdf/, [Accessed December 2015]

[45] R. Murty, J. Padhye, R. Chandra, A. Wolman, B. Zill, “Designing high performance enterprise wi-fi networks,” Proc. 5th USENIX Symposium on Networked Systems Design and Implementation, San Francisco, CA, USA, 16-18 April 2008.

[46] R. Chandra, P. Bahl, “MultiNet: Connecting to multiple IEEE 802.11 networks using a single wireless card,” in Proc. INFOCOM 2004. 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, Hong Kong, 7-11 Mar. 2004.

[47] The CAIDA UCSD equinix-chicago- 20150219-130000, https://data. caida.org/datasets/passive-2015/equinix-chicago/20150219-130000.UTC/equinix-chicago.dirA.20150219-125911.UTC.anon.pcap.gz

[48] B. Ginzburg, A. Kesselman, “Performance analysis of A-MPDU and A-MSDU aggregation in IEEE 802.11n,” Sarnoff Symposium, 2007 IEEE, vol., no., pp.1,5, April 30 2007-May 2 2007.

[49] 3Com® Switch 4200 Family. Data Sheet, available at http:// ftp.maxdata.de/Accessories/Connectivity/3Com/Datasheets/200806_3Com_OfficeConnect_4226T.pdf

[50] Intel White Paper “Impact of the Intel Data Plane Development Kit (Intel DPDK) on Packet Throughput in Virtualized Network Environments,” available at https://networkbuilders.intel.com/docs/ IntelDPDK_PacketThroughputVirtualNetwork.pdf

[51] R. Bolla, R. Bruschi, F. Davoli, F .Cucchietti, “Energy Efficiency in the Future Internet: A Survey of Existing Approaches and Trends in Energy-Aware Fixed Network Infrastructures”, Communications Surveys & Tutorials, IEEE, vol.13, no.2, pp.223, 244, 2nd Quarter 2011.

[52] D. Murray, T. Koziniec, K. Lee, and M. Dixon, “Large MTUs and internet performance,” in High Performance Switching and Routing (HPSR), IEEE 13th International Conference on, pp. 82-87, 2012.

[53] T. Selvam, S. Srikanth, “A frame aggregation scheduler for IEEE 802.11n,” Communications (NCC), 2010 National Conference on, vol., no., pp.1, 5, 29-31 Jan. 2010.

[54] J. Liu, M. Yao, Z. Qiu, “Enhanced Two-Level Frame Aggregation with Optimized Aggregation Level for IEEE 802.11n WLANs,” in Communications Letters, IEEE , vol.19, no.12, pp.2254-2257, Dec. 2015

[55] P. Cameron, D. Crocker, D. Cohen, J. Postel, RFC1692, Transport Multiplexing Protocol (TMux), Aug. 1994.

[56] R. Pazhyannur, I. Ali, C. Fox, RFC3153, PPP Multiplexing, Aug. 2001.

[57] B. Thompson, T. Koren, D. Wing, RFC4170, Tunneling Multiplexed Compressed RTP (TCRTP), Nov. 2005

[58] R. M. Pereira, L.M. Tarouco, “Adaptive Multiplexing Based on E-model for Reducing Network Overhead in Voice over IP Security Ensuring Conversation Quality,” in Proc. Fourth international Conference on Digital Telecommunications, Washington, DC, 53-58 , July 2009

[59] K. Pentikousis, E. Piri, J. Pinola, F. Fitzek, T. Nissilä, I. Harjula, “Empirical evaluation of VoIP aggregation over a fixed WiMAX testbed,” In Proc. 4th international Conference on Testbeds

and Research infrastructures For the Development of Networks & Communities. Innsbruck, Austria, Mar. 2008.

[60] J. Saldana, J. Fernandez-Navajas, J. Ruiz-Mas, D. Wing, M. A. M. Perumal, M. Ramalho, G. Camarillo, F. Pascual, D. R. Lopez, M. Nunez, D. Florez, J. A. Castell, T. de Cola, M. Berioli, “Emerging Real-time Services: Optimizing Traffic by Smart Cooperation in the Network,” IEEE Communications Magazine, Vol. 51 n. 11 pp 127-136, Nov 2013.

