Experimenting With Commodity 802.11 Hardware: Overview and Future Directions

Pablo Serrano, *Member, IEEE*, Pablo Salvador, Vincenzo Mancuso, *Member, IEEE*, and Yan Grunenberger

***Abstract*—The huge adoption of 802.11 technologies has triggered a vast amount of experimentally-driven research works. These works range from performance analysis to protocol enhancements, including the proposal of novel applications and services. Due to the affordability of the technology, this experimental research is typically based on commercial off-the-shelf (COTS) devices, and, given the rate at which 802.11 releases new standards (which are adopted into new, affordable devices), the field is likely to continue to produce results. In this paper, we review and categorise the most prevalent works carried out with 802.11 COTS devices over the past 15 years, to present a timely snapshot of the areas that have attracted the most attention so far, through a taxonomy that distinguishes between performance studies, enhancements, services, and methodology. In this way, we provide a quick overview of the results achieved by the research community that enables prospective authors to identify potential areas of new research, some of which are discussed after the presentation of the survey.**

***Index Terms*—Wireless LAN, 802.11, experimentation, commercial off-the-shelf.**

I. Introduction

THE reasons for the success of the 802.11 standard [1] are many-fold: the use of unlicensed spectrum, the reduction of cost due to economies of scale, their ease of management, or the ability of the IEEE 802.11 Standard Group to maintain the development of subsequent amendments to overcome limitations as they are detected. The research community has not remained oblivious to this success, but quite the opposite. Indeed, searching in *Google Scholar* for the number of scientific contributions per year with the term "802.11" provides the references per year illustrated in Fig. 1. These results confirm that 802.11 has attracted a significant amount of attention from the scientific community, with more than 165k citations until 2014. As the figure shows, the number of references experienced a sustained growth until 2010 (13 years after the first standard was published!) and seems to have "stabilised" during the last years.

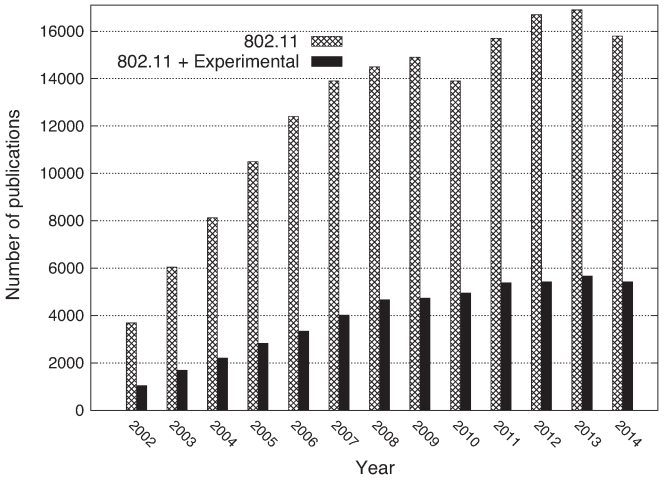

Fig. 1. Number of scientific contributions per year according to *Google Scholar* as of January 31st, 2015.

One particular feature of this area of research is the amount of work that have been performed through experimentation with real-life devices. Indeed, given the wide availability of this technology and the small cost of the devices, many researchers have based their findings on commercial off-the-shelf (COTS) devices. We illustrate this also in Fig. 1, with the search term "802.11 + Experimental". According to these results, between 20% and 34% of the scientific contributions were based on experimentation, showing a similar trend in terms of results as the global one.

Motivated by these results, and the maturity of 802.11 research, in this work we perform an extensive survey of the experimentation performed with 802.11 COTS devices. In this way, we also help future researchers and practitioners to understand the achievements and areas of research addressed so far, so it is less likely that they end up "reinventing the wheel" when facing issues already tackled. We provide a detailed overview of the state of the art via a thorough taxonomy, and provide a summary of the methodologies used to perform the works. Building on these analyses, we discuss some potential ideas for future areas of research.

The rest of this article is organised as follows: in Section II, we present the methodology that we follow to collect the set of references and introduce the taxonomy that we use to display the works. Based on this taxonomy, in Sections III–VI, we provide, for each category, an overview of the most relevant results. In Section VII, we provide a summary of the methodologies followed in the reviewed papers to conduct the experiments,

Manuscript received September 4, 2014; revised February 12, 2015; accepted March 22, 2015. Date of publication March 30, 2015; date of current version May 19, 2015. This work has been partly supported by the European Community through the CROWD project (FP7-ICT-318115) and by the Madrid Regional Government through the TIGRE5-CM program (S2013/ICE-2919). Y. Grunenberger's work was carried out while he was with Telefonica I+D.

P. Serrano is with Department of Telematic Engineering, Universidad Carlos III de Madrid, 28911 Madrid, Spain (e-mail: pablo@it.uc3m.es).

P. Salvador and V. Mancuso are with IMDEA Networks Institute, 28912 Leganés, Spain, and also with Department of Telematic Engineering, Universidad Carlos III de Madrid, 28911 Madrid, Spain (e-mail: josepablo.salvador@imdea.org; vincenzo.mancuso@imdea.org).

Y. Grunenberger was with Telefonica I+D, 08019 Barcelona, Spain. He is now with Qualcomm Spain, 08005 Barcelona, Spain (e-mail: yan-tid@grunenberger.net).

Digital Object Identifier 10.1109/COMST.2015.2417493

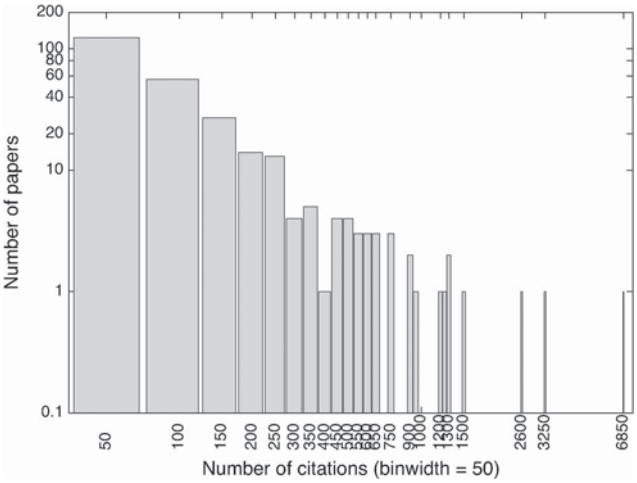

Fig. 2. Distribution of the number of citations per paper.

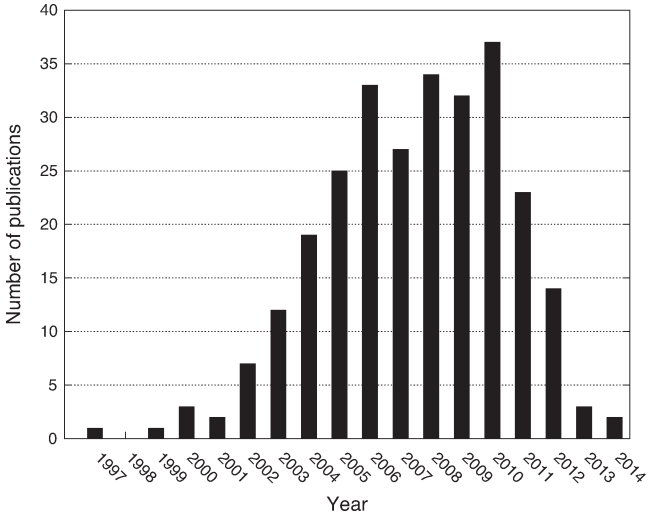

Fig. 3. References in our survey per year of publication.

and in Section VIII we point out some future areas of research and conclude the article.

II. Overview

We decided to limit our study to those works based on COTS 802.11 interfaces, and to not consider those studies based on Software Defined Radio platforms, e.g., WARP, GNU-Radio or SoftWifi. Although this decision leaves out, among others, remarkable works on extensions to 802.11, like new channel bonding schemes [2] or sub-channel random access [3], we believe that this decision provides a more accurate vision of the research performed on Wi-Fi networks, as the above specialised hardware typically requires notable investments in terms of resources and focuses on the PHY enhancements.

A. Methodology

We collected our set of references by first reviewing the published papers in the main conferences from 1999 till 2013, checking references therein, and performing searches in the main databases of the area, namely, ACM Digital Library,[1] Citeseer,[2] Google Scholar,[3] and IEEE Xplore.[4] Then, we updated our data over the years by eliminating duplicates and identifying those papers citing the ones already in our set. To focus on the most relevant contributions, we decided to leave out of our survey those papers that are older than 5 years and have less than 10 citations. Our study covers approximately 300 papers, with around 1200 authors publishing in more than 60 different venues over almost 15 years. We provide in Fig. 2 a histogram of the number of papers, grouped by their number of citations (according to Google Scholar as of January 31st 2015) in bins of width 50.

To illustrate the amount of work sampled over the years, we counted the number of publications collected per year, and represented the corresponding numbers in Fig. 3. From the figure, we can identify that the amount of works for the "early years" of 802.11 experimentation shows the same growth depicted in Fig. 1, but for the most recent years our study consists of a relatively smaller number of results. This is caused for (at least) two main reasons: first, the proliferation of Software Defined Radio (SDR) platforms to mimic the operation of 802.11, which are becoming more affordable and supports the implementation of advanced schemes, way beyond the features of COTS platforms and drivers; second, the unavoidable bias for older, "classic" papers when gathering data from databases, as less timely papers on a topic have a smaller chance to get attention from the research community. Despite these two issues, we believe that our dataset accurately captures the main achievements in 802.11 experimentation.

B. Taxonomy

We believe that the most insightful way categorise previous works is to categorise them by *purpose*, i.e., the main motivation behind the work. Based on this, our taxonomy is divided into the following four main blocks, depicted in Fig. 4:

Basic Functionality: Here we perform evaluations of the default behaviour, i.e., measurements tailored to understand certain limitations of the standard or well-known protocols running over 802.11, and "good practises" to maximise the performance with a plain, *Vanilla* configuration. Here we also place those works aiming at the validation of analytical models over real-life deployments.

Services: In this category, we report those works in which the focus is not on basic performance, but to understand the behaviour of a particular service in WLANs, e.g., providing seamless mobility, performing efficient paging, or even analysing the symptoms of poor performance to support easy troubleshooting.

Enhancements: Many times, once an issue has been identified in any of the above categories, researchers have proposed enhancements over the default behaviour to address it. In this

[1] http://dl.acm.org
[2] http://citeseerx.ist.psu.edu
[3] http://scholar.google.com
[4] http://ieeexplore.ieee.org/Xplore/home.jsp

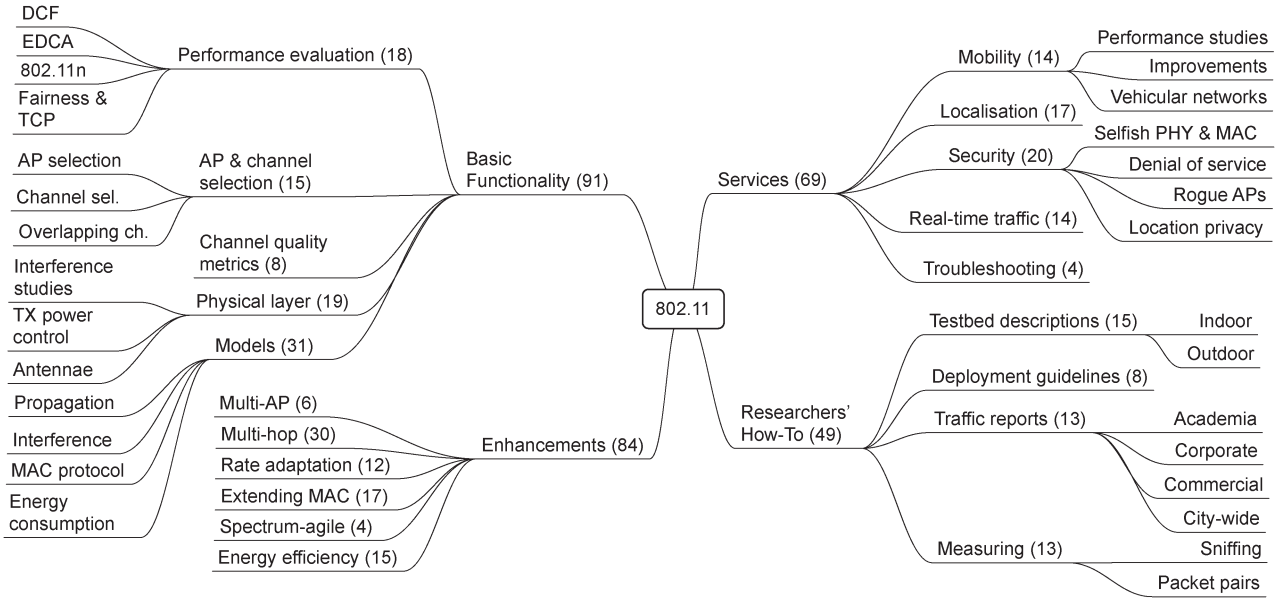

Fig. 4. Taxonomy proposed. In parenthesis, number of papers reviewed.

category we place those works proposing extensions and improvements to the standard, which range from relatively simple modifications for multi-AP management, to the proposal of new MACs that change the backoff rules of 802.11.

Researcher How-To: Finally, here we categorise those works in which researchers have not presented a new scheme, or analysed with great care the performance of the protocol, but instead the main focus is on the research methodology itself. These works aim at supporting other researchers interested in 802.11 experimentation, by providing actual traffic measurements from real life deployments, describing "best practises" to deploy testbeds, or analysing the performance of the building blocks of proposed extensions (e.g., sniffing traffic, inferring techniques).

C. Related Surveys on 802.11 Aspects

One distinct feature of our survey is that we focus exclusively on experimental work carried out with commercial devices, while previous surveys focus on a specific topic, such as mesh networks [4] or localisation [5], without distinguishing between theoretical, simulation-based and experimental contributions. Based on the categories proposed in our taxonomy, we provide for the interested reader a snapshot of the most relevant surveys in Table I, which is split into four sections according to our four main categories.[5] While performing this revision, we identified four (sub)categories in which we could not find a related survey: (*i*) Location privacy, (*ii*) Rogue APs and suspicious activity, (*iii*) Traffic and user activity reports, and (*iv*) Extending the 802.11 MAC. As we will discuss in Section VIII, we believe that some of these areas will receive significant attention in the next years.

Table I also provides the year of publication of each survey, the total number of citations according to Google Scholar (column 'Citations'), and the total number of citations over the years since the survey was published (column 'Rate'). We highlight in bold typeface the five most cited papers and the five papers with the highest citation rate, which are not necessarily the same: on the one hand, while the survey on MIMO propagation [6] is among the five most cited papers, its citation rate is not that high; on the other hand, despite the survey on energy efficiency [7] is very recent, it is already among the papers with the highest citation rate. This points out that, as we will also discuss later on, green networking has recently attracted a lot of attention from the research community.

[5]Note that a given survey may fall into different categories.

III. Basic Functionality

In this section, we focus on those papers that address the "default" functionality of 802.11, to provide performance assessment figures, understand the observed behaviour, or derive and validate analytical models. For reader's convenience, we have summarised the reported works per sub-categories in Table II(a). We also provide in Table II(b) the most relevant contributions, i.e., the 10 papers most cited or with the highest citation rate (as defined in the section above), with their relative position in brackets and highlighting in bold typeface the the ten papers most cited across all categories.

A. Performance Evaluation

1) DCF: One of the first papers to assess the performance of WLANs is the work of [39], in which authors report results from several tests on a single-hop path involving two 2.4 GHz DSSS interfaces with a maximum rate of 2 Mbps for different hardware platforms, device drivers, operating systems, and for both UDP and TCP traffic. Although many of their conclusions are hardware-related issues (e.g., host processing), and they may have been obsoleted by the progress in radio and chipset manufacturing, in this seminal paper they already identify some limitations when running TCP over WLAN. These issues,

TABLE I
OVERVIEW OF PREVIOUS SURVEYS ON 802.11 ASPECTS

Category	Subcategory	Ref.	Title	Year	Citations	Rate
Performance evaluation	DCF, EDCA, 802.11n	[8]	A Survey of Multicasting over Wireless Access Networks	2013	15	15
		[9]	**A Survey of QoS Enhancements for IEEE 802.11 Wireless LAN**	**2004**	**314**	31.40
		[10]	PHY/MAC Enhancements and QoS Mechanisms for Very High Throughput WLANs: A Survey	2013	25	25
	Fairness & TCP	[11]	A Survey of TCP Enhancements for Last-hop Wireless Networks	2006	47	5.87
		[12]	A Survey of TCP over Ad Hoc Networks	2005	172	19.11
AP and channel selection	AP selection	[13]	Load Balancing in IEEE 802.11 Networks	2009	32	6.40
	Channel selection, Overlapping Channels, Channel quality metrics	[14]	Channel Assignment Schemes for Infrastructure-Based 802.11 WLANs: A Survey	2010	60	15
Physical layer	Interference, TX power control, Antennae	[15]	Improving Spatial Reuse in Multihop Wireless Networks - A Survey	2009	63	12.60
Models	Propagation	**[6]**	**Survey of Channel and Radio Propagation Models for Wireless MIMO Systems**	**2007**	**341**	44.85
	Interference	[16]	Modeling Interference in Wireless Ad Hoc Networks	2010	90	22.50
	MAC protocol	[17]	Performance Analysis of IEEE 802.11 MAC Protocols in Wireless LANs: Research Articles	2004	302	30.20
	Energy consumption	**[7]**	**A Survey of Energy-Efficient Wireless Communications**	**2013**	154	**77**
Mobility	Performance studies, improvements	[18]	Fast-handoff support in IEEE 802.11 wireless networks	2007	104	14.85
		[19]	A Survey on Handoffs - Lessons for 60 GHz Based Wireless Systems	2012	20	10
	Vehicular networks	[20]	Inter-vehicle communication systems: a survey	2008	244	40.66
		[21]	Mobility and handoff management in vehicular networks: a survey	2011	66	22
Localisation		**[5]**	**Survey of Wireless Indoor Positioning Techniques and Systems**	**2007**	**1414**	**202.42**
Security	Denial of service	[22]	Denial-of-Service Attacks and Countermeasures in IEEE 802.11 Wireless Networks	2009	81	16.20
	Selfish PHY and MAC configurations	[23]	MAC layer misbehavior in wireless networks: challenges and solutions	2008	32	5.33
Real-time traffic		[24]	IEEE 802.11 Load Balancing: An Approach for QoS Enhancement	2008	27	4.50
		[25]	A Survey of Medium Access Mechanisms for Providing QoS in Ad-Hoc Networks	2013	18	18
		[26]	Resource Reservation Schemes for IEEE 802.11-Based Wireless Networks: A Survey	2013	7	7
Troubleshooting		[27]	Performance Issues with IEEE 802.11 in Ad Hoc Networking	2005	138	15.33
		[28]	A survey of MAC layer solutions to the hidden node problem in ad-hoc networks	2012	10	5
Multi-AP management		[13]	Load Balancing in IEEE 802.11 Networks	2009	32	6.4
Multi-hop networks		[29]	IEEE 802.11s Multihop MAC: A Tutorial	2011	47	15.67
		[4]	**Wireless mesh networks: a survey**	**2005**	**3761**	**417.89**
		[30]	Wireless Mesh Networks Design - A Survey	2012	59	29.50
		[31]	Admission Control Schemes for 802.11-Based Multi-Hop Mobile Ad hoc Networks: A Survey	2009	72	14.40
Rate adaptation		[32]	Rate Adaptation Algorithms for IEEE 802.11 Networks: A Survey and Comparison	2008	34	5.67
Energy efficiency		**[33]**	**A Survey of Energy Efficient Network Protocols for Wireless Networks**	**2001**	**975**	**75**
		[7]	**A Survey of Energy-Efficient Wireless Communications**	**2013**	154	**77**
		[34]	A survey of energy efficient MAC protocols for IEEE 802.11 WLAN	2011	42	14
Spectrum-agile schemes		[35]	A Survey on MAC Strategies for Cognitive Radio Networks	2010	181	45.25
Testbed descriptions		[36]	Hardware and Software Solutions for Wireless Mesh Network Testbeds	2008	25	4.17
Deployment guidelines		[37]	Survey of Experimental Evaluation Studies for Wireless Mesh Network Deployments in Urban Areas Towards Ubiquitous Internet	2013	13	13
Measuring		[38]	A Taxonomy of IEEE 802.11 Wireless Parameters and Open Source Measurement Tools	2010	15	3.75

related to the bidirectional nature of the communication and timer expirations, will be revisited by subsequent works as described below. Reference [40] extends these results with one of the first comprehensive studies on the performance of multi-rate 802.11b WLANs in an ad-hoc scenario. They also report the drop in performance when using TCP (in particular, as compared to UDP), and they identify the performance issues and unfairness in the distribution of resources when capture effect or hidden nodes are present, providing intuitive explanations for the observed behaviour. Some preliminary results on the transmission range for the modulation and coding scheme (MCS) in outdoors are reported. More heterogeneous wireless links are considered in the evaluation of the Roofnet mesh network with 37 nodes [41], which reports figures on the

TABLE II
OVERVIEW BASIC. (a) WORKS THAT FOCUS ON THE BASIC FUNCTIONALITY OF 802.11. (b) MOST RELEVANT CONTRIBUTIONS

(a)

Performance evaluation	DCF	[39]–[42]
	EDCA	[43]–[46]
	Fairness & TCP	[47]–[52]
	802.11n	[53]–[56]
AP and channel selection	AP selection	[57]–[64]
	Channel selection	[65]–[68]
	Overlapping channels	[69]–[71]
Channel quality metrics		[72]–[79]
Physical layer	Interference studies	[80]–[84]
	TX power control	[85]–[89]
	Antennae	[90]–[98]
Models	Propagation	[91], [99]–[103]
	Interference	[100], [104]–[107]
	MAC protocol	[48], [49], [51], [108]–[113]
	Energy consumption	[114]–[124]

(b)

Ref.	Year	Citations		Rate		Category
[108]	**2003**	**1254**	**(1)**	**104.50**	**(2)**	**Models**
[72]	**2004**	**1149**	**(2)**	**104.45**	**(3)**	**Channel quality metrics**
[41]	**2005**	**877**	**(3)**	**87.70**	**(4)**	**Performance evaluation**
[122]	2010	528	(4)	105.60	(1)	Models
[99]	2004	500	(5)	45.45	(5)	Models
[86]	2005	399	(6)	39.90	(6)	Physical layer
[50]	2003	341	(7)	28.42	(10)	Performance evaluation
[47]	2000	329	(8)	21.93	(11)	Performance evaluation
[80]	2005	309	(9)	30.9	(8)	Physical Layer
[70]	2006	260	(10)	28.89	(9)	AP and channel selection
[104]	2004	222	(11)	20.18	(13)	Models
[60]	2006	182	(15)	20.22	(12)	AP and channel selection
[77]	2010	180	(17)	36.00	(7)	Channel quality

end-to-end throughput, link quality and latency of different 802.11b variable distance links under TCP traffic. More results on the inter-hop interference are reported as well, along with the inability of the RTS/CTS exchange to improve performance.

