

A Technological overview of the guifi.net community network

Davide Vega^a, Roger Baig^b, Llorenç Cerdà-Alabern^a, Esunly Medina^a, Roc Meseguer^a, Leandro Navarro^a

^a*Departament of Computer Architecture, Universitat Politècnica de Catalunya
Barcelona, Spain*

^b*Foundation for the Neutral, Free and Open Network - guifi.net
Gurb, Catalonia*

Abstract

This work presents a technological analysis of guifi.net, a free, neutral, and open-access community network. Guifi.net consists of more than 27,000 operational nodes, which makes it the world's largest community network in terms of the number of nodes and coverage area. This paper describes the characteristics of the network, the link level topology, its growth over a decade, and its resilience in terms of availability and reachability of network nodes. Our study is based on open data published by guifi.net regarding its nodes and wireless links, monitoring information, community database, and its web portal. The data includes historical information that covers the lifetime of the network. The scale and diversity of the network requires a separate analysis of the subsets of the entire dataset by area or by separating the core from the leaf nodes. This shows some degree of diversity in local characteristics caused by several demographic, geographic, technological, and network design factors.

We focus on the following aspects: technological network diversity, topology characteristics, evolution of the network over time, analysis of robustness, and its effect on networking service availability. In addition, we analyse how the community, the technology used, the geographical region where the network is deployed, and its self-organised structure shape the network properties and determine its strengths and weaknesses.

The study demonstrates that the guifi.net community network is diverse in technological choices for hardware, link protocols, and channels and uses a combination of routing protocols yet provides a common private IP network. The graph topology follows a power-law distribution for links in regions up to a few thousand Km^2 , limited to the scope of wireless links. Network growth has two aspects: a geographic growth of the network core using long distance links with wireless or fibre, and the local growth in density with leaf low-cost leaf nodes. The resilience of the network derived from the nodes' uptime and the structure of the graph varies across different regions with more fragile leafs than core nodes and diverse degrees of graph resilience to random failures or coordinated attacks, such as natural causes, depending on the network planning, structure, and maturity. The guifi.net community network results from a loosely coupled and decentralised organic growth that



exhibits large local differences, diverse growth, and maturity under a common community license and social network.

Keywords: Community network, Wireless network, Topology patterns, Network characterisation, Resilience

1. Introduction

Today, the Internet connects the world; however, the availability of sustainable, cost-effective, and quality services for all citizens is still challenging. Community networking, also known as bottom-up networking, is an emerging model for the future Internet, where communities of citizens build, operate, and own open IP-based networks. It is also a key infrastructure for individual and collective digital participation [1]. Hundreds of community networks operate in very diverse areas. These networks are usually run by non-profit organisations and can cooperate with local stakeholders – including commercial service providers – to develop community services, including local networking, voice, data, and Internet access. These large, decentralised, dynamic, and heterogeneous structures raise challenges that can be of interest to researchers, both as a source of inspiration and as a field to apply their research findings [2].

This paper focuses on guifi.net, which is the world's largest community network, to the best of our knowledge. The network started in 2004, and ten years later it has surpassed 27,000 operational nodes and around 13,400 users [3]. Most nodes are located in Catalonia and nearly all are in the Iberian Peninsula (Spain and Portugal). There are many more community networks around the world, with local variations in aspects, such as structure, operation, population, coverage, and technology with the common goal of empowering all citizens to access and participate in the digital world.

The purpose of this paper is to describe and analyse this large-scale community network to understand its characteristics in terms of structure, scale, dynamics, and decentralisation. In addition, we identify the challenges that Internet protocols and service providers must face to be able to operate in these networks.

In Section 2, this paper presents a measurement study of guifi.net and extends prior findings presented in [4, 5] based on a smaller portion of the data. The collected data include management information, such as network structure, from the community node and traffic database, SNMP logs, and active traffic measurements on routing and wireless interfaces.

After a description of related work and data collection in Section 3, our study analyses the following aspects: hardware network diversity (Section 4), topology characteristics (Section 5), evolution of the network (Section 6), availability of network nodes (Section 7), analysis of resilience (Section 8) as well as the consequences on network services and applications. We analyse how the social community, the technology, the region where the network is deployed,

Email addresses: dvega@ac.upc.edu (Davide Vega), lllorenç@ac.upc.edu (Llorenç Cerdà-Alabern), meseguer@ac.upc.edu (Roc Meseguer), leandro@ac.upc.edu (Leandro Navarro)

and its self-organised structure shape the community network and determine its properties, strengths, and weaknesses. Finally, the paper discusses related work and conclusions in Section 9 and concludes.

2. The Guifi.net Network

Guifi.net [6, 7] is defined as an open, free, and neutral network built by its members, who are citizens and organisations pooling their resources and coordinating efforts to build and operate a local network infrastructure. The underlying principle behind guifi.net is the common pool resource (CPR) model as the optimal method to manage a network [8, 9]. Most of the network links in guifi.net are wireless [4], but there is an increasing number of fibre links being used [10].

The community network is built upon an interconnection agreement in which each new participant is given the right to use the network for any purpose unless it affects the operation of the network or the freedom of other users, the right to know and learn any detail of the network and its components, and the freedom of joining or extending the network following the same conditions. The only limitation is that this network cannot be used in a way that affects its operation or the freedom of other users.

The network started in 2004, and ten years later it has more than 27,000 operational nodes. Most nodes are located in Catalonia and nearly all are in the Iberian Peninsula (Spain and Portugal). In 2008, the community members created the guifi.net Foundation, a non-profit organisation responsible for the coordination of the community and the provision of deployment support for the users. The guifi.net Foundation encourages the deployment of the network, but it does not manage it. Therefore, decisions concerning network growth and maintenance are made by the network users.

Typically, guifi.net grows very quickly; in a week about, 30 nodes can become operational and more than one hundred new nodes can be planned (created on the web interface but not yet operational). Moreover, the network offers a wide range of services, provided by individuals, social groups, and small non-profit or commercial service providers. Guifi.net is also open and welcoming to researchers; together with AWMN (Greece) and FunkFeuer (Austria), it is part of the experimental testbed Community-Lab. This testbed was inspired by PlanetLab, and its main goal is to promote and facilitate research on community networking [2].

Currently, at the physical level, guifi.net combines several technologies with wireless and optical fibre being the most common. Due to its affordability, accessibility, and ease of deployment, Wi-Fi was the first technology to be used and is still the most popular; it is fully supported by the web tools, and its use is widespread among professionals and volunteers. The initial nodes of guifi.net were deployed in 2004. Figure 1 depicts the evolution of the total operational nodes over time. Optical fibre was first introduced in 2009¹.

Topologically speaking, Wi-Fi and optical fibre networks are rather similar [4, 10]. In both cases, end-user nodes (the *nodes*) are connected to a central point (the *supernodes*

¹<http://guifi.net/node/23273>

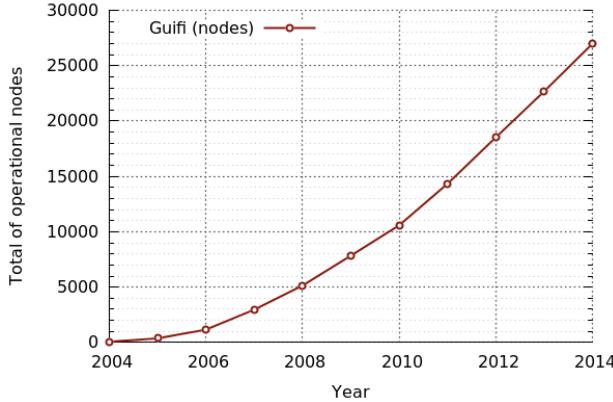


Figure 1: Growth of guifi.net in terms of the total number of operational nodes.

in Wi-Fi and the Point-of-Presence Internet Exchange (PoPIX) in optical fibre), and supernodes are connected to each other through dedicated links as the backbone. In Wi-Fi, the *infrastructure mode* (i.e., the combination of master-client mode for nodes to supernode connections and dedicated Point-to-Point (PtP) links between supernodes) has been shown to be much more efficient than solutions based on IEEE 802.11 ad-hoc mode [11, 12]. Nonetheless, some parts of the network operate in Ad-Hoc mode. In Wi-Fi, practically all of the links are deployed by guifi.net. In contrast, for optical fibre deployments, most of the PtP links are subcontracted dark fibres². Figure 2 shows the current distribution of the operational PoPIX (15 total). In the areas where the two technologies coexist, optical fibre links replace Wi-Fi links in the backbone. Such fibre links form a backhaul that results in a more efficient topology, amending the abnormal situation of having a backbone with several tenths of Wi-Fi hops.

At the IP level, guifi.net uses IPv4 RFC1918 private addresses. The IP addresses had been initially mapped to network interfaces according to guidelines issued by the Free Networks project. This project, which started in 2000 but has been unmaintained for years, had the aim of harmonising the $10/8$ block allocation among community networks. Currently, the full $10/8$ address space is considered, although in practice only some $/16$ blocks are being used. The IPs are allocated to supernodes in $/27$ chunks³ and each one of the nodes receive one of these IPs. In addition, the $172.16/12$ block⁴ chunks are used for the PtP backbone links. Nonetheless, this range is not routed; hence, $10/8$ and $172.16/12$ addresses are frequently referred to as *public* and *private* addresses, respectively.

At the routing level, the network is split into *Autonomous Systems*; most of them are internally running Open Shortest Path First (OSPF) and interconnected via Border Gateway Protocol (BGP). Number and name assignments and allocations are made foreseeing the

²So far all of them to the Catalan national dark fibre provider <http://www.xarxaoberta.cat/en/about-xoc>

³Such small netmask is a legacy of the address space scarcity in the times of Free Networks ($10/8$ were assigned to each community network regardless of its size – while guifi.net already had thousands of nodes the other community networks had only tenths).

⁴Currently just the $172.25/16$ block are used. Assignments are made in $/30$.