[61] J. Saldana, D, de Hoz, J. Fernandez-Navajas, J. Ruiz-Mas, F. Pascual, D. R. Lopez, D. Florez, J. A. Castell, M. Nunez. "Small-Packet Flows in Software Defined Networks: Traffic Profile Optimization". Journal of Networks, 10(4), 2015, 176-187. doi:10.4304/jnw.10.4.176-187.

[62] A. Raschellà, J.Pérez-Romero, O. Sallent, A. Umbert, “On the use of POMDP for Spectrum Selection in Cognitive Radio Networks”, 8th International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM 2013), Washington DC USA, 08 - 10 July 2013.

[63] J. Saldana, J. L. de la Cruz, L. Sequeira, J. Fernandez-Navajas, J. Ruiz-Mas, “Can a Wi-Fi WLAN Support a First Person Shooter?,” NetGames 2015, The 14th International Workshop on Network and Systems Support for Games Zagreb, Croatia, December 3-4, 2015.

[64] E. Kohler, R. Morris, B. Chen, J. Jannotti, M.F. Kaashoek, “The Click modular router,” ACM Transactions on Computer Systems (TOCS), 18(3), 263-297, 2000.

[65] M. Dick, O. Wellnitz, L. Wolf, “Analysis of factors affecting players' performance and perception in multiplayer games,” in Proc. 4th ACM SIGCOMM workshop on Network and system support for games (NetGames '05). ACM, New York, NY, USA, 1-7, 2005.

[66] S.M. Günther, M. Leclaire, J. Michaelis, G. Carle, “Analysis of Injection Capabilities and Media Access of IEEE 802.11 Hardware in Monitor Mode,” in Proc. 14th IEEE/IFIP Symposium on Network Operations and Management (NOMS 2014), May, 2014, Krakow, Poland.

[67] S. R. Garner, “Weka: The waikato environment for knowledge analysis,” Proceedings of the New Zealand computer science research students conference. 1995.

[68] C. Griwodz, P. Halvorsen, “The fun of using TCP for an MMORPG,” Proc. international workshop on Network and operating systems support for digital audio and video (NOSSDAV 2006). ACM, New York, NY, USA. doi: 10.1145/1378191.1378193

[69] CC. Wu, KT. Chen, CM. Chen, P. Huang, CL. Lei, “On the Challenge and Design of Transport Protocols for MMORPGs,” Multimedia Tools and Applications, 2009, Vol. 45, No. 1: 7-32. doi: 10.1007/s11042-009-0297-5

[70] M. Suznjevic, O. Dobrijevic, M. Matijasevic, “MMORPG Player actions: Network performance, session patterns and latency requirements analysis,” Multimedia Tools Appl. 45, 2009, 1-3: 191-214. doi: 10.1007/s11042-009-0300-1

[71] Newzoo, Free Global Trend Report 2012-2016.
Available online: http://www.newzoo.com/wp-content/uploads/2011/06/Newzoo_Free_Global_Trend_Report_2012_2016_V2.pdf, [Accessed Apr 2014]

[72] CNet, World of Warcraft subscriber base hits 12 million.
Available at http://www.cnet.com/news/world-of-warcraft-subscriber-base-hits-12-million/, [Accessed Apr 2014].

[73] IEEE 802.11k, 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 1: Radio Resource Measurement of Wireless LANs.

[74] IEEE Std 802.11™-2012 (Revision of IEEE Std 802.11-2007) Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[75] Wi-Fi Alliance, Wi-Fi Multimedia™ (WMM®) http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-wmm-programs, [Accessed Nov 2015].

[76] IEEE 802.11e-2005 - 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: Medium Access Control (MAC) Quality of Service Enhancements.

[77] B. Thompson, T. Koren, D. Wing, RFC4170, Tunneling Multiplexed Compressed RTP (TCRTP), Nov. 2005.