The above works stick to the performance of unicast traffic. The poor performance of the default open loop multicast mechanism of DCF is experimentally assessed in [42], in which the lack of the "feedback loop" results in a three-fold problem: no tuning of the contention parameters; no MCS adaptation; and no frame retransmission. They also emulate the behaviour of a leader-based multicast scheme, showing a large room for improvement, as the recent 802.11aa standard confirms (see Section IV-D).

2) EDCA: The EDCA access scheme of the 802.11e amendment specifies that the variables regulating the channel access can be set to different values for different classes of traffic, thus supporting traffic differentiation. In [43] authors analyse the impact of some of these parameters, namely the CW and the $AIFS$, on the traffic distribution under saturation conditions. The results show that the CW is well suited to support traffic engineering while the $AIFS$ provides an effective service differentiation to support real-time applications. These results are extended in [44], analysing the impact of the various EDCA parameters on the service received by voice traffic when there are data stations in the WLAN, and showing that even moderate values of $AIFS$ effectively prioritise the real-time traffic. In [45], authors present a framework to support proportional fairness through EDCA differentiation, while the work of [46] compares two CW-tuning schemes based on control theory, one centralised and one distributed, under a different set of scenarios showing that the centralised mechanism considerably enhances overall network throughput, transfer delay and fairness.

3) Fairness and TCP: For the case of **fairness**, in [47] authors analyse the distribution of resources for the case of two Lucent WaveLAN cards,[6] computing the Jain's fairness index for different time windows and showing that WLANs are short-term unfair (hundreds of ms), which can significantly degrade performance for the case of TCP, as discussed next. These results are confirmed in [49] for the case of 802.11b cards, and extended to up to 5 stations, showing that fairness worsens as the number of stations increases and that CW-tuning could improve fairness.

The issue of **TCP performance over Wi-Fi** has received notable attention from the research community. The seminal work [50] presents a detailed study on the interaction between the MAC protocol and TCP on single-hop scenarios, identifies the AP's queue size as the cause of unfairness between downlink and uplink traffic, as well as proposes a solution based on modifying the behaviour of the transport layer consisting on the variation of the TCP receiver window at the AP so that uplink and downlink TCP flows share equal bandwidth. Other experimental approaches tackle the issue at the MAC layer: in [51], authors identify that the DCF access mode does not give enough resources to the AP, and propose a setting of EDCA to prioritise its access; in [52], authors propose to use the *Idle Sense* adaptive scheme (described in Section V-D) to prioritise AP transmissions when needed.

4) 802.11n: With 802.11n, the PHY functionality is extended to standardise channel diversity techniques (MIMO), frame aggregation, and channel bonding. The performance of these new techniques is assessed in [53] for the case of an indoor scenario, also quantifying the impact of channel overlap and 802.11g interference. They show that the throughput of an 802.11n link can be degraded up to 85% due to the presence of active 802.11g stations, and that while frame aggregation can mitigate this impairment, the use of channel bonding does not provide any benefit. In [54], they evaluate 802.11n performance for an open environment with long distance links, also assessing the improvements of the new functionalities and reaching transmission distances up to 1800 m.

The performance of closely located 802.11n radios is addressed in [55], identifying (with the help of a spectrum analyser) the reasons for the performance impairments: the short distances exacerbates the effects of filter imperfections, near-field radiation and saturation. They also report how the impact of these can be mitigated through the use of metal shielding, antenna separation and directionality. Finally, the features of 802.11n can also be used to detect non-Wi-Fi RF devices with an accuracy between 91–96%, as reported in [56], by fingerprinting their interference over the sub-carriers.

[6]Note that there are some differences between the Wavelan CSMA/CA protocol and DCF, as described in [48].

B. AP and Channel Selection

For a WLAN consisting of a number of different APs, one key problem for a client is to decide which AP to associate with; correspondingly, the APs have to decide which frequency to use, given that their number is relatively limited. We next describe the main works addressing these issues.

1) AP Selection: AP selection should not be based exclusively on signal strength, as this results in uneven load distribution and poor performance of the overall network [57]. Based on this, there has been a lot of work on designing improved algorithms to decide which AP to join, most of them based on the current estimated load or envisioned performance upon joining. In [58] authors propose to compute the *potential bandwidth* based on passive measurements (e.g., the time delay between beacon frames). In [59] authors present the implementation of a scheme (IQU) based on announcing information about queue lengths. Another active procedure against strongest-signal-strength connections is Virgil [60], in which authors propose to perform scans and quick associations not only to estimate the quality of the connection to the Internet, but also to check for blocked ports (to maintain the quality of services currently in use). In [61], authors first discuss three different metrics (channel quality, time required to serve, and AP capacity) and then propose a new integrated figure: the *expected throughput*, a cross-layer metric that combines PHY and MAC information, rather than deciding on an isolated parameter.

Other works have analysed the interactions between users. To speed up the selection process, in [62] authors present *Wifi-Reports*, a collaborative service to store historical information about AP performance, this being defined based on backhaul capacity, services (i.e., ports) available, and the history of failed associations or other connectivity issues, where the focus is set on obtaining accurate information (due to privacy issues and potentially fraudulent reports). When users do not collaborate and act selfishly, the performance of the WLAN can be far from optimal. In [63], authors present a game-theoretic study and implementation of a distributed AP selection scheme, whose aim is to lessen the impact of selfish behaviour by maximising the minimal throughput among the stations (i.e., max-min fairness), while the recent work of [64] investigates the incentives to move users between APs to improve performance based on a centralised approach that collects information.

2) Channel Selection: The mapping of APs to available channels can be centralised (a single entity is responsible to compute the configuration for all nodes) or distributed (each AP estimates the best channel to use). Centralised schemes typically require a powerful machine to (offline) compute the solution and a communication channel with each AP, while distributed schemes are easier to implement but might result in a worse performance due to their myopic vision.

One of the first **centralised** (and static) designs is reported in [65], in which authors also provide some other deployment recommendations like, e.g., strategies for AP placement (we will review these in Section VI). In [66], authors propose a dynamic approach, by deploying "intelligent agents" that retrieve information from every AP using SNMP, and then adapt the allocation of channels to the current network conditions (as agents communicate, the solution is centralised).

The use of **distributed** schemes provides better scalability and dynamisms but results more challenging, which attracts more attention from the research community. In [67], APs exchange broadcast messages to estimate interference, to construct the same network graph, and then run a heuristic to minimise interference among cells (the scheme is validated in a scenario with 3 APs). Another scheme is the *Communication Free Learning* algorithm, validated in [68] in a deployment consisting of 5 APs and 5 clients, using 802.11a. This algorithm relies on the frame error rate, as a channel quality metric, measured over a 10-second interval.

3) Overlapping Channels: In most channel assignment techniques, a common assumption is that only non-overlapping channels should be used, and therefore the assignment should only consider, e.g., 1, 6 and 11 for the case of 802.11b. This assumption is challenged in [69], where authors analyse the impact of adjacent interference as a function of distance (i.e., received power) and advocate for the use of overlapping channels as an opportunity to increase spatial reuse. They further extend their work in [70] to account for more MCS and a different technology (802.16), revisiting previous channel assignment algorithms and showing notable performance improvements. In [71] authors measure that even in (assumed) orthogonal channels, a jammer can impair the performance of a communication link: a relatively low degradation is observed for 802.11g, but a notable degradation ($> 90\%$) for the case of 802.11a.

C. Channel Quality Metrics

As hinted above, the issue of how to properly estimate the "quality" of a link is critical, and therefore has received a lot of attention from the research community. In the seminal measurement work from the Roofnet deployment [72], authors report that although link distance and SNR have an impact on performance when the amount of packets lost is moderate, the main source of losses is multipath fading. They conclude, (somehow surprisingly) that the correlation between the Packet Delivery Ratio (PDR) and the Signal-to-Noise Ratio (SNR) is small and therefore "one cannot expect to use S/N as a predictive tool." This result is revisited with the FRACTEL testbed [73], [74], composed of long-distance links, in which authors analyse the relation between the PDR and the Relative Signal Strength Indicator (RSSI), but distinguishing between *interference-prone* and *interference-free* scenarios, depending on the presence or absence, respectively, of external Wi-Fi sources. The results contrast those from [72], showing that interference is the primary cause of unpredictable performance and therefore the SNR is a good estimator for PDR when there is no interference. Similarly, in [75] authors confirm via extensive measurements of mesh networks that SNR is a good indicator of the optimal bit rate for a given link, although the relation between these variables is link-specific. This is also studied in [76], where authors consider the performance of the same channel over different links, showing significant variations in both 802.11a and 802.11g.

With the arrival of new 802.11n NICs, which report Channel State Information (CSI), new schemes are proposed to overcome the limitations of RSSI [77]. With these NICs, the CSI reports the amplitude and the phase of each of the subcarriers, therefore by computing it at the receiver and sending it back to the transmitter the propagation is calibrated through the analysis of the fading, scattering, and power decay of the transmitted signal. In [77] authors leverage CSI to propose the *effective SNR* metric to accurately estimate the packet loss rate and capture the frequency-selective fading of the signal. The four typical metrics used, namely, RSSI, PDR, Signal-to-Interference-plus-Noise Ratio (SINR), and Bit-Error Rate (BER) are analysed and discussed in [78]. The conclusion, not surprisingly, is that each metric reveals interesting aspects of the link, but none can provide the whole picture on its own. Finally, a key issue when dealing with PDR is to distinguish between the possible sources of packet losses, namely, noise, collision or interference (i.e., hidden nodes). In [79] authors present an analysis to properly account for these metrics in order to estimate the various parameters of the link, thus providing accurate information to, e.g., a rate adaptation scheme.

D. Physical Layer

1) Interference Studies: Another key challenge for WLAN planning and operation is to accurately understand the impact of interference, which can be estimated with active and passive techniques. One of the main challenges of **active monitoring** is its poor scalability: with N nodes there are up to N^2 links. The results of their characterisation (i.e., interactions) are extremely time consuming. To tackle this, the use of heuristics can save time, but at the cost of accuracy [80]. In [80] authors present another heuristic based on the broadcast interference ratio (BIR), i.e., the reduction in goodput of broadcast traffic when they are active simultaneously as compared to when they are active individually, which is an accurate estimation to the link interference ratio (LIR), i.e., the same ratio but for unicast traffic. However, metrics such as BIR or LIR do not provide a complete description of the interference relationships in a network [81]. Indeed, an "interferer" can be considered as: a node that is within the carrier sensing range of a transmitter (and forces channel deferral), or a hidden node that causes collisions at the intended receiver. In [81], authors present a methodology to gather a comprehensive interference map, which consists of delivery ratios, carrier sense matrix, hidden terminal matrix and the effect of multiple sources of interference. The measurement complexity is also reduced by building on some assumptions about the relations between the different types of interference.

Another challenge introduced by active techniques is that they require to halt the activities of the network to measure interference. In contrast, **passive monitoring** runs during network operation and does not affect its performance. In [82], authors limit their study to the probabilities of collision (p_c) and channel deferral (p_d), and based on the assumption that the impact of the latter is more important than the impact of the former, propose a methodology to model p_d. Another passive approach is proposed in [83], where interference at the wireless links is inferred via multiple linear regression of the throughput logs collected at the central routers. Despite there is some computational complexity because of the regression, the system is fast enough to run in real time. Finally, given that by rate-limiting conflicting links the impact of interference can be lessened, in [84] authors present a management framework (MIDAS) to quantify this relationship (named "activity hare"). Based on this framework, a manager can predict how much a node has to be chocked in order to, e.g., achieve fairness across flows.

2) Transmission Power Control: Another mechanism to lessen the impact of interference is to perform a cautious transmission power control (TPC), as higher received power leads to higher transmission rates, but also the higher risk of interference to other links. In [85], authors address three reference scenarios, namely, *i*) completely overlapping links, in which TPC is of little use, *ii*) hidden-links, where TPC can be used to restore fairness, and *iii*) potentially disjoint links, in which TPC can lead to huge performance improvements. Given the tight coupling between link quality and the best MCS to use, other works have studied how to jointly operate power and rate selection, namely, PERF [86] and Simphony [87]. In [86], authors show that because 802.11 hotspots deployments are unplanned, this results in a degraded performance for end users. To lessen the impact of the lack of planning, they propose the PERF (Power Estimated Rate Fallback) algorithm, which aims at decreasing the transmission while maintaining the required SNR for the target transmission rate.

A key issue when performing experimental TPC is the *granularity* of the hardware, in terms of the supported number of power levels (typically between 1 dBm and 20 dBm, depending on the hardware, country and PHY layer), and the time responsiveness of the interface (i.e., the delay between committing a given configuration and this being actually used). For the case of indoor environments, in [88] authors show that there is no need to go beyond 3–5 discrete power levels. The "fidelity" of commercial equipment when adjusting the transmission power is studied in [89], showing that 802.11 cards do not accurately translate a given configurations level to an actual power, which challenges the deployment of power algorithms proposed in the literature.

3) Antennae: The reduced costs of Wi-Fi have motivated its use for **long-distance links**, based on directional antennae; given that these are normally larger than the usual omnidirectional antennae, the Fraunhofer distance[7] is typically longer for the former than the latter, which may affect performance depending on the relative position of the antennae (in terms of distances and angles). This is addressed in [90], where authors report how performance is affected in a multi-hop scenario with long links, varying the physical configuration of a relay node with two directional antennae. Another study of the performance of directional antennae is presented in [91], in which they use thee different models: a 24 dBi parabolic dish, a 14 dBi patch, and an 8-element array with steerable direction. Authors also present a new model for channel propagation

[7]The Fraunhofer distance, defined as $d_f = 2D^2/\lambda$, where D is the largest dimension of the antenna and λ the wavelength, is used to compute the far-field region, i.e., where propagation is like in "free space".

(as discussed in the next section). A more challenging environment is presented in [92], where authors describe the mechanisms required in a 15-antennae setting to use them simultaneously and achieve the maximum capacity (3 channels in 802.11g and 12 channels in 802.11a).

Directional antennae are well suited for long-distance, planned links. For the case of indoor environments, in a set of works [93]–[96] authors have analysed the use of **switched beam antennae**, which provide the benefits of directional antennae to some extent, while keeping some ability to adapt the configuration to the scenario. The problem with indoor environments is the severe multi-path effect, which prevents a drastic reduction of interference. Another approach is the use of sector antennae [97], which requires explicit measurements of all the configurations as the performance with single-sector activation differs from the one with multi-sector activation (the reason being the impact of the array feeding the antennae).

Finally, in order to take advantage of path diversity, it is common that wireless cards are provided with two or more input ports, so they can switch to the antenna providing the best performance (note that this is not MIMO, but runs at a different timescale). This supports a mechanism to periodically probe the performance of the different antennae to choose the best one. However, as reported in [98], not only the **antenna diversity** algorithm (which is typically proprietary, or at least not well documented) may lead to no improvements, but also it can lead to poor and/or unstable performance in some scenarios—in particular when the antennae provide very heterogeneous gains, or one of them is disconnected.

E. Derivation and Validation of Theoretical Models

There are basically two types of works on modelling the performance of 802.11 networks, namely, *i*) those that present a new model, derived through either analysis or experimentation, and *ii*) empirical studies designed to confirm (or challenge) previous analytical models or their assumptions.

1) Propagation: One of the first works to challenge the usual wireless (simulation) assumptions is [99]. Using a falsifiable version of the assumptions, authors show via experimentation that none of the following "axioms" used in simulations to model radio propagation are true: the world is flat, transmission areas are circular, all radios have equal range, propagation is symmetric, interfaces have perfect sensitivity and signal strength is a simple function of distance. Along the same lines, in [100] authors use an FPGA to emulate the channel link, which gives complete control over signal propagation, and perform a detailed analysis of the link-level behaviour of real hardware. They address a variety of issues that range from the impact of off-channel interference and reception to the asymmetry of links. The effect of the MCS used is pseudo-analytically deducted in [101], based on experimentally fit curves, for the cases of 11 Mbps (802.11b) and 6 Mbps (802.11g). The (rather striking) result is that the higher MCS is more robust, leading to fewer packet loss ratios for the same SNR. Another common assumption is that path loss and antenna gain are independent variables. This is challenged in [91], in which authors first analyse that this is not the case for directional antennae (due to the impact of the secondary paths in multipath-prone environments), and then proposed an integrated model which jointly accounts for the direction and the length of the communication link. A similar, measurement-driven approach is presented in [102], where authors present a model for the communication channel in an office environment. Up to 28 path loss prediction models are analysed in [103] for the case of a rural deployment, none of them providing accurate results in terms of the root mean squared errors. They propose different metrics to compare the performance of the models (e.g., ability to order links by channel quality), and find out that in some cases the best performing models would not be the ones chosen for the considered environment, and that in many cases the simplest models (e.g., two-ray) outperform the more complex ones.

2) Interference: A particular case that has received a lot of attention is the *capture effect*, i.e., when a frame is correctly received even if its transmission overlaps in time with other transmissions.[8] In [104], authors report that in a collision under a 802.11b scenario involving RTS frames, and extensible to any frame, the stronger frame survives in practically all cases, despite timing differences of ± 20 μs. A more detailed analysis is performed in [100], with different MCS and relative reception power, and delays up to 96 μs, showing that the most sensible time is right at the beginning of the transmission. While these works focus on the case of 802.11b, in [105] authors analyse the case of 802.11a, and report that the stronger frame can be decoded correctly regardless of the timing relation with the weaker frame. Furthermore, when the stronger frame arrives later, there are different patterns depending on whether the receiver has been successfully synchronised to the previous (weaker) frame or not.

Considering a less particular phenomenon, the interactions between interference and carrier sensing are analysed in [106], in which authors provide a comprehensive taxonomy of the possible relations between link pairs (deriving up to 16 topology cases). Based on these framework, they derive a methodology based on RSS measurements to predict the performance of a given configuration. This same "coupled flows" problem is analysed in [107], where authors build on the classical Markov-chain modelling of the competing flows to predict the throughput obtained by each link.

3) MAC Protocol: When in a WLAN some stations use a lower MCS than others, the performance of all hosts is considerably degraded. The reason for this is that DCF provides channel access fairness (in the long term, as we discuss next), but stations with lower MCS occupy the medium for relatively longer periods of time, thus decreasing the overall performance—this is known as the *performance anomaly* effect [108]. The issue of MAC *fairness* is addressed for the case of a 2-station network in [48], where fairness is computed based on

[8]There are many approaches to model this case, e.g., *i*) both frames are lost, *ii*) the frame received with the larger signal-to-interference ratio is correctly received, *iii*) the stronger frame is correctly received, provided it arrived first, and *iv*) even if did not arrive first, the stronger frame will be correctly decoded if it arrived during the preamble of the weak frame.

TABLE III
OVERVIEW OF THE SERVICES WORKS. (a) WORKS THAT FOCUS ON THE SERVICES OFFERED BY 802.11. (b) MOST RELEVANT CONTRIBUTIONS

(a)

Mobility	Performance studies	[125]–[128]
	Improvements	[129]–[134]
	Vehicular networks	[135]–[138]
Localisation		[60], [139]–[154]
Security	Denial of service	[71], [155]–[161]
	Selfish PHY and MAC configurations	[162]–[165]
	Location Privacy	[166]–[170]
	Rogue APs and suspicious activity	[171]–[173]
Real-time traffic		[44], [174]–[186]
Troubleshooting		[187]–[190]

(b)

Ref.	Year	Citations		Rate		Category
[139]	**2000**	**6810**	**(1)**	**454**	**(1)**	**Localisation**
[125]	**2003**	**935**	**(2)**	**77.92**	**(2)**	**Mobility**
[161]	2003	696	(3)	58.00	(3)	Security aspects
[140]	2002	618	(4)	47.54	(6)	Localisation
[142]	2005	547	(5)	54.70	(4)	Localisation
[191]	2004	531	(6)	48.27	(5)	Localisation
[153]	2004	468	(7)	42.55	(7)	Localisation
[145]	2005	375	(8)	37.50	(8)	Localisation
[129]	2004	311	(9)	28.27	(10)	Mobility
[182]	2003	266	(10)	22.17	(12)	Real-time traffic
[160]	2007	219	(11)	27.37	(11)	Security aspects
[136]	2008	215	(12)	30.71	(9)	Mobility

the number of consecutive transmissions from one station. In that paper, authors demonstrate that DCF is indeed fair even in the short term scale (the work is extended for more hosts in [49], but without an analytical model). The issue of MAC fairness is revisited and systematically addressed in [109], where authors quantify fairness as a deviation from an ideal fair queueing system. Based on the findings, they derive the stochastic service curve model to predict packet delays in the WLAN. A semi-analytical approach to compute the capacity of a wireless link is presented in [110], in which authors use measurements to first capture the interference relationships between links, and then they build on a Markov Chain to estimate the link capacity; the performance bounds of a system based on carried sense are derived and confirmed in [111].

Based on the seminal paper by Bianchi, many works have extended the model to characterise the performance of EDCA (e.g., see [112] and references therein), but few have been validated in an experimental setting. One of the few works to perform this comparison is [51], in which it is shown that, in saturation conditions, the modelling of the differentiation provided by TXOP is accurate, as well as the CW differentiation, but for the case of large AIFS the model becomes quite inaccurate, as the per-slot independence used in most Markov Chain models no longer holds. These observations are further extended in [113], in which authors review the popular assumptions for Wi-Fi modelling and assess the extent to which they are accurate in an experimental scenario.

4) Energy Consumption: A number of previous works have addressed the energy consumption of the **wireless interface**, aiming at a per-packet characterisation. The seminal work of [114] shows that transmission/reception of an 802.11 frame has a linear dependency on its length. This result is caused by the four different states a wireless NIC can be in, namely: sleep, idle, receiving and transmitting. [114] also identifies a fixed cost per frame, caused by control frames (e.g., RTS/CTS). The results are extended in [115] for different modulation and coding schemes and transmission power configurations, and a similar approach is followed in a recent work [116] for the case of 802.11n. While in these cases the 802.11 interface is treated as a whole, [117] distinguishes between the (approximately constant) Application-Specific Integrated Circuit (ASIC) consumption, and the Power Amplifier (PA) consumption occurring only outside idle periods.

