

Characterizing home networks with HomeNet Profiler

Lucas DiCioccio^{†‡} Renata Teixeira^{*‡} Catherine Rosenberg[‡]
[†]Technicolor [‡]UPMC Sorbonne Universites * CNRS [‡] University of Waterloo

Technicolor Technical Report
Number: **CR-PRL-2011-09-0001**
First Publication: Sep. 2011

Abstract: This paper presents the first large-scale study of home networks. We design *HomeNet Profiler*, a tool that runs on an end-host in the home to collect data from home networks. HomeNet Profiler collects a wide range of measurements including: the set of devices, the set of services (with UPnP and Zeroconf), the home gateway configuration, and the characteristics of the WiFi environment. Since the release of HomeNet Profiler in April 2011, we have collected data on 1191 distinct homes. Our analysis leads to a number of insights on current home networks. Home networks are diverse; some home networks connect just one end device, whereas others have more than a dozen. In most home networks, however, only a small fraction of devices are powered on during our measurements. The support for UPnP and Zeroconf is still limited. We observe significant differences among the WiFi neighborhoods (i.e., the WiFi networks around a home) in different countries. The signal strength of in-home WiFi, however, is surprisingly good independently of geography.



1. INTRODUCTION

The availability of cheap broadband Internet is popularizing Internet access from home. Typical home communication and entertainment services such as phone, television, and gaming are migrating to operate over IP and users often access Internet services and applications from home. A household today can have a variety of networked devices ranging from personal devices like laptops and smart phones to printers, game consoles, and media centers. These devices connect among themselves and to the Internet via a local-area network—a *home network*. With the increase in broadband penetration, home networks are becoming an important part of the “Internet experience”. A better understanding of home network performance and configurations should enable research in a number of areas, for example: home network troubleshooting and management techniques, the design of Internet applications that perform well from home networks, and home content management and distribution.

Unfortunately, there is little data on home networks. Most previous measurement efforts have focused on residential access links [10, 14, 15]. The lack of data on home networks is partially due to the challenges of collecting home network data on a large scale. The vast majority of home networks are behind network-address translators, so a measurement point outside the home cannot measure the characteristics of the home network itself. Although it is feasible to deploy measurement points inside the homes of a few volunteers (as HomeMaestro did in the UK [13]), it is hard to argue that any small set of homes is representative. The effort necessary to recruit a large number of volunteers is a hurdle in itself.

This paper addresses this challenge with *HomeNet Profiler*, a tool to collect home network configuration and performance data¹. Users run HomeNet Profiler from an end-host directly connected to their home network. Because it runs from inside the home, HomeNet Profiler can perform a number of measurements to learn about the home network, for instance: scan the local network for the active set of network devices; query available services and devices via protocols such as Universal Plug and Play (UPnP); and measure the quality of the wireless network (if any). HomeNet Profiler incorporates a number of features to help recruit a large number of volunteers (we discuss our design decisions in more detail in Section 2). First, we implement it as a Java executable so that it works for most operating systems and network configurations. Second, HomeNet Profiler performs one-time measurements. Although continuous measurements from a single home can help understand variations in home network performance and configurations, many users feel uncomfortable downloading software in their machines and our main goal is to measure a large number of homes. Third, HomeNet Profiler generates a report to help users learn more about their home network

¹HomeNet Profiler is available in English and French from: <http://cmon.lip6.fr/hnp>.

as an incentive.

Between April and June 2011, users from 37 different countries ran HomeNet Profiler in 1191 distinct homes. We recruited these users via email and announcements on some web sites. Section 3 describes our dataset. We summarize the main findings of our analysis as follows.

- Home networks are diverse (Section 4). The total number of end devices connected to home networks varies from 1 to over 20, with low correlation to the number of people in a household. In addition, only a few of these devices are active at any given time.
- The deployment of auto-configuration protocols such as UPnP and Zeroconf is limited (Section 5). Some end-hosts and home devices have no support for these protocols. Even when devices support the protocol, some queries are not implemented correctly.
- Although we only obtain WiFi measurements in less than half of the homes, the quality of home WiFi networks is often good (Section 6). The median signal strength is -50dBm, which indicates that users are often close to their access points.

Although these findings shed new light on home networks, they are just a first step. Ultimately, our goal is to help home users diagnose problems in their home networks as well as distinguish when performance problems are caused by the home network versus the Internet access provider or beyond.

2. DESIGN

This section discusses the requirements of HomeNet Profiler, our design decisions, and implementation.

2.1 Requirements

The primary requirement for a home network data collection tool is that it **runs from inside the home**. Measurements from outside the home cannot have visibility into the home network configuration and its devices, which we want to measure. The goal of measuring a large diversity of home networks and the fact that it is not possible to collect data inside a user’s home without explicit user agreement and participation imposes additional requirements:

- **Ease of use.** The tool should be simple to run, even for users who are not tech-savvy.
- **Portability.** The tool should work for most home network and end-host configurations.
- **Respect users’ privacy.** Users are unlikely to run a measurement tool inside their homes if the tool collects information that they consider private or any personally identifiable information. In fact, our data collection effort to comply with the rules of the French National Commission of Informatics and Freedom.²

²Commission nationale de l’informatique et des libertés (CNIL): <http://www.cnil.fr/english/>.

- **Light user commitment.** We are asking home users to do us a favor by allowing us to collect data inside their homes. We cannot ask users to commit too much time or resources, otherwise only few users will participate.
- **Incentive for participation.** Some users will run research tools altruistically. However, if users can get something out of the experiment, then we are more likely to get a larger number of participants.