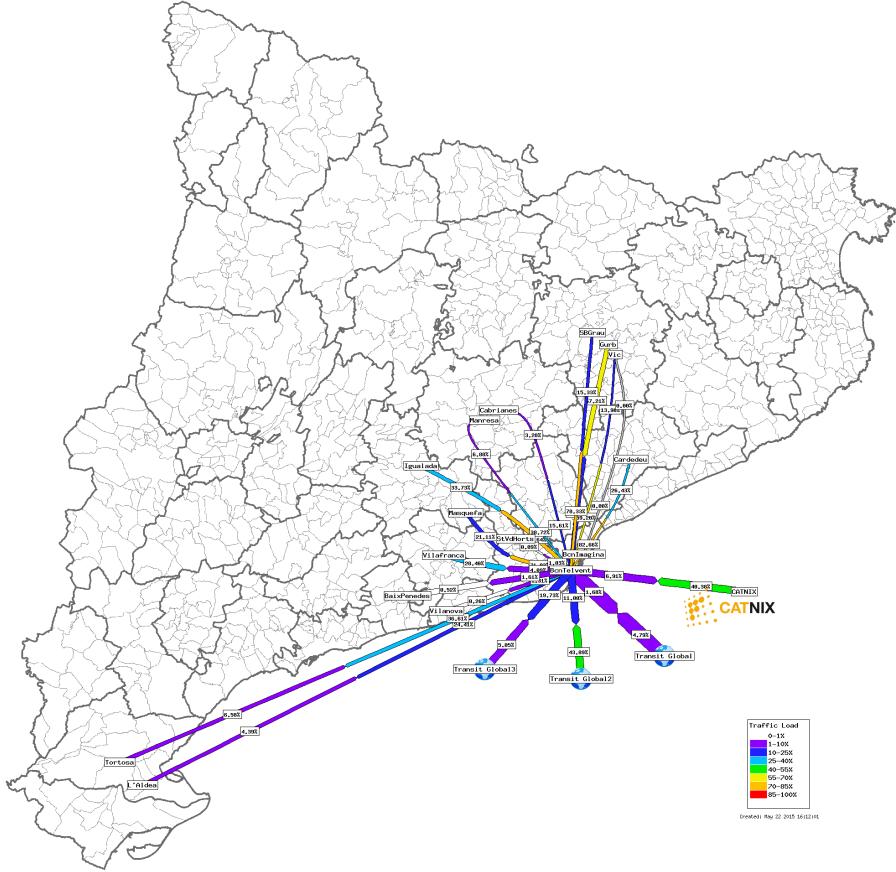


Figure 2: guifi.net Optical Fibre backbone links (May 2015).

network as a completely single network (i.e., for compatibility reasons). In addition, in September 2014 about 2,900 routes were announced at the largest BGP cloud⁵.

With respect to the network interconnection, guifi.net is connected to many networks, including the Internet, in different ways. Peering with other networks is the preferred method because this fits better with the principles of the project, carriers, and domestic Internet connections. Network interconnection is made available following the conditions established by the individuals or groups that are offering it.

The guifi.net Foundation is a member of the Catalan Exchange Point (CATNIX⁶), which has about 39 peers (counting IPv4 and IPv6) and three 1 Gbps Internet uplinks. Two of these uplinks are operated by the Foundation and the other by an Internet Service Provider (ISP). Both the uplinks that are operated by the Foundation and the CATNIX connections are distributed among participating ISPs, which, in turn, redistribute them among their customers. Figure 3 shows the evolution of the total inbound and outbound guifi.net traffic over the last year. The network is also part of the Community-Lab experimental testbed;

⁵Because block aggregation is not automated

⁶<http://www.catnix.net/en/>

therefore, guifi.net has a network level federation with several other European community networks [2].

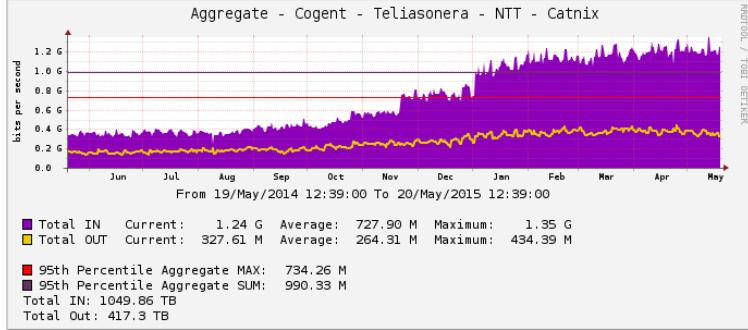


Figure 3: Evolution total transit exchanged by guifi.net.

The most common method for users to make their domestic Internet connections available to other guifi.net members is through proxies (usually web proxies). Guifi.net has developed a proxy federation system, which allows any user to freely use all the network proxies using the same credentials. The DSL lines belonging to public administrations (councils, libraries, telecentres, etc.) are usually made available to guifi.net participants through this proxy federation system because it offers several technical and legal guarantees.

3. Methodology and Data Collection

Although community networks are open and inclusive by nature, collecting data from them can be challenging due to the nature of the network, its decentralised structure, the number of members involved, the formal and informal structures of governance, and the technical barriers due to its heterogeneity. In addition, the network grows according to the needs of the users, and they are responsible for installing, configuring, and maintaining their own nodes as well as the network services and management tools. This fact makes it more difficult to keep track of the state and evolution of the network, which also affects the collection of data.

We used historical data from several open data repositories of the guifi.net community. The data contains information collected since the beginning of the network in 2004. Analysing this data, we can observe the growth of the network, both socially and computationally in terms of wireless links, monitoring information, membership, and web portal. Additionally, in 2014 and 2015, we performed several active measurements over the network for short periods (from a few days up to a couple of weeks).

Both active measurements and data collection were constrained to avoid any negative effects on the operation of the network. Therefore, although most of our data requirements were granted by the guifi.net Foundation, our access to logs was limited (only open and anonymized data), and our experiments were conducted in a way that would not significantly affect network performance.

All the data collected allowed us to capture and understand the specific characteristics of the guifi.net network. We collected information from the following sources:

- *Network description*: expressed in the Community Networks Markup Language (CNML), an XML-based language used to describe community networks. Guifi.net publishes a snapshot of its network structure every 30 minutes with a description of registered nodes, links, and their configurations. In the CNML description, the information is arranged according to different geographical *zones* in which the network is organised. This information has been used to build topology graphs (see [5] for more details).
- *Node database*: a dump of the community network database that, in addition to the data described in CNML, includes other details about dates and people involved in the creation and update of the configuration of nodes and links.
- *List of federated users*: a list of user identifiers with password hashes for authentication on the diverse services offered by guifi.net, mainly on federated web proxies. In February 2015, we registered 12,797 user identifiers used on about 300 web proxy servers.
- *Periodic infrastructure logs*: we analysed the logs of a guifi.net proxy widely used by community members to access Internet content. These logs contain information about the amount of data transferred, active sessions, users, and traffic patterns.
- *Simple Network Management Protocol (SNMP) snapshots*: we collected information concerning 3,668 nodes using SNMP requests and scripts to reach nodes via SSH. Examples of the information collected in each node are statistics about the uptime, the total number of nodes linked to it, addresses of its neighbours (ARP tables), current channel number, number of failed transmissions, background noise level, routing tables, etc.
- *Link data traffic logs*: this service (also known as a graph server) is a distributed and hierarchical monitoring system that collects metrics about the in/out traffic, delays, and availability of all nodes and link interfaces registered. In each geographical *zone*, one or more servers are continuously collecting information via SNMP requests to nodes and storing it on Round-Robin Database (RRD). Any request to the guifi.net web server of a given node will be managed by the graph server responsible for delivering the traffic graph.

4. Hardware of the network nodes

In this section, we analyse the hardware, firmware, and setup used in guifi.net. Our objective is to characterise the different hardware and software choices made by network members. This analysis will allow us gain an understanding of how an open, free, and neutral network led by a diverse range of individual and independent choices results in a cohesive IP network.

In the guifi.net community (as in any human community), collective actions are coordinated among members, but a high number of decisions are also individually made. Never-

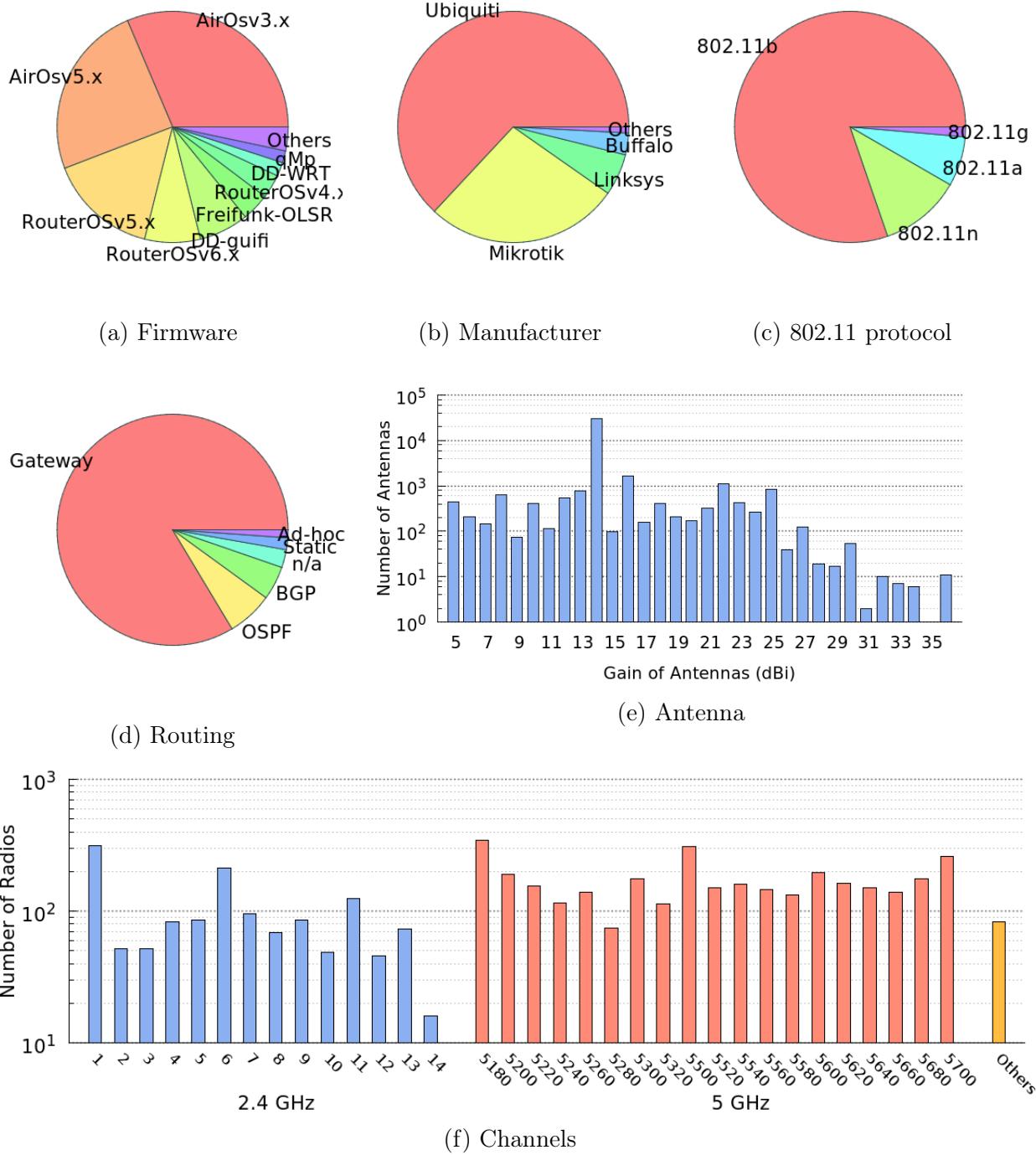


Figure 4: Diversity of guifi.net wireless network nodes

theless, many practical experiences, lessons learnt, and knowledge are shared not only within the community but also with users of other community networks.