Other works have addressed the experimental characterisation of the consumption of the **complete device**, either a laptop [118]–[120] or a mobile phone [121]–[123]. Some of these works deal with specific issues, such as quantification of the consumption of components in addition to that from the interfaces (e.g., CPU, screen, memory) [122], power consumption measurements via available APIs for estimating the battery discharge state [120], assessment of trade-off between CPU consumption due to data compression and wireless consumption due to data transmission [119]. However, none of these provide a per-packet characterisation of the energy consumption. In [118] authors present an analysis of the communication costs of complete transfers, and it is mentioned that in addition to the actual transmission or reception, there might be additional energy costs associated to packet processing. Along the same lines, in [123] authors report that message size can have a non-intuitive impact on the energy consumption. Finally, in a recent work [124] authors have performed a detailed experimental analysis of 802.11-enabled devices, characterising the per-packet power consumption by the wireless card and the internal processing of the device.

IV. SERVICES

We next revise those papers that enhance or extend a service provided by the default capabilities of 802.11, these works being overviewed in Table III(a). As in the previous section, we summarise in Table III(b) the most relevant contributions.

A. Mobility

Works dealing with mobility can be classified depending on their main focus: performance studies, aimed to understand the handoff process; improvements, motivated by the former; and the particular case of vehicular networks, which has received increasing attention over the last several years.

1) Performance Studies: One of the first analysis of handoff in 802.11 is [125], where authors quantify the different components of the procedure (basically consisting in probing, re-association, and authentication), prove that the dominant factor of the handoff latency corresponds to the probing phase and identify that different vendors provide different performance, which is caused by two issues: 1) the standard does

not specify the actual procedures to, e.g., identify when a handoff is needed (i.e., the "trigger"), and 2) some cards are not compliant with the state machine specified by the standard for the probing phase.[9] The fact that active scanning can be very time-consuming, in particular when compared against other control procedures (although for the case of IPv6 the situation is slightly different [126]), motivates many of the improvements described in the next section. The trigger for the handoff process is the main focus on the analysis of the traces collected at the 67th IETF meeting [127], where it is identified that due to network congestion, clients may (wrongly) assume poor radio conditions, leading to high handoff rates. These introduce an even higher load in the network, dramatically reducing performance in periods of high congestion. A comparative study of handoff between public Wi-Fi APs and 3G in walk and drive experiments is presented in [128], revealing that Wi-Fi performance suffers during transients (as identified in the above works), but compensates this with higher throughputs in static conditions.

2) Improvements: A handoff can be divided in three phases: (*i*) discovering a set of candidate APs to move to; (*ii*) triggering the handoff; and (*iii*) updating the forwarding path. Based on these, we analyse the main works improving handoff performance.

To reduce the **discovery** time, in [129] authors propose to refine the probing with topology information, by building a *neighbour graph* (NG) with information about channels used. The scenario consists in an 802.11b mobile station roaming in an area covered by 20 APs, and the NG is built through an initial measurement campaign. By probing only the channels where APs in the NG operate, the roaming station reduces scanning latency by 80.7% w.r.t. full-scanning and 30.8% compared to observed-scanning. Authors also propose an NG-pruning algorithm, in which only the neighbouring APs with an acceptable signal quality are probed. This method improves full-scanning latency by 83.9% and observed-scanning latency by 42.1% on average. Another strategy is to leverage on a second wireless interface to perform the scanning [130], which substantially improves performance but the practicality is arguable.

Concerning the **trigger mechanism**, the usual scheme is to trigger the handoff only when conditions are very bad. In contrast, in [131] authors propose to constantly monitor beacons strength, and based on short- and long-trends of these signals, pro-actively trigger the handoff. It is also noted that "same channel" handoffs result in better performance than changing to a different channel. The HaND proposal [132] builds on the wired infrastructure for sending probing responses from candidates AP to the AP the client is currently associated with, and relies on the AP (and not the client) to trigger the handoff.

Finally, handoff performance can also be improved by adequately designing the **forwarding architecture** of the network. In the seminal analysis of Mobile IP [133], authors show how performance improves by opportunistically forwarding and filtering frames. Another strategy is to keep the IP layer oblivious to the handoffs, making the whole wireless network a single layer-2 hop, which is particularly effective for the case of mesh networks [134]. This approach modifies the usual DHCP configuration to track the quality of the links, and builds on gratuitous ARP messages to update addresses and perform handoffs.

3) Vehicular Networks: In [135], authors analyse the connectivity between APs and clients inside vehicles, showing that there are periods of poor connectivity as devices approach and move away from the point of attachment, which are difficult to predict as they do not consistently occur at the same spot. In a follow-up paper [136] running on DieselNet[10] they study different handoff policies and propose the ViFi protocol, which is a mobility protocol for interactive application that tries to connect to multiple base stations simultaneously. ViFi requires the vehicle to designate an AP as its anchor and the rest of nearby APs are auxiliary. The anchor provides Internet connectivity, while the auxiliary APs might act as relays, depending on whether they overhear or not the frame acknowledgement. As the vehicle moves it can designate a new anchor, which requires coordination to prevent packet losses. A similar study, but for the case of a mesh networks, is presented in [137], where they analyse the impact on service disruption of different handoff policies (e.g., always strongest signal, long-term averaged quality scoring of APs), and diagnose the reasons for the performance issues (e.g., impact of a multi-hop backhaul, association failures). In [138], authors analyse different mechanisms to improve performance, namely, handoff based on RF fingerprinting and the use of pre-fetching, each improving performance by a factor of two.

B. Localisation

Given its presence in almost any portable device, Wi-Fi has been extensively used for localisation works, with the general approach being to leverage on readings to make an estimation of the location of the user, either based on triangulation or an off-line calibration phase. We can classify these works depending on the type of readings used, the design of the calibration phase, or the analysis on the accuracy of these systems.

One of the first localisation systems is *Radar* [139], which builds on the **Received Signal Strength** (RSS) indicator. In that seminal work, authors compare the performance in terms of accuracy of fingerprinting, propagation models, and choosing the AP with the strongest signal received, which have different trade-offs in terms of complexity, training phase and accuracy. Their proposal, for indoor environments, combines a data collection phase (also known as the *offline phase*) that builds a RF signal strength data base, with a signal propagation model that takes into account a wall attenuation factor (WAF) and provides an estimation of the distance to a given AP. These distances are later used to estimate the user's location by means of triangulation. In [140], authors perform an extensive measurement campaign to later use a Bayesian approach to accurately predict the location, but it has the disadvantages of the amount of data to process and the length of the training phase. Furthermore, in a follow-up paper [191] it is showed

[9] As we will see in Section IV-C2, this no compliance is common.

[10] https://dome.cs.umass.edu/umassdieselnet

that use of a Gaussian fit over the collected data (instead of keeping all samples) results in a simpler and faster calibration, and can result in a more robust system. The *Horus* system [142] builds from a detailed analysis of the data from the calibration phase to derive a probabilistic model for the signal strength received from APs, including the use of clustering to group map locations to reduce the computational requirements. After thorough measurements, it is concluded that signal strength follows a Gaussian distribution, with a detailed analysis of the reasons for channel variations (e.g., small scale variations) and how to reduce their impact on performance. In [143], authors address the problem of *tracking* a mobile node, by considering not only the current measurements but also previous ones, which is processed using Viterbi's algorithm. Finally, in [144], authors show that using multiple antennae at the same devices can greatly improve the location accuracy by reducing the small-scale variations.

Alternative metrics, **other than the RSS**, have also been considered. In [145], authors analyse that, for outdoor scenarios, the number of times an AP is detected by the driver at a given distance can provide enough accuracy and requires a simpler calibration phase. They claim this measurement varies much more predictably than the variation of the signal strength vs. distance. However, their proposal achieves much less accuracy than other methods, it requires the use of GPS, and it also needs an offline phase (i.e., wardriving). The angle of arrival is proved to be effective for localisation purposes in VORBA [146], where authors deploy a node over a turntable. This approach removes the need of a calibration phase but requires more specialised APs. Along similar lines, the use of directional information to locate APs is presented in [192], where authors perform measurements while on the move to compute the *gradient* of the local RSS variations. Finally, leveraging on the accuracy of the internal card clocks, recent works have proposed the use of the *time of flight* (i.e., the time between a data frame is sent and the ACK is received) to locate users [147], [148].

One of the main challenges of location systems is to **optimise the calibration phase**. For the case of nodes with fixed locations, in [149] authors explore the idea of *self-mapping*, in which only a few known locations are fed into the system at first, and then through the use of measurements and graph techniques, new locations are inferred. In [150], authors present an analytical framework to understand the impact of the relative location of the *landmark* nodes, i.e., those with known positions, based on the error of the estimation. Then, they propose an algorithm to derive the optimal location of the landmark nodes given a floorplan. To speed-up the calibration phase, the ARIADNE system [151] uses the floorplan to generate a 3D map, which feeds a propagation model based on ray-tracing, and then uses one measurement to estimate the parameters of the propagation model. This idea is pushed further in WiGEM [152], where the training phase is eliminated by dividing the area into locations and then using an expectation-maximisation algorithm to compute the propagation model.

Finally, some works have analysed the **limits of the accuracy** with localisation. In [153], authors analyse the impact of the training set, both in terms of number and location of the fingerprints, on the accuracy of different indoor location algorithms. The main result is that there is a fundamental limit on the accuracy of fingerprinting schemes, which at some point does not improve with a larger set of samples, but can be improved only through better hardware or the use of propagation model. A similar problem is addressed in [154] through the use of the ORBIT testbed, with a more thorough analysis to understand the impact of the location algorithm, and the importance of high quality RSS measurements.

C. Security Aspects

Here we review the most prevalent works dealing with security and privacy aspects of WLANs, but not including the paper techniques specific to the cryptographic schemes (e.g., vulnerability of WEP, exchange of keys).

1) Denial of Service Techniques: One of the most obvious attacks on Wi-Fi networks is *jamming*, i.e., the transmission of frames (or, more generally, radio signals) to deliberately disrupt communications. In [155], authors perform a detailed analysis of the impact of jamming on the PDR, and build on the observed results to propose an algorithm, based on gradient descent (with multiple vantage points) to locate the source of the jamming activity. To lessen the impact of jamming, channel hopping is a common technique [71], [156]. In [71], authors use game theory to model the scenario, to derive the optimal strategy to switch channel. In [156], the scenario is modelled with a Stackelberg competition, where the jammer tries to follow the randomised sequence of channels the legitimate node uses. One key contribution of this work is the derivation of the time a user has to stay in the chosen channel, which is a trade-off between the probability of being jammed and performance. Another mechanism to lessen the impact of jamming is to adapt the transmission rate, power and carrier sensing thresholds, which is proposed in the ARES framework [157]. By mixing these techniques, ARES leads to significant improvements in both 802.11a and 802.11n scenarios.

More sophisticated cases of jamming are analysed in [158]–[160]. In [158], authors consider a more "subtle" version of jamming, in which the attacker targets a single node to trigger the rate adaptation at the AP, thus causing the performance anomaly. To lessen this attack they propose FIJI, a framework that includes a technique to detect this attack and a traffic shaping mechanism to lessen its impact. In [159], authors analyse the case of jamming in encrypted wireless ad-hoc networks, where an attacker might efficiently disrupt communications by inferring the packet exchanges (e.g., TCP's initial exchange) and jam only key frames, and propose the use of padding, artificial delays or packet batching to disrupt these schemes. Finally, in [160], authors show that 802.11 equipment (the study considers different hardware from different vendors) is extremely vulnerable to certain patterns of weak interference, due to the specifics of the design of the reception chain at the network interface card. To prevent these threat, they propose and prototype a channel-hopping strategy by modifying the `hostap` driver, which switches channels every 10 ms and estimates whether the channel is under a malicious attach or not.

In addition to jamming, other techniques to deny service are reviewed in [161]: spoofing of management frames to deauthenticate or disassociate, altering the operation of power saving mechanisms, or by taking advantage of the virtual carrier sensing scheme (accessing the channel before other stations and reserving the medium for the maximum amount of time). They confirm the feasibility of each of these attacks on commodity hardware, and propose and prototype some mechanisms to overcome them or at least mitigate their effects. We next review the techniques based on the misconfiguration of the access parameters.

2) Selfish PHY and MAC Configurations: With the arrival of the 802.11e amendment, users were given the ability to change the configuration of their MAC parameters, in this way enabling traffic differentiation between applications and/or users. This feature has a cost, which is that users are also able to tune their MAC configurations aiming at a larger share of the wireless resources. Indeed, as reported in [163], even pre-EDCA cards already presented a behaviour misaligned with the standard rules, which resulted in different bandwidth shares for competing stations in a WLAN and, correspondingly, unfairness among users. However, despite this severe concern, not very much experimental work has been carried out to detect selfish configurations (and to restore fairness). The DOMINO software [164] is composed of a set of tests (based on heuristics and statistics), to be performed by the AP to detect if a user is scrambling frames, using different timings, backoff configurations, etc. While most of the results are obtained with simulations, the experimentation part is devoted to the detection of selfish CW configurations. This is also the main focus of [165], where a sequential hypothesis test on the successfully received packets is proposed to detect misbehaving nodes—similarly to [164], most of the results are derived from simulations. Finally, in [162] authors analyse how to detect overly high thresholds for carrier sensing (i.e., no sensing) by sending probe messages with a relatively low transmission power.

3) Location Privacy: An increasing concern nowadays is the preservation of the privacy of the location. As described in Section IV-B, many passive methods exist to accurately track the position of a node with their collaboration (or at least, being associated to an AP), but even without their collaboration it is possible to track a user: in [166], authors propose the use of a high gain antenna to sniff all APs a mobile is able to detect (because of the discovery mechanism) and then, based on the location of these APs, infer its location.

As shown in [167], the use of pseudonyms does not guarantee anonymity, because of *implicit identifiers* and *identifying characteristics* of 802.11 traffic: frequent destination addresses (such as the email server), SSID probes from past visited networks, etc. To protect privacy, in [168] authors perform an entropy analysis of three schemes to improve user privacy: periodically changing the MAC address (which have to be supported by APs); modifying the transmission power control (TPC) scheme to decrease the precision of the location algorithm; as well as artificially introducing silent periods in the wireless activity to blur inference mechanism. The effectiveness of varying TPC is assessed with experimentation in [168], while authors in [169] focus on the inference of users' activities by matching encrypted traffic against application profiles (e.g., web browsing, bulk downloads, video watching). It was shown that just 5 seconds of traffic activity are enough to achieve an 80% accuracy in matching.

In order to overcome these issues, an identifier-free protocol is presented in [170], which builds on 802.11 operation but removing all explicit identifiers (e.g., L2 addresses), using in their prototype an "anonymous" 802.11 header (constant fields and addresses) and nodes running in promiscuous mode. The price to pay is a higher overhead, which is about 10%.

4) Rogue APs and Suspicious Activity: Securing the infrastructure is of little use when malicious or "naive" employees (innocently) connect a new, non-secured AP to the wired network. Two approaches have been proposed to identify these *rogue* APs: by sniffing, analysing and testing wireless connections [171], or by inferring unexpected wireless activity at the gateway [172]. In [171], authors rely on a central controller that triggers additional tests when a suspicious public Wi-Fi is detected (e.g., ping to internal servers). In [172], authors use a packet-pair technique (discussed in Section VI-D2) to distinguish between traffic from wired and wireless networks, and trigger the corresponding actions when, e.g., an unauthorised IP address is connected through Wi-Fi. The use of sniffers can also be used to detect "suspicious" activities usually caused by malicious software (e.g., bots), namely, port scanning and TCP flooding, as shown in [173] where authors estimate that 1% of the total TCP traffic during the 67th IETF meeting was caused by "malware," which has significant impact on the performance of the WLAN.

D. Real-Time Traffic

The original standard was based on a best effort service, which poses significant challenges when providing an adequate service to real-time traffic, namely, voice and video. For the case of **voice traffic**, some works [174], [175] focus on the experimental derivation of the maximum number of calls supported in an 802.11b WLAN, analysing the impact of the preamble size, use of rate control, type of codec or the voice generation interval. Based on these limitations, some works propose legacy-friendly solutions to improve the performance of voice: in *Softspeak* [176], authors reduce contention by aggregating voice frames at the AP in the downlink, and forcing a TDMA-like operation in the uplink; in *OmniVoice* [177], which considers a deployment with multiple APs and mobility, voice performance is improved by using a single channel and coordinating the transmissions of the APs, which use the *CTS-to-self* mechanism to reserve the channel.

Following the arrival of EDCA and its traffic differentiation scheme, in [44] authors analyse the impact of changing the contention parameters in the delay performance of VoIP. For the case of wireless multi-hop networks, in [178], [179] authors assess the benefits of using packet aggregation and header compression, plus the use of labels to perform fast path switching when conditions worsen; motivated by the use of mesh networks in emergency scenarios, in [180] it is described as a robust "push-to-talk" distributed service.

TABLE IV
OVERVIEW OF THE WORKS THAT FOCUS ON ENHANCEMENTS. (a) OVERVIEW OF THE WORKS THAT FOCUS ON ENHANCEMENTS. (b) MOST RELEVANT CONTRIBUTIONS

(a)

Multi-AP management	[193]–[198]
Multi-hop networks	[199]–[228]
Rate adaptation	[229]–[240]
Extending the MAC layer	[46], [141], [241]–[255]
Energy efficiency	[124], [256]-[269]
Spectrum-agile schemes	[270]–[273]

(b)

Ref.	Year	Citations		Rate		Category
[206]	**2003**	**3219**	**(1)**	**268.25**	**(1)**	**Multi-hop networks**
[204]	**2004**	**2539**	**(2)**	**230.82**	**(2)**	**Multi-hop networks**
[253]	**2006**	**1463**	**(3)**	**162.56**	**(3)**	**Extending MAC layer**
[229]	**1997**	**1271**	**(4)**	**70.61**	**(8)**	**Rate adaptation**
[213]	**2005**	**1226**	**(5)**	**122.60**	**(4)**	**Multi-hop networks**
[207]	2004	874	(6)	79.45	(6)	Multi-hop networks
[200]	2006	704	(7)	78.22	(7)	Multi-hop networks
[230]	2004	604	(8)	54.91	(10)	Rate adaptation
[203]	2005	566	(9)	56.60	(9)	Multi-hop networks
[231]	2005	492	(10)	49.20	(11)	Rate adaptation
[194]	2004	427	(11)	38.82	(12)	Multi-AP management
[238]	2010	400	(12)	80.00	(5)	Rate adaptation
[265]	2006	324	(13)	36.00	(13)	Energy efficiency

For the case of **video traffic**, providing an adequate service typically proves more challenging due to the larger bandwidth required. A basic assessment of the 802.11b/g/n standards is presented in [181], where a two-link testbed is used to quantify the number of video flows each technology supports, and the impact of the mode of operation (unicast vs. multicast), via the Mean Opinion Scores of 10 test subjects. An analysis of the mechanisms affecting performance of video is presented in the seminal work of [182], where a novel adaptive cross-layer architecture is presented, focused on 802.11a PCF mode performance and based on the evaluation of the mechanisms at different layers, namely, retransmissions, packetization, forward error correction, and scalable video encoding. The packetization policy is extensively tested in [183] for the case of vehicular environments, showing that larger packets are preferred when conditions are more predictable; in [184], authors analyse the effectiveness of packet level FEC for video multicast with multi-rate capability in a two-node 802.11b scenario, deriving guidelines for the FEC use. The use of cross-layer techniques is also addressed in [185], where the benefits of link adaptation schemes, based on cross-layer techniques, is presented. Finally, motivated by the poor performance of multicast transmission in 802.11 WLANs, the 802.11 recently released a new family of schemes in the 802.11aa amendment (the Group Addressed Transmission Service), which are assessed in a recent work [186].

E. Troubleshooting

Finally, we review those papers bringing diagnosing services to 802.11 WLANs, to address performance issues as the ones classified in [187]: connectivity and authentication problems, congestion, interference, poor planning, or unauthorised APs (as discussed in Section IV-C4). In that work, authors present a framework based on a central controller that is also able to remotely control clients to diagnose these issues. Another tool is *WiFiProfiler* [188], whose focus is on diagnosing misconfiguration of the WLAN parameters or the management plane, e.g., DHCP non working, ports blocked, wrong WEP key. The tool is developed over the VirtualWiFi driver [188], which enables a cooperative diagnosing protocol to exchange information about the network health, even across devices connected to different networks or also disconnected. The idea of using a common control plane for devices connected to different networks is pushed with RxIP [189], where the Internet is used as a common control plane to implement a P2P-alike architecture. In this way, APs in the neighbourhood that identify a hidden node scenario can coordinate their transmissions using a token-based scheme. Finally, given the complexity of multi-hop deployments, the SCUBA tool [190] supports an interactive focus and context visualisation, to support a user-friendly diagnosis.

V. ENHANCEMENTS

In this section, we focus on those papers that propose extensions and improvements to the 802.11 standard, with an overview presented in Table IV(a). Like before, we summarise in Table IV(b) the contributions with the largest impact.

A. Multi-AP Management

Although the presence of multiple APs supports performance improvements due to, e.g. mobility, it poses some challenges since transport protocols, in particular TCP, tend to perform poorly when there are simultaneous network connections, due to packet re-ordering and the heterogeneity of the links [193]. To benefit from the availability of multiple APs, in [194] and [195] two systems to simultaneously connect stations to multiple APs are presented. The first one focuses on the software mechanism to enable multiple virtual wireless cards on top of a single physical card, while the second focuses on fast switching between APs, these being transparent to TCP and upper layers. Both works demonstrate the feasibility of aggregating AP resources at one physical card, either via wireless card virtualisation or via opportunistic and dynamic selection of the AP, which improves capacity but could provide unfair results in terms of access to resources.

Regarding capacity studies, THEMIS [196] is a single-radio system designed to fairly share the user's load over multiple in-range APs. A similar idea is exploited in [197], to activate the minimum number of DSL connections needed in a neighbourhood to satisfy the current demand, thus saving energy in the DSL connection (energy efficient operation of Wi-Fi is discussed below). Finally, with AP virtualisation, care should

be put in the uplink, as simple schemes do not guarantee fairness and a controller is required to restore it [198].

B. Multi-Hop Networks

Wireless multi-hop networks (or mesh networks) based on 802.11 have received a vast amount of attention from the research community, thanks to the availability of the hardware. Their operation is typically based on the use of a transport protocol, operating over a routing/forwarding scheme, which eventually relies on the MAC to deliver traffic hop by hop over the wireless links. As the original standard was not intended for multi-hop operation,[11] the use of 802.11 in these scenarios requires facing a number of challenges, which we next overview.

Concerning their deployment, **channel assignment** plays a fundamental role in minimising inter-link interference, in particular when considering that the 802.11 carrier sense mechanism is overly pessimistic and overestimates the impact of concurrent transmissions [199]. In [200], a centralised dynamic scheme based on a broadcast radio interface is presented, showing notable improvements over static schemes. The impact of the granularity of channel assignment decisions (packet, link or flow level) is studied in [201], proposing a novel scheme based on flow graphs.