2.2 Design decisions

The design requirements outlined in the previous section lead to some high-level design and implementation decisions.

First, HomeNet Profiler is *end-host based*. We considered two possible measurement points inside the home: the home router or gateway; or one of the end-hosts connected to the home network. Although some home users are now deploying routers that are dedicated to measurements [19], a hardware deployment requires a higher commitment from users than a simple software download on an end-host.

Second, HomeNet Profiler runs *on demand*. While continuous measurements would give us a more complete picture of home network performance and configuration, many users feel uncomfortable installing a data collection tool that runs continuously on their machines because of the possible impact on machine performance and of privacy concerns. Inspired by the success of Netalyzr [14], HomeNet Profiler performs a series of measurements upon explicit user request. Users may run HomeNet Profiler as many times as they want.

Third, HomeNet Profiler is a *Java executable JAR*. Java facilitates the deployment of HomeNet Profiler on machines with different operating systems. Ideally, we wanted to follow the Netalyzr approach and run HomeNet Profiler from a browser as a signed Java applet. Unfortunately, some of the measurements we want to collect are not possible from an applet. It is hard to load system libraries such as the Windows Native WiFi interface from an applet and we need root access on Linux, which is not possible from an applet. Instead, a Java executable JAR can collect the datasets we want and yet it is simple for users to run because there is no installation or configuration required.

Finally, HomeNet Profiler takes *user perspective* into account with a user survey. The user survey complements our measurements. It allows us to obtain information that would be hard to infer automatically from the measurements (such as finding devices which are turned off, or telling if a user has an Internet service plan that includes VoIP and IPTV). Survey results also serve to validate the measurements.

As an incentive for users to run HomeNet Profiler, users can see a detailed report of the measurements we execute once they are finished. These reports help users learn more about their home network configuration and performance.

Before the measurements start, HomeNet Profiler lets the user select which measurements it will perform. Therefore,

users who are uncomfortable with some of the measurements we execute can still run HomeNet Profiler with a subset of the measurements. Users can also skip the survey.

System overview. We design HomeNet Profiler as a client/server application. The server hosts the HomeNet Profiler website, which users visit to run the HomeNet Profiler client. Once the client finishes loading in the user's machine, HomeNet Profiler starts in a separate window. Users then complete the survey while the measurement modules run on the background. Upon completion, the client sends all collected data to the server and redirects the browser to the report page, which is also generated and stored at the server. At the end of the measurements, HomeNet Profiler only leaves a local, randomly chosen, identifier on the user's machine to track multiple runs from the same end-host. A *run* refers to one execution of HomeNet Profiler. We refer to a computer running HomeNet Profiler as an *agent*.

Next, we describe the individual measurement modules, the design of the survey and the report, and some key implementation choices.

2.3 Measurement modules

We select a broad range of measurements to learn as much as possible about the home network. At the same time, measurements should not take too long to execute, otherwise users might give up in the middle of the experiment. Our main goal is to discover the devices connected to the home network, the protocols they support (for instance, home devices are often expected to support UPnP [20] and Zeroconf [4]), and the services they provide as well as the network technologies connecting the home to the Internet and inside the home. When the home network has WiFi, neighboring networks may also affect the home network performance. Thus, we measure the quality of all visible WiFi networks. In addition to these direct measurements of the home network configuration and performance, we collect the configuration of the machine running HomeNet Profiler as well as the list of applications installed and running on the machine. The configuration of the machine and the list of running applications help us interpret the results (in case some configuration prevents some of our measurements or some running application interferes with our measurements), whereas the list of installed applications sheds light on the applications commonly available on end-hosts (which should help the future development of an end-host tool to diagnose problems in home networks).

The HomeNet Profiler client has the following measurement modules. To address privacy concerns and comply with French laws, we anonymize all personally identifiable information using SHA1.

Device scan: searches the home network for active network devices. This module first sends UDP packets on Port 9 (i.e., the discard port) to all IP addresses in the sub-network of the agent to generate ARP requests to populate the ARP cache. We use UDP packets because sending ARP packets

directly requires root access on most operating systems. We impose a limit of 10 seconds to perform the scan to avoid long delays when sub-networks are too large. (Our measurement campaign confirms that the vast majority of scans finishes in less than 10 seconds.) After the cache is updated, this module reads the ARP cache to collect the vendor ID and the SHA1 hash of the MAC address as well as the IP address (when the IP is private) of each network interface on the LAN. If the IP address is public, we just record the presence of a public IP.

Service scan: queries two commonly-used protocols to advertise services in home electronics: Zeroconf and UPnP. We opt for querying these protocols instead of a port scan per device, because a port scan is intrusive and may take several minutes to complete. For UPnP, we package the SBBI third-party library with our JAR. We could not do the same for Zeroconf, so we use the jmdns library on MacOS and Windows and the avahi-browse script on Linux. If the end-host does not have the corresponding library, we cannot get Zeroconf results. In our tests, we also had cases where one machine in the home detected a UPnP device, whereas another machine in the same home did not. We suspect that these cases happen because the latter machine has a firewall that blocks the UPnP multicast queries. Thus, the absence of UPnP or Zeroconf services is either because no device speaks these protocols or because the end-host cannot complete the queries.