[78] J. Saldana, “Simplemux. A generic multiplexing protocol,” draft-saldana-tsvwg-simplemux-02 (Jan. 2015). Available at http://datatracker.ietf.org/doc/draft-saldana-tsvwg-simplemux/

[79] J. Saldana, I. Forcen, J. Fernandez-Navajas, J. Ruiz-Mas, “Improving Network Efficiency with Simplemux,” IEEE CIT 2015, International Conference on Computer and Information Technology, pp. 446-453, 26-28 October 2015, Liverpool, UK.

[80] J. Saldana, D. Wing, J. Fernandez-Navajas, M.A.M. Perumal, F. Pascual Blanco, “Tunneling Compressed Multiplexed Traffic Flows (TCM). Reference Model,”draft-saldana-tsvwg-tcmtf-09” (Contributing authors: Gonzalo Camarillo, Michael A. Ramalho, Jose Ruiz Mas, Diego Lopez Garcia, David Florez Rodriguez, Manuel Nunez Sanz, Juan Antonio Castell Lucia). (Jun. 2015) Available at http://datatracker.ietf.org/doc/draft-saldana-tsvwg-tcmtf/

[81] J. Saldana et al, “Alternative Network Deployments. characterization, technologies and architectures,” draft-irtf-gaia-alternative-network-deployments-01, (Jul. 2015) Available at http://datatracker.ietf.org/ doc/draft-irtf-gaia-alternative-network-deployments/

[82] L. Cerda-Alabern, “On the topology characterization of Guifi.net,” Proceedings Wireless and Mobile Computing, Networking and Communications, IEEE 8th International Conf, pp. 389-396, 2012.

[83] C. Rey-Moreno, I. Bebea-Gonzalez, I. Foche-Perez, R. Quispe-Taca, L. Linan-Benitez and J. Simo-Reigadas, “A telemedicine WiFi network optimized for long distances in the Amazonian jungle of Peru,” Proceedings of the 3rd Extreme Conference on Communication: The Amazon Expedition, ExtremeCom '11 ACM, 2011

[84] M. Ford, “Workshop report: reducing internet latency,” ACM SIGCOMM Computer Communication Review, Volume 44, Issue 2, pp 80-86, 2014.

[85] J. Saldana, J. Fernandez-Navajas, J. Ruiz-Mas, E. Viruete Navarro, L. Casadesus, “Online FPS Games: Effect of Router Buffer and Multiplexing Techniques on Subjective Quality Estimators,” Multimedia Tools and Applications, Volume 71, Issue 3, pp 1823-1856, August 2014, Springer. doi 10.1007/s11042-012-1309-4.

[86] M. Suznjevic, J. Saldana, “Delay Limits for Real-Time Services,” draft-suznjevic-dispatch-delay-limits-00. (Dec. 2015). Available at http://datatracker.ietf.org/doc/draft-suznjevic-dispatch-delay-limits/

[87] K. Sandlund, G. Pelletier, L-E. Jonsson, RFC 5795, The Robust Header Compression (ROHC) Framework, 2010.

[88] Internet Assigned Numbers Authority (IANA) Assigned Internet Protocol Numbers, available at http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

[89] A. Botta, A. Dainotti, A. Pescapè, "A tool for the generation of realistic network workload for emerging networking scenarios", Computer Networks (Elsevier), 2012, Volume 56, Issue 15, pp 3531-3547.

Annex A. Simplemux Proposal for Packet grouping at Layer 3

This annex briefly describes Simplemux protocol, which is specified in [8]. The aim of the protocol is the reduction of the overhead of Layer 3 multiplexing, while keeping the design as simple as possible. The main elements are the *separators*, i.e. the small headers inserted before each packet. The *length* of the multiplexed packet that comes next is the main information included in these separators.