Individual freedom is reflected in the analysis of the hardware and software heterogeneity. That diversity may be a characteristic feature of large community networks, in contrast with smaller ones, where there may be more homogeneity. Figure 4 summarises the range of choices in wireless guifi.net nodes.

Among the more than 27,000 nodes studied, we discovered that 13 different firmware versions were running simultaneously (Figure 4a). Of these, 56% are different versions of AirOS, and 26% run RouterOS firmware versions. Both firmwares are based on General Public License (GPL) source code but include proprietary binary modules from Ubiquiti Networks and MikroTik, respectively. This variety of versions for the same firmware illustrates that deployed devices are not updated or changed until they fail or become congested. For instance, RouterOS version 6 was released in 2013, version 5 in 2010, version 4 in 2009, and version 3 in 2008.

Ubiquiti devices are the most common hardware used in guifi.net (Figure 4b) at 32% of the deployed devices NanoStation. Ubiquiti devices are designed for easy installation, for example, outdoor boxes, integrated antenna, Passive Power over Ethernet (POE). On the other hand, MikroTik devices (RouterBoard) offer better performance and flexibility but require outdoor boxes, antennas, wireless radios, and pigtails. *Supernodes* with several links require devices with multiple radios and multiple antennas. Therefore, Ubiquiti devices are used for end-user nodes and MikroTik devices are used for *supernodes*. Currently, supernodes combine multiple components (hybrid supernodes), for instance, a RouterBoard device as the core of the router connected through Ethernet with Ubiquiti devices, which are used as radios and antennas.

Figure 4c shows the choices made for the selection of Wi-Fi protocols with more than 81% of the devices using the oldest 802.11b specification. In the 2.4 GHz band, channel allocation is almost equally distributed among the 13 channels (from 2.412 GHz to 2.472 GHz) available for use in Europe (Figure 4f). Nevertheless, in the 5 GHz band, there are some unused channels. Currently, guifi.net is testing the 24 GHz band.

In contrast to other community networks [13], the adjacent channel allocation in guifi.net does not cause interference since 75% of the devices use directional antennas (Figure 4e). However, other sources of wireless interferences are caused by some devices that are using high transmission power by misconfiguration and by the use of third-party equipment.

Figure 4e shows a high diversity of antenna gains, which correspond to the specific requirements of each physical location and link distance. The diversity observed is mainly caused by the freedom that guifi.net users have in order to use any solution they are comfortable with to build their nodes. This is not the most common case in Wireless Community Networks as described in Section 9.

Concerning routing, Figure 4d shows the distribution of the protocols used inside the network. The majority (83.71%) of the nodes are using an undefined gateway protocol, which is usually an alias for Interior Gateway Protocols (IGP). Other protocols are equally popular, with 6.62% and 5.43% of nodes using Open Shortest Path First (OSPF) and Border Gateway Protocols (BGP), respectively. This smaller fraction of the network, where the nodes are using IGP and OSPF, constitutes the network backbone. In contrast, the small percentage of ad-hoc devices corresponds to mesh clouds built in urban areas, such as Barcelona (Spain),

and are not part of this study (see [14]).

5. Topology Analysis at the Link Level

In the next sections, we are going to study and review the guifi.net network characteristics from link structure to network evolution. In this section, we begin with our observations about the topological structure in order to use the conclusions as a baseline to understand the behaviour in upper protocol layers. This will allow us to understand the construction and structural properties of the network.

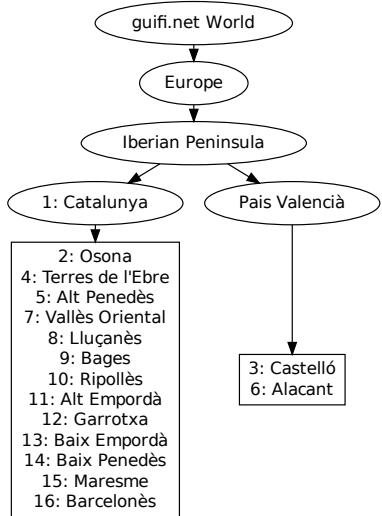


Figure 5: Zones considered, ordered by the number of nodes.

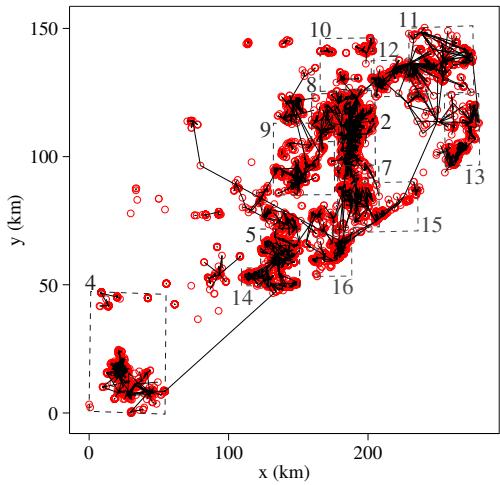


Figure 6: Catalonia zone. Axes are in km.

The analysis is based on the CNML information downloaded on January 5th, 2015⁷. The CNML file is organized into a tree hierarchy of zones. The root zone is named *guifi.net World*. Each zone can be divided in other zones that cover smaller geographical areas. We refer to each division as *levels*, with the root zone at level 1. Here, we have considered zones up to level 5. From them, we have chosen 15 leaf zones that have graphs with the largest number of nodes. Figure 5 shows the resulting zone tree. To explore the resemblance of aggregated zones with the leafs in the analysis, we also considered the Catalonia level 4 zone.

Figure 6 shows the geographical position of the nodes and links in the Catalonia zone. Catalonia leaf zones are marked with dashed lines and numbers corresponding to those given in Figure 5. Note from Figure 6 that not all nodes in a zone are connected in a single cluster. Isolated clusters correspond to users that started a new group of nodes inside a zone and did not have the ability to establish links with other clusters in the zone. Several reasons explain this limitation, such as the geographical distribution of the population within the territory or the absence of other guifi.net users in surrounding areas.

⁷The CNML file can be downloaded from <http://guifi.net/en/guifi/cnml/3671/detail>

zone	whole		base-graph		core-graph		terminals
	nodes/links/km ²	nodes/links	degree	nodes/links	degree	$\alpha/p\text{-val}$	$r/\mu/p\text{-val}$
1	19,654/19,286/22,056	12,161/12,511	1/2.1/525	711/1,061	1/3/28	2.7/0.07	0.24/16/0.31
2	8,383/8,189/3,524	7,753/7,920	1/2/525	311/478	1/3.1/26	2.8/0.5	0.15/24/0.096
3	4,916/4,451/3,344	3,562/3,674	1/2.1/266	205/317	1/3.1/23	2.7/0.62	0.25/16/0.054
4	1,840/1,819/28	888/911	1/2.1/148	50/73	1/2.9/10	2.8/0.32	0.27/17/0.81
5	1,551/1,534/74	1,391/1,405	1/2/152	67/81	1/2.4/8	2.8/0.35	0.65/20/1
6	1,330/1,292/23	650/650	1/2/223	16/16	1/2/4	4.2/0.91	0.36/40/0.14
7	1,037/993/31	763/766	1/2/121	47/50	1/2.1/5	2.8/0.07	0.74/15/0.31
8	972/932/50	730/737	1/2/99	31/38	1/2.5/5	2.9/0.64	0.33/23/0.71
9	701/671/308	503/510	1/2/81	44/51	1/2.3/14	3.3/0.65	0.47/10/0.92
10	580/570/230	291/293	1/2/125	12/14	1/2.3/5	2.8/0.3	0.86/23/0.71
11	579/589/119	526/543	1/2.1/48	54/71	1/2.6/8	2.7/0.81	0.64/8.7/0.3
12	567/598/131	311/391	1/2.5/69	55/135	1/4.9/20	2.1/0.51	0.18/4.7/0.49
13	554/546/151	472/480	1/2/72	31/39	1/2.5/9	3.1/0.47	0.76/14/0.42
14	455/452/38	445/448	1/2/93	23/26	1/2.3/5	3.2/0.51	0.44/18/0.66
15	429/410/538	295/308	1/2.1/118	31/44	1/2.8/13	2.6/0.39	0.38/8.5/0.084
16	419/279/1,911	221/234	1/2.1/23	67/80	1/2.4/8	3.1/0.1	1.3/2.3/0.3
μ	1,621/1,555/700	1,253/1,285	1/2.1/144	70/101	1/2.7/11	2.9/0.48	0.52/16/0.47
c_v	1.3/1.4/1.7	1.6/1.6	0/0.061/0.85	1.2/1.3	0/0.26/0.64	0.16/0.49	0.6/0.57/0.68

Table 1: Summary of zone graphs. *base-graph* refers to the largest cluster of the *whole* graph. *core-graph* is obtained from *base-graph* by removing nodes with unitary degree. For degree columns it is given min/mean/max. Fittings with p-value < 0.1 are in bold.

In order to ensure the consistency of our characterization, we considered the largest cluster in every zone. This cluster is called the *base-graph* of the zone.

These facts lead to separately considering the distribution of nodes belonging to *non-expert users* from those nodes forming the core. The former can be identified as *terminal nodes* (i.e., nodes in the base-graph having a degree equal to one). The core can be obtained by removing such nodes. Note that by doing this we obtain another connected graph that also has nodes with a degree of one (those with a degree of two in the base-graph, connected to one terminal node). Thus, we should use the term *core-graph* to refer to the graph that results from removing terminal nodes from the base-graph. Table 1 summarises the number of nodes, links, and degrees of the base-graph and core-graph for each zone. For the degree, the table shows the minimum, mean, and maximum values. The last two columns are used in the statistical characterisation of graphs. Finally, the last two rows give the mean (μ) and coefficient of variation ($c_v = \sigma/\mu$) of the values of the corresponding column.

5.1. Degree Distribution

It is well known that networks built following a preferential attachment process end up with a degree that follows a power-law distribution [15]. In guifi.net, it is reasonable to assume that such process has happened in the formation of the core. For instance, nodes that have a better connection to the Internet are likely to be preferred. We found that a

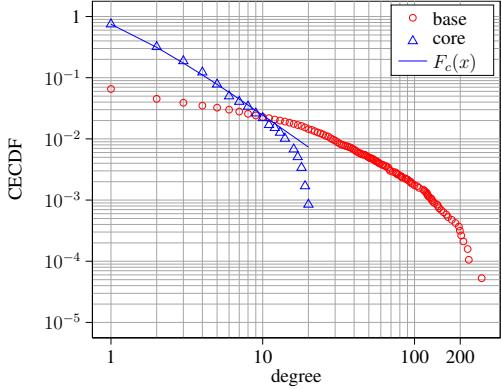


Figure 7: CECDF log₁₀-log₁₀ plot of the degree of the base and the core graphs of the Catalonia zone. Core-graph fits with a power law $F_c(x)$.