Configuration of the UPnP gateway: collects (in cases where the home gateway has UPnP) the home gateway model, the upstream connectivity type and synchronization speeds (e.g. Cable 4Mbps upload, 1Mbps download), as well as the traffic counters, which reports the number of bytes and packets transferred. Our prior work [9] showed with few examples that UPnP traffic counters are often incorrect (either there is no response or the gateway always responds with the same value). We also perform a simple test to verify whether the UPnP traffic counter is accurate: we compare the UPnP traffic counter with HomeNet Profiler's host traffic counters (e.g. `ifconfig` on Linux) before and after issuing 20 pings within a 200 ms interval.

WiFi networks: collects the list of access points found with a WiFi scan. For each access point we collect the ESSID (or the network name), the BSSID (the MAC address of the access point), the channel number, and the Received Signal Strength Indicator (RSSI). For privacy reasons, we only collect the SHA1 hash of ESSIDs and BSSIDs. We distinguish between the *in-home WiFi*, which is the one the end-host is connected to, and *neighbor WiFi*s. On MacOS, the `airport` command-line tool provides all this information. On Linux, we use `iwconfig`, which unfortunately requires sudo rights. On Windows, we use the Win32 Native WiFi API. This library is not available on old windows XP (prior to SP3), so we can only collect WiFi information for newer Windows machines. We also observed that some Linux WiFi drivers only report information for the network the end-host

is associated to.

Netalyzr [14]: performs a number of tests related to the access network configuration, security, and performance. At each execution, HomeNet Profiler downloads the latest version of Netalyzr's command-line client. Once Netalyzr finishes, HomeNet Profiler saves the report identifier. As soon as the report is available on Netalyzr's site, we parse it to extract the upload and download Internet capacity to present on the report given to the user. We also point users to the full Netalyzr report.

Computer configuration: collects the name and version of the operating system; the end-host's network configuration, including the list of DNS servers and TCP parameters; and the list of network interfaces with the corresponding IP address (if it is private, otherwise we just flag the IP as public) as well as the SHA1 hash of the MAC address and the vendor-id part of the MAC address. On MacOS and Linux we collect network configuration with the `sysconfig` tool; on Windows, we use Win32 API, which gives less detailed information.

Running applications: captures the list of processes running on the end-host as well as the list of TCP ports listening for incoming connections and open UDP ports. We also collect system services in MacOS and Windows.

Installed applications: lists the applications we find on the `PATH` environment variable. It may not reflect the full list of installed applications.

Aside from these measurements taken from the client, when HomeNet Profiler's server receives the collected measurements, it maps the client's public IP address to its geographical location and AS number using the Maxmind database. We discard the public IP address after this mapping. HomeNet Profiler also sends meta-data such as the duration of each module and whether the HomeNet Profiler process was running with sudo privileges.

2.4 Survey module

HomeNet Profiler complements and validates measurements with a user survey, which runs in parallel to the other measurement modules. We design the survey to be fast for users to complete (approximately five minutes) and easy for us to interpret the results. Hence, all questions but the last are multiple choice. The nine multiple-choice questions focus on the user (whether she is answering the survey from home, where she lives, and her level of expertise on networking), the services the user subscribes to at home (i.e., Internet plan details, the type of TV, phone, and video-on-demand service), and the types and number of devices usually connected to the home network. The free-form question allows users to give us more details about particular home network configurations or optimizations that we do not ask in the multiple-choice questions. The survey is available in French and English. Similar to the measurement modules, users can skip the survey. In particular, users who run HomeNet Profiler multiple times can fill out the survey only once.

2.5 Report design

As incentive for users to participate, HomeNet Profiler presents a report at the end of the measurements with the results (also in English and French). We focus the report on a sub-set of the measurements that should be interesting to users: the wireless quality environment, access link performance, home gateway information obtained from UPnP, and the list of active network devices and services. The report provides some advices to improve home network performance (for instance, if the user’s access point operates on a channel that is crowded, we suggest changing the channel). We also add references to websites that give more details about each of the measurements in the report. Non-expert users can learn more about home networks from these links. HomeNet Profiler’s website has an example report.

2.6 Implementation

HomeNet Profiler has two main components: the client and the server. We implement the server as a web application written in Ruby. To ensure that users can download the client, upload measurements, and see the reports without blocking on the server side, we replicate the server with eight processes: four processes handle the data collection and the other four handle the rendering of report pages (which takes longer). The data HomeNet Profiler generates is complex and may vary among clients (for example, Windows and MacOS have the concept of service, whereas Linux only has processes). As a result, we store the data in MongoDB, a more flexible schema-free database instead of a SQL database.

The HomeNet Profiler client is a Java executable JAR implemented mainly in JRuby with some Ruby and Java libraries. We package JRuby with our JAR because it is usually not installed on end user’s computers. When no Ruby or Java library exists (for instance, for doing a WiFi scan on MacOS), we parse shell scripts or wrap C libraries. Ruby’s flexibility allows us to implement measurements quickly, whereas Java brings portability and the Swing cross-platform graphical user interface. The main drawback of embedding JRuby is that the runtime library takes approximately 9 out of the 13 Mbytes in HomeNet Profiler’s JAR file. Despite the portability of Java, we had to solve a number of platform-specific issues when interfacing with low-level libraries. To help users report these problems, we added a bug-report mechanism, which uploads debug traces from the client to the server. This mechanism was particularly helpful after the larger release of HomeNet Profiler, because we do not personally know all the participants.