Simplemux does not act at Layer 2, but at upper layers, so it has been proposed to the IETF [78]. It does not require a session setup, since the idea is that a specific IANA Protocol Number [88] could be reserved for Simplemux. Thus, if the destination machine receives a packet with this protocol number, and if it implements Simplemux, it just demultiplexes it and extracts the packets. There is no need to set up a session or to store any session parameters.

The objective of Simplemux is not to multiplex packets at the end hosts, i.e. the ones originating the flows. Although this is still possible, the benefit would be small, since the probability of having a high number of small-packet flows between the same pair of machines is low. Thus, the idea is to run Simplemux between a pair of network core machines (Ingress and Egress), shown in Figure 33, to optimise traffic flows sharing this path. The optimisation therefore covers a number of network hops, but the intermediate routers just have to route packets at the IP level, so they do not have to implement Simplemux.

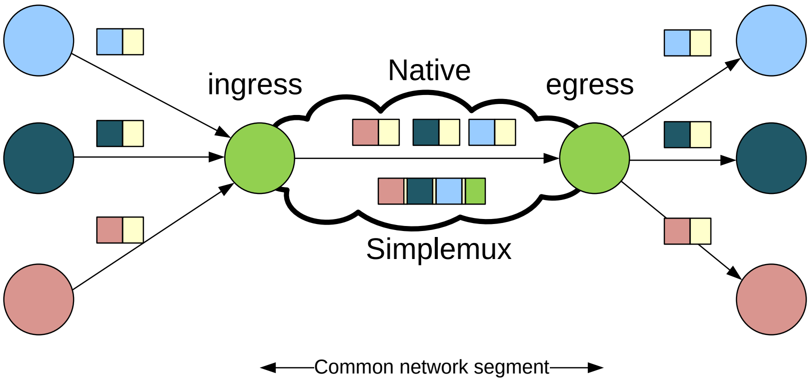


Figure 33: Simplemux optimisation between an Ingress and an Egress machine

The protocol allows the inclusion of packets belonging to different protocols. This provides a high degree of flexibility, since it avoids the necessity of creating one tunnel for each kind of traffic. As an example, ROHC-compressed packets *(Protocol number* = 142) may travel with normal IP packets *(Protocol number* = 4), as shown in Figure 34.

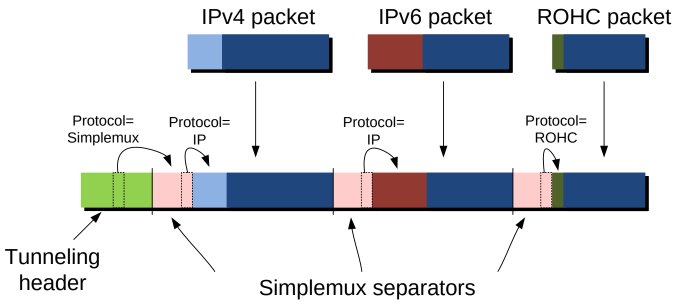
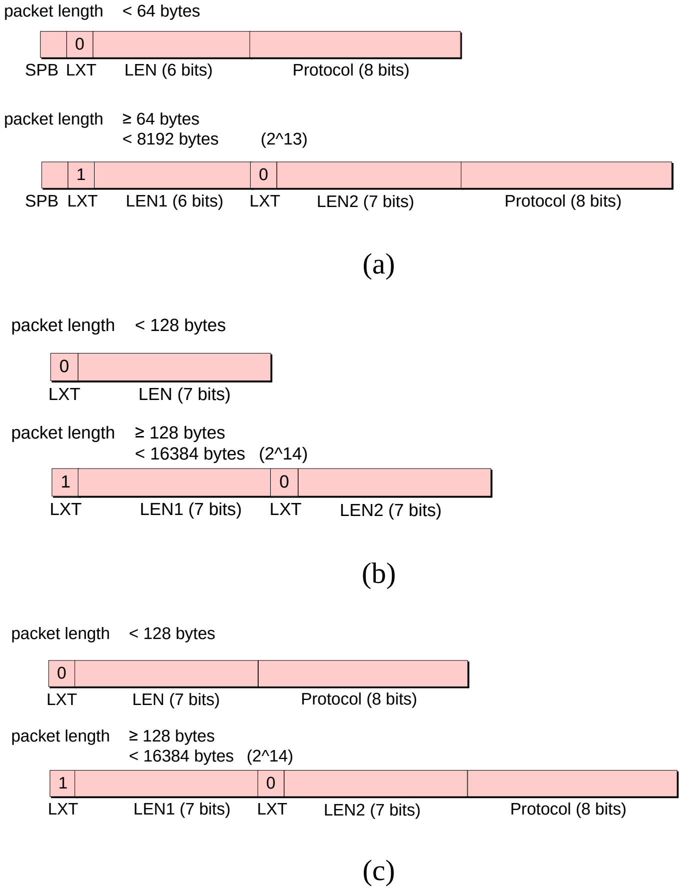