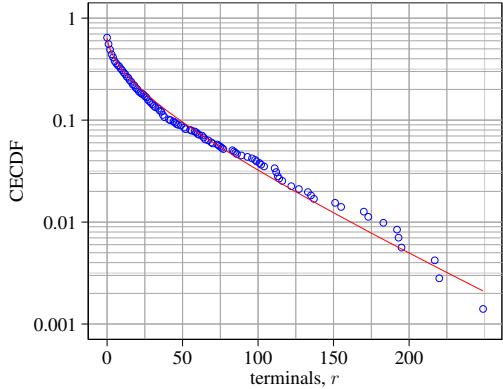


Figure 8: CECDF semi-log₁₀ plot of the number of terminals attached to core-nodes in the Catalonia zone and negative binomial fit.

discrete power law with cut-off $x_{min} = 2$ is a good match for the core-graph. Thus, we tested the complementary Probability Density Function (PDF) for the core-graph degree:

$$F_c(x) = P(X > x) = (1 - p(1)) \frac{\zeta(\alpha, x + 1)}{\zeta(\alpha, 2)}, \quad x \in \{1, 2, \dots\} \quad (1)$$

where $p(1)$ is the proportion of nodes in the core-graph with a degree equal to one, and

$$\zeta(\alpha, x) = \sum_{n=x}^{\infty} n^{-\alpha}$$

is the generalised Hurwitz zeta function. We have estimated α using the R package [16], which implements the method described in [17]. For goodness of fit, we have used the p-value provided by the same R package. It is important to note that the p-value estimates the probability that the empirical samples could have been obtained from the conjectured distribution. We must assume that the power-law hypothesis is ruled out when the p-value < 0.1 .

The column $\alpha/p\text{-val}$ in Table 1 gives the computed values for every zone, and those values that have $p\text{-value} < 0.1$ are marked in bold. These results show that the core-graph of the Catalonia zone has a p-value of 0.07, and therefore is not a very good match for a power-law. This fact is confirmed by Figure 7, which plots the Complementary Empirical Cumulative Distribution Function (CECDF) of the base and core graphs of the Catalonia zone in logarithmic scale. Note that the complementary distribution of a power law follows a straight line in such a scale. As shown in the figure, the degree distribution of the base-graph is far from a power-law. The distribution of the core-graph degree matches the estimated power-law in the first decade (solid line in the figure). However, for higher degree values, the tail of the CECDF decreases faster than a power-law. This can be explained by the fact that the Catalonia zone covers a large geographical area (around 22.000 km², as shown in Table 1). Therefore, long distances and the orographic characteristics of the zone are

likely to prevent the establishment of links among nodes with higher degrees, breaking the preferential attachment process that originates the power-law. However, if we look at the other sub-zones in the table, which have areas at one or two orders of magnitude lower, we can see that only one of them has a p-value smaller than 0.1. Thus, in general, we conclude that the power-law distribution is a good match for the degree distribution of zones up to a few thousand km².

We have found that number of terminals, T , attached to core-nodes is well fitted by a negative binomial distribution with parameters r and mean μ , i.e. $P(T = k) = \binom{k+r-1}{k} p^k (1-p)^r$, $k = 0, 1, 2, \dots$, where $p = \frac{\mu}{\mu+r}$. Last column of Table 1 gives the values of these parameters obtained for each zone. Note that only in three cases was obtained a p-value smaller than 0.1. Indeed, figure 8 which shows a semi-log plot of the CECDF of the number of terminals in the Catalonia zone and its negative binomial fit, confirms this matching.

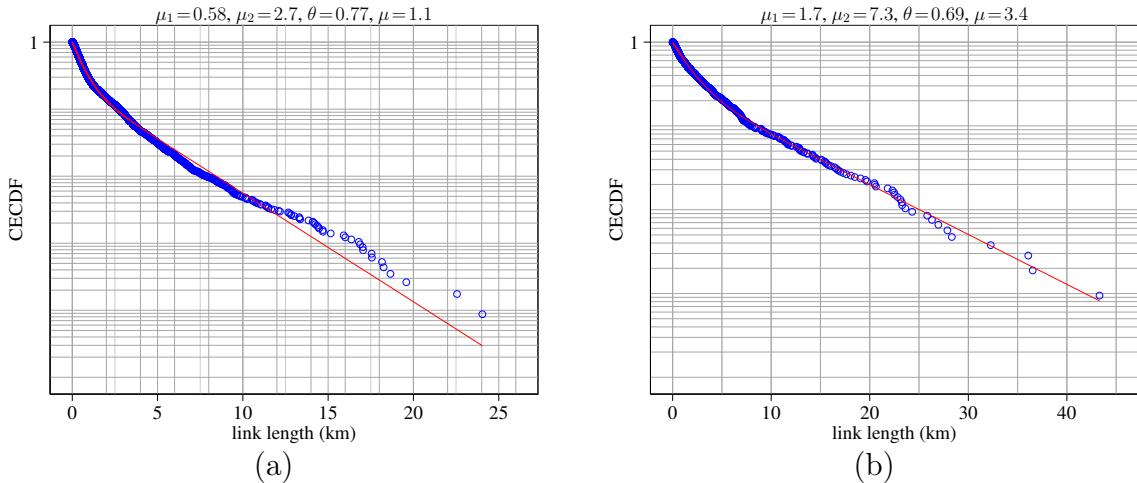


Figure 9: Link length distribution fitting of (a) links of terminal nodes, and (b) links of core-graph nodes of Catalonia zone. Means are in km, μ is the overall mean.

5.2. Link Length Distribution

The link length distribution is a very interesting characteristic of a wireless network, due to its strong influence on the signal transmission in the radio channel. We found that the link length distribution can be approximated by a combination of two exponential functions. If we consider L as the complementary CDF of the link length, X , then:

$$L(x|\lambda_1, \lambda_2, \theta) = P(X > x) = \theta e^{-\lambda_1 x} + (1 - \theta) e^{-\lambda_2 x} \quad (2)$$

Figure 9 shows a semi-log₁₀ plot of the link length CECDF of the Catalonia zone and its fitness using equation (2) (solid line). Figure 9(a) has been obtained for the links of terminal nodes and Figure 9(b) for the links of core-graph nodes. The figure shows that in both cases the link length distribution is very well characterized by the combination of the two exponential functions. This can be explained by the fact that links can be grouped into two sets. One set of short links characterising the connection of nodes is located in relatively close

geographical areas, for instance, villages in rural zones or suburbs in Barcelona. Another set is formed by longer distance links interconnecting nodes from different groups of the former set of links. We found that 77% of terminal nodes belong to the first group ($\theta = 0.77$), with a mean link length of $\mu_1 = 0.58$ km. The remaining 23% belong to long distance links with a mean of $\mu_2 = 2.7$ km. Core-graph links are likely to cover longer distances. Indeed, we discovered that the means obtained for the core-graph are approximately three times higher ($\mu_1 = 1.7$ km and $\mu_2 = 7.3$ km).

6. Network evolution

Guifi.net has experienced a steady growth in the number of members and coverage area and is now considered a well-known reference for social and technical participation. Moreover, the deployment of the physical networking infrastructure has been constantly evolving and adapting to the circumstances of the moment. Some of the decisions made by guifi.net members were forced by external factors, such as the geography and demographics of the Catalonia region or the technologies available at the time, while others were driven by technical reasons or technological choices. In this section we analyse the impact of the decisions made and review the historical evolution of the network during the period between 2004 and 2013 in three level 5 zones: Osona, Castelló, and Barcelona.

6.1. Geographic growth

Osona (*rural area, unplanned deployment*). Like any communication network, the physical deployment of guifi.net has been constrained by the demographic and geographic environment. Osona was the first region where guifi.net was deployed. It is an inland county with an extension of roughly more than 1,260 Km^2 . In 2009, Osona had a population density of around 0.12 inhabitants/ Km^2 with high-density inequality between its different areas. Figure 10 illustrates the evolution of guifi.net in Osona. Each map contains a snapshot of the network topology at the end of the year. Nodes and links depicted in light colours represent elements that already existed in the previous snapshot of the network. In contrast, new links that were added during the year under consideration are shown in darker colours. All the elements have been placed according to geographic coordinates.

During the first years (from 2004 in Figure 10a to 2006 in Figure 10c), founders focused their efforts on improving the software and hardware technologies behind guifi.net, limiting the network deployment to a small area centred in their own town and some surrounding areas. Because wireless technologies by then were not as mature as they are today, any potential community members were computer savvy people with high interest in new technologies. In 2006, guifi.net members decided to expand the network to other cities in the zone by creating large distance links. It resulted in a two-phase deployment, marked by the lack of initial knowledge in the first phase and a learning process during the second.

Castelló (*rural area, planned deployment*). Deployments made in Castelló took advantage of the first experiments in Osona. In Castelló, the deployment started in 2009, and a group of guifi.net members planned part of it to accelerate the process of providing coverage to the territory. Castelló is a coastal county with a geographical area of 6,679 Km^2 and a



Figure 10: Evolution of the Osona sub-network from 2004 to 2013.

density of 90.18 inhabitants/ Km^2 (by 2009). Compared to Osona, the zone contains larger cities and covers a geographical extension six times bigger. Figure 11 shows the evolution of the deployment of guifi.net in Castelló from the creation of the first node until 2013.

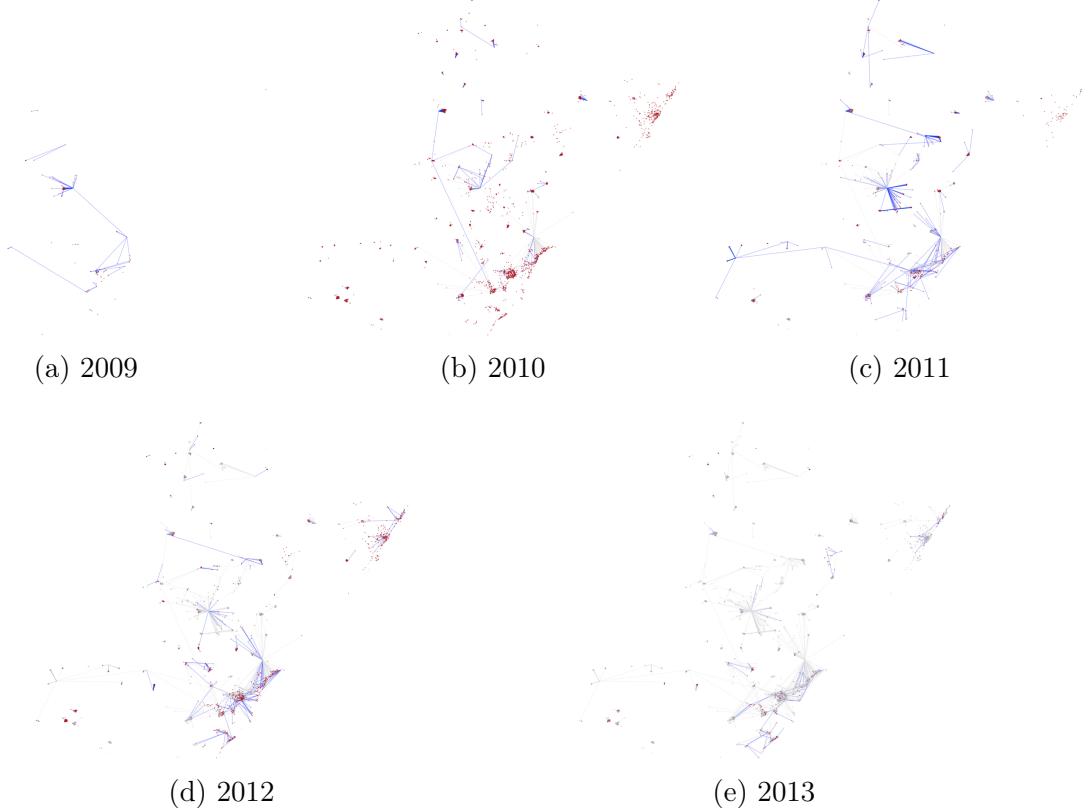


Figure 11: Evolution of the Castelló sub-network from 2006 to 2013.