We ran a pilot study with a small group of students, colleagues, and friends from France, Brazil, Canada, and the United States. The purpose of this study was to test measurement modules in different homes and operating systems and to adjust the survey questions and report content before the larger release. During the pilot, testers ran HomeNet Profiler 152 times from 47 different agents. The remainder of

Module	Runs	Agents	Homes	Duration		
				5%	Median	95%
Survey	1078	1040	969	1 min.	3 min.	10 min.
Computer conf.	1640	1342	1180	< 1 s.	< 1 s.	2 s.
Installed apps.	1484	1205	1054	< 1 s.	2 s.	11 s.
Running apps.	1531	1242	1089	< 1 s.	< 1 s.	3 s.
Service scan	1630	1333	1172	10 s.	10 s.	20 s.
UPnP Gateway	1631	1339	1176	10 s.	14 s.	39 s.
Device scan	1633	1338	1173	< 1 s.	1 s.	11 s.
WiFi	1631	1335	1172	< 1 s.	10 s.	11 s.
Netalyzr	1628	1335	1173	11 s.	4 min.	6 min.
Total	1673	1354	1191	45 s.	3 min.	6 min.

Table 1: Popularity and duration of measurements.

this paper ignores all data collected on these runs.

3. MEASUREMENT CAMPAIGN

Starting on April 4 2011, we sent emails advertising HomeNet Profiler to family, friends, and colleagues as well as mailing lists of networking researchers. On April 18th, we posted an announcement on the grenouille.com website. Grenouille is a community website that tracks the performance of access ISPs in France. Until June 10 2011, 1354 unique agents ran HomeNet Profiler 1673 times. In this section, we first evaluate HomeNet Profiler—which measurement modules users chose to run and the duration of each module. Then, we describe our method to pre-process the collected data to get a single representative run per home. Finally, we summarize the data we collected from the 1191 distinct homes.

3.1 Measurement popularity and duration

We evaluate how HomeNet Profiler performs in the large-scale deployment and which measurement modules are most popular among users. Table 1 shows the total number of runs and agents that ran HomeNet Profiler and how many ran each measurement module (this table also presents the number of homes for later reference). We see that 23% of the 1354 agents skipped the user survey. The survey is the only module that requires active user participation, so it is natural that some people prefer to skip it. Besides the survey, some users are also uncomfortable with collecting of the list of running and installed applications. Interestingly, different users chose to skip different types of measurements (only in 56% of the 1673 total runs, users chose to run all measurement modules). This suggests that to attract a larger number of users, it is important to give users the flexibility to customize data collection.

Table 1 also shows the median, the 5th percentile, and the 95th percentile duration of each module. All modules run within a few seconds, except for Netalyzr and the user survey. It is natural that these two modules take longer. Netalyzr performs 92 different tests, most of them connecting to hosts that are outside the home network. The survey time depends on user participation. The median time to complete the survey is 3 minutes, which is relatively short and reflects our desire to make the survey easy and quick to answer. In

27% of the runs when users answer the survey, the background measurements complete before the survey. Thus, users get the report as soon after they finish the survey. For the majority of runs when measurements end after the survey, users only wait for a few minutes and the report comes up automatically after the results are uploaded. The median waiting time after completing the survey is 2 minutes. Overall, the duration of a run varies considerably across users, but for the vast majority of users it takes less than 6 minutes.

3.2 Data pre-processing

We face two main issues to select a single representative run per home. First, although we ask people to run HomeNet Profiler from home, some people miss or ignore this request. Thus, we need to eliminate all runs from machines that are not connected to a home network. Second, people may run HomeNet Profiler multiple times in the same home. To avoid biasing the results towards any single home, we need to identify the set of different runs from the same home network and select a single representative run per home. We do this in 3 steps.

Step 1: Identifying runs from homes.

One of the survey questions explicitly asks users whether they are running HomeNet Profiler from a machine connected to their home network. Unfortunately, users may not answer the survey or may mistakenly mark that they are at home when they are not. Users answered the survey on 1078 runs and they claimed to be at home on 963 of these runs. We develop a heuristic to identify runs from homes based on the assumption that we can label ASes as residential versus not.

Our heuristic works as follows. Every run has a corresponding AS number, which we collect at the server. For each AS number, we increment a counter when a user reports to be at home and we decrement this counter when the user reports otherwise. We then label every AS that has a strictly positive counter as residential. We say that a run is from a home if the corresponding AS is labeled as residential. When there is only one run from an AS, this heuristic will just label the run according the user’s response (if any). Our manual verification of the list of residential ASes found rare cases of mislabeled ASes (a user that claims to be at home, when connected to a research network). We manually removed these runs. Although this heuristic may misclassify some runs from small business as residential (some residential ISPs also offer services to small businesses), it will filter out ASes that only connect academic/governmental institutions and large enterprises.

Step 2: Identifying multiple runs from the same home.

The random identifier that HomeNet Profiler leaves in the user’s computer identifies multiple runs from the same machine, but users may also run HomeNet Profiler from different machines in the same home. We detect that two runs from different machines are in the same home with the results of the network scan module. If we find network inter-

Beginner	Intermediate	Expert	No Answer	Total
4 %	29 %	65 %	2 %	969

Table 2: User expertise.

Win.XP	Win.7	MacOS	Linux	Other	Total
28 %	46 %	17 %	7 %	2 %	1022

Table 3: Operating system of HomeNet Profiler agents.

faces with the same hashed MAC address in runs from different agents, we say that they are from the same home. We find 112 such network interfaces, measured by 196 different agents. Our inspection of these interfaces showed that some of them correspond to virtual machines (e.g., the vendor-id is VMware or Parallels). In some cases, we also measure the same MAC address from agents in different cities but in the same AS. Some ISPs seem to configure multiple home gateways with the same MAC address, maybe to facilitate management. To address these cases, we add an extra constraint to our filter and only consider that two runs are in the same home if they are in the same city. After applying this filter, we have 52 homes with more than one agent. For runs that skip the network scan, we consider that they come from different homes.