Figure 34: Scheme of a Simplemux packet including different protocols

However, there will be many cases where all the packets included in a multiplexed bundle belong to the same protocol. Therefore, the format of the first separator is slightly different from the rest. It includes a *Single Protocol Bit (SPB)* which is set when packets belonging to a single protocol are carried, thus saving a byte on each of the subsequent separators. In addition, all the bytes of the separators include a *Length eXTension bit (LXT)* which is set when the length of the packet requires an extra byte. This permits Simplemux to multiplex packets of any length, also allowing it to adjust the size of the field according to the packet length.

The format of the separators is shown in Figure 35. In a), the format of the *first* separator is shown, in b) the *non-first* separators when a single protocol is carried, and in c) the *non-first* separator when packets belong to different protocols.

It can be observed that the overhead required by Simplemux separators is minimal. For example, if a set of small packets belonging to the same protocol travel together, the first separator would require two or three bytes, but the rest of the packets would only need a single byte, or two if they are bigger than 128 bytes.


packet length < 64 bytes
0
SPB LXT LEN (6 bits) Protocol (8 bits)
packet length ≥ 64 bytes
< 8192 bytes (2^13)
1
0
SPB LXT LEN1 (6 bits) LXT LEN2 (7 bits) Protocol (8 bits)
packet length < 128 bytes
0
LXT LEN (7 bits)
packet length ≥ 128 bytes
< 16384 bytes (2^14)
1
0
LXT LEN1 (7 bits) LXT LEN2 (7 bits)
packet length < 128 bytes
0
LXT LEN (7 bits) Protocol (8 bits)
packet length ≥ 128 bytes
< 16384 bytes (2^14)
1
0
LXT LEN1 (7 bits) LXT LEN2 (7 bits) Protocol (8 bits)

(a)

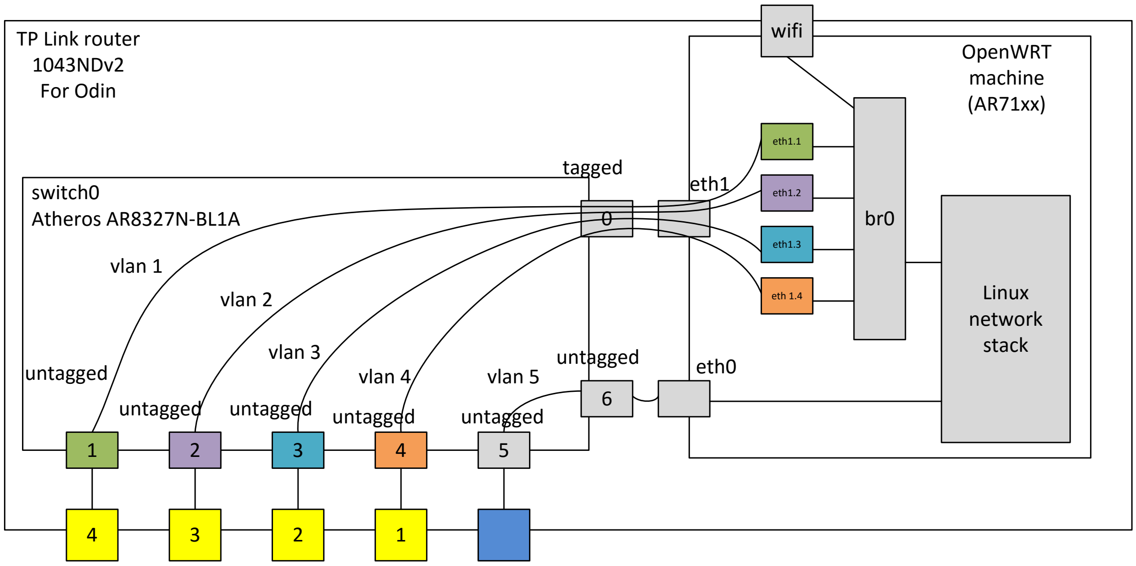
(b)