The network deployment was planned to be completed in two years. During the first year, guifi.net members covered a large area by creating long-distance radio-links among the main cities and by building *supernodes* to allow connectivity to their citizens. This method is easier and cheaper in comparison with the cost and effort required for wired networks. The second year, most efforts were focused on completing a communication ring between cities, which provided an alternative for connectivity in case of a link failure. The following years, since 2011, the infrastructure has been expanded and the attention of the members has been focused on reaching isolated areas inside Castelló and improving the redundancy inside the urban cores as more members joined the network. This deployment plan highlights one of the main advantages of wireless technologies.

Barcelona (urban area, unplanned deployment). Figure 12 shows the evolution of the guifi.net network deployment in the Barcelona zone, which includes only the nodes and links deployed in the Catalan capital. The city has a total area of 101.9 Km^2 and a density of 15,991 inhabitants/ Km^2 . Given the number of potential users and the geographical area, Barcelona is considered an independent level 5 zone in the guifi.net structure. However,



Figure 12: Evolution of the Barcelona sub-network from 2006 to 2013.

compared to the previous zones, Barcelona is a very large urban area with high broadband coverage in almost every district. This fact makes it less interesting for potential users and hence, less attractive to third-party investors – like the city council. In this case, although the deployment of the network was not planned, we can still find similarities with the deployment of Castelló, as both started with the deployment of radio-links covering long distances during the first years. However, in Barcelona this was caused by the distribution of different heights of the buildings in the area.

In this section, we described three different models of growth in guifi.net, which are representative of the deployment strategies used in this community network. As stated previously, the use of one a model was highly dependent on the environmental characteristics of the deployment area (urban or rural) and the period when it took place. Planned deployments proved to be a fast way to cover large rural areas, but they required some technical knowledge and skill from the community members and also the cooperation of public entities to fund the initial expenses.

6.2. Network growth

Regardless of the geographical constrains, nodes in a network can be interconnected in many different ways and provide several degrees of redundancy. The network evolution will give us an idea of how close the real network deployment is to the static model builds in Section 5. Figure 13 shows the total amount of operative elements – nodes and links – in three level 5 zones during the period from 2004 to 2014. We can observe that nodes and links tend to grow at roughly the same speed in the whole network (Figure 13a). This is caused by the fact that when someone wants to be part of the community, the individual usually extends the network by creating a new node and connecting it to an existing one, as illustrated in Figure 14. We can also observe that the average number of links is slightly smaller than the number of networking devices. This can be explained by a behavioural pattern followed by newcomers, who focus their initial efforts on installing and registering a new node and afterwards trying to connect it to the network.

The core networks in Figure 13b, which only contain nodes with more than one link with the largest network component, show big differences between the growth rate of nodes and links after 2010 and 2011 – one year after the creation of the guifi.net Foundation. By that time, the network was mature enough and had some experienced users, which also maintained most of the core infrastructure. Therefore, it started to provide networking access and other services through their *supernodes*, increasing the number of end-users that were directly connected to the core infrastructure.

We can observe in Figure 13 that the guifi.net growth ratio was not only driven by the three individual zones studied. In order to understand such behaviour, we performed a comparison of the link and node growths with the evolution of their degrees and link distances, as shown in Figures 14 and 15. In the former figure, the solid lines represent the average node degree in each zone by the end of the year, while in the latter figure, the solid lines represent the average distance of the radio links in each zone. Both figures contain two subfigures (a) and (b), which show the differences between the entire *base-graph* and the

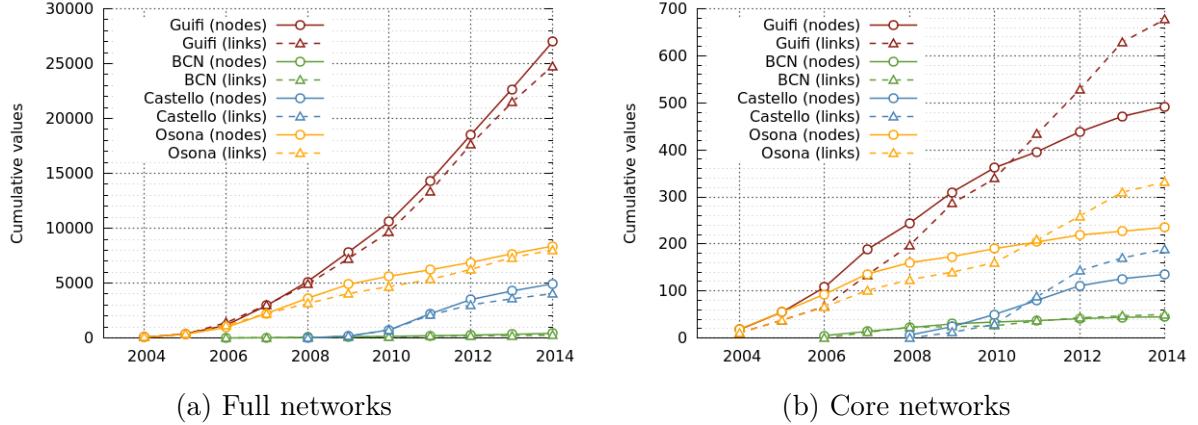


Figure 13: Growth in node and link network from 2004 to 2014.

core-graph, respectively. The bars in all the figures represent the number of nodes that the zone contains at the end of the same period.

Rural and urban zones show different degree patterns over time regardless of whether or not the topological deployment had been planned. According to the figures, it seems that during the first years the degree distribution of nodes in rural areas (e.g., Osona and Castelló) decreases with time following the power-law (Figure 14) until stabilising at a constant value. In contrast, for urban areas (e.g., Barcelona city) the degree distribution remains almost constant from the beginning at the same value that rural areas achieve in latter stages. This is because nodes in urban areas do not need to guarantee redundancy or high connectivity with core nodes (Figure 14b). These needs are covered by different means; in guifi.net, they share members' broadband connectivity using peering agreement policies with "conventional" telecommunication operators. The rate at which rural networks converge to a constant average degree is clearer in Figure 14a, which shows how fast the average degree decreases in Castelló (a large geographic area) compared to Osona (a smaller geographic area).

Differences between planned and unplanned network deployment are highlighted in Figure 15. Besides the obvious difference in scale due to the geographic area covered, what is interesting is how all three sub-networks change their tendencies in building longer or shorter links. While unplanned networks (Barcelona and Osona) maintain a constant average distance between nodes in the core network (Figure 15b), in planned ones, such as Castelló, the average distance decreases as in the power-law when most of the territory is covered. Interestingly, the growth model of unplanned networks increases the distance between links only in the last mile. We can generalize this observation and state that the deployment cost – and possibly the maintenance as well – of core networks is less expensive in unplanned networks than in planned ones. On the contrary, for the last mile, the cost is cheaper for end-users to join planned networks like "regular telecommunication networks" than unplanned ones, as in that case they will not need to build long distance links, which usually require more expensive equipment than shorter distance links.

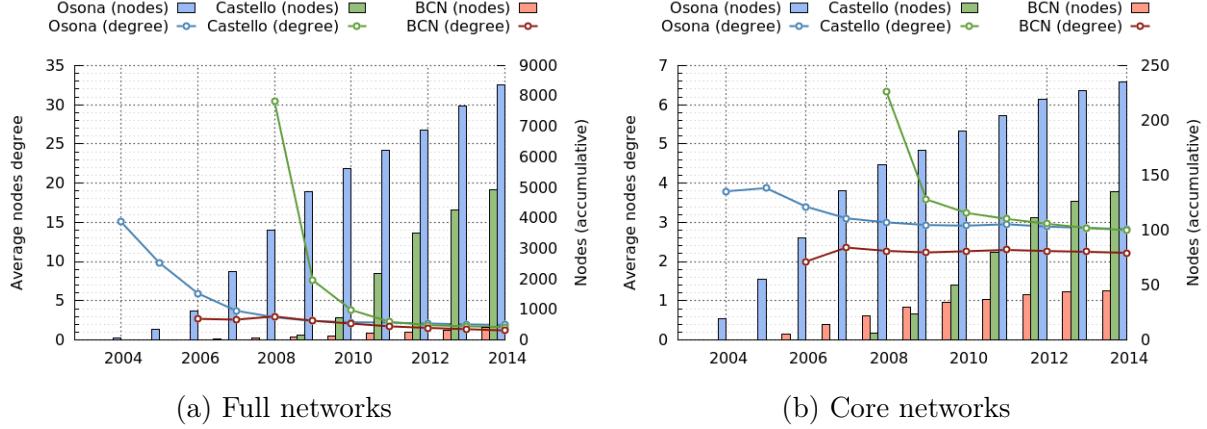


Figure 14: Growth in average node degree from 2004 to 2014.

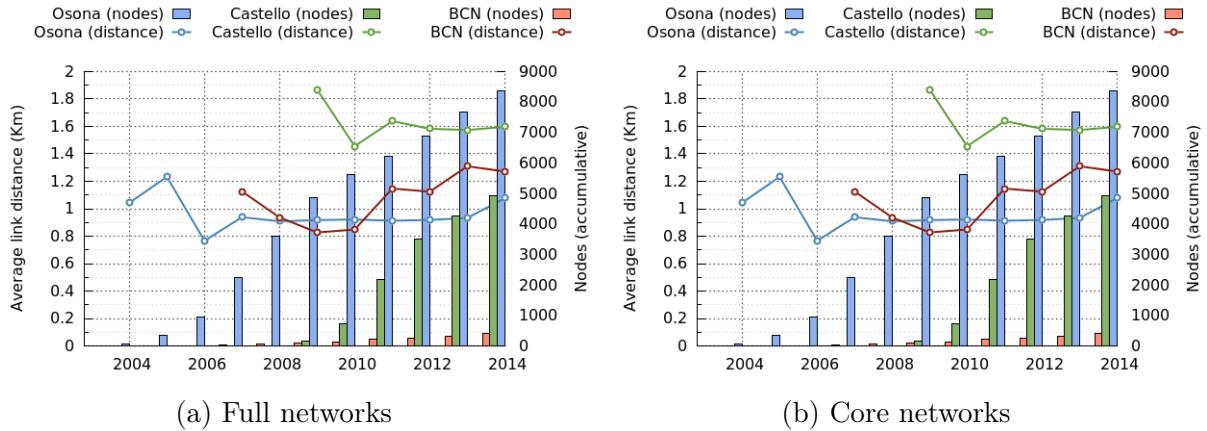


Figure 15: Growth in distance for radio links from 2004 to 2014.