Step 3: Selecting one run per home.

Our analysis only considers one run per home. When there are multiple agents in a home, we select the first agent to run HomeNet Profiler. When there are multiple runs from an agent, we select the last valid run for any given analysis. For example, if an analysis only requires the results from one measurement module, we only consider the latest report for this module. When we consider reports from different modules, we take the reports from the latest run with all these modules. The selection of a single valid run per home also ensures that in case a user runs HomeNet Profiler on the same laptop in different homes, we will only study one of the home networks. After applying Step 1 and 2, we infer that our data comes from a total of 1191 distinct homes. The rest of this paper only study valid runs from these home networks. The number of homes varies for the different analysis depending on the measurement modules we study (Table 1 presents the number of homes per module).

3.3 Data description

We present some high level characteristics of users running HomeNet Profiler and their home networks.

Table 2 describes the expertise of the users answering the survey. The majority of users are self-declared experts in computer networking. This high-number of expert and intermediate users is due to our recruiting method (even the grenouille.com site is mostly read by people who are in general curious about ISP performance). Expert users are more likely to have more sophisticated home networks with the latest gadgets. This bias may be an advantage, because expert users might be some years ahead of market and the home networks we measure may be a better representation

of how most home networks will look like in the near future.

Table 3 presents the split of our agents according to the operating system of the end-host. The vast majority of end-hosts run some version of Windows, which is expected from market shares.

Users ran HomeNet Profiler from home networks in 37 countries and 167 different ASes. Table 4a shows the number of home networks and ASes we measure overall and for the top-five countries in our data. France dominates our data, mainly because of the announcement on the Grenouille website. This table shows that we obtain measurements from a fair number of different ASes in the top five countries.

When we study trends across ASes, we only consider ASes for which we have measurements from at least ten homes. Table 4b lists these ASes and the access technologies they provide as reported on their website. HomeNet Profiler’s survey includes three questions about which technologies home users have to receive phone, TV, and video on demand (VoD) at home. Table 4b includes the number of users who answered that their Internet plan includes VoIP, IPTV, or VoD service (which are commonly referred to as triple-play services). The majority of homes in French ISPs have triple-play services, but these services are not as common in other countries.

The survey also asks users to pick the type of Internet access technology they have at home from a multiple choice list. In a number of answers to this question, users claim to have cable or Ethernet, when the ISP only offers ADSL or fiber connections. Clearly, some of the questions in our survey are too technical for some users. The questions about the technology of Internet, TV, phone, and VoD access are particularly challenging. In fact, some users contacted us by email expressing concern about the answers to these questions. In the rest of this paper, we focus on the survey answers that are easier for users such as the number and types of devices they have at home.

We next analyze three aspects of our dataset: the diversity of home networks, the UPnP and Zeroconf support, and the WiFi environment.

4. DIVERSITY OF HOME NETWORKS

This section studies the diversity of home networks in terms of number and types of devices.

4.1 Number of devices

We study the diversity of home networks in terms of devices with two metrics: the number of active devices and the total number of devices.

Number of active devices. We infer the number of active devices from the results of the device scan module. The scan discovers all network interfaces that are active and currently connected to the home network, except the interface of the host running HomeNet Profiler. Hence, we add one to the number of interfaces found during the scan to get the number of devices connected to the home network. A device

could have more than one active network interface, so our results are an upper bound in the number of devices. Given that usually a device has exactly one active network interface at any given time, in most cases the number of network interfaces and devices match.

When we compute this metric for our dataset, we encounter two cases where results are inaccurate. First, virtual machines may advertise a MAC address, even though they do not correspond to a physical device. We filter out such virtual interfaces based on the Organization Unique Identifier (OUI). We remove all interfaces with OUI of virtual machine vendors (in our dataset, these are VMWare and Parallels). A total of 58 home networks has at least one virtual interface. Second, in few homes the end-host connects directly via a modem to the provider network. Thus, the sub-network we scan is not confined to the home network, but it includes part of the provider network and the neighborhood of the home. We can identify these cases, because often the IP addresses of the devices are public. When the provider uses carrier-grade network address translation (NAT), however, this technique will fail because all IP addresses are private. Fortunately, in this case, operators deploy ARP proxies to prevent flooding the network with ARP requests. The proxy will answer all ARP requests for a given home. We filter out homes where the ratio of the number of unique IP addresses per MAC address is larger than 10 (to handle cases with NATs) or lower than 0.1 (to handle the other cases). We discarded 28 runs where the end-host was directly connected to the provider network.

Total number of devices. Some devices may not be active at the time HomeNet Profiler runs, for instance people often leave their printers off when they are not using it. We estimate the total number of devices that belong to the home network from the answers to the user survey. We explicitly ask users to report the number of devices of each type that usually connect to their home network. This question only asks about end devices such as printers, laptops, or desktops. We do not explicitly ask about networking equipment such as routers or WiFi access points. Hence, we add one to the total number of devices users report to account for the home gateway to be able to compare this value with the number of active devices. Note that even if the home has a modem plus an access point, the device scan module will only measure one of these devices. Although users may forget some devices or mistype the number of a given device, we expect most users to answer this question correctly.