One of the first challenges of mesh operation is the design of the **routing metric and protocol**, as wireless conditions vary over time (e.g., the foliage affects the link performance in the TFA testbed [202]) and therefore the protocol has to adapt to those. There is a notable number of approaches tested in practice: in [203], authors report on the impact of opportunistic routing in the Roofnet testbed; the Expected Transmission Time (ETT) scheme is assessed in [204]; the Expected number of Transmissions On a Path (ETOP) in [205]; the Expected Transmission Count (ETX) [206] shows good performance for stationary conditions [207]. In this work, authors also propose Link-Quality Source Routing (LQSR), which extends routing metrics with link quality information but needs to rapidly adapt in dynamic scenarios, as otherwise is outperformed by routing schemes based in minimum hop count. Various schemes such as link bandwidth (BW), ETX, ETT and some of its variants are evaluated in [208], with the main conclusion being that they are very sensitive to background traffic and, especially in presence of multiple flows, they result in very suboptimal routing decisions.

Some schemes propose to couple the routing to the MAC operation: the Expected Transmission cost in Multi-rate wireless networks (ETM) jointly accounts for link-rate adaptation and congestion levels [209], outperforming ETT and ETOP; the Contention-Aware Transmission Time (CATT) routing metric is presented in [210], also leading to substantial gains over ETX and ETT; building on the correlation between losses in the wireless medium, the *Divert* scheme [211] operates a fine-grain path selection, reducing loss rates with respect to schemes using fixed flow paths. As alternative to "traditional" routing schemes, the use of opportunistic mechanisms, i.e., that nodes decide on a per-frame basis whether to forward it or not, is proposed in the ExOR scheme [213]. With ExOR, which is studied on the evolved Roofnet testbed (a 38-node 802.11b outdoor network), nodes decide whether a packet has to be forwarded or not, and transmissions do not contain an explicit next-hop address field, since each node in radio range can decode the transmission and act as a router. Note that the use of a routing protocol can result in the starvation of data flows, as its low-rate traffic can degrade performance due to hidden nodes and capture effect [215], or because of the use of robust encoding [216], which consumes more airtime. However, as routing cannot be eliminated, some works propose to reduce its overhead building on label switching and distributed hashing [217]. Finally, the design of incentives to support opportunistic routing is addressed and validated in [214].

One key challenge of routing is ensuring **stability**, as the dynamics of wireless channels can lead to *route flapping*. To solve this, a simple route update strategy based on hysteresis is proposed in [218], while a historically-assisted scheme is proposed in [219]. However, even for the case of static routes the MAC protocol of 802.11 can lead to the instability (and consequently packet loss) of transmission queues [220], which is theoretically analysed in [221], proposing the use of *throttling* to prevent this issue. Indeed, the use of **rate limiting** has been widely explored in mesh networks to enhance performance, e.g., to prevent the so-called starvation phenomenon [202], [222], using AIMD-based control to distribute wireless resources among concurrent flows [223], and should dynamically adapt to the time-varying capacity of the wireless network for its effectiveness [224].

Finally, the **performance of TCP** over mesh networks has received a lot of attention by the research community. In [225], authors present a model for the two-hop scenario, and show that controlling the flow rates substantially improves performance. Another model is validated in [226], explaining how the closed-loop control of TCP unbalances the resource allocation, but can be lessened through MAC tuning. These interactions between TCP congestion control and 802.11 MAC are also identified as the origin of TCP poor performance in [227], and addressed by tuning the TXOP parameter of the different wireless nodes. A different approach to enhance the performance of TCP in 802.11 networks is presented in [228], in which the authors show how to optimally split TCP flows over multiple wireless paths, this resulting in enhanced network utilisation and fairness.

C. Rate Adaptation

Rate adaptation (RA), i.e., the algorithm that adapts the MCS to the observed radio conditions, has received a lot of attention from the research community. One of the main purposes of an RA algorithm is to timely **react to varying radio conditions**, by decreasing the MCS when radio conditions are poor and increasing the MCS when they improve. The seminal AutoRate Fallback (ARF) scheme [229] from WaveLAN-2 cards proposes a very simple approach, namely, increasing the MCS after ten consecutive successes, and decreasing it after two consecutive failures. The ARF mechanism does not result very agile when radio conditions change and results in sub-optimal performance due to the basic probing scheme, and

[11] This was partially fixed later in the 802.11s.

therefore has motivated a number of research works to improve the performance of RA. With Adaptive Multi Rate Retry (AMRR) [230], the number of consecutive successes before increasing the MCS varies with radio conditions following a Binary Exponential Backoff (BEB) process, to prevent very frequent probing and adapt continuously the threshold for the rate decision. In Sample Rate [231], a more judiciously probing is performed, only in those MCS that would result in shorter transmission times: after 4 consecutive failures a MCS will be discarded, and every 10 consecutive successes a novel rate with smaller transmission time will be sampled. Meanwhile, the decision process of CHARM [232] leverages past history about the link quality to the intended destination; while RAM [233] uses a receiver-based approach (based on ACKs) to handle channel asymmetry.

The abundance of RA schemes also triggered some works to **compare their performance**, in order to understand their behaviour under different settings. In [234], authors perform various controlled experiments to compare three algorithms (AMRR, SampleRate and ONOE, all of them available with the MadWifi driver) in similar RSSI conditions, by putting a laptop inside a microwave oven and keeping its door open or closed; they also analyse the impact of rate adaptation on the application under study, namely, voice, video streaming, web browsing or file transfer. Another study is carried out in [235], where the performance of these three RA schemes is analysed in both indoor and outdoor mesh deployments, to understand the impact of channel variations and interference (namely, collisions) on performance, this being a major cause of their poor performance.

Indeed, the inability to distinguish the cause of a frame loss, i.e., to **distinguish between poor radio channel and collisions**, has motivated another set of research works, which extend the basic operation of the protocol to support this differentiation: in WOOF [236], the scheme uses 1-second measurement intervals to estimate the channel occupation (and therefore, interference conditions); the COLLIE mechanism [237] builds on signal measurements collected at the AP to identify the causes for a packet loss; with CARA [238], the RTS/CTS exchange is used to help make this distinction. Finally, the recent H-RCA [239] mechanism, which aims at minimising the average time that a packet is on the medium considering also its retransmission, builds on the TXOP parameter (i.e., transmission of burst of frames) of the EDCA standard to perform this differentiation.

Finally, given the particularities of the relatively recent 802.11n standard, some works [240] have already pointed out that existing RA schemes do not perform well in these settings, as they do not take advantage of the available MIMO features. MiRA [240] alternates between single and dual stream modes for transmission and proposes an inter and intra-mode rate prioritising intra-mode. It also proposes an adaptive probing to reduce the overhead, which leverages frame aggregation and block acknowledgement to probe the selected rate.

D. Extending the MAC Layer

Earlier works have addressed how to improve the **contention-based access**. One simple mechanism to compensate the overhead introduced by the CSMA/CA access scheme is to aggregate multiple frames into a single MAC frame [241], through the use of an aggregation sub-layer between the LLC and the MAC. Similarly, prior to the adaptive CW techniques based on the EDCA standard discussed in Section III-A2 (e.g., [46]), in [242] authors report the implementation of the *Idle Sense* mechanism, which basically consists of adapting the CW based on the number of idle slots between transmissions to optimise the 802.11 DCF protocol performance. Although authors required some insight from the vendor, with this implementation it was also demonstrated that existing platforms were able to support enhancements without major modifications. Another proposal partly related with standard mechanisms (namely, the "reverse direction" mechanism of 802.11n) is VoIPiggy [243], a mechanism to piggyback small (voice) frames over L2 acknowledgements, which is therefore well suited for bi-directional communications. Again, the implementation is performed over commodity 802.11 hardware, leveraging on the reverse-engineered OpenFWWF firmware.[12] The same platform is used to introduce the Wireless MAC processor [244], a novel paradigm in which anyone can program new MACs over commodity hardware, by specifying the state machine to be executed by the firmware, which can be loaded in real-time (the so-called MAClets [245]).

In addition, performance can be improved by introducing **synchronisation between nodes**, so the network operates in a TDMA fashion. In [246], authors introduce an *overlay* MAC layer over the Click modular router, which loosely synchronises nodes so the network operates in a decentralised TDMA-like fashion (where a slot is the time to send ten 1500-byte frames) according to a WFQ policy. A more tightly synchronisation is achieved in [247] using real-time Linux (the so-called SySI-MAC framework), which is used to implement Soft-TDMAC, a MAC protocol for multi-hop networks. Another TDMA-like operation is proposed in [247], achieving microsecond-level accuracy. In a less rigid time-scale, for the case of mesh deployments with long distance links and multiple directional antennae per node, in [248] authors develop a protocol to enable simultaneous transmissions (and receptions) at every node.

The ARQ scheme of 802.11 is another source of inefficiency, because it can take a significant amount of time even when only a few symbols may have been wrong. To address this, a number of works have proposed mechanisms to improve the **frame recovery** mechanism. In [141], the Multi-Radio Diversity system is presented, which is based on combining different copies of the same frame (divided into blocks) as received at different APs, to try to recover it. In [249], authors propose that overhearing nodes aware of a failed transmission perform an *opportunistic retransmission* before the sender transmits, leveraging on the differentiation provided by EDCA. A number of works [250]–[252] propose *partial packet recovery* schemes, in which the frame is divided into blocks, which are independently protected, so the receiver decides whether to trigger the complete retransmission or just parts of the original frame, sometimes using a different encoding (depending on the

[12]http://www.ing.unibs.it/\ignorespacesopenfwwf/

retransmission round) or even piggybacking over regular (i.e., not retransmitted) frames.

Finally, the use of **network coding** has been addressed in a number of works, which typically leverage on the broadcast nature of the medium and bi-directional communications: in [253] authors describe the COPE scheme, implemented with the Click router running over Netgear cards, which is based on nodes promiscuously listening to the medium to store frames and then, based on reception reports, decide which frames to transmit to maximise the throughput with a single transmission. In case of delayed or missing reports COPE leverages routing metrics, such as ETX, to estimate the packet delivery probability of the neighbouring links; in [254], the interactions between network coding and TCP are further explored, while in [255] the COPE framework is extended with transmission rate control, to enable adequate overhearing, based on channel quality and neighbour information.

E. Energy Efficiency

The Power Save Mode (PSM) of 802.11 enables wireless clients in infrastructure mode to keep their interfaces in sleep mode, and switch to the awake mode only to listen to beacon frames from the AP, where the Traffic Indication Map (TIM) announces incoming traffic for the clients. As the standard does not specify how to configure the operation of PSM, many works have turned to PSM to propose energy-efficient operation, typically based on adaptive schemes that judiciously trade-off performance for power consumption.

In general, the default beacon interval of 100 ms introduces non-negligible delays on the operation of PSM, which can be particularly harmful when interacting with **request-response protocols** and, in particular, the Network File System [256]. In that paper, authors propose a novel framework that decides if the interface has to switch to the Constantly Active Mode (CAM) of operation, based on empirically-collected distribution of applications' behaviour, energy consumption and switching delays of the 802.11 interfaces. Furthermore, they propose the use of an interface for application to provide some "hints" about their intent and activity.

Given that mobility-related operations are not PSM-friendly, in [257] authors present the Cell2Notify architecture for VoIP over WLAN, where the mobile terminal has the Wi-Fi interface switched off and activates it when it is notified of an incoming call via the cellular interface. The standby time of smartphones is increased, at the cost of a larger delay when establishing the call.

Other energy-efficient approaches over PSM are tailored to the case of **voice**, based on predicting the length of the next silent period to maximise the amount of time in sleep state [258], or on explicitly trading-off performance for energy savings, by delaying traffic up to the maximum tolerable delay (to preserve application quality) to maximise the amount of time in sleep mode [259]. This approach is **generalised** with Catnatp [260], where authors present an architecture based on a middle box, which builds on the concept of "application data unit" (ADU) instead of frame. In this way, the middle box stores all frames composing an ADU before delivering it to the wireless client in a batch, so it can maximise the amount of time in idle mode (or even in the suspend-to-RAM mode of laptops).

Given that the PSM announces in the TIM the availability of traffic for a number of stations, it triggers their simultaneous awakening. To prevent this, which can introduce significant delays as stations have to wait for others' transmissions, authors propose in NAPman [261] to optimise the **scheduling** of the transmissions by using virtualised APs, so the "wake-up windows" of different clients (receiving different TIM) are staggered over time. For the case of multiple APs in range, authors present in Sleepwell [262] a system that achieves energy efficiency by evading network contention, which builds on a distributed scheme for APs to fairly share the channel, and modify timestamps so associated (and unmodified) clients are "moved" to the adequate period of time.

A different set of works have addressed the **optimisation of the wireless interface**. In [263], authors illustrate how the choice of the CW alters the energy of the WLAN, and propose a criterion to share resources between stations with very efficient interfaces and those with more consuming interfaces. In [264], authors tweak the operation of PSM to trigger the PS-polls only when the quality of the received beacon is above a certain threshold, similarly to opportunistic scheduling.

When there are **multiple interfaces** in the same device, the challenge is to use the most efficient one. This is analysed in [265] for the case of Wi-Fi vs. Bluetooth, by firstly measuring the efficiency of different inter-technology switching—as this can lead to energy wastage—and then proposing the CoolSpots mechanism, based on Wi-Fi power saving and Bluetooth sniff mode. A similar analysis is performed in [266] for the case of Wi-Fi vs. 3G. In both works, the designed algorithm is based on variables such as the context (i.e., location) information, past history, device motion, etc. Furthermore, with Cool-Tether [267] authors propose to simultaneously use multiple paths for *web stripping* with an HTTP proxy, with various mobile nodes to operate in a tethering-like way, to minimise the energy consumed for a transaction. A recent work [124] has uncovered that some non-negligible consumption (the so-called *cross-factor*) is due to internal operations in the devices, so techniques such as coalescing or batching can also reduce the energy consumption within the device.

Finally, the use of **resource on demand** schemes has been assessed in experimental conditions: in [268] for the case of long distance links, where authors use 802.15.4 devices to detect incoming transmissions, and then power up the (more consuming) 802.11 links; and in [269], for the case of indoor WLANs, where the objective is to guarantee coverage in a physical area while minimising the number of APs switched on to guarantee a given performance.

F. Spectrum-Agile Schemes

Although COTS 802.11 hardware does not typically support spectrum agility, i.e., the ability to quickly change the spectrum occupied during transmissions, this has not precluded some experimental work in this area with Wi-Fi technology. For instance, the *DSASync* framework [270], whose focus is on the

TABLE V
RESEARCHER'S HOW-TO OVERVIEW (a) WORKS THAT FOCUS ON RESEARCHERS' HOW-TO. (b) MOST RELEVANT CONTRIBUTIONS

(a)

Testbed descriptions	Indoor	[274]–[281]
	Outdoor	[41], [282]–[287]
Deployment guidelines		[65], [202], [288]–[293]
Traffic and user activity reports	Academic	[294]–[298]
	Corporate	[299], [300]
	Commercial	[62], [301]
	City-wide	[41], [293], [302]–[303]
Measuring	Sniffing	[202], [298], [302]–[308]
	Packet-pairs	[309]–[312]

(b)

Ref.	Year	Citations	Rate	Category
[41]	**2005**	**877 (1)**	**87.7 (1)**	**Testbed descriptions, Traffic & user activity reports**
[296]	2004	725 (2)	65.91 (2)	Traffic & user activity reports
[295]	2002	623 (3)	47.92 (3)	Traffic & user activity reports
[297]	2002	594 (4)	45.70 (5)	Traffic & user activity reports
[299]	2003	491 (5)	40.92 (6)	Traffic & user activity reports
[275]	2005	467 (6)	46.70 (4)	Traffic & user activity reports
[294]	2000	423 (7)	28.2 (9)	Testbed descriptions
[304]	2006	275 (8)	30.56 (7)	Traffic & user activity reports
[282]	2007	230 (9)	28.75 (8)	Measuring
[274]	2002	227 (10)	17.46 (12)	Testbed descriptions
[202]	2006	225 (11)	25.00 (10)	Measuring, deployment guidelines
[298]	2005	182 (12)	18.20 (11)	Traffic & user activity reports, measuring

TABLE VI
MOST RELEVANT 802.11 TESTBEDS

Testbed	Indoor	Outdoor	# Nodes	Technology	Mode	Size
APE [274]	✓	✓	37	802.11b	Ad-hoc	174 m
ORBIT [275]	✓	✗	400	802.11b/g	Infra & mesh	464 m^2
Slicing [276]	✓	✗	15	802.11b	-	6-floor building
Testbed on a desktop [277]	✓	✗	7	802.11b	Ad-hoc	-
Teaching [278], [279]	✓	✗	15	802.11b	Emulator	-
Common Code [280]	✓	✗	12	802.11a	Infra	800 m^2
MiNTm [281]	✓	✗	12	802.11a	Mesh	-
WiLDNet [282]	✓	✓	4	802.11b	Mesh	Up to 65 km
Roofnet [41]	✗	✓	37	802.11b	Mesh	4 km^2
MobiMESH [283]	✓	✓	-	802.11b/g/h	Mesh	-
CVeT (UCLA) [284]	✗	✓	30	802.11a/b/g/n/p	Mesh	0.05 km^2
Digital Gangetic Plains [285]	✗	✓	8	802.11b	Mesh	Up to 38 km
QuRiNet [286]	✗	✓	34	802.11b	Mesh	8 km^2
DTN [287]	✗	✓	8	802.11b	Mesh	Campus

performance of TCP in white spaces environments, is assessed in an 802.11 setting, using the `madwifi` driver. In [271], authors use a setting with two wireless cards on different channels to implement a packet-level diversity scheme, where the sender distributes the packet transmissions across different frequency bands.

Some other recent works build on the ability to change the configuration of the phase-locked loop (PLL) of the Atheros-based card, which enables the ability to select the channel width between 5 and 40 MHz. With *SampleWidth* [272], authors make the case for adapting the channel width, demonstrating that low throughput demands a narrower channel, increases the transmission range and improves energy efficiency, showing throughput improvements of 60% in a two-node scenario. In a follow-up work [273], authors consider the case of a multi-AP deployment and propose to adapt each AP's channel width depending on the traffic demand, based on an analysis of the impact of interference on different configurations.

VI. RESEARCHERS' HOW-TO

In this section we present those works that focus on the methodology of the experimentation, and therefore provide the basis for the performance of measurements or research: testbed descriptions (along with some "best practises"), traffic analysis, or techniques to perform the measurements. Table V(a) presents a snapshot of these works, and Table V(b) overviews the contributions with the largest impact.

A. Testbed Descriptions

Although all papers considered describe the testbed used, here we focus on those that put special emphasis on the description, either because they were among the first to report some issues with respect to deployment, or because a particular feature of the deployment is worth mentioning. We provide a summary of the testbeds in Table VI. Some of the testbeds do not have a paper explicitly devoted to describe them, however other reviewed papers leverage on these testbeds to perform their experimental evaluation. We have included these testbeds as well for completeness reasons.

1) Indoor: One of the first indoor testbeds is APE [274], composed of 37 laptops, where the focus is set on the reproducibility of the experiments, which is achieved through the strict specification of a script specifying the "choreography" of the experiment, with instructions for the testers, who walk around with nodes based on the Orinoco chipset and a modified version of the driver to test different routing protocols. One of the most famous testbeds used for experimentation is ORBIT [275], an open deployment consisting of 400 nodes in which users: have full access to the radio nodes used; can download and run their own OS image and software packages; control and reboot the nodes; as well as have access to each node console

logs. In this way, researchers can book in advance the testbed to run the designed wireless experiment (*á la* PlanetLab[13] [313]). One extension to this "open testbed" paradigm, which makes a more efficient use of the resources, is presented in [276]. In this paper (which extends the work for the NITlab[14] deployment) authors build on the observation that experimental practitioners rarely use *all* of the devices available but instead only use a small fraction of them, and therefore the infrastructure can be shared only if the spectrum is properly allocated. To this aim, they propose to introduce spectrum slicing.

One key issue when deploying a wireless testbed in a laboratory (a constrained physical space) is antenna radiation. In particular, when distances are small, i.e., same order of magnitude as the wavelength, nodes cannot be assumed to behave as ideal "point radiators," but instead inter-node interference may be very significant. In [277], authors propose two actions to keep the size of the testbed small, namely, (*i*) shield the NIC to prevent radiation except from the intended antenna connector, and (*ii*) use a toolbox of cables, attenuators, splitters and combiners to emulate the scenario, thus controlling the radio conditions and guaranteeing repeatability of the experiments. This idea is pushed further in [278], where the RF signals from the nodes are processed by an FPGA (after mixing with local oscillator), thus enabling the emulation of radio conditions. This not only ensures repeatability of the results, but also supports testing performance under a large variety of different scenarios. Indeed, [279] reported the use of the testbed in [278] for teaching purposes. In [280], authors introduce `CommonCode`, a code-reuse platform so researchers can use almost the same code when performing simulations and when running the actual experiments.

Finally, for the case of experiments requiring repeatable mobility patterns (e.g., MANETs research), in [281] authors present the use of 12 wireless devices mounted over automated vacuum cleaners, which have been *hacked* to support the reprogramming of their movement algorithms.

2) Outdoor: While the actual deployment of indoor devices is typically straightforward (although some recommendations and pitfalls to avoid should be followed as described in the next section), this is not the same for the case of outdoor scenarios, which involves dealing with other issues like, e.g., antenna alignment.[15] Incidentally, one of the first papers describing the deployment of an outdoor scenario is RoofNet [41], where 37 nodes are set-up in a 4 km^2 area in Cambridge, Massachusetts, using omnidirectional antennae. The design of Roofnet assumed that some users will voluntarily share their DSL access (depending on Acceptable Use Policies), but eventually had only four Internet gateways: two located in ordinary residences, and two on university buildings (for an overview of technical issues when designing a real mesh network see, e.g., the MobiMESH description [283]). For the case of vehicular networks, the CVeT testbed [284] is composed of 30 vehicles running different 802.11 technologies and software framework for management and debugging, and builds on a wireless mesh backhaul.

Mesh networking is particularly well suited for non-urban environments, in which Internet connectivity is sparse and the electrical power supply may not be available or may experience power outages. To address these issues, one option is to use directional antennae to cover long distances, such as, 38 km [285] or 65 km [282], and another option is to use batteries and solar panels to support network operation without electric plugs. Indeed, as discussed in [285], a solar panel could provide a round-the-clock average of about 8 W, and as shown in QuRiNet [286] solar energy is used to power the devices communicating 34 nodes spread over 2000 acres (approx. 8 km^2) of wilderness. Finally, in [287], authors describe a hardware and software architecture for energy-efficient *throwboxes* (i.e., stationary and battery-power nodes to enhance the capacity of DTNs) to be used in the DieselNet network.