In summary, we have seen three different models of deployment – unplanned and planned deployment in rural areas and unplanned deployment in urban areas. To the best of our knowledge, there is no planned deployment in urban areas in guifi.net. We think that this is caused by the lack of support by urban public administrations and the lack of interest of many citizens, resulting in more effort from the members of the community. Our conclusions were supported by opinions from several network activists [9].

7. Availability and reachability of the network nodes

One of the aspects that distinguish community networks, such as guifi.net, from regular telecommunication networks is the inherent commitment of its members to maintain their own nodes. As is the case in any social community, the knowledge and involvement of individuals can vary; therefore there are no guarantees of connectivity or quality of service. Furthermore, the quality and state of the heterogeneous hardware also influences the stability of the links and network performance. In this section, we explore this aspect by analysing

the availability and reachability of guifi.net nodes. This can be used as an indirect metric of the quality of connectivity that new members may expect from the network.

Figure 16 depicts the semi-log₁₀ Empirical Cumulative Distribution Function (ECDF) plot of the *sysUpTime* reported by the SNMP service on each base and core graph on a random day in 2013. *sysUpTime* is a Linux kernel counter timer that resets to zero every time a node is rebooted or shut down, independently of the reason that causes this. Commonly, users do not tend to deliberately reboot the device unless they have to perform an upgrade, which is not very common. Hence, the number of days reported by the *sysUpTime* is a relatively good measure of the device availability due to random failures. We also reported the last time a node had been rebooted – voluntarily or not – which gave us a direct measure of its availability.

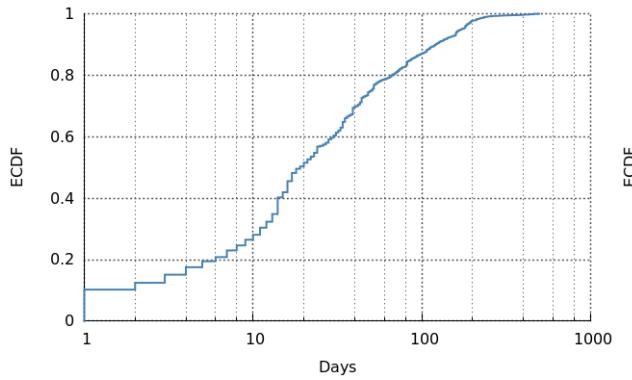


Figure 16: ECDF of node sysUptime

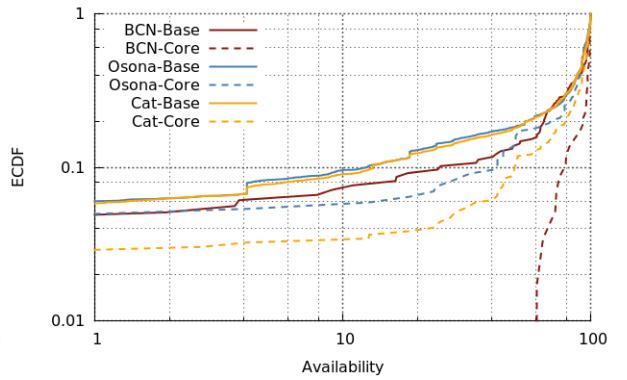


Figure 17: ECDF of node availability

There is a high number of nodes (about 10%) that have been restarted during the last day, while there are also some nodes that had not been reset for almost one year. In comparison with the uptime reported in a similar study on PlanetLab [18], a guifi.net node has a higher probability of being disconnected or not reachable from the network. The fact that PlanetLab showed a higher average *sysUpTime* on its nodes may be because it is an experimental testbed running on much more stable computers and environment.

Another significant difference between testbeds like PlanetLab and community projects like guifi.net is related to the reachability of their devices. While the former typically uses academic networks to reach the Internet and other participating networks, the wireless community networks tend to use only their own infrastructure to reach other nodes. In practical terms, this means that guifi.net members are not only responsible for the maintenance of their nodes, but also for ensuring a minimum standard of connectivity with other parts of the network. Figure 17 shows, as an example, the reachability of each node on the base and the core-graphs built as a log₁₀-log₁₀ Empirical Cumulative Distribution Function (ECDF). The reachability of a node has been calculated using the average availability of all the devices on its location. The average availability of a device is the percentage of *ping* requests that the node replies when requested by the graph-server system. As a result, Figure 17 shows the probability of a node being contacted.

The resulting analysis shows that 10% of the nodes in the base networks are reachable from the network 10% or less of the time. Numbers are even worse on the core-graph, which is supposed to be the most stable part of the network. In general, for the guifi.net core, half of the nodes have reachability of 10% or less. However, the core network of the Barcelona area is an exception because it has better reachability compared to other core networks, up to 60% in the worst case. This may be explained by the higher accessibility and proximity between nodes in such urban networks.

8. Analysis of the network resilience

In this section, we discuss the resilience of the network resulting from the topological structure built during the past years. We intentionally limit our analysis to the three level 5 zones of Barcelona, Osona, and Castelló, as analysing the entire network would result in many uncertainties. Such uncertainties would be caused by the fact that different sparse geographic zones are connected among themselves through agreements with ISPs, and we cannot infer that information from our dataset. As a result, the analysis in this section focuses on determining the resilience of guifi.net as an independent network without relying on other third-party infrastructures to support it.

Multiple definitions of robustness and resilience in the literature depend on the granularity of the study and the assumptions made. We used the *robustness coefficient* (R) proposed in [19], which provides an easy method to compare our results and to understand the robustness of a topology at the link level – or, in general, any graph – when facing continuous disconnection of its nodes. The formal definition is the following:

$$R = \frac{A_1}{A_2} = \frac{\sum_{k=0}^N kS_k}{(N/6)(N+1)(N-1)} \quad (3)$$

where N represents the number of nodes in the largest component of the network and S_k the nodes that remain connected when the first k top-ranked nodes have been removed.

Figure 18 shows the R coefficient for all three core-graphs. It has been calculated as the number of nodes that remain connected to the largest network component when top-ranked nodes are progressively being removed. On an ideal network, continuous disconnections would result in a decrease in the number of nodes connected – one unit each time a node is removed. That is, the size of the largest component decreases only due to the node that has been recently removed, while all other nodes remain part of the largest (single) component until they themselves are removed. However, in a real network, the disconnection of one node could, depending on the graph structure, disconnect more nodes from the main component. The coefficient R has been calculated as the ratio of areas, A_1 and A_2 , between the real and ideal network profile.

In scenarios with a random selection of nodes, the robustness coefficient is a good measure of the average resilience of the topology. Both, best- and worst-case scenarios can also be studied if the nodes are ranked using a structural metric. By definition, to rank nodes in the best-case scenario, we would have to disconnect, at each step, the edge-nodes of the

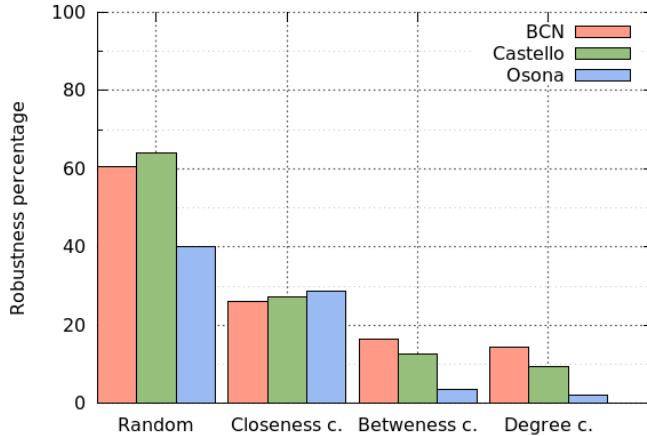


Figure 18: Network robustness coefficient R when top-ranked nodes are removed

graph, which will generate a maximum R coefficient of one. In order to analyse the worst-case scenario, we chose to disconnect nodes in terms of *degree*, *closeness*, and *betweenness centrality*.

Degree centrality is the fraction of nodes to which a particular node is connected. Nodes with a high degree centrality have a high number of connections to the rest of the network and therefore are more resilient than other nodes to random failures. *Closeness centrality* for a connected graph is defined as the inverse of the average distance to all other nodes. The *distance* for unweighted graphs is defined as the number of hops, while it is defined as the sum of weights that each link has to traverse for weighted graphs. Closeness centrality is a good measure of how efficient a particular node is in propagating information through the network. The *betweenness centrality* of a particular node n on an unweighted graph is defined as the sum of the fraction of all pairs' shortest paths that pass through n . On a weighted graph, the edge weights are taken into account. Nodes with higher betweenness centrality are part of the path used by other nodes to efficiently propagate information in the network, which makes them a critical point of failure. In our particular case, we computed these measures using an unweighted graph, which represents the connectivity pattern between devices. Weights can be added to the graph to represent traffic measurements (e.g., round trip time (RTT) and traffic congestion) but it would require a temporal analysis.

Guifi.net in Barcelona and Osona areas show the same robustness coefficient R as other autonomous systems (AS) studied in 2000 [19], when nodes are randomly disconnected. On the other hand, the topological tree-structure present in both areas makes them about 50% more resilient to coordinated attacks than the baseline networks. This feature was expected in planned networks, such as like Castelló, due to the design decisions made. However, it was not expected in Barcelona. We believe that the simultaneous development of the network in different areas of the city produced such a tree-structure. Regarding the Osona network, it still has similar robustness when nodes are ranked using the closeness centrality. This network also shows a very poor resilience in frontal sustained attacks to other central nodes. This is caused by the organic growth model described in Section 6.2, which was involuntarily

centred on the initial nodes that are now the core of the graph.

Moreover, we can observe that all networks have a very similar robustness coefficient against sustained attacks when nodes are ranked using closeness centrality. It is explained by the similarities between the assortativity in the different networks in which, regardless of the different demography, geography, and growth model, new links are usually created using the same criteria – extending the network by being connected to someone close to them.

8.1. Implications for network services

For most of their members, community networks like guifi.net are mainly a networking infrastructure to access Internet services without having to rely on traditional ISPs. The topological resilience discussion provides a baseline to compare both models, but cannot be used to generalize service resilience, as they may have different quality requirements. Web access, for example, requires users to have access to a DNS server to translate domain names into IP addresses and also a gateway (called proxy servers in guifi.net) to access the Internet.