Results. Figure 1 shows the cumulative distribution of the number of active devices and the total number of devices across all homes. The total number of devices per home ranges between 2 and 28. This wide range shows that the number of devices that connect to a home network in a regular basis varies considerably among different home networks. The range of the number of active devices, however, is smaller than that of the total number of devices. Approximately 80% of homes have at most four active devices dur-

Country	Homes	AS
France	795	28
United States	113	37
Italy	49	5
Brazil	45	9
Canada	42	10
Overall	1191	167

(a) Homes and ASes per country.

AS Name	Country	Access Technology	Triple play			Homes
			TV	VOD	VoIP	
Free	France	ADSL / Fiber	218	143	298	386
France Telecom	France	ADSL / Fiber	45	41	78	139
Numericable	France	Cable / Fiber	14	19	53	95
Neuf Cegetel	France	ADSL / Fiber	34	27	39	76
Bouygues Telecom	France	ADSL / Fiber	17	15	32	46
Telecom Italia	Italy	ADSL	2	1	2	23
Oi Velox	Brazil	ADSL	0	0	1	17
Cegetel	France	ADSL	8	3	11	17
Verizon	United States	ADSL / Fiber	5	6	4	16
Rogers	Canada	Cable	0	0	1	13
AT&T	United States	ADSL / Fiber	2	1	0	12
Comcast	United States	Cable	1	1	2	11
GVT	Brazil	ADSL / Fiber	1	0	1	11

(b) Top ASes.

Table 4: Characteristics of the data collected with HomeNet Profiler between April and June 2011.

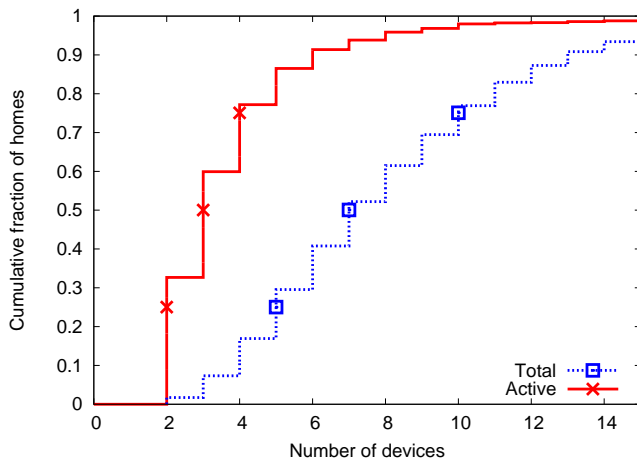


Figure 1: Number of active devices versus the total number of devices per home.

ing our tests and 30% have exactly two devices. The minimum number of active devices is two, which corresponds to the machine running HomeNet Profiler and the home gateway. In general, the number of active devices in home networks is small. Only 22 homes have more than ten active devices during our measurements. These results are similar across countries (not shown). We only find some minor differences. In particular, home networks in Italy and Brazil usually have fewer devices (both active and total) than home networks in North America and France.

The difference between the total number of devices and the number of active devices is large for all countries. The number of total devices only matches the number of active devices for 10% of the homes. This difference happens because home networks often have inactive devices. Users turn some devices off when they are not in use (for example, printers, media servers, or televisions). Moreover, some devices are mobile and may not be inside the home at all times (for example, smartphones or laptops).

One explanation for the wide range in the number of total devices in home networks may be the number of people living in each household. One of the survey questions asks the number of people in the household. We have 469 answers to

this question. We use the Pearson correlation coefficient to study the correlation between the number of devices present and the size of the household. This coefficient is only 0.31. Some devices such as home gateways and printers serve all members of a household, irrespective of the number of people. Thus, we also compute the correlation between the number of reported laptops and desktops and the size of a household. Even though the correlation coefficient is 0.38 in this case, it is still low. The correlation is even lower (only 0.12) when considering the number of active devices. Thus, the number of people in a household has only a small impact on determining the number of devices connected to home networks.

Takeaway. The total number of devices that connect to home networks varies considerably across homes, but the number of devices that is active at any given time is small.

4.2 Types of devices

We now investigate the diversity of home networks according to the types of devices. HomeNet Profiler has two mechanisms to identify the types of devices. First, the survey asks users the number of devices of each type. Second, the device scan stores the OUI of each device, which can give some indications on the type of device (for example, Linksys makes WiFi access points).

Results. Table 5 presents the percentage of homes with each type of device considering the answers to the user survey; the last column presents the total number of homes with answers to this question. We only show devices that appear in at least 30% of homes overall. As expected, desktops and laptops are the most popular devices. Interestingly, laptops are consistently more popular than desktops. Smartphones are also popular across all countries (more than half of the homes have at least one smartphone). These numbers reflect market trends. Tablets, however, are not yet popular. Only 14% of homes have a tablet. The percentages of users with IP phones and TVs are much higher in France than in other countries. Given that most French ISPs offer triple-play services, we conjecture that these users got confused when answering the question. They declare to have an IP

Country	Desktop	Laptop	Smartphone	Printer	Console	Phone	TV	Homes
France	85%	87%	57%	49%	38%	61%	41%	594
United States	72%	90%	71%	45%	43%	20%	18%	87
Brazil	77%	97%	52%	20%	27%	7%	2%	40
Italy	79%	97%	64%	38%	35%	10%	10%	39
Canada	82%	94%	51%	60%	22%	17%	5%	35
Overall	81%	90%	60%	46%	36%	46%	31%	903

Table 5: Types of devices based on the survey.

phone when in fact their provider delivers VoIP to a regular phone (similarly, for TV). We also observe more printers in Canada and more gaming consoles in the United States.