B. Deployment Guidelines

In this section we focus on those papers where a significant part of the contribution is the discussion of the design and criteria used to deploy the testbed. In many cases, these papers have an explicit section on "lessons learnt" (e.g., [288]–[290]) to summarise the main takeaway ideas from the experiences of the researchers.[16]

One of the first papers to report the design of a large-scale WLAN is [65]. In this (now old) paper, authors describe in great detail the deployment of APs at Carnegie Mellon University, in which a great deal of effort is devoted to provide coverage while minimising overlap between APs, based on geometrical considerations. As described in Section III-B2, they also briefly describe the use of a design tool to aid with channel assignment. Another paper describing the design considerations (e.g., platform selection, management plane) of an indoor testbed is [288], in which authors discuss the deployment of an indoor mesh network at University of California at Santa Barbara. A similar experience is reported in [289], where authors advocate for the use of Power over Ethernet APs to support a better remote control, and they also detail the design of the IP addressing scheme. Finally, in [290], authors deploy the testbed under the panels of the raised floor, a space easily accessible and physically well protected, thus preventing wire disconnection or unwanted movements of the equipment.

Another set of papers build on tailored measurements to derive guidelines for the deployment and configuration of WLANs: in [292], authors advocate for the use of load balancing, adaptive power control and frequency allocation for the case of single-hop networks; in [202] it is reported the deployment of a two-tier urban mesh network; and finally, in [293], authors provide an extensive report on the performance of a commercial mesh deployment.

[13] http://www.planet-lab.org

[14] http://nitlab.inf.uth.gr/NITlab/

[15] We cannot help but quote from [282]: "We thank [people] for braving wind, sun, rain and crazy taxi drivers to set up long-distance links [. . .] so that we can run our experiments."

[16] For a survey on recommendations when performing experimental work, we refer the reader to [291].

TABLE VII
SUMMARY OF TRAFFIC REPORTS

Ref.	Year	Environment	# Users	# APs	Time period
[294]	2000	Campus building	74	12	12 weeks
[295]	2002	Campus	2000	476	11 weeks
[296]	2004	Campus	7000	550	17 weeks
[297]	2002	Conference building	195	4	52 hours
[298]	2005	Conference building	1138	38	2 days
[299]	2003	Campus industrial	1366	131, 36, 10	4 weeks
[300]	2005	Corporate environment	11, 21	-	1 month
[301]	2006	Commercial area	-	4	14,400 min
[62]	2009	Commercial area	13 spots	-	1 week
[41]	2005	City-wide	16	37	24 hours
[302]	2008	City-wide	29000	500	28 and 5 days
[293]	2008	City-wide	627	250	100 hours
[304]	2008	City-wide	-	1200, 965	-

C. Traffic and User Activity Reports

Here we classify those works that analyse, over relatively long periods of time, the usage patterns of the wireless medium through, e.g., the volume of traffic per hour, type of traffic, or AP load in terms of user association and mobility. Note that we do not aim to extensively report *all* experimental works where there is some traffic activity reported, but only those in which the usage can be considered representative of regular (i.e., non-research) activity. We present in Table VII a snapshot of the surveyed studies (in the Table, with "nodes" we refer to either APs or Mesh Nodes).

1) Academic Environment: One of the first studies is [294], where authors analyse a 12-week trace from 12 APs distributed across a 6-floor building. Data is gathered via SNMP queries, and they analyse the behaviour of the 74 users detected in terms of load, user mobility, and the type of application being used (including `irc` and `Eudora`!). A larger deployment is analysed in [295], consisting of 476 APs over 161 buildings, describing the aggregate traffic per day (with spikes of almost 250 GB), activity per AP (the median being 39 MB), or the protocol type, with `HTTP` being the most active and a proprietary backup solution the second most active. In a later follow-up work authors perform an updated study on 17-week traces [296], comparing the result vs. the ones from the initial network deployment. In this comparison, they identify the rise of peer-to-peer, streaming multimedia traffic, and an increased heterogeneity of user devices. The greater client heterogeneity motivates a new metric, "session diameter", to show differences in mobility w.r.t. laptops, although users were overall non-mobile. As a particular case of academic scenario, in [297] authors analyse the traffic recorded over three days of ACM SIGCOMM'01, with 195 different clients connected to 4 APs. They report a vast majority of HTTP and SSH traffic and, perhaps not surprisingly, a strong correlation between the conference schedule and the network load. A similar work is the report of the traffic during the 62nd IETF meeting [298], with 2 days of data from 38 APs providing access to 1138 participants. In contrast to the previous case, here the distribution of users and AP load is quite uneven, due to the large size of the deployment.

2) Corporate Environment: In [299], authors present an analysis of 4 weeks of traffic in a corporate environment. The WLAN is deployed across 3 buildings, with 131, 36 and 10 APs per building, and includes up to 1366 different clients. They report large variety across users, with for example, 40% of the load being due to 10% of the most active users. As expected, the traffic pattern is very different from the one typically observed in academic environments, with little (if any) activity past 8 PM. Another study is presented in [300], in which authors first analyse the *wired* traffic from 11 users in a corporate environment, and then replay the traffic over a 21-node mesh network using different configurations, to understand if an indoor mesh could replace the wired access (the answer being yes).

3) Commercial Deployments: Authors analyse in [301] the wireless traffic of the public WLAN in four different restaurants from the same commercial chain in Austin, Texas. The network utilisation is not very high, with the average hourly by-directional rate being 10 MB for the restaurant with the highest load. In this restaurant, the time of the day has a strong impact of the traffic activity, with peaks around 1 Mbps, and most of the traffic is HTTP. In contrast to this single-provider, free WLAN study, in [62] authors perform a comprehensive study of commercial hotspots in the city of Seattle over the course of 1 week. They report various figures related to performance, namely, the success rate when associating to the AP, the TCP download rate, and the responsiveness in terms of downloading a given web page, as well as port and applications blocking. Based on the heterogeneity observed, they propose a collaborative service to collect historical information about AP performance (described in Section III-B1).

4) City-Wide Studies: The Roofnet paper [41] showed some usage statistics, although the network load was quite small: during a 24 h period of time, 16 out of the 37 nodes accessed the Internet, with the gateway forwarding an average of 160 kbps of data. Results from the Google Wi-Fi network in California are reported in [302], consisting of 500 mesh APs that provide service to approximately 15000 smartphones, 1000 modems (i.e., the recommended devices to connect to the network) and 14000 regular devices (i.e., computers). In such large deployment, three distinct user populations are identified, depending on their usage and mobility patterns, e.g., smartphone users are concentrated along travel corridors, and although they do not consume a lot of traffic, their peak activity is correlated with commute times. In [293], authors present a measurement study of a commercial mesh network deployed in Madison consisting of more than 250 nodes. In that report, authors find that the bottleneck is the access link (backbone links are robust) and that in contrast to core ISPs, peaks occur in night-time and the client distribution is quite uneven. Finally, in [303] authors perform active probing to characterise the wireless network of residential users from two neighbourhoods in Pittsburgh, identifying the broadband vendor, bandwidth, and the AP vendor.

D. Measuring

In the previous section, most of the studies are based on gathering usage statistics from the APs via standard techniques, e.g., SNMP queries. In this section, we analyse those papers partly dealing with the measurement process.

1) Sniffing: Due to the nature of the wireless medium, sniffing the "ground truth" of the wireless activity is extremely

challenging. In the measurement report from the 62nd IEFT meeting [298], authors build on their knowledge of the AP topology to carefully select the physical location for the deployment of three sniffers, on channels 1, 6 and 11. Later, they analyse the capture trace to check consistencies (e.g., DATA frames shall precede ACK frames) to estimate missing frames, which ranges between 3% and 20%. However, the fact that a frame is missing in the trace-file does not necessarily imply that it was not delivered over the wireless medium, and therefore the only way to obtain the "complete" picture (including not only time but also location information) is to deploy multiple sniffers at various locations, and later on to merge the trace-files. This is the approach presented in Jigsaw [304], in which authors present a measurement infrastructure consisting of 150 synchronised monitoring devices that are able to capture concurrent transmissions at different physical locations. Thanks to the strict synchronisation between nodes, they can later all merge all captured data and generate the complete trace-file, which includes concurrent transmissions (i.e., collisions) and can help to diagnose performance impairments. Another centralised scheme for diagnosis purposes is MOJO [305], which presents the deployment and calibration of various sniffers to accurately identify the root causes of wireless anomalies. Still, it should be noted that these devices are not ideal devices and therefore may miss some frames, as analysed in an anechoic environment in [306] via controlled experimentation.

While the above addresses the effectiveness of sniffing, a different challenge is how to get the most out of the resources available. In [307], authors design a framework in which the *focus* of the monitoring device is changed, depending upon the observed network conditions (e.g., instead of equally sampling all channels, focus on those with more activity). A related technique is the use of the "mark-and-sweep" methodology [303], which consists of a first sweep to obtain a rough estimation of the environment (e.g., signal quality), and a second sweep with emphasis on those areas previously defined as of interest. Finally, In [308], authors measure the "served area" of two operation mesh networks (Google WiFi [302] and TFA [202]) by performing an estimation of propagation, based on nodes' deployment and terrain information from digital maps, and then identifying locations of interest where measurements have to be made to refine the estimation.

2) Packet-Pairs: Estimating the available capacity in 802.11 WLANs is more challenging than in wired networks, as the MAC layer introduces a severe bias in the estimation of **active** tools such as, e.g., Spruce or Pathload. In [309], authors perform an extensive comparison study of these active bandwidth estimation tools in a wireless mesh network, and compare their performance against a very simple passive estimation tool. Not surprisingly, the use of these probe-based tools is not recommended for 802.11, as the time between two consecutive messages from the same source can have high variability. This is further analysed in [310], where authors describe how the different packets of a probing sequence observe a different state of the CSMA/CA-based network, and therefore dispersion-based measurements should use long packet trains to obtain accurate estimations. A bandwidth estimation tool specifically envisioned for 802.11 WLANs is `WBest` [311], which combines both a packet pair and a packet train technique, outperforming the classical tools for wired networks.

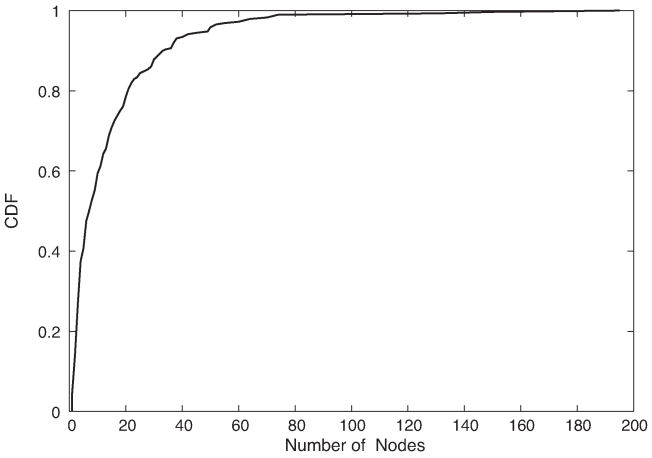

Fig. 5. CDF of the number of nodes used.

In contrast to the above techniques, which require sending probe traffic, in [312] they propose a **passive** technique based on analysing the "ACK pairs" of TCP connections. More specifically, the approach consists of analysing the trace-file collected at a wired point of the network and perform Bayesian inference on the delay between consecutive ACKs from remote stations. In this way, they are able to infer if the flow traversed a 10 Mbps, 100 Mbps Ethernet, or an 802.11g WLAN.

VII. Summary Statistics of Methodologies Used

Here we present some summary statistics on the methodologies followed by experimentalists, to identify patterns and help to spot new areas of research, discussed in the next section. We first analyse the **size of the testbed** deployed to perform the experimentation, by reviewing all papers in our collection and identifying the total number of wireless nodes used (note that a node with various interfaces still counts as one node). We were able to perform this analysis for 97% of the papers, as unfortunately in some of them the testbed description was not including this information. We provide the resulting cumulative distribution function in Fig. 5.

According to the results, more than 80% of the papers involved less than 20 nodes, which nowadays can be considered as a relatively small number. Indeed, despite the reduced cost of 802.11 devices, it results somewhat surprising that few works have used more than 100 nodes, in particular given the high transmission rates supported by 802.11a/g/n. Although the higher the number of nodes the more difficult is to perform measurements or gather the results, testing high transmission rates with a small number of nodes prevents, e.g., reaching the capacity limits of a given technology, or the impact of the control and signalling load for *crowded* scenarios. As we discuss next, we conjecture a rise of experimental research in *extremely-dense* scenarios.

We next analyse the use of the different **PHY standards** over the years. To this aim, we count the total number of papers using each of the PHY considered (namely, 802.11b, 802.11a, 802.11g and 802.11n) and provide the relative amount of works

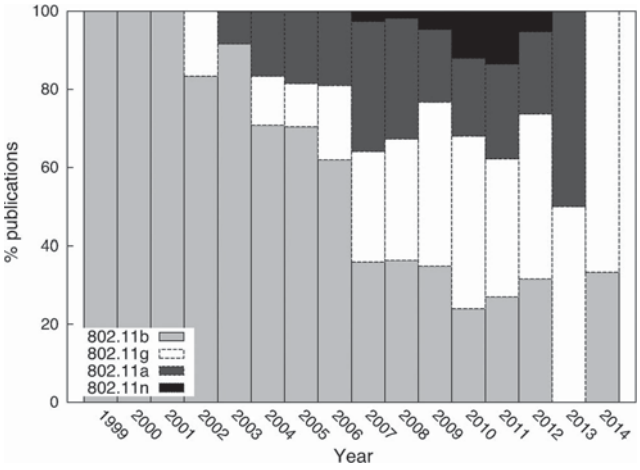

Fig. 6. Relative presence of each PHY layer over the years.

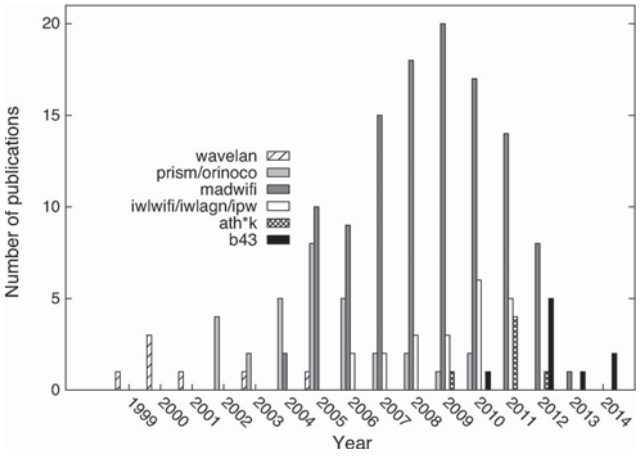

Fig. 7. Driver in the experimental setup over the years.

using each of these standards over the years in Fig. 6. The results can be summarised as follows:

- Not surprisingly, the widely adopted 802.11b was prevalent in the early years of Wi-Fi, and only since 2007 on its "market share" of research works has been below 50%.
- Both 802.11a and 802.11g shared a quite similar amount of presence over the years until 2008. Since then, it seems researchers tend to favour the PHY operating in the 2.4 GHz.
- The "recent" 802.11n amendment has not received significant attention yet, with a quota that is always below 10%. We conjecture that this is because of the higher costs of fully-featured 802.11n devices, and the inherent challenges of configured more advanced PHY layers.

Finally, we analyse the **software driver** used in the experimental setup. More specifically, we went through the works considered, identifying which of the following five types of drivers was used (we could perform this identification for approximately 80% of the papers considered):

- `wavelan`: This driver was the first to arrive, supporting WaveLAN cards, which used a slightly modified version of the 802.11 standard.
- `prism/orinoco`: This driver can be considered as the *evolution* of the wavelan family.
- `madwifi`: This driver support Atheros-based wireless cards.
- `iwlwifi/iwlagn/ipw`: These drivers support Intel cards.
- `ath*k`: These modern drivers support the Atheros-based family of wireless cards.
- `b43`: This driver is used with Broadcom chipsets.[17]

We plot the total number of papers per driver and year in Fig. 7. As the figure illustrates, during the first years there was very little diversity in the configurations used by researchers (i.e., all work was performed using `wavelan`). After a "convulse history" of merges and acquisitions involving different companies (Lucent, Proxim, etc.), `orinoco` was the driver of choice, supported in Linux and gathering support from different 802.11b card vendors. However, in 2004/05 the `madwifi` driver irrupted and took over most 802.11 experimentation, thanks to its support for Atheros-based cards that became the "de facto" standard for experimentation,[18] although there was a notable presence of `iwlwifi/iwlagn/ipw` drivers, as Intel is the main manufacturer of integrated wireless cards.

The last official release of `madwifi` was in 2008, and it has been superseded by new drivers for Atheros chipsets, namely, ath5k (for 802.11a/b/g), ath9k (for 802.11n), and the recent ath10k that supports the new 802.11ac amendment. However, `madwifi` kept a notable presence until recently, when it is finally "loosing" its hegemony to modern drivers (e.g. the `ath*k` family for Atheros and `b43` for Broadcom) which are compatible with the Linux `mac80211` framework included in Linux kernels since version 2.6.22.

VIII. Open Challenges and Future Trends

Based on the review of the work presented in the previous sections, which covers the most significant experimental works performed with 802.11 COTS devices, we now identify a number of open challenges and future research directions. As briefly hinted when reviewing related surveys on 802.11 aspects, we expect that energy efficient operation of networks and devices will continue to attract attention from the research community in the short-term future, and eventually will be considered as another key performance metric such as, e.g., throughput or delay. Also, the fact that previous surveys did not explicitly focus on aspects such as security or privacy in 802.11 networks suggests that this area is still gaining momentum, and therefore we expect more contributions in this context. We next discuss in more detail these and other areas that we envision will attract 802.11 experimenters in the near future.

Assessment of New Amendments: Of course, as standards are approved or hardware becomes available, assessing their

[17]Note that these two families, `ath*k` and `b43`, have access to the firmware or define physical primitives at the driver level increasing the flexibility offered to researchers.

[18]We conjecture that this was partly caused by the fact that Atheros chipsets were among the first to support the tuning of the MAC parameters, apart from the solid reputation of the brand.

performance through experimentation will help to understand in which scenarios they perform best, configuration guidelines, and the corresponding performance limits or hardware impairments. In particular, we believe that 802.11ac, 802.11ad and 802.11af will attract notable attention, given their outstanding new features: for instance, 802.11ac enables MU-MIMO (which could enable efficient operation in very-dense scenarios), 802.11ad uses the mm-Wave band (i.e., line-of-sight communication, thus motivating the use of steerable antennae), and 802.11af operates in the TV white space spectrum (VHF and UHF bands), enabling an extended signal coverage but operating in a non-ISM band. As the hardware to support these becomes available,[19] we envision a boost in the works analysing the performance of these standard amendments, including the analysis of the energy consumption of novel interfaces and protocols, and the design of efficient mechanisms to select the best available medium access scheme, depending on operation conditions.

Physical Layer Flexibility: In relation with the above, as new amendments introduce novel but more complex features in the PHY layer, we expect a subset of these to become available with COTS devices. In this way, it will be possible to develop relatively advanced PHY schemes over the available features of affordable devices, instead of investing large amounts of resources to prototype over software defined radios. Some of these potential features are: access to per-carrier channel state information, dynamic re-configuration of OFDM, antenna steering schemes, etc., which will also require performance assessment studies over the configuration space.

New MAC Designs: Undoubtedly, these new standards, which range from a practically line-of-sight communications to the UHF propagation paradigm, will foster the design of new MAC mechanisms and protocols. In the case of 802.11ad, maintaining a directional communications will require tracking user mobility, for antenna steering, which will introduce the need to locate users with far higher precision than current localisation techniques. Regarding to 802.11af operation in the UHF band, the challenge imposed by hidden nodes is exacerbated, thus requiring the need to adapt current MAC schemes or to develop new ones. In addition, the increased flexibility of 802.11 platforms at both the MAC and PHY layers will motivate the design of cross-layer schemes, which will dynamically adapt to the heterogeneous conditions in which 802.11 is employed.

Heterogeneous Networking: As mobile devices with multiple wireless interfaces become the norm, we expect more and more research work on the optimal use of the available resources. This research will range from the "classical" interface selection optimisation and traffic off/onloading, which should consider both user- and network-oriented performance figures (due to, e.g., fairness considerations from hidden nodes, very-dense scenarios), to the dynamic set-up and release of Device-to-Device (D2D) communications, both for local, peer-to-peer like transmission of files, and for opportunistic 3G/4G/5G sharing. These techniques will require an accurate estimation of the scenario conditions, in terms of terminal localisation, link qualities, and user preferences, and will also need to face side considerations such a trust management and privacy preservation.

Coexistence and Cooperation With Cellular Technologies: The growing demand of mobile data traffic and the scarcity of available radio spectrum will "extend" LTE to unlicensed bands (5 GHz), in which 802.11 already operates. The co-existence of these two technologies will likely impair Wi-Fi users [314], as the access to the channel relies on sensing and a random backoff counter, whereas LTE transmits almost continuously. This will foster the research on inter-technology interference and coordinated transmission, as well as standardisation efforts, as the recently approved IEEE 802.11af standard or the IEEE 802.11ax Task Group. Also, the increasing number of users, their constant mobility—as well as their constant demand for being always connected—foster the new paradigm called *Wi-Fi Passpoint*, also known as Hotspot 2.0, which enables user authentication though cellular-like procedures (by means of the SIM cards), thus easing the burden of the association process. This will enable the design of better off-loading (and on-loading) mechanisms, including almost seamless handover across technologies, and will probably impact the existing ecosystem of mobile operators.

SDN-Inspired Operation of 802.11: One key challenge with flexible, reconfigurable, and heterogeneous 802.11 scenarios is their control and management, as each protocol layer or specific standard may introduce a different set of primitives for its configuration. In order to ease management, there is currently the trend to adapt Software Defined Networking (SDN), originally intended for wired, local scenarios, to wireless networks [315]. Actually, it may be argued that this separation of control and data plane for the switching fabric already exists, to some extent, in the wireless domain. Indeed, the IETF standardised several years ago the Control And Provisioning of Wireless Access Points (CAPWAP) protocol [316], which was supposed to be technology-agnostic, but was only particularised for 802.11 operation and never benefited from a wide deployment. With the current challenges of wireless networks, we envision a reboot of research activities along this path, but notably extending the current vision of SDN for wireless networks: not only the controller(s) should be able to reach the end terminals, to support more efficient operation, but also they should reach lower layers of the wireless stack, to adapt the operation of the wireless technology (e.g., the channel width of 802.11n) to the network conditions.