We used a procedure very similar to the one described previously to check the robustness of the web access service in front of nodes failures. We ranked the nodes according to centrality metrics and progressively removed them from the main network component. Then, we kept track of the number of nodes that lost access to all DNS servers or to all web proxy servers.

Figure 19 compares the result of our analysis in the three zones considered, after removing up to 20 of the top nodes, according to the three criteria of centrality. The worst results were obtained in the Osona zone (Figure. 19c), which is particularly sensitive to the degree centrality and is offering key services. The figure also shows important differences between Barcelona and Castelló that were not captured in our previous experiments. In Barcelona, web access depends only on a few top nodes; therefore, the removal of a few key proxies will have a very significant impact on the service provision. In contrast, in Castelló, the result of removing any network node will have a linear impact on services. This second model appears to be more resilient to coordinated service attacks and demonstrates the advantage of planning the deployment. However, from a cost/effort perspective, given the structure of the network in Barcelona, only a few nodes will be required to ensure some degree of Internet access.

9. Related work

In this section we present a summary of previous studies on real-world wireless network deployments.

An analysis of the RoofNet network is presented in [21, 22]. RoofNet was deployed in an urban environment. The authors reported their findings on the link level characteristics of an 802.11 (2.4 GHz) mesh network. The RoofNet study focused on the link level characteristics of the deployment. In our work, we also studied the link level; however, we focused on topology patterns, and the network under consideration is a much larger network than the one presented in RoofNet. Similarly, another study presented an analysis regarding the

Table 2: Comparison of this study with prior measurement studies reported in literature.

	No. of Nodes	Typical link length	Intended usage	Architecture	Env.	Wireless technology
DGP [20]	17	Up to few tens of Km	Testbed	High gain antennas on tall towers	Rural	Single Tier 802.11 (2.4 GHz)
RoofNet [21, 22]	≈50	Mostly < 500 m	Testbed	Omni antennas on rooftops	Urban	Single Tier 802.11 (2.4 GHz)
MadMesh [23]	250	Mostly < 500 m	Commercial	Omni & dirnl. antennas on poles	Urban	Two Tier 802.11 (2.4 & 5 GHz)
Google [24, 25]	500	Mostly < 500 m Max. 9.6 Km	Private	Omni antennas on light poles	Urban	Single Tier 802.11 (2.4 GHz)
Meraki [26]	1407 (110 nets)	—	Private	—	Urban & Indoor	Single Tier 802.11 (2.4 & 5 GHz)
TFA [27, 28]	18	—	Non commercial	—	Urban	802.11b (15dBi omni.)
Funk-Feuer [29]	380 (Wien & Graz nets)	—	Community	Dirnl. antennas on rooftops and poles	Urban	Single Tier 802.11 (2.4 & 5 GHz)
Ninux [29, 30]	131	—	Community	Dirnl. antennas on rooftops and poles	Urban	Single Tier 802.11 (2.4 & 5 GHz)
AWMN [31]	2473	—	Community	Dirnl. antennas on rooftops and poles	Urban	Two Tier 802.11 (2.4 & 5 GHz)
guifi.net [4]	> 27,000	Mostly < 1 Km Max. 43 Km	Community	Dirnl. antennas on rooftops and poles	Urban & Rural	Multi Tier 802.11 (2.4 & 5 GHz)

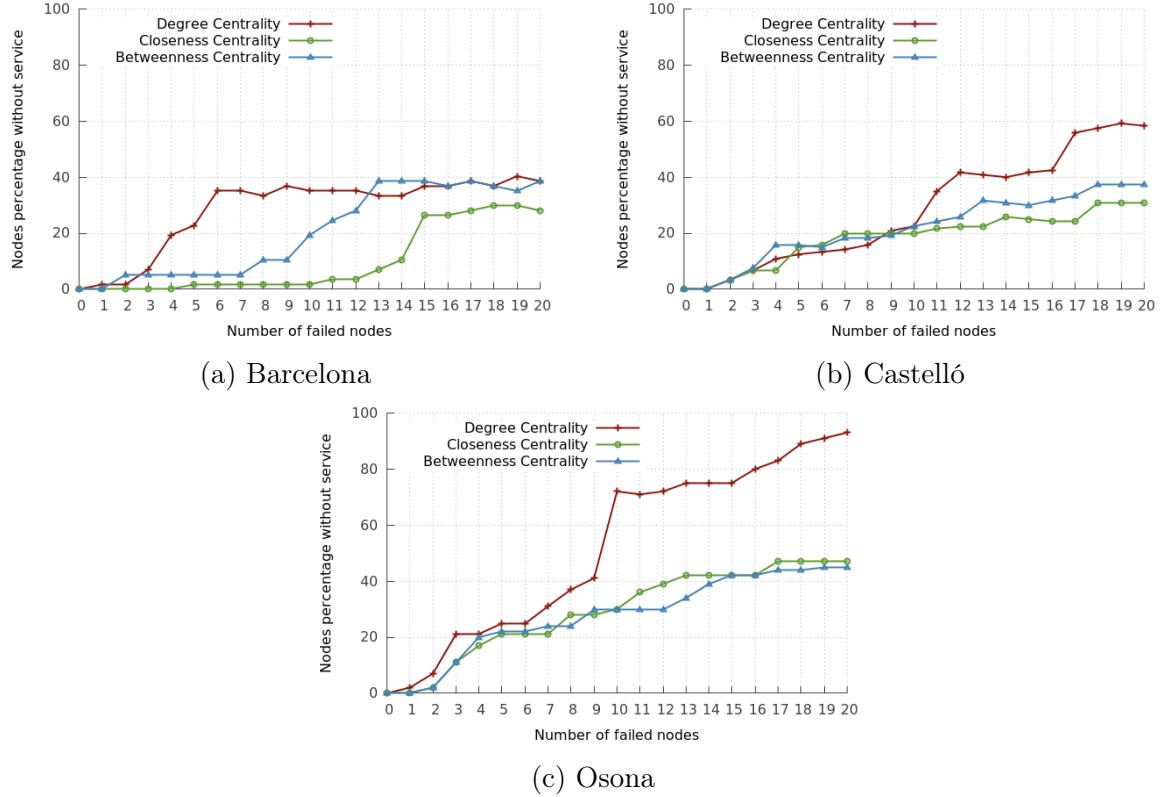


Figure 19: Ratio of nodes that do not have web access (no DNS or Proxy access) when top-ranked nodes are removed

DPG network [20], which looks at the link level characteristics of outdoor mesh networks. Nevertheless, such work can only be applied to rural settings.

It is important to note that the study that we present in this paper was performed over a real-world community network, while all the studies mentioned previously were conducted on customised testbeds, explicitly built for experimentation.

There are also some studies on wireless networks with real users instead of only experimental networks.

For example, the MadMesh network [23] reported a measurement study of such a network deployment and its planning. This deployment is a two-tier architecture and operates in both the 2.4 GHz and 5 GHz bands, while guifi.net has a multi-tier architecture and uses several network technologies. In addition, our study was conducted in a community network, while the MadMesh study was performed on a commercial mesh network.

Another interesting study is the Google Wi-Fi network presented in [24, 25]. It evaluates different aspects of a metropolitan area mesh network. It estimates the coverage properties of the Google Wi-Fi mesh network [25] and presents the usage characteristics for different user devices in the same Google Wi-Fi network [24]. This study of the Google Wi-Fi network provides a greater understanding of a metropolitan area Wi-Fi mesh. One of the main differences of this work in comparison to our study is that, due to the large size of the

network, we were able to analyse its characteristics in a variety of environments and not only in a metropolitan area. Although we only focus on the guifi.net deployment in Catalonia, the dimension of the network (over 27,000 nodes) is considerably larger than any of the networks analysed in the studies presented above.

Wireless mesh network traffic was characterised by Johnson et al. [32]. Their study focused on web traffic and the use of proxies to access Internet content in rural areas. In addition, in [33] the authors emphasised the importance of the analysis of web traffic patterns. Consequently, in our work we analysed the logs of several guifi.net proxies to study usage traffic inside the network.

One further work, a study of 110 mesh networks based on Meraki devices [26], focused on performance at the link level. They studied the impact of the SNR of a link on the bit rate for that link. They also studied the impact of an opportunistic routing protocol. Likewise, we also studied the link level but focused on topology patterns.

Finally, the community networks FunkFeuer in Wien, FunkFeuer Graz, and Rome Ninux networks have been studied in [29, 30]. These are all homogeneous mesh networks based on the Optimized Link State Routing (OLSR) ad-hoc routing protocol. These studies focused on the topological properties of the link level and the routing performance.

A complementary perspective from social sciences is presented in [34]. It looks at a rural Wi-Fi mesh network and the importance of a bottom-up or participatory design. Although the context of the study is rural Africa, the characteristics of the community, the environment, and the scale are completely different. Nevertheless, it has the same open and participatory nature as guifi.net, which demonstrates the value and effectiveness of this approach to bootstrap and grow network infrastructures.

In Table 2, we compared our research with prior related work on real-world Wi-Fi network deployments. As we can observe, our study has some unique features: a) the scale of our network is much larger in terms of the number nodes, b) the network uses several technologies for links, and c) it is open and community focused in nature.

The Guifi community network has also been studied considering the organisational [7] and social participation of its users [3]. Its crowdsourced nature, design principles, and governance as a common-pool resource infrastructure [9] have been studied. This paper complements previous works on guifi.net and focuses on technological aspects of this network.

10. Conclusions

This paper presents a technological analysis of the guifi.net community network. It was created by its participants, who pool their resources and efforts, to build and operate a local network infrastructure that is considered a common pool resource. guifi.net consists of more than 27,000 operational nodes, which makes it the world's largest community network in terms of the number of nodes and coverage area.

The principles of the network – freedom, openness and neutrality – reflect the following different aspects: 1) extensive diversity of the technological choices for hardware, wireless and optical media, link protocols, channels, routing protocols, contributing to building a common private IP network, 2) a link-level graph with a power-law degree distribution for

the local scope in the range of low-cost wireless links that reflects respect towards preferential attachment, 3) diversity in local growth patterns according to local geographic, demographic, and organisational characteristics with a complementary process of expansion, both in the geographic reach of the network core with long distance wireless or fibre links and the local growth in density with low-cost leaf nodes, 4) IP network resilience with diverse availability and reachability of network nodes in different areas according to the local choices on network planning, structure, and maturity, and 5) application level resilience for Internet or Web access against random or critical failures using of multiple application servers, DNS name servers, Internet/web gateways, and many other services spread across the network.

The guifi.net community network is the result of a loosely coupled and decentralised organic growth for more than a decade, despite the evolution of the technology and social demand. The community exhibits diverse technological and organisational choices, diverse growth, and maturity under a common community license as well as an engaged social network committed to developing its local common network infrastructure.