We also study the vendor for all devices that are active during the device scan measurements using the OUI. Table 6 shows the three most frequent device vendors for every AS with more than ten homes (the last column shows the total number of homes with these measurements). The numbers in parenthesis are the percentage of homes with at least one active device from a given vendor.

Given that the scan only measures active devices, it is natural that the most common device vendors are home gateways and WiFi access points vendors. We see a clear correlation between some equipments and the AS. For example, the Freebox is the home gateway of Free, and hence we only see it in home networks that subscribe to Free (similarly, for Pirelli in Telecom Italia’s network and Actiontec in Verizon’s). In these cases, the home gateway comes with the subscription to the Internet access service. Other popular vendors are standard WiFi access point vendors such as D-Link, Linksys, and Netgear. These vendors are present in almost all countries. Apple is popular both in AT&T and in Comcast. Apple makes access points, computers, smartphones, and tablets. We cannot distinguish these different types of devices from the vendor OUI alone. Overall, no vendor dominates the market. The device vendors that we observe in home networks are fairly diverse.

Takeaway. The types of devices that people connect to their home networks are similar, with some pointed differences among countries. When we study the small set of devices that are active during our measurements, however, we find that device vendors are diverse. In particular, home gateways are often determined by the ISP.

5. UPnP AND ZEROCONF SUPPORT

This section studies the typical services that home devices provide via UPnP and Zeroconf protocol. Then, we focus on how widely home gateways support UPnP.

5.1 Types of services

This section characterizes the types of services available in home networks. Although users may access some devices directly (for instance, access a printer via its USB port), we only focus on services that are available via the home network. HomeNet Profiler collects the list of services advertised via both UPnP and Zeroconf.

Rank	Zeroconf	UPnP
1	Apple File Sharing (47%)	InternetGateway (80%)
2	SMB (38%)	MediaServer (45%)
3	HTTP (32%)	WiFi Device (10%)
4	SSH (31%)	MediaRenderer (5%)
5	SFTP (31%)	Printer (3%)
6	Sleep Proxy (28%)	SetTopBox (3%)
7	Remote Frame Buffer (28%)	Basic (1%)
8	IPP (26%)	WiNAS (1%)
9	Airport (23%)	RemoteUI (<1%)
10	DAAP (20%)	MessageReceiver (<1%)
Homes	234	581

Table 7: Most frequent Zeroconf and UPnP services.

Results. We have 1172 reports from distinct homes for the service scan module. We find devices that advertise UPnP services in 581 homes and Zeroconf services in 234 homes. The number of homes with at least one Zeroconf device is low, because we could not find the Zeroconf library in 841 homes (mainly on Windows machines). In the remaining 97 homes, HomeNet Profiler found no Zeroconf services in the home network. Although we ship the UPnP library with HomeNet Profiler, there are some cases where we cannot find UPnP-enable devices, because the configuration of the end host blocks the queries (as discussed in Section 2.3). Moreover, in the service scan module we use the UPnP wildcard query to find any UPnP service available. Some devices may implement UPnP, but not answer the wildcard queries as we see in the next section.

Irrespective of the cause, the fact that we can only discover the available services automatically with UPnP in approximately 50% of the homes and in less than 25% of homes for Zeroconf shows that the adoption of these services is moving slowly. For the automatic discovery and configuration of services to work both the device offering the service and the end-host have to support the protocol. In all the cases where we have no UPnP nor Zeroconf, we can safely infer that the particular end-host we measured from would not be able to access these services.

Next, we characterize the types of UPnP and Zeroconf services we find for the homes where our measurements were successful. We find 159 different services via Zeroconf and only 25 via UPnP. Table 7 presents the top-ten UPnP and Zeroconf services. Many popular Zeroconf services are specific to Apple (for example, Apple File Sharing, Sleep Proxy, and Airport). This result is not surprising because Apple started Zeroconf. Other popular Zeroconf services are remote access services (SSH and Remote Frame Buffer) and services to share printers (IPP) or files (SMB, SFTP, and DAAP). HTTP is also used for sharing personal web pages in

AS	Most popular vendors			Homes
Free	Freebox (83%)	Apple (10%)	Asustek (9%)	366
France Telecom	Sagem (71%)	HP (11%)	Apple (10%)	138
Numericable	Netgear (51%)	Broadcom (24%)	Hon Hai (13%)	90
Neuf Cegetel	SFR (82%)	Netgem (29%)	Netgear (12%)	74
Bouygues Telecom	Sagem (60%)	Thomson (34%)	Unknown (26%)	46
Telecom Italia	Pirelli (36%)	Asustek (13%)	Linksys (9%)	22
Cegetel	SFR (66%)	Netgem (22%)	Tecom (11%)	18
Oi Velox	D-Link (41%)	Linksys (35%)	TP-Link (11%)	17
Verizon	Actiontec (66%)	Motorola (33%)	Apple (33%)	15
Rogers	Linksys (53%)	D-Link (23%)	HP (15%)	13
AT&T	Apple (50%)	2Wire (41%)	Netgear (33%)	12
Comcast	Apple (63%)	Linksys (36%)	VMWare (27%)	11
GVT	D-Link (36%)	TP-Link (27%)	Apple (18%)	11

Table 6: Most frequent device vendors found in device scan.

MacOS.³ UPnP is mainly used for advertising devices such as Internet gateways, media servers, and WiFi access points.