Security and Privacy Issues: Finally, we envision that security will continue to attract attention from the research community, as users become more aware of the potential threats to their privacy and the value of their data. On the one hand, in addition to the integration with cellular technologies discussed above, we envision that technologies such as Near Field Communication or Visible Light Communication, which do not share the same broadcasting characteristics as Wi-Fi, could be exploited to improve security. For instance, as these technologies enable a better control of communication, they could be used as low-bandwidth, secure channels to exchange critical information (in a similar way as, e.g., photo cameras can be used to install

[19]Which is already the case for 802.11ad http://www.qca.qualcomm.com/mobile-connectivity/wigig-802-11ad.

certificates via QR codes). On the other hand, the spread of localisation mechanisms and localisation-based services is becoming a serious source of potential security threats. In particular, considering that current terminals periodically probe for known WLANs, the privacy of 802.11 users becomes easily vulnerable to abuse. In this regard, although some devices already perform randomisation of the MAC address when performing this probing (e.g., the iPhone), available approaches are far from a complete solution for privacy. However, within the IEEE 802, there is a recently established Study Group, whose aim is to define a privacy threat model and recommended practises protocols. The proposals of such Study Group are likely to be the subject of the next wave of experimentation in the field of security in WLANs.

IX. Summary

Motivated by the wide adoption of commodity 802.11 hardware by the research community, we have performed an extensive review of the experimental work carried out over the past years. More specifically, our motivation was two-fold: on the one hand, to give a detailed and updated snapshot of the topics that have received most of the attention, so researchers and practitioners are aware of the main achievements so far (so they do not need to re-invent the wheel); on the other hand, to help identify trends or missing areas so researchers can plan their future activities.

One of the main contributions of the survey is to propose a taxonomy to categorise the vast amount of existing work; although some of them address two or more of the identified categories, we believe that for most of the papers their main contribution is accurately represented in the taxonomy. It is worth mentioning that a notable amount of works fall on the "how-to" category, which includes recommendations for testbed deployments and methodologies to obtain accurate results. Another key related contribution of our survey is the analysis of these deployments, in terms of number of nodes, PHY standard and driver used. Again, our survey identifies the trends over the past years in terms of the set-up employed to perform experimentation, and also help to identify some existing "gaps" (e.g., very few research is performed using a large number of nodes).

Finally, we have presented some open challenges for future work with commodity 802.11 hardware. With no pretence of completeness, but based on the analysis of existing work and our own experiences, we propose five different (but related) research areas, which we believe will help prospective authors to identify potential areas for their future work.

References

[1] *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*, IEEE Std. 802.11 WG, 2012.

[2] M. Y. Arslan *et al.*, "Auto-configuration of 802.11n WLANs," in *Proc. ACM CoNEXT*, 2010, pp. 27:1–27:12.

[3] K. Tan *et al.*, "Fine-grained channel access in wireless LAN," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 147–158, Aug. 2010.

[4] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[5] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 37, no. 6, pp. 1067–1080, Nov. 2007.

[6] P. Almers *et al.*, "Survey of channel and radio propagation models for wireless MIMO systems," *EURASIP J. Wireless Commun. Netw.*, vol. 2007, no. 1, Jan. 2007, Art. ID. 019070.

[7] D. Feng *et al.*, "A survey of energy-efficient wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 167–178, 1st Quart. 2013.

[8] J. Vella and S. Zammit, "A survey of multicasting over wireless access networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 718–753, 2nd Quart. 2013.

[9] Q. Ni, L. Romdhani, and T. Turletti, "A survey of QoS enhancements for IEEE 802.11 wireless LAN," *Wireless Commun. Mobile Comput.*, vol. 4, no. 5, pp. 547–566, Aug. 2004.

[10] E. Charfi, L. Chaari, and L. Kamoun, "PHY/MAC enhancements and QoS mechanisms for very high throughput WLANs: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1714–1735, 4th Quart. 2013.

[11] B. Sardar and D. Saha, "A survey of TCP enhancements for last-hop wireless networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 3, pp. 20–34, 3rd Quart. 2006.

[12] A. Al Hanbali, E. Altman, and P. Nain, "A survey of TCP over ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 3, pp. 22–36, 3rd Quart. 2005.

[13] L.-H. Yen, T.-T. Yeh, and K.-H. Chi, "Load balancing in IEEE 802.11 networks," *IEEE Internet Comput.*, vol. 13, no. 1, pp. 56–64, Jan./Feb. 2009.

[14] S. Chieochan, E. Hossain, and J. Diamond, "Channel assignment schemes for infrastructure-based 802.11 WLANs: A survey," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 1, pp. 124–136, 1st Quart. 2010.

[15] B. Alawieh, Y. Zhang, C. Assi, and H. Mouftah, "Improving spatial reuse in multihop wireless networks—A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 3, pp. 71–91, 3rd Quart. 2009.

[16] P. Cardieri, "Modeling interference in wireless ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 4, pp. 551–572, 4th Quart. 2010.

[17] H. Zhai, Y. Kwon, and Y. Fang, "Performance analysis of IEEE 802.11 MAC protocols in wireless LANs: Research articles," *Wireless Commun. Mobile Comput.*, vol. 4, no. 8, pp. 917–931, Dec. 2004.

[18] S. Pack, J. Choi, T. Kwon, and Y. Choi, "Fast-handoff support in IEEE 802.11 wireless networks," *IEEE Commun. Surveys Tuts.*, vol. 9, no. 1, pp. 2–12, 1st Quart. 2007.

[19] B. V. Quang, R. V. Prasad, and I. Niemegeers, "A survey on handoffs-lessons for 60 GHz based wireless systems," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 1, pp. 64–86, 1st Quart. 2012.

[20] M. Sichitiu and M. Kihl, "Inter-vehicle communication systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 2, pp. 88–105, 2nd Quart. 2008.

[21] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. I. Kim, "Mobility and handoff management in vehicular networks: A survey," *Wireless Commun. Mobile Comput.*, vol. 11, no. 4, pp. 459–476, Apr. 2011.

[22] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks," *Comput. Std. Interfaces*, vol. 31, no. 5, pp. 931–941, Sep. 2009.

[23] L. Guang, C. Assi, and A. Benslimane, "MAC layer misbehavior in wireless networks: Challenges and solutions," *IEEE Wireless Commun.*, vol. 15, no. 4, pp. 6–14, Aug. 2008.

[24] I. Jabri, N. Krommenacker, T. Divoux, and A. Soudani, "IEEE 802.11 load balancing: An approach for QoS enhancement," *Int. J. Wireless Inf. Netw.*, vol. 15, no. 1, pp. 16–30, Mar. 2008.

[25] M. Natkaniec, K. Kosek-Szott, S. Szott, and G. Bianchi, "A survey of medium access mechanisms for providing QoS in ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 592–620, 2nd Quart. 2013.

[26] X. Yu, P. Navaratnam, and K. Moessner, "Resource reservation schemes for IEEE 802.11-based wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1042–1061, 3rd Quart. 2013.

[27] C. Chaudet, D. Dhoutaut, and I. Lassous, "Performance issues with IEEE 802.11 in ad hoc networking," *IEEE Commun. Mag.*, vol. 43, no. 7, pp. 110–116, Jul. 2005.

[28] K. Kosek-Szott, "A survey of MAC layer solutions to the hidden node problem in ad-hoc networks," *Ad Hoc Netw.*, vol. 10, no. 3, pp. 635–660, May 2012.

[29] R. Carrano, L. Magalhaes, D. Saade, and C. Albuquerque, "IEEE 802.11s multihop MAC: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 1, pp. 52–67, 1st Quart. 2011.

[30] D. Benyamina, A. Hafid, and M. Gendreau, "Wireless mesh networks design—A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 299–310, 2nd Quart. 2012.

[31] L. Hanzo, II and R. Tafazolli, "Admission control schemes for 802.11-based multi-hop mobile ad hoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 78–108, 4th Quart. 2009.

[32] S. Biaz and S. Wu, "Rate adaptation algorithms for IEEE 802.11 networks: A survey and comparison," in *Proc. IEEE ISCC*, Jul. 2008, pp. 130–136.

[33] C. E. Jones, K. M. Sivalingam, P. Agrawal, and J. C. Chen, "A survey of energy efficient network protocols for wireless networks," *Wireless Netw.*, vol. 7, no. 4, pp. 343–358, Sep. 2001.

[34] S.-L. Tsao and C.-H. Huang, "A survey of energy efficient MAC protocols for IEEE 802.11 WLAN," *Comput. Commun.*, vol. 34, no. 1, pp. 54–67, Jan. 2011.

[35] A. De Domenico, E. Strinati, and M. Di Benedetto, "A survey on MAC strategies for cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 1, pp. 21–44, 1st Quart. 2012.

[36] R. Riggio *et al.*, "Hardware and software solutions for wireless mesh network testbeds," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 156–162, Jun. 2008.

[37] S. Vural, D. Wei, and K. Moessner, "Survey of experimental evaluation studies for wireless mesh network deployments in urban areas towards ubiquitous Internet," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 223–239, 1st Quart. 2013.

[38] D. Dujovne, T. Turletti, and F. Filali, "A taxonomy of IEEE 802.11 wireless parameters and open source measurement tools," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 2, pp. 249–262, 2nd Quart. 2010.

[39] G. Xylomenos and G. Polyzos, "TCP and UDP performance over a wireless LAN," in *Proc. IEEE INFOCOM*, Mar. 1999, vol. 2, pp. 439–446.

[40] G. Anastasi, E. Borgia, M. Conti, and E. Gregori, "IEEE 802.11 ad hoc networks: Performance measurements," in *Proc. IEEE ICDCS Workshops*, 2003, pp. 758–763.

[41] J. Bicket, D. Aguayo, S. Biswas, and R. Morris, "Architecture and evaluation of an unplanned 802.11b mesh network," in *Proc. ACM MobiCom*, 2005, pp. 31–42.

[42] D. Dujovne, T. Turletti, and P. Planete, "Multicast in 802.11 WLANs: An experimental study," in *Proc. ACM MSWiM*, 2006, pp. 2–6.

[43] A. Banchs, A. Azcorra, C. Garcia, and R. Cuevas, "Applications and challenges of the 802.11e EDCA mechanism: An experimental study," *IEEE Netw.*, vol. 19, no. 4, pp. 52–58, Jul./Aug. 2005.

[44] I. Dangerfield, D. Malone, and D. Leith, "Experimental evaluation of 802.11e EDCA for enhanced voice over WLAN performance," in *Proc. IEEE WiOpt*, Apr. 2006, pp. 1–7.

[45] V. A. Siris and G. Stamatakis, "Optimal CWmin selection for achieving proportional fairness in multi-rate 802.11e WLANs: Test-bed implementation and evaluation," in *Proc. ACM WiNTECH*, 2006, pp. 41–48.

[46] P. Serrano, P. Patras, A. Mannocci, V. Mancuso, and A. Banchs, "Control theoretic optimization of 802.11 WLANs: Implementation and experimental evaluation," *Comput. Netw.*, vol. 57, no. 1, pp. 258–272, Jan. 2013.

[47] C. E. Koksal, H. Kassab, and H. Balakrishnan, "An analysis of short-term fairness in wireless media access protocols," in *Proc. ACM SIGMETRICS*, 2000, pp. 118–119.

[48] G. Berger-Sabbatel, A. Duda, O. Gaudoin, M. Heusse, and F. Rousseau, "Fairness and its impact on delay in 802.11 networks," in *Proc. IEEE GLOBECOM*, Nov. 2004, vol. 5, pp. 2967–2973.

[49] G. Berger-Sabbatel, A. Duda, M. Heusse, and F. Rousseau, "Short-term fairness of 802.11 networks with several hosts," in *Proc. IFIP MWCN*, Springer-Verlag, Boston, MA, USA, Oct. 2004, vol. 162, pp. 263–274.

[50] S. Pilosof, R. Ramachandran, D. Raz, Y. Shavitt, and P. Sinha, "Understanding TCP fairness over wireless LAN," in *Proc. IEEE INFOCOM*, Mar. 2003, vol. 2, pp. 863–872.

[51] A. C. H. Ng, D. Malone, and D. J. Leith, "Experimental evaluation of TCP performance and fairness in an 802.11e test-bed," in *Proc. ACM E-WIND*, 2005, pp. 17–22.

[52] E. Lopez-Aguilera *et al.*, "An asymmetric access point for solving the unfairness problem in WLANs," *IEEE Trans. Mobile Comput.*, vol. 7, no. 10, pp. 1213–1227, Oct. 2008.

[53] V. Shrivastava, S. Rayanchu, J. Yoonj, and S. Banerjee, "802.11n under the microscope," in *Proc. ACM IMC*, 2008, pp. 105–110.

[54] U. Paul, R. Crepaldi, J. Lee, S.-J. Lee, and R. Etkin, "Characterizing WiFi link performance in open outdoor networks," in *Proc. IEEE SECON*, 2011, pp. 251–259.

[55] S. Lakshmanan, J. Lee, R. Etkin, S.-J. Lee, and R. Sivakumar, "Realizing high performance multi-radio 802.11n wireless networks," in *Proc. IEEE SECON*, 2011, pp. 242–250.

[56] S. Rayanchu, A. Patro, and S. Banerjee, "Airshark: Detecting non-WiFi RF devices using commodity WiFi hardware," in *Proc. ACM IMC*, 2011, pp. 137–154.

[57] G. Judd and P. Steenkiste, "Fixing 802.11 access point selection," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 32, no. 3, pp. 31–31, Jul. 2002.

[58] S. Vasudevan, K. Papagiannaki, C. Diot, J. Kurose, and D. Towsley, "Facilitating access point selection in IEEE 802.11 wireless networks," in *Proc. ACM/USENIX IMC*, 2005, pp. 26–26.

[59] A. Jardosh, K. Mittal, K. Ramachandran, E. Belding, and K. Almeroth, "IQU: Practical queue-based user association management for WLANs," in *Proc. ACM MobiCom*, 2006, pp. 158–169.

[60] A. Nicholson, Y. Chawathe, M. Chen, B. Noble, and D. Wetherall, "Improved access point selection," in *Proc. ACM/USENIX MOBISYS*, 2006, pp. 233–245.

[61] K. Sundaresan and K. Papagiannaki, "The need for cross-layer information in access point selection algorithms," in *Proc. ACM IMC*, 2006, pp. 257–262.

[62] J. Pang, B. Greenstein, M. Kaminsky, D. McCoy, and S. Seshan, "Wifi-reports: Improving wireless network selection with collaboration," in *Proc. ACM/USENIX MOBISYS*, 2009, pp. 123–136.

[63] F. Xu, C. Tan, Q. Li, G. Yan, and J. Wu, "Designing a practical access point association protocol," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[64] X. Fafoutis and V. A. Siris, "Handover incentives for self-interested WLANs with overlapping coverage," *IEEE Trans. Mobile Comput.*, vol. 11, no. 12, pp. 2033–2046, Dec. 2012.

[65] A. Hills, "Large-scale wireless LAN design," *IEEE Commun. Mag.*, vol. 39, no. 11, pp. 98–107, Nov. 2001.

[66] F. Gamba, J.-F. Wagen, and D. Rossier, "Towards adaptive WLAN frequency management using intelligent agents," in *Ad-Hoc, Mobile, and Wireless Networks*, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2003, pp. 116–127.

[67] E. Villegas, R. Ferro, and J. Aspas, "Implementation of a distributed dynamic channel assignment mechanism for IEEE 802.11 networks," in *Proc. IEEE PIMRC*, Sep. 2005, vol. 3, pp. 1458–1462.

[68] D. Malone, P. Clifford, D. Reid, and D. Leith, "Experimental implementation of optimal WLAN channel selection without communication," in *Proc. IEEE DySPAN*, Apr. 2007, pp. 316–319.

[69] A. Mishra, E. Rozner, S. Banerjee, and W. Arbaugh, "Exploiting partially overlapping channels in wireless networks: Turning a peril into an advantage," in *Proc. ACM/USENIX IMC*, 2005, pp. 311–316.

[70] A. Mishra, V. Shrivastava, S. Banerjee, and W. Arbaugh, "Partially overlapped channels not considered harmful," in *Proc. ACM SIGMETRICS*, 2006, pp. 63–74.

[71] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, "On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 10, pp. 3258–3271, Oct. 2010.

[72] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris, "Link-level measurements from an 802.11b mesh network," in *Proc. ACM SIGCOMM*, 2004, pp. 121–132.

[73] K. Chebrolu, B. Raman, and S. Sen, "Long-distance 802.11b links: Performance measurements and experience," in *Proc. ACM MobiCom*, 2006, pp. 74–85.

[74] B. Raman, K. Chebrolu, D. Gokhale, and S. Sen, "On the feasibility of the link abstraction in wireless mesh networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 2, pp. 528–541, Apr. 2009.

[75] K. LaCurts and H. Balakrishnan, "Measurement and analysis of real-world 802.11 mesh networks," in *Proc. ACM IMC*, Nov. 2010, pp. 123–136.

[76] A. P. Subramanian, J. Cao, C. Sung, and S. R. Das, "Understanding channel and interface heterogeneity in multi-channel multi-radio wireless mesh networks," in *Proc. IEEE PAM*, 2009, pp. 89–98.

[77] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel measurements," in *Proc. ACM SIGCOMM*, 2010, pp. 159–170.

[78] A. Vlavianos, L. Law, I. Broustis, S. Krishnamurthy, and M. Faloutsos, "Assessing link quality in IEEE 802.11 wireless networks: Which is the right metric?" in *Proc. IEEE PIMRC*, Sep. 2008, pp. 1–6.

[79] D. Giustiniano, D. Malone, D. Leith, and K. Papagiannaki, "Measuring transmission opportunities in 802.11 links," *IEEE/ACM Trans. Netw.*, vol. 18, no. 5, pp. 1516–1529, Oct. 2010.

[80] J. Padhye *et al.*, "Estimation of link interference in static multi-hop wireless networks," in *Proc. ACM/USENIX IMC*, 2005, pp. 28–28.

[81] D. Niculescu, "Interference map for 802.11 networks," in *Proc. ACM IMC*, 2007, pp. 339–350.

[82] A. Kashyap, U. Paul, and S. R. Das, "Deconstructing interference relations in WiFi networks," in *Proc. IEEE SECON*, 2010, pp. 1–9.

[83] K. Cai, M. Blackstock, M. J. Feeley, and C. Krasic, "Non-intrusive, dynamic interference detection for 802.11 networks," in *Proc. ACM IMC*, 2009, pp. 377–383.

[84] E. Magistretti, O. Gurewitz, and E. Knightly, "Inferring and mitigating a link's hindering transmissions in managed 802.11 wireless networks," in *Proc. ACM MobiCom*, 2010, pp. 305–316.

[85] I. Broustis, J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "Implications of power control in wireless networks: A quantitative study," in *Proc. IEEE PAM*, 2007, pp. 83–93.

[86] A. Akella, G. Judd, S. Seshan, and P. Steenkiste, "Self-management in chaotic wireless deployments," in *Proc. ACM MobiCom*, 2005, pp. 185–199.

[87] K. Ramachandran, R. Kokku, H. Zhang, and M. Gruteser, "Symphony: Synchronous two-phase rate and power control in 802.11 WLANs," in *Proc. ACM/USENIX MOBISYS*, 2008, pp. 132–145.

[88] V. Shrivastava, D. Agrawal, A. Mishra, S. Banerjee, and T. Nadeem, "Understanding the limitations of transmit power control for indoor WLANs," in *Proc. ACM IMC*, 2007, pp. 351–364.

[89] F. B. Abdesslem, L. Iannone, M. D. de Amorim, K. Kabassanov, and S. Fdida, "On the feasibility of power control in current IEEE 802.11 devices," in *Proc. IEEE PerCom Workshops*, 2006, pp. 468–473.

[90] T. Ireland, A. Nyzio, M. Zink, and J. Kurose, "The impact of directional antenna orientation, spacing, and channel separation on long-distance multi-hop 802.11g networks: A measurement study," in *Proc. IEEE WiOpt*, Apr. 2007, pp. 1–6.

[91] E. Anderson, C. Phillips, D. Sicker, and D. Grunwald, "Modeling environmental effects on directionality in wireless networks," in *Proc. IEEE WiOpt*, 2009, pp. 564–570.

[92] S. Kakumanu and R. Sivakumar, "Glia: A practical solution for effective high datarate WiFi-arrays," in *Proc. ACM MobiCom*, 2009, pp. 229–240.

[93] X. Liu *et al.*, "DIRC: Increasing indoor wireless capacity using directional antennas," in *Proc. ACM SIGCOMM*, 2009, pp. 171–182.

[94] M. Blanco, R. Kokku, K. Ramachandran, S. Rangarajan, and K. Sundaresan, "On the effectiveness of switched beam antennas in indoor environments," in *Proc. IEEE PAM*, 2008, pp. 122–131.

[95] S. Lakshmanan, K. Sundaresan, S. Rangarajan, and R. Sivakumar, "The myth of spatial reuse with directional antennas in indoor wireless networks," in *Proc. IEEE PAM*, 2010, pp. 51–60.

[96] S. Lakshmanan, K. Sundaresan, S. Rangarajan, and R. Sivakumar, "Practical beamforming based on RSSI measurements using off-the-shelf wireless clients," in *Proc. ACM IMC*, 2009, pp. 410–416.

[97] A. P. Subramanian, H. Lundgren, and T. Salonidis, "Experimental characterization of sectorized antennas in dense 802.11 wireless mesh networks," in *Proc. ACM MobiHoc*, 2009, pp. 259–268.

[98] D. Giustiniano, G. Bianchi, L. Scalia, and I. Tinnirello, "An explanation for unexpected 802.11 outdoor link-level measurement results," in *Proc. IEEE INFOCOM*, 2008, pp. 2432–2440.

[99] D. Kotz *et al.*, "Experimental evaluation of wireless simulation assumptions," in *Proc. ACM MSWiM*, 2004, pp. 78–82.

[100] G. Judd and P. Steenkiste, "Understanding link-level 802.11 behavior: Replacing convention with measurement," in *Proc. ICST WICON*, 2007, pp. 19:1–19:10.

[101] K. D. Huang, D. Malone, and K. R. Duffy, "The 802.11g 11 Mb/s rate is more robust than 6 Mb/s," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1015–1020, Apr. 2011.

[102] R. Aguero, M. Garcia-Arranz, and L. Munoz, "Accurate simulation of 802.11 indoor links: A "bursty" channel model based on real measurements," *EURASIP J. Wireless Commun. Netw.*, vol. 2010, no. 1, Feb. 2010, Art. ID. 380 410.

[103] C. Phillips *et al.*, "The efficacy of path loss models for fixed rural wireless links," in *Proc. IEEE PAM*, 2011, pp. 42–51.