The analysis introduced in this paper identifies several aspects that affect the design, growth, and resilience of the network and its services. This should help in bootstrapping and developing sustainable, scalable, and effective community networks in other communities. Regions of the world that are inspired by the guifi.net example can complement other Internet models from the academic and commercial worlds. This fact could significantly contribute to the collective mission of enabling every citizen to access and participate in the digital world.

Acknowledgements

We greatly thank all the people from the guifi.net community network. There are thousands, but our special thanks go to a few who have shared not only their network but also their knowledge, wisdom, guidance, time, and smiles.

This work was partially supported by the European Community through the projects “Community Networks Testbed for the Future Internet” (CONFINE): FP7-288535, and “A Community Networking Cloud in a Box” (Clommunity): FP7-317879, and by the Spanish government under contract TIN2013-47245-C2-1-R.

References

- [1] J. Avonts, B. Braem, C. Blondia, A questionnaire based examination of community networks, in: International Conference on Wireless and Mobile Computing (WiMob), 2013, pp. 8–15. doi:[10.1109/WiMOB.2013.6673333](https://doi.org/10.1109/WiMOB.2013.6673333).
- [2] B. Braem, C. Blondia, C. Barz, H. Rogge, F. Freitag, L. Navarro, J. Bonicioli, S. Papathanasiou, P. Escrich, R. Baig Viñas, A. L. Kaplan, A. Neumann, I. Vilata i Balaguer, B. Tatum, M. Matson, A case for research with and on community networks, SIGCOMM Comput. Commun. Rev. 43 (3) (2013) 68–73. doi:[10.1145/2500098.2500108](https://doi.org/10.1145/2500098.2500108).
- [3] D. Vega, R. Meseguer, F. Freitag, Analysis of the social effort in multiplex participatory networks, in: Economics of Grids, Clouds, Systems, and Services (GECON), 2014, pp. 67–79. doi:[10.1007/978-3-319-14609-6_5](https://doi.org/10.1007/978-3-319-14609-6_5).

- [4] D. Vega, L. Cerdà-Alabern, L. Navarro, R. Meseguer, Topology patterns of a community network: Guifi.net, in: International Conference on Wireless and Mobile Computing (WiMob), 2012, pp. 612–619. doi:[10.1109/WiMOB.2012.6379139](https://doi.org/10.1109/WiMOB.2012.6379139).
- [5] L. Cerdà-Alabern, On the topology characterization of guifi.net, in: International Conference on Wireless and Mobile Computing (WiMob), 2012, pp. 389–396. doi:[10.1109/WiMOB.2012.6379103](https://doi.org/10.1109/WiMOB.2012.6379103).
- [6] Open, Free and Neutral Network Internet for everybody, <http://guifi.net/en>.
- [7] M. Oliver, J. Zuidweg, M. Batikas, Wireless commons against the digital divide, in: IEEE International Symposium on Technology and Society (ISTAS), 2010, pp. 457–465. doi:[10.1109/ISTAS.2010.5514608](https://doi.org/10.1109/ISTAS.2010.5514608).
- [8] R. Baig, R. Roca, L. Navarro, F. Freitag, Guifi.net: A network infrastructure commons, in: Proceedings of the Seventh International Conference on Information and Communication Technologies and Development, ICTD ’15, ACM, 2015, pp. 27:1–27:4. doi:[10.1145/2737856.2737900](https://doi.org/10.1145/2737856.2737900).
- [9] R. Baig, R. Roca, F. Freitag, L. Navarro, guifi.net, a crowdsourced network infrastructure held in commons, *Computer Networks, Special Issue on Crowdsourcing*.
- [10] A. Domingo, M. Van der Wee, S. Verbrugge, M. Oliver, Deployment strategies for ftth networks and their impact on the business case: A comparison of case studies, in: ITS Biennial Conference, The Net and the Internet - Emerging Markets and Policies, 2014.
URL <http://hdl.handle.net/10419/106863>
- [11] C. Chaudet, D. Dhoutaut, I. Lassous, Performance issues with ieee 802.11 in ad hoc networking, *Communications Magazine, IEEE* 43 (7) (2005) 110–116. doi:[10.1109/MCOM.2005.1470836](https://doi.org/10.1109/MCOM.2005.1470836).
- [12] R. Meseguer, E. Medina, S. F. Ochoa, J. A. Pino, A. Neyem, L. Navarro, D. Royo, Communication support for mobile collaborative work: An experimental study, *International Journal of Information Technology & Decision Making* 11 (06) (2012) 1035–1063. doi:[10.1142/S0219622012400147](https://doi.org/10.1142/S0219622012400147).
- [13] G. Castignani, L. Loiseau, N. Montavont, An evaluation of ieee 802.11 community networks deployments, in: International Conference on Information Networking (ICOIN), 2011, pp. 498–503. doi:[10.1109/ICOIN.2011.5723148](https://doi.org/10.1109/ICOIN.2011.5723148).
- [14] L. Cerdà-Alabern, A. Neumann, P. Escrich, Experimental evaluation of a wireless community mesh network, in: International Conference on Modeling, Analysis & Simulation of Wireless and Mobile Systems (MSWiM), 2013, pp. 23–30. doi:[10.1145/2507924.2507960](https://doi.org/10.1145/2507924.2507960).
- [15] A. Barabási, R. Albert, Emergence of scaling in random networks, *science* 286 (5439) (1999) 509. doi:[10.1126/science.286.5439.509](https://doi.org/10.1126/science.286.5439.509).
- [16] S. G. Colin, Fitting heavy tailed distributions: the poweRlaw package, r package version 0.20.5 (2014).
- [17] A. Clauset, C. Rohilla Shalizi, M. E. J. Newman, Power-law distributions in empirical data, *SIAM Review* 51 (4) (2009) 661–703. doi:[10.1137/070710111](https://doi.org/10.1137/070710111).
- [18] H. Verespej, J. Pasquale, A characterization of node uptime distributions in the planetlab test bed, in: International Symposium on Reliable Distributed Systems (SRDS), 2011, pp. 203–208. doi:[10.1109/SRDS.2011.32](https://doi.org/10.1109/SRDS.2011.32).
- [19] M. Piraveenan, S. Uddin, K. Chung, Measuring topological robustness of networks under sustained targeted attacks, in: International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2012, pp. 38–45. doi:[10.1109/ASONAM.2012.17](https://doi.org/10.1109/ASONAM.2012.17).
- [20] K. Chebrolu, B. Raman, S. Sen, Long-distance 802.11b links: performance measurements and experience, in: International conference on Mobile computing and networking (MobiCom), 2006, pp. 74–85. doi:[10.1145/1161089.1161099](https://doi.org/10.1145/1161089.1161099).
- [21] D. Aguayo, J. Bicket, S. Biswas, G. Judd, R. Morris, Link-level measurements from an 802.11 b mesh network, *ACM SIGCOMM Computer Communication Review* 34 (4) (2004) 121–132. doi:[10.1145/1030194.1015482](https://doi.org/10.1145/1030194.1015482).
- [22] J. Bicket, D. Aguayo, S. Biswas, R. Morris, Architecture and evaluation of an unplanned 802.11 b mesh network, in: International conference on Mobile computing and networking (MobiCom), 2005, pp. 31–42. doi:[10.1145/1080829.1080833](https://doi.org/10.1145/1080829.1080833).
- [23] V. Brik, S. Rayanchu, S. Saha, S. Sen, V. Srivastava, S. Banerjee, A measurement study of a commercial-grade urban wifi mesh, in: Internet Measurement Conference (IMC), 2008, pp. 111–124.

- [doi:10.1145/1452520.1452534](https://doi.org/10.1145/1452520.1452534).
- [24] M. Afanasyev, T. Chen, G. Voelker, A. Snoeren, Usage patterns in an urban wifi network, *IEEE/ACM Transactions on Networking* 18 (5) (2010) 1359–1372. [doi:10.1109/TNET.2010.2040087](https://doi.org/10.1109/TNET.2010.2040087).
 - [25] J. Robinson, R. Swaminathan, E. W. Knightly, Assessment of urban-scale wireless networks with a small number of measurements, in: International conference on Mobile computing and networking (MobiCom), 2008, pp. 187–198. [doi:10.1145/1409944.1409967](https://doi.org/10.1145/1409944.1409967).
 - [26] K. LaCurts, H. Balakrishnan, Measurement and analysis of real-world 802.11 mesh networks, in: Internet Measurement Conference (IMC), 2010, pp. 123–136. [doi:10.1145/1879141.1879158](https://doi.org/10.1145/1879141.1879158).
 - [27] J. Camp, J. Robinson, C. Steger, E. Knightly, Measurement driven deployment of a two-tier urban mesh access network, in: International Conference on Mobile Systems, Applications and Services (MobiSys), 2006, pp. 96–109. [doi:10.1145/1134680.1134691](https://doi.org/10.1145/1134680.1134691).
 - [28] J. Camp, V. Mancuso, O. Gurewitz, E. Knightly, A measurement study of multiplicative overhead effects in wireless networks, in: Conference on Computer Communications (INFOCOM), 2008. [doi:10.1109/INFOCOM.2008.24](https://doi.org/10.1109/INFOCOM.2008.24).
 - [29] L. Maccari, R. Lo Cigno, A week in the life of three large wireless community networks, *Ad Hoc Networks* 24, Part B (2015) 175–190. [doi:10.1016/j.adhoc.2014.07.016](https://doi.org/10.1016/j.adhoc.2014.07.016).
 - [30] L. Maccari, An analysis of the ninux wireless community network, in: International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 1–7. [doi:10.1109/WiMOB.2013.667332](https://doi.org/10.1109/WiMOB.2013.667332).
 - [31] P. Frangoudis, G. Polyzos, V. Kemerlis, Wireless community networks: an alternative approach for nomadic broadband network access, *Communications Magazine, IEEE* 49 (5) (2011) 206–213. [doi:10.1109/MCOM.2011.5762819](https://doi.org/10.1109/MCOM.2011.5762819).
 - [32] D. L. Johnson, V. Pejovic, E. M. Belding, G. van Stam, Traffic characterization and internet usage in rural africa, in: International conference companion on World wide web (WWW), 2011, pp. 493–502. [doi:10.1145/1963192.1963363](https://doi.org/10.1145/1963192.1963363).
 - [33] S. Ihm, V. S. Pai, Towards understanding modern web traffic, in: Internet Measurement Conference (IMC), 2011, pp. 295–312. [doi:10.1145/2068816.2068845](https://doi.org/10.1145/2068816.2068845).
 - [34] C. Rey-Moreno, Z. Roro, W. D. Tucker, M. J. Siya, N. J. Bidwell, J. Simo-Reigadas, Experiences, challenges and lessons from rolling out a rural wifi mesh network, in: Symposium on Computing for Development (DEV), 2013, pp. 1–10. [doi:10.1145/2442882.2442897](https://doi.org/10.1145/2442882.2442897).