(c)

Figure 35: Scheme of Simplemux separators: a) first separator; b) non-first separator when all the packets belong to the same protocol; c) non-first separator including the Protocol Number

Annex B. Adaptation of an AP for its use with Odin

The original scheme of the internal switch of the TP-Link 1043ND AP can be found in the OpenWrt wiki[21]. The scheme has to be modified in order to make it able to run with OpenvSwitch. Four VLANs are defined, and the bridge *br0* is then controlled by the OpenFlow controller.



- **Tagged** means that the switch gives the VLAN header field to the end node hearing in that switch port
- If the switch port is **untagged**, the machine is not able to see the VLAN header

The configuration of the interfaces, firewall and wireless set-up files has to be modified this way:

A. Edit the content of `/etc/config/network` file:

```
config interface 'loopback'
      option ifname 'lo'
      option proto 'static'
      option ipaddr '127.0.0.1'
      option netmask '255.0.0.0'

config interface 'lan1'
      option ifname 'eth1.1'
      option force_link '1'
      option proto 'static'
      option netmask '255.255.255.0'
      option ip6assign '60'
      option ipaddr '192.168.1.5'

config interface 'lan2'
        option ifname 'eth1.2'
        option force_link '1'
        option proto 'static'
        option netmask '255.255.255.0'
        option ip6assign '60'
        option ipaddr '192.168.2.5'

config interface 'lan3'
        option ifname 'eth1.3'
        option proto 'static'
```

[21] http://wiki.OpenWrt.org/_detail/media/wr1043ndv2-schematics.png?id=toh%3Atp-link%3Atl-wr1043nd

```
config interface 'lan4'
        option ifname 'eth1.4'
        option proto 'static'

config interface 'wan'
      option ifname 'eth0'
      option proto 'static'
      option netmask '255.255.255.0'
      option ipaddr '155.210.157.226'
      option gateway '155.210.157.254'
      option broadcast '155.210.157.255'
      option dns '155.210.12.9'

config switch
      option name 'switch0'
      option reset '1'
      option enable_vlan '1'
        option enable_learning '0'

config switch_vlan
      option vlan '1'
      option ports '1 0t'
      option device 'switch0'

config switch_vlan
        option vlan '2'
        option ports '2 0t'
        option device 'switch0'

config switch_vlan
        option vlan '3'
        option ports '3 0t'
        option device 'switch0'

config switch_vlan
        option vlan '4'
        option ports '4 0t'
        option device 'switch0'

config switch_vlan
        option vlan '5'
        option ports '5 6'
        option device 'switch0'
```

B. Edit the content of the `/etc/config/firewall` file:

```
config defaults
        option syn_flood        1
        option input            ACCEPT
        option output           ACCEPT
        option forward          ACCEPT
```

C. Edit the content of the `/etc/config/wireless` file:

```
config wifi-device 'radio0'
option type 'mac80211'
option hwmode '11n'
option path 'platform/qca955x_wmac'
option htmode 'HT20'
option txpower '30'
option country 'US'
option channel '6'

config wifi-iface
option device 'radio0'
option network 'lan'
option mode 'ap'
option encryption 'none'
option ssid 'wi5-unizar-226'
```