Takeaway. End-hosts today cannot rely on UPnP or Zeroconf for automatic service discovery. Only a small fraction of end-hosts running HomeNet Profiler were able to query UPnP and Zeroconf services. When available, these protocols are mainly used for file sharing, configuring network equipment, and printing.

5.2 UPnP at home gateways

Home gateways are the connection point between the home network and the Internet. They are also central to the connectivity of devices inside the home. UPnP-enabled gateways allow home devices to auto-configure their network settings. We study the fraction of home gateways that respond to UPnP queries and how accurately they answer to these queries.

Results. Out of the 1176 homes where users run the measurement module to extract the configuration of the UPnP gateway, we find 632 homes where the gateway answers to UPnP queries. This number is higher than the number of homes with UPnP services (in the previous section), because here we query directly for gateway services, whereas in the previous section wildcard queries are used. Some home gateways (51 in our measurements) implement the UPnP protocol but do not answer wildcard queries. Home devices can only communicate with these gateways via UPnP if they explicitly query for an Internet gateway.

We can infer which vendors implement UPnP with the results from the device scan module. We infer that a device is the home gateway from its IP address and OUI. In total, we find 103 distinct gateway vendors (note that some companies make home gateways under different brands). For 53 of these vendors we find at least one gateway that answers to UPnP queries. Not all gateways of the same vendor support UPnP. These cases can correspond to runs for which the end-host blocks our queries, devices on which the user or the ISP have disabled UPnP (or simply have not enabled it if UPnP is not on by default), or instances when vendors only implement UPnP in some of their gateway models. UPnP queries

can also retrieve the gateway model name and firmware version. We find 117 distinct gateway models.

UPnP provides one query that returns the traffic counters (i.e., the number of bytes and packets transferred). This counter, if available and implemented correctly, could be used by end-host based diagnosis tools to infer cross-traffic from the home network. In all homes for which we find an UPnP gateway, we perform a test to verify whether the traffic counter is consistent (as discussed in Section 2). More than half of the UPnP gateways in our measurements (exactly 327 gateways) always return a fixed value for this query, which indicates that traffic counters are often hardcoded. As a result, home devices cannot completely trust this query to infer traffic in the home.

Takeaway. Home devices cannot fully rely on UPnP to discover the home gateway and infer properties of home traffic. The completeness and correctness of the UPnP implementation depends on the home gateway models.

6. WIFI ENVIRONMENT

WiFi is becoming the preferred way to connect home devices. This section studies the number of WiFi networks we measure, their channel usage, and signal strength.

6.1 Number of WiFi networks

HomeNet Profiler collects WiFi measurements from 463 individual homes. This number is surprisingly small compared to the 1172 runs of the WiFi measurement module for three main reasons. First, we only find 642 homes where the end-host has a WiFi interface. Second, among these homes, the WiFi was only active in 515 end-hosts. Finally, in 40 of the homes with an active WiFi interface the end-hosts ran Windows XP or Windows 2003, for which the native WiFi library may not be available.

Fortunately, each HomeNet Profiler client may detect several WiFi networks, i.e., the network the end-host is associated to as well as neighbor networks. Hence, we can study a much larger number of WiFi networks. We identify a WiFi network by a pair BSSID (the access point) and ESSID (the WiFi network). HomeNet Profiler measures 3951 BSSID-ESSID pairs (an average of 8 per home), 3944 of them had

³<http://docs.info.apple.com/article.html?path=Mac/10.5/en/8236.html>

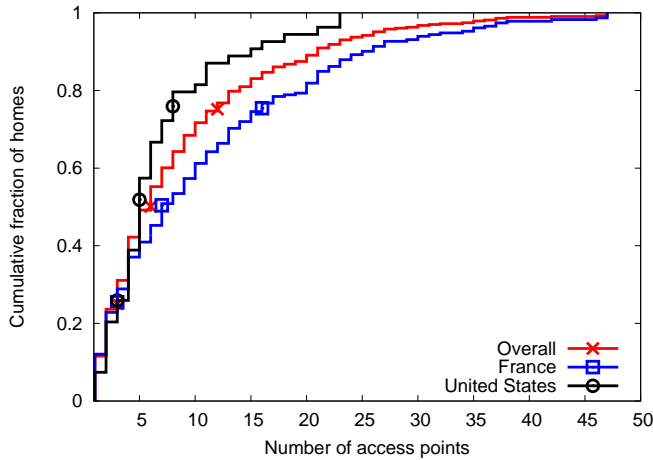


Figure 2: Density of WiFi neighborhood.

channel information. We discard the rare cases when we have no channel data.

Overall, we found 3611 unique access points (or BSSIDs). This number is lower than the total number of BSSID-ESSID pairs, because some WiFi access points advertise more than one WiFi network. Some home users configure two separate WiFi networks in the same access point to separate guest users from home users or to share their access point with a WiFi community (such as Fon). We find only 2480 unique ESSIDs, which implies that many WiFi networks have the same name. Although we do not collect plain ESSIDs, we test the SHA1 for “FreeWifi”, which is the WiFi community of Free, and find that 216 different access points broadcast this ESSID. In addition, out of the 964 users who answered our question on whether they open their WiFi to a community, 273 said yes. WiFi communities are becoming popular (at least in France).

Takeaway. Although we obtain WiFi measurements from less than half of the homes (which seems surprisingly low), we can measure a large number of neighbor WiFi networks per home.

6.2 WiFi neighborhood

We study *neighbor access points* by selecting one ESSID per BSSID for each home (i.e., the same BSSID can appear multiple times if we measure two homes in the same neighborhood