[104] A. Kochut, A. Vasan, A. U. Shankar, and A. Agrawala, "Sniffing out the correct physical layer capture model in 802.11b," in *Proc. IEEE ICNP*, 2004, pp. 252–261.

[105] J. Lee *et al.*, "An experimental study on the capture effect in 802.11a networks," in *Proc. ACM WINTECH*, 2007, pp. 19–26.

[106] J. Lee *et al.*, "RSS-based carrier sensing and interference estimation in 802.11 wireless networks," in *Proc. IEEE SECON*, 2007, pp. 491–500.

[107] J. Camp, E. Aryafar, and E. Knightly, "Coupled 802.11 flows in urban channels: Model and experimental evaluation," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[108] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, "Performance anomaly of 802.11b," in *Proc. IEEE INFOCOM*, Mar. 2003, vol. 2, pp. 836–843.

[109] M. Bredel and M. Fidler, "Understanding fairness and its impact on quality of service in IEEE 802.11," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 1098–1106.

[110] A. Kashyap, S. Das, and S. Ganguly, "A measurement-based approach to modeling link capacity in 802.11-based wireless networks," in *Proc. ACM MobiCom*, 2007, pp. 242–253.

[111] M. Z. Brodsky and R. T. Morris, "In defense of wireless carrier sense," in *Proc. ACM SIGCOMM*, 2009, pp. 147–158.

[112] P. Serrano, A. Banchs, P. Patras, and A. Azcorra, "Optimal configuration of 802.11e EDCA for real-time and data traffic," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2511–2528, Jun. 2010.

[113] K. Huang, K. Duffy, and D. Malone, "On the validity of IEEE 802.11 MAC modeling hypotheses," *IEEE/ACM Trans. Netw.*, vol. 18, no. 6, pp. 1935–1948, Dec. 2010.

[114] Y. He, R. Yuan, X. Ma, and J. Li, "The IEEE 802.11 power saving mechanism: An experimental study," in *Proc. IEEE WCNC*, 2008, pp. 1362–1367.

[115] J.-P. Ebert, B. Burns, and A. Wolisz, "A trace-based approach for determining the energy consumption of a WLAN network interface," in *Proc. Eur. Wireless*, Feb. 2002, pp. 230–236.

[116] D. Halperin, B. Greenstein, A. Sheth, and D. Wetherall, "Demystifying 802.11n power consumption," in *Proc. USENIX HotPower*, 2010, pp. 1–5.

[117] E. Rantala, A. Karppanen, S. Granlund, and P. Sarolahti, "Modeling energy efficiency in wireless Internet communication," in *Proc. ACM MobiHeld*, Aug. 2009, pp. 67–68.

[118] "Power consumption and energy efficiency comparisons of WLAN Products," White Paper, Atheros Communications, San Jose, CA, USA, Apr. 2004.

[119] J. D. Vega and R. Chabukswar, "Data transfer over wireless LAN power consumption analysis," Intel Corp., Mountain View, CA, USA, White paper, Feb. 2009.

[120] E. Lochin, A. Fladenmuller, J.-Y. Moulin, S. Fdida, and A. Manet, "Energy consumption models for ad-hoc mobile terminals," in *Proc. Med-Hoc Net*, Jun. 2003, pp. 1–8.

[121] G. Perrucci, F. Fitzek, and J. Widmer, "Survey on energy consumption entities on the smartphone platform," in *Proc. IEEE VTC Spring*, May 2011, pp. 1–6.

[122] A. Carroll and G. Heiser, "An analysis of power consumption in a smartphone," in *Proc. USENIX ATC*, Jun. 2010, p. 21.

[123] A. Rice and S. Hay, "Measuring mobile phone energy consumption for 802.11 wireless networking," *Pervasive Mobile Comput.*, vol. 6, no. 6, pp. 593–606, Dec. 2010.

[124] A. Garcia-Saavedra, P. Serrano, A. Banchs, and G. Bianchi, "Energy consumption anatomy of 802.11 devices and its implications on modeling and design," in *Proc. ACM CoNEXT*, 2012, pp. 24:1–24:12.

[125] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 2, pp. 93–102, Apr. 2003.

[126] A. Cabellos-Aparicio, R. Serral-Gracia, L. Jakab, and J. Domingo-Pascual, "Measurement based analysis of the handover in a WLAN MIPv6 scenario," in *Proc. IEEE PAM*, 2005, pp. 203–214.

[127] R. Raghavendra, E. M. Belding, K. Papagiannaki, and K. C. Almeroth, "Understanding handoffs in large IEEE 802.11 wireless networks," in *Proc. ACM IMC*, 2007, pp. 333–338.

[128] R. Gass and C. Diot, "An experimental performance comparison of 3G and Wi-Fi," in *Proc. IEEE PAM*, 2010, pp. 71–80.

[129] M. Shin, A. Mishra, and W. A. Arbaugh, "Improving the latency of 802.11 hand-offs using neighbor graphs," in *Proc. ACM/USENIX MOBISYS*, 2004, pp. 70–83.

[130] V. Brik, A. Mishra, and S. Banerjee, "Eliminating handoff latencies in 802.11 WLANs using multiple radios: Applications, experience, and evaluation," in *Proc. ACM/USENIX IMC*, 2005, pp. 27–27.

[131] V. Mhatre and K. Papagiannaki, "Using smart triggers for improved user performance in 802.11 wireless networks," in *Proc. ACM/USENIX MOBISYS*, 2006, pp. 246–259.

[132] X. Chen and D. Qiao, "HaND: Fast handoff with null dwell time for IEEE 802.11 networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.
[133] H. Yokota, A. Idoue, T. Hasegawa, and T. Kato, "Link layer assisted mobile IP fast handoff method over wireless LAN networks," in *Proc. ACM MobiCom*, 2002, pp. 131–139.
[134] Y. Amir, C. Danilov, M. Hilsdale, R. Musaloiu-Elefteri, and N. Rivera, "Fast handoff for seamless wireless mesh networks," in *Proc. ACM/USENIX MOBISYS*, 2006, pp. 83–95.
[135] R. Mahajan, J. Zahorjan, and B. Zill, "Understanding WiFi-based connectivity from moving vehicles," in *Proc. ACM IMC*, 2007, pp. 321–326.
[136] A. Balasubramanian, R. Mahajan, A. Venkataramani, B. N. Levine, and J. Zahorjan, "Interactive WiFi connectivity for moving vehicles," in *Proc. ACM SIGCOMM*, 2008, pp. 427–438.
[137] A. Giannoulis, M. Fiore, and E. W. Knightly, "Supporting vehicular mobility in urban multi-hop wireless networks," in *Proc. ACM MobiSys*, 2008, pp. 54–66.
[138] P. Deshpande, A. Kashyap, C. Sung, and S. Das, "Predictive methods for improved vehicular WiFi access," in *Proc. ACM/USENIX MOBISYS*, 2009, pp. 263–276.
[139] P. Bahl and V. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proc. IEEE INFOCOM*, 2000, vol. 2, pp. 775–784.
[140] A. M. Ladd *et al.*, "Robotics-based location sensing using wireless ethernet," in *Proc. ACM MobiCom*, 2002, pp. 227–238.
[141] A. Miu, H. Balakrishnan, and C. E. Koksal, "Improving loss resilience with multi-radio diversity in wireless networks," in *Proc. ACM MobiCom*, 2005, pp. 16–30.
[142] M. Youssef and A. Agrawala, "The Horus location determination system," *Wireless Netw.*, vol. 14, no. 3, pp. 357–374, Jun. 2008.
[143] A. B. M. Musa and J. Eriksson, "Tracking unmodified smartphones using Wi-Fi monitors," in *Proc. ACM SenSys*, 2012, pp. 281–294.
[144] K. Kleisouris, Y. Chen, J. Yang, and R. Martin, "The impact of using multiple antennas on wireless localization," in *Proc. IEEE SECON*, 2008, pp. 55–63.
[145] Y.-C. Cheng, Y. Chawathe, A. LaMarca, and J. Krumm, "Accuracy characterization for metropolitan-scale Wi-Fi localization," in *Proc. ACM/USENIX MOBISYS*, 2005, pp. 233–245.
[146] D. Niculescu and B. Nath, "VOR Base stations for indoor 802.11 positioning," in *Proc. ACM MobiCom*, 2004, pp. 58–69.
[147] D. Giustiniano and S. Mangold, "CAESAR: Carrier sense-based ranging in off-the-shelf 802.11 wireless LAN," in *Proc. ACM CoNEXT*, 2011, pp. 10:1–10:12.
[148] P. Gallo, D. Garlisi, F. Giuliano, F. Gringoli, and I. Tinnirello, "WMPS: A positioning system for localizing legacy 802.11 devices," *IEEK Trans. Smart Process. Comput. J.*, vol. 1, no. 2, pp. 106–116, Oct. 2012.
[149] A. LaMarca, J. Hightower, I. Smith, and S. Consolvo, "Self-mapping in 802.11 location systems," in *Proc. ACM UbiComp*, 2005, pp. 87–104, vol. 3660.
[150] Y. Chen, J.-A. Francisco, W. Trappe, and R. Martin, "A practical approach to landmark deployment for indoor localization," in *Proc. IEEE SECON*, 2006, pp. 365–373.
[151] Y. Ji, S. Biaz, S. Pandey, and P. Agrawal, "ARIADNE: A dynamic indoor signal map construction and localization system," in *Proc. ACM/USENIX MOBISYS*, 2006, pp. 151–164.
[152] A. Goswami, L. E. Ortiz, and S. R. Das, "WiGEM: A learning-based approach for indoor localization," in *Proc. ACM CoNEXT*, 2011, pp. 3:1–3:12.
[153] E. Elnahrawy, X. Li, and R. Martin, "The limits of localization using signal strength: A comparative study," in *Proc. IEEE SECON*, 2004, pp. 406–414.
[154] G. Chandrasekaran *et al.*, "Empirical evaluation of the limits on localization using signal strength," in *Proc. IEEE SECON*, 2009, pp. 1–9.
[155] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S. V. Krishnamurthy, "Lightweight jammer localization in wireless networks: System design and implementation," in *Proc. IEEE GLOBECOM*, 2009, pp. 1–6.
[156] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *Proc. IEEE INFOCOM*, May 2007, pp. 2526–2530.
[157] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, and C. Gkantsidis, "A measurement-driven anti-jamming system for 802.11 networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 4, pp. 1208–1222, Aug. 2011.
[158] I. Broustis, K. Pelechrinis, D. Syrivelis, S. V. Krishnamurthy, and L. Tassiulas, "A software framework for alleviating the Eects of MAC-aware jamming attacks in wireless access networks," *Wireless Netw.*, vol. 17, no. 6, pp. 1543–1560, Aug. 2011.
[159] T. Brown and J. James, "Jamming and sensing of encrypted wireless ad hoc networks," in *Proc. ACM MobiHoc*, 2006, pp. 120–130.
[160] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," in *Proc. ACM SIGCOMM*, 2007, pp. 385–396.
[161] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proc. USENIX SSYM*, 2003, pp. 1–13.
[162] K. Pelechrinis, Y. Guanhua, S. Eidenbenz, and S. Krishnamurthy, "Detecting selfish exploitation of carrier sensing in 802.11 networks," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 657–665.
[163] G. Bianchi *et al.*, "Experimental assessment of the backoff behavior of commercial IEEE 802.11b network cards," in *Proc. IEEE INFOCOM*, 2007, pp. 1181–1189.
[164] M. Raya, I. Aad, J.-P. Hubaux, and A. El Fawal, "DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots," *IEEE Trans. Mobile Comput.*, vol. 5, no. 12, pp. 1691–1705, Dec. 2006.
[165] C. Jaehyuk, A. Min, and K. Shin, "A lightweight passive online detection method for pinpointing misbehavior in WLANs," *IEEE Trans. Mobile Comput.*, vol. 10, no. 12, pp. 1681–1693, Dec. 2011.
[166] X. Fu *et al.*, "The digital Marauder's map: A WiFi forensic positioning tool," *IEEE Trans. Mobile Comput.*, vol. 11, no. 3, pp. 377–389, Mar. 2012.
[167] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 user fingerprinting," in *Proc. ACM MobiCom*, 2007, pp. 99–110.
[168] T. Jiang, H. Wang, and Y.-C. Hu, "Preserving location privacy in wireless LANs," in *Proc. ACM/USENIX MOBISYS*, 2007, pp. 246–257.
[169] F. Zhang, W. He, X. Liu, and P. G. Bridges, "Inferring users' online activities through traffic analysis," in *Proc. ACM WiSec*, 2011, pp. 59–70.
[170] B. Greenstein *et al.*, "Improving wireless privacy with an identifier-free link layer protocol," in *Proc. ACM/USENIX MOBISYS*, 2008, pp. 40–53.
[171] P. Bahl *et al.*, "Enhancing security of corporate Wi-Fi networks using DAIR," in *Proc. ACM/USENIX MOBISYS*, 2006, pp. 1–14.
[172] W. Wei *et al.*, "Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs," in *Proc. ACM IMC*, 2007, pp. 365–378.
[173] B. Stone-Gross *et al.*, "Malware in IEEE 802.11 wireless networks," in *Proc. IEEE PAM*, 2008, pp. 222–231.
[174] S. Sangho and H. Schulzrinne, "Experimental measurement of the capacity for VoIP traffic in IEEE 802.11 WLANs," in *Proc. IEEE INFOCOM*, May 2007, pp. 2018–2026.
[175] P. Dini, O. Font-Bach, and J. Mangues-Bafalluy, "Experimental analysis of VoIP call quality support in IEEE 802.11 DCF," in *Proc. IEEE CSNDSP*, 2008, pp. 443–447.
[176] P. Verkaik, Y. Agarwal, R. Gupta, and A. C. Snoeren, "Softspeak: Making VoIP play well in existing 802.11 deployments," in *Proc. USENIX NSDI*, 2009, pp. 409–422.
[177] N. Ahmed, S. Keshav, and K. Papagiannaki, "OmniVoice: A mobile voice solution for small-scale enterprises," in *Proc. ACM MobiHoc*, 2011, p. 5.
[178] D. Niculescu, S. Ganguly, K. Kim, and R. Izmailov, "Performance of VoIP in a 802.11 wireless mesh network," in *Proc. IEEE INFOCOM*, Apr. 2006, pp. 1–11.
[179] S. Ganguly *et al.*, "Performance optimizations for deploying VoIP services in mesh networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 11, pp. 2147–2158, Nov. 2006.
[180] Y. Amir, R. Musaloiu-Elefteri, and N. Rivera, "A robust push-to-talk service for wireless mesh networks," in *Proc. IEEE SECON*, 2010, pp. 1–9.
[181] A. Kostuch, K. Gierowski, and J. Wozniak, "Performance analysis of multicast video streaming in IEEE 802.11 b/g/n testbed environment," in *Proc. IFIP WMNC*, 2009, vol. 308, pp. 92–105.
[182] M. van der Schaar, S. Krishnamachari, S. Choi, and X. Xu, "Adaptive cross-layer protection strategies for robust scalable video transmission over 802.11 WLANs," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 10, pp. 1752–1763, Dec. 2003.
[183] P. Bucciol, E. Masala, N. Kawaguchi, K. Takeda, and J. De Martin, "Performance evaluation of H. 264 video streaming over inter-vehicular 802.11 ad hoc networks," in *Proc. IEEE PIMRC*, 2005, vol. 3, pp. 1936–1940.
[184] O. Alay, T. Korakis, Y. Wang, and S. Panwar, "An experimental study of packet loss and forward error correction in video multicast over IEEE 802.11b network," in *Proc. IEEE CCNC*, 2009, pp. 1–5.

[185] L. Haratcherev, J. Taal, K. Langendoen, R. Lagendijk, and H. Sips, "Optimized video streaming over 802.11 by cross-layer signaling," *IEEE Commun. Mag.*, vol. 44, no. 1, pp. 115–121, Jan. 2006.
[186] P. Salvador, L. Cominardi, F. Gringoli, and P. Serrano, "A first implementation and evaluation of the IEEE 802.11aa group addressed transmission service," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 1, pp. 13–18, Jan. 2014.
[187] A. Adya, P. Bahl, R. Chandra, and L. Qiu, "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks," in *Proc. ACM MobiCom*, 2004, pp. 30–44.
[188] R. Chandra, V. N. Padmanabhan, and M. Zhang, "WiFiProfiler: Cooperative diagnosis in wireless LANs," in *Proc. ACM MobiSys*, 2006, pp. 205–219.
[189] J. Manweiler, P. Franklin, and R. R. Choudhury., "RxIP: Monitoring the health of home wireless networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 558–566.
[190] A. P. Jardosh, P. Suwannatat, T. Hollerer, E. M. Belding, and K. C. Almeroth, "SCUBA: Focus and context for real-time mesh network health diagnosis," in *Proc. IEEE PAM*, 2008, pp. 162–171.
[191] A. Haeberlen *et al.*, "Practical robust localization over large-scale 802.11 wireless networks," in *Proc. ACM MobiCom*, 2004, pp. 70–84.
[192] D. Han, D. G. Andersen, M. Kaminsky, K. Papagiannaki, and S. Seshan, "Access point localization using local signal strength gradient," in *Proc. IEEE PAM*, 2009, pp. 99–108.
[193] K.-H. Kim and K. G. Shin, "Improving TCP performance over wireless networks with collaborative multi-homed mobile hosts," in *Proc. ACM/USENIX MOBISYS*, 2005, pp. 107–120.
[194] R. Chandra, P. Bahl, and P. Bahl, "MultiNet: Connecting to multiple IEEE 802.11 networks using a single wireless card," in *Proc. IEEE INFOCOM*, Mar. 2004, vol. 2, pp. 882–893.
[195] S. Kandula, K. C.-J. Lin, T. Badirkhanli, and D. Katabi, "FatVAP: Aggregating AP backhaul capacity to maximize throughput," in *Proc. USENIX NSDI*, 2008, pp. 89–104.
[196] D. Giustiniano *et al.*, "Fair WLAN backhaul aggregation," in *Proc. ACM MobiCom*, 2010, pp. 269–280.
[197] E. Goma *et al.*, "Insomnia in the access or how to curb access network related energy consumption," in *Proc. ACM SIGCOMM*, Aug. 2011, pp. 338–349.
[198] G. D. Bhanage, D. Vete, I. Seskar, and D. Raychaudhuri, "SplitAP: Leveraging wireless network virtualization for flexible sharing of WLANs," in *Proc. IEEE GLOBECOM*, 2010, pp. 1–6.
[199] K. Jamieson, B. Hull, A. Miu, and H. Balakrishnan, "Understanding the real-world performance of carrier sense," in *Proc. ACM E-WIND*, 2005, pp. 52–57.
[200] K. N. Ramachandran, E. M. Belding, K. C. Almeroth, and M. M. Buddhikot, "Interference-aware channel assignment in multi-radio wireless mesh networks," in *Proc. IEEE INFOCOM*, Apr. 2006, pp. 1–12.
[201] R. Vedantham, S. Kakumanu, S. Lakshmanan, and R. Sivakumar, "Component based channel assignment in single radio, multichannel ad hoc networks," in *Proc. ACM MobiCom*, 2006, pp. 378–389.
[202] J. Camp, J. Robinson, C. Steger, and E. Knightly, "Measurement driven deployment of a two-tier urban mesh access network," in *Proc. ACM MobiSys*, 2006, pp. 96–109.
[203] S. Biswas and R. Morris, "Opportunistic routing in multi-hop wireless networks," in *Proc. ACM SIGCOMM*, Aug. 2005, pp. 69–74.
[204] J. Padhye, R. Draves, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in *Proc. ACM MobiCom*, 2004, pp. 114–128.
[205] G. Jakllari, S. Eidenbenz, N. W. Hengartner, S. V. Krishnamurthy, and M. Faloutsos, "Link positions matter: A noncommutative routing metric for wireless mesh networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 1, pp. 61–72, Jan. 2012.
[206] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proc. ACM MobiCom*, Sep. 2003, pp. 134–146.
[207] R. Draves, J. Padhye, and B. Zill, "Comparison of routing metrics for static multi-hop wireless networks," in *Proc. ACM SIGCOMM*, 2004, pp. 133–144.
[208] S. M. Das, H. Pucha, K. Papagiannaki, and Y. C. Hu, "Studying wireless routing link metric dynamics," in *Proc. ACM IMC*, 2007, pp. 327–332.
[209] T.-S. Kim, G. Jakllari, S. V. Krishnamurthy, and M. Faloutsos, "A unified metric for routing and rate adaptation in multi-rate wireless mesh networks," in *Proc. IEEE MASS*, 2011, pp. 242–251.
[210] E. Genetzakis and V. Siris, "A contention-aware routing metric for multi-rate multi-radio mesh networks," in *Proc. IEEE SECON*, 2008, pp. 242–250.
[211] A. Miu, G. Tan, H. Balakrishnan, and J. Apostolopoulos, "Divert: Fine-grained path selection for wireless LANs," in *Proc. ACM/USENIX MOBISYS*, 2004, pp. 203–216.
[212] Z. Li, B. Li, D. Xu, and X. Zhou, "iFlow: Middleware-assisted rendezvous-based information access for mobile ad hoc applications," in *Proc. ACM/USENIX MOBISYS*, 2003, pp. 71–84.
[213] S. Biswas and R. Morris, "ExOR: Opportunistic multi-hop routing for wireless networks," in *Proc. ACM SIGCOMM*, 2005, pp. 133–144.
[214] F. Wu, T. Chen, S. Zhong, L. E. Li, and Y. R. Yang, "Incentive-compatible opportunistic routing for wireless networks," in *Proc. ACM MobiCom*, 2008, pp. 303–314.
[215] J. Camp, V. Mancuso, O. Gurewitz, and E. Knightly, "A measurement study of multiplicative overhead effects in wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 76–80.
[216] I. Broustis, K. Pelechrinis, D. Syrivelis, S. V. Krishnamurthy, and L. Tassiulas, "Quantifying the overhead due to routing probes in multi-rate WMNs," in *Proc. IEEE WCNC*, 2010, pp. 1–6.
[217] D. Sampath and J. Garcia-Luna-Aceves, "PROSE: Scalable routing in MANETs using prefix labels and distributed hashing," in *Proc. IEEE SECON*, 2009, pp. 1–9.
[218] K. Ramachandran, I. Sheriff, E. Belding, and K. Almeroth, "Routing stability in static wireless mesh networks," in *Proc. IEEE PAM*, 2007, pp. 73–83.
[219] S. Miskovic and E. W. Knightly, "Routing primitives for wireless mesh networks: Design, analysis and experiments," in *Proc. IEEE INFOCOM*, 2010, pp. 2793–2801.
[220] A. Aziz, D. Starobinski, and P. Thiran, "Elucidating the instability of random access wireless mesh network," in *Proc. IEEE SECON*, 2009, pp. 1–9.
[221] A. Aziz, D. Starobinski, and P. Thiran, "Understanding and tackling the root causes of instability in wireless mesh networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 4, pp. 1178–1193, Aug. 2011.
[222] V. Mancuso, O. Gurewitz, A. Khattab, and E. W. Knightly, "Elastic rate limiting for spatially biased wireless mesh networks," in *Proc. IEEE INFOCOM*, 2010, pp. 1720–1728.
[223] S. Rangwala, A. Jindal, K.-Y. Jang, K. Psounis, and R. Govindan, "Understanding congestion control in multi-hop wireless mesh networks," in *Proc. ACM MobiCom*, 2008, pp. 291–302.
[224] A. Aziz, J. Herzen, R. Merz, S. Shneer, and P. Thiran, "Enhance & Explore: An adaptive algorithm to maximize the utility of wireless networks," in *Proc. ACM MobiCom*, 2011, pp. 157–168.
[225] Y. Li, L. Qiu, Y. Zhang, R. Mahajan, and E. Rozner, "Predictable performance optimization for wireless networks," in *Proc. ACM SIGCOMM*, 2008, pp. 413–426.
[226] O. Gurewitz, V. Mancuso, S. Jingpu, and E. Knightly, "Measurement and modeling of the origins of starvation of congestion-controlled flows in wireless mesh networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 6, pp. 1832–1845, Dec. 2009.
[227] T. Li, D. Leith, V. Badarla, D. Malone, and Q. Cao, "Achieving end-to-end fairness in 802.11e based wireless multi-hop mesh networks without coordination," *Mobile Netw. Appl.*, vol. 16, no. 1, pp. 17–34, Feb. 2011.
[228] B. Radunovic, C. Gkantsidis, D. Gunawardena, and P. Key, "Horizon: Balancing TCP over multiple paths in wireless mesh network," in *Proc. ACM MobiCom*, 2008, pp. 247–258.
[229] A. Kamerman and L. Monteban, "WaveLAN-II: A high-performance wireless LAN for the unlicensed band," *Bell Lab Tech. J.*, vol. 2, no. 3, pp. 118–133, Autumn 1997.
[230] M. Lacage, M. H. Manshaei, and T. Turletti, "IEEE 802.11 rate adaptation: A practical approach," in *Proc. ACM MSWiM*, 2004, pp. 126–134.
[231] J. Bicket, "Bit-rate selection in wireless networks," M.S. thesis, Dept. Elect. Eng. Comput. Sci., MIT, Cambridge, MA, USA, 2005.
[232] G. Judd, X. Wang, and P. Steenkiste, "Efficient channel-aware rate adaptation in dynamic environments," in *Proc. ACM MobiSys*, 2008, pp. 118–131.
[233] X. Chen, P. Gangwal, and D. Qiao, "RAM: Rate adaptation in mobile environments," *IEEE Trans. Mobile Comput.*, vol. 11, no. 3, pp. 464–477, Mar. 2012.
[234] S. Pal, S. R. Kundu, K. Basu, and S. K. Das, "IEEE 802.11 rate control algorithms: Experimentation and performance evaluation in infrastructure mode," in *Proc. IEEE PAM*, 2006, pp. 1–10.

[235] E. Ancillotti, R. Bruno, and M. Conti, "Experimentation and performance evaluation of rate adaptation algorithms in wireless mesh networks," in *Proc. ACM PE-WASUN*, 2008, pp. 7–14.
[236] P. Acharya, A. Sharma, E. Belding, K. Almeroth, and K. Papagiannaki, "Congestion-aware rate adaptation in wireless networks: A measurement-driven approach," in *Proc. IEEE SECON*, 2008, pp. 1–9.
[237] S. Rayanchu, A. Mishra, D. Agrawal, S. Saha, and S. Banerjee, "Diagnosing wireless packet losses in 802.11: Separating collision from weak signal," in *Proc. IEEE INFOCOM*, 2008, pp. 735–743.
[238] S. Kim, L. Verma, S. Choi, and D. Qiao, "Collision-aware rate adaptation in multi-rate WLANs: Design and implementation," *Comput. Netw.*, vol. 54, no. 17, pp. 3011–3030, Dec. 2010.
[239] K. Huang, K. Duffy, and D. Malone, "H-RCA: 802.11 collision-aware rate control," *IEEE/ACM Trans. Netw.*, vol. 21, no. 4, pp. 1021–1034, Aug. 2013.
[240] I. Pefkianakis, Y. Hu, S. Wong, H. Yang, and S. Lu, "MIMO rate adaptation in 802.11n wireless networks," in *Proc. ACM MobiCom*, 2010, pp. 257–268.
[241] Y. Kim, S. Choi, K. Jang, and H. Hwang, "Throughput enhancement of IEEE 802.11 WLAN via frame aggregation," in *Proc. IEEE VTC Fall*, Sep. 2004, pp. 3030–3034.
[242] Y. Grunenberger, M. Heusse, F. Rousseau, and A. Duda, "Experience with an implementation of the Idle sense wireless access method," in *Proc. ACM CoNEXT*, 2007, pp. 24:1–24:12.
[243] P. Salvador, V. Mancuso, P. Serrano, F. Gringoli, and A. Banchs, "VoIP-iggy: Analysis and implementation of a mechanism to boost capacity in IEEE 802.11 WLANs carrying VoIP traffic," *IEEE Trans. Mobile Comput.*, vol. 13, no. 7, pp. 1640–1652, Jul. 2014.
[244] I. Tinnirello *et al.*, "Wireless MAC processors: Programming MAC protocols on commodity hardware," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1269–1277.
[245] G. Bianchi *et al.*, "MAClets: Active MAC protocols over hard-coded devices," in *Proc. ACM CoNEXT*, 2012, pp. 229–240.
[246] A. Rao and I. Stoica, "An overlay MAC layer for 802.11 networks," in *Proc. ACM/USENIX MOBISYS*, 2005, pp. 135–148.
[247] P. Djukic and P. Mohapatra, "Soft-TDMAC: A software-based 802.11 overlay TDMA MAC with microsecond synchronization," *IEEE Trans. Mobile Comput.*, vol. 11, no. 3, pp. 478–491, Mar. 2012.
[248] B. Raman and K. Chebrolu, "Design and evaluation of a new MAC protocol for long-distance 802.11 mesh networks," in *Proc. ACM MobiCom*, 2005, pp. 156–169.
[249] M.-H. Lu, P. Steenkiste, and T. Chen, "Design, implementation, and evaluation of an efficient opportunistic retransmission protocol," in *Proc. ACM MobiCom*, 2009, pp. 73–84.
[250] K. C.-J. Lin, N. Kushman, and D. Katabi, "ZipTx: Harnessing partial packets in 802.11 networks," in *Proc. ACM MobiCom*, 2008, pp. 351–362.
[251] B. Han *et al.*, "Maranello: Practical partial packet recovery for 802.11," in *Proc. USENIX NSDI*, 2010, pp. 205–218.
[252] J. Xie, W. Hu, and Z. Zhang, "Revisiting partial packet recovery in 802.11 wireless LANs," in *Proc. ACM/USENIX MOBISYS*, 2011, pp. 281–292.
[253] S. Katti *et al.*, "XORs in the Air: Practical wireless network coding," in *Proc. ACM SIGCOMM*, 2006, pp. 243–254.
[254] Y. Huang, M. Ghaderi, D. Towsley, and W. Gong, "TCP performance in coded wireless mesh networks," in *Proc. IEEE SECON*, 2008, pp. 179–187.
[255] T.-S. Kim *et al.*, "A framework for joint network coding and transmission rate control in wireless networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.
[256] M. Anand, E. Nightingale, and J. Flinn, "Self-tuning wireless network power management," in *Proc. ACM MobiCom*, 2003, pp. 176–189.
[257] Y. Agarwal *et al.*, "Wireless wakeups revisited: Energy management for VoIP over Wi-Fi smartphones," in *Proc. ACM/USENIX MOBISYS*, 2007, pp. 179–191.
[258] A. J. Pyles, Z. Ren, G. Zhou, and X. Liu, "SiFi: Exploiting VoIP silence for WiFi energy savings in smart phones," in *Proc. ACM UbiComp*, 2011, pp. 325–334.
[259] V. Namboodiri and L. Gao, "Towards energy efficient VoIP over wireless LANs," in *Proc. ACM MobiHoc*, 2008, pp. 169–178.
[260] F. R. Dogar, P. Steenkiste, and K. Papagiannaki, "Catnap: Exploiting high bandwidth wireless interfaces to save energy for mobile devices," in *Proc. ACM/USENIX MOBISYS*, 2010, pp. 107–122.
[261] E. Rozner, V. Navda, R. Ramjee, and S. Rayanchu, "NAPman: Network-assisted power management for WiFi devices," in *Proc. ACM/USENIX MOBISYS*, 2010, pp. 91–106.
[262] J. Manweiler and R. Choudhury, "Avoiding the rush hours: WiFi energy management via traffic isolation," in *Proc. ACM/USENIX MOBISYS*, 2011, pp. 253–266.
[263] A. Garcia-Saavedra, P. Serrano, A. Banchs, and M. Hollick, "Balancing energy efficiency and throughput fairness in IEEE 802.11 WLANs," *Pervasive Mobile Comput.*, vol. 8, no. 5, pp. 631–645, Oct. 2012.
[264] X. Chen, S. Jin, and D. Qiao, "M-PSM: Mobility-aware power save mode for IEEE 802.11 WLANs," in *Proc. IEEE ICDCS*, Jun. 2011, pp. 77–86.
[265] T. Pering, Y. Agarwal, R. Gupta, and C. Power, "CoolSpots: Reducing the power consumption of wireless mobile devices with multiple radio interfaces," in *Proc. ACM/USENIX MOBISYS*, 2006, pp. 220–232.
[266] A. Rahmati and L. Zhong, "Context-for-wireless: Context-sensitive energy-efficient wireless data transfer," in *Proc. ACM MobiSys*, 2007, pp. 165–178.
[267] A. Sharma, V. Navda, R. Ramjee, V. N. Padmanabhan, and E. M. Belding, "Cool-Tether: Energy efficient on-the-fly WiFi hot-spots using mobile phones," in *Proc. ACM CoNEXT*, 2009, pp. 109–120.
[268] N. Mishra, K. Chebrolu, B. Raman, and A. Pathak, "Wake-on-WLAN," in *Proc. ACM WWW*, 2006, pp. 761–769.
[269] A. P. Jardosh *et al.*, "Green WLANs: On-demand WLAN infrastructures," *Mobile Netw. Appl.*, vol. 14, no. 6, pp. 798–814, Dec. 2009.
[270] A. Kumar, "Managing TCP connections in dynamic spectrum access based wireless LANs," in *Proc. IEEE SECON*, 2010, pp. 1–9.
[271] E. Vergetis, E. Pierce, M. Blanco, and R. Guerin, "Packet-level diversity-from theory to practice: An 802.11-based experimental investigation," in *Proc. ACM MobiCom*, 2006, pp. 62–73.
[272] R. Chandra, R. Mahajan, T. Moscibroda, R. Raghavendra, and V. Bahl, "A case for adapting channel width in wireless networks," in *Proc. ACM SIGCOMM*, 2008, pp. 135–146.
[273] S. Rayanchu, V. Shrivastava, S. Banerjee, and R. Chandra, "FLUID: Improving throughputs in entreprise wireless LANs through flexible channelization," in *Proc. ACM MobiCom*, 2011, pp. 1–12.
[274] H. Lundgren, D. Lundberg, J. Nielsen, E. Nordstrom, and C. Tschudin, "A large-scale testbed for reproducible ad hoc protocol evaluations," in *Proc. IEEE WCNC*, Mar. 2002, vol. 1, pp. 412–418.
[275] D. Raychaudhuri *et al.*, "Overview of the ORBIT radio grid testbed for evaluation of next-generation wireless network protocols," in *Proc. IEEE WCNC*, 2005, pp. 1664–1669.
[276] A.-C. Anadiotis *et al.*, "Towards maximizing wireless testbed utilization using spectrum slicing," in *Proc. ICST TRIDENTCOM*, 2010, pp. 299–314.
[277] J. Kaba and D. Raichle, "Testbed on a desktop: Novel testbed strategies for multi-hop MANET routing protocol development," in *Proc. ACM MobiHoc*, 2001, pp. 164–172.
[278] G. Judd and P. Steenkiste, "Using emulation to understand and improve wireless networks and applications," in *Proc. USENIX NSDI*, 2005, pp. 203–216.
[279] P. Steenkiste, "The use of a controlled wireless testbed in courses," in *Proc. SIGCSE ITiCSE*, 2009, pp. 80–84.
[280] J. Lee, J. Lee, K. Lee, and S. Chong, "CommonCode: A code-Reuse platform for wireless network experimentation," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 156–163, Mar. 2012.
[281] P. De *et al.*, "MiNT-m: An autonomous mobile wireless experimentation platform," in *Proc. ACM/USENIX MOBISYS*, 2006, pp. 124–137.
[282] R. Patra *et al.*, "WiLDNet: Design and implementation of high performance WiFi based long distance networks," in *Proc. USENIX NSDI*, 2007, pp. 87–100.
[283] A. Capone, M. Cesana, S. Napoli, and A. Pollastro, "MobiMESH: A complete solution for wireless mesh networking," in *Proc. IEEE MASS*, Oct. 2007, pp. 1–3.
[284] M. Cesana, L. Fratta, M. Gerla, E. Giordano, and G. Pau, "C-VeT the UCLA campus vehicular testbed: Integration of VANET and Mesh networks," in *Proc. Eur. Wireless*, Apr. 2010, pp. 689–695.
[285] P. Bhagwat, B. Raman, and D. Sanghi, "Turning 802.11 inside-out," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, pp. 33–38, Jan. 2004.
[286] D. Wu, D. Gupta, and P. Mohapatra, "QuRiNet: A wide-area wireless mesh testbed for research and experimental evaluations," *Ad Hoc Netw.*, vol. 9, no. 7, pp. 1221–1237, 2011.
[287] N. Banerjee, M. Corner, and B. Levine, "Design and field experimentation of an energy-efficient architecture for DTN throwboxes," *IEEE/ACM Trans. Netw.*, vol. 18, no. 2, pp. 554–567, Apr. 2010.
[288] H. Lundgren *et al.*, "Experiences from the design, deployment, and usage of the UCSB MeshNet testbed," *IEEE Wireless Commun.*, vol. 13, no. 2, pp. 18–29, Apr. 2006.

[289] I. Broustis, J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "A blueprint for a manageable and affordable wireless testbed: Design, pitfalls and lessons learned," in *Proc. ICST TRIDENTCOM*, May 2007, pp. 1–6.
[290] P. Serrano *et al.*, "FloorNet: Deployment and evaluation of a multihop wireless 802.11 testbed," *EURASIP J. Wireless Commun. Netw.*, vol. 2010, no. 1, Apr. 2010, Art. ID. 153102.
[291] M. P. Comeras, J. M. Bafalluy, and M. R. Esteso, "Techniques for improving the accuracy of 802.11 WLAN-based networking experimentation," *EURASIP J. Wireless Commun. Netw.*, vol. 2010, no. 1, Apr. 2010, Art. ID. 527 847.
[292] I. Broustis, K. Papagiannaki, S. Krishnamurthy, M. Faloutsos, and V. Mhatre, "Measurement-driven guidelines for 802.11 WLAN design," *IEEE/ACM Trans. Netw.*, vol. 18, no. 3, pp. 722–735, Jun. 2010.
[293] V. Brik *et al.*, "A measurement study of a commercial-grade urban WiFi mesh," in *Proc. ACM IMC*, 2008, pp. 111–124.
[294] D. Tang and M. Baker, "Analysis of a local-area wireless network," in *Proc. ACM MobiCom*, 2000, pp. 1–10.
[295] D. Kotz and K. Essien, "Analysis of a campus-wide wireless network," in *Proc. ACM MobiCom*, 2002, pp. 107–118.
[296] T. Henderson, D. Kotz, and I. Abyzov, "The changing usage of a mature campus-wide wireless network," in *Proc. ACM MobiCom*, 2004, pp. 187–201.
[297] A. Balachandran, G. M. Voelker, P. Bahl, and P. V. Rangan, "Characterizing user behavior and network performance in a public wireless LAN," in *Proc. ACM SIGMETRICS*, 2002, pp. 195–205.
[298] A. P. Jardosh, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer, "Understanding congestion in IEEE 802.11b wireless networks," in *Proc. ACM/USENIX IMC*, 2005, pp. 25–25.
[299] M. Balazinska and P. Castro, "Characterizing mobility and network usage in a corporate wireless local-area network," in *Proc. ACM/USENIX MOBISYS*, 2003, pp. 303–316.
[300] J. Eriksson, S. Agarwal, P. Bahl, and J. Padhye, "A feasibility study of mesh networks for an all-wireless office," in *Proc. ACM/USENIX MOBISYS*, 2006, pp. 69–82.
[301] C. Na, J. Chen, and T. Rappaport, "Measured traffic statistics and throughput of IEEE 802.11b public WLAN hotspots with three different applications," *IEEE Trans. Wireless Commun.*, vol. 5, no. 11, pp. 3296–3305, Nov. 2006.
[302] M. Afanasyev, T. Chen, G. M. Voelker, and A. C. Snoeren, "Analysis of a mixed-use urban WiFi network: When metropolitan becomes neapolitan," in *Proc. ACM IMC*, 2008, pp. 85–98.
[303] D. Han *et al.*, "Mark-and-sweep: Getting the "Inside" scoop on neighborhood networks," in *Proc. ACM IMC*, Oct. 2008, pp. 99–104.
[304] Y.-C. Cheng *et al.*, "Jigsaw: Solving the puzzle of enterprise 802.11 analysis," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 36, no. 4, pp. 39–50, Oct. 2006.
[305] A. Sheth, C. Doerr, R. Han, D. Grunwald, and D. Sicker, "MOJO: A distributed physical layer anomaly detection system for 802.11 WLANs," in *Proc. ACM/USENIX MOBISYS*, 2006, pp. 191–204.
[306] P. Serrano, M. Zink, and J. Kurose, "Assessing the fidelity of COTS 802.11 sniffers," in *Proc. IEEE INFOCOM*, 2009, pp. 1089–1097.
[307] U. Deshpande, C. McDonald, and D. Kotz, "Refocusing in 802.11 wireless measurement," in *Proc. IEEE PAM*, 2008, pp. 142–151.
[308] J. Robinson, R. Swaminathan, and E. W. Knightly, "Assessment of urban-scale wireless networks with a small number of measurements," in *Proc. ACM MobiCom*, 2008, pp. 187–198.
[309] D. Gupta, D. Wu, P. Mohapatra, and C.-N. Chuah, "Experimental comparison of bandwidth estimation tools for wireless mesh networks," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 2891–2895.
[310] M. Portoles-Comeras, A. Cabellos-Aparicio, J. Mangues-Bafalluy, A. Banchs, and J. Domingo-Pascual, "Impact of transient CSMA/CA access delays on active bandwidth measurements," in *Proc. ACM IMC*, 2009, pp. 397–409.
[311] M. Li, M. Claypool, and R. Kinicki, "WBest: A bandwidth estimation tool for IEEE 802.11 wireless networks," in *Proc. IEEE LCN*, Oct. 2008, pp. 374–381.
[312] W. Wei *et al.*, "Identifying 802.11 traffic from passive measurements using iterative Bayesian inference," *IEEE/ACM Trans. Netw.*, vol. 20, no. 2, pp. 325–338, Apr. 2011.
[313] B. Chun *et al.*, "PlanetLab: An overlay testbed for broad-coverage services," *SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 3, pp. 3–12, Jul. 2003.
[314] F. Abinader *et al.*, "Enabling the coexistence of LTE and Wi-Fi in unlicensed bands," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 54–61, Nov. 2014.
[315] C. Bernardos *et al.*, "An architecture for software defined wireless networking," *IEEE Wireless Commun. Mag.*, vol. 21, no. 3, pp. 52–61, Jun. 2014.
[316] P. Calhoun, M. Montemurro, and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) protocol specification," Internet Engineering Task Force, Fremont, CA, USA, RFC 5415 (Proposed Standard), Mar. 2009.

Pablo Serrano received the telecommunication engineering and Ph.D. degrees from the Universidad Carlos III de Madrid (UC3M) in 2002 and 2006, respectively. He has been with the Telematics Department of UC3M since 2002, where he currently holds the position of Associate Professor. He was a Visiting Researcher at the Computer Network Research Group at the University Massachusetts Amherst in 2007, and at Telefonica Research Center in Barcelona in 2013. He has over 60 scientific papers in peer-reviewed international journal and conferences. He serves on the Editorial Board of IEEE COMMUNICATIONS LETTERS, has been a Guest Editor for *Computer Networks*, and has served on the TPC of a number of conferences and workshops including IEEE INFOCOM, IEEE WoWMoM and IEEE Globecom.

Pablo Salvador received the telecommunication engineering and M.Sc. degrees in telematics engineering from Universidad Carlos III de Madrid (UC3M) in 2010 and 2011, respectively. He was awarded as nationwide finalist of the Telematics Association for his B.Sc. project. In 2010, he performed an internship at NEC Laboratories Europe. In 2014, he was a Visiting Scholar at the Rice Networks Group at the University of Rice, Houston, TX, USA. Pablo is currently working on his Ph.D. at the Institute IMDEA Networks, while being involved in various European research projects such as FLAVIA and CROWD. His primary research interests focus on the performance evaluation of wireless networks.

Vincenzo Mancuso received the Ph.D. degree in electronic, computer science, and telecommunications from the University of Palermo, Italy, in 2005. He has been a Research Assistant Professor at IMDEA Networks Institute, Madrid, Spain, since September 2010. Previously, he built his research experience by working with University of Palermo, Rice University (Houston, TX, USA), and INRIA Sophia Antipolis (France). His research activities focus on analysis, design, and experimental evaluation of protocols and architectures for the control of wireless networks, including SDN solutions for IEEE 802.11, 3GPP LTE-A, SDR-based networks and D2D mechanisms for such networks. He is also currently working on non-invasive measurement techniques, analysis and optimization for power saving strategies in packet cellular networks (3GPP LTE-A), and energy efficient ethernet (IEEE 802.3az).

Yan Grunenberger received the engineering diploma and Ph.D. degrees from the Grenoble University, France (INPG), in 2004 and 2008, respectively. He has been working on implementing fair Wi-Fi access methods, cross-layer architectures (LIG, Grenoble, France), mobileapps (Mootwin, Grenoble, 2009), as well as sensors networks and Software DefinedRadio (CTTC, Barcelona, 2010). From 2011 to 2014, he was a member of the Telefonica Research group located in Barcelona, where his research was centered on studying energy and performance aspects of mobile and home networks. He is now working on security aspects in radio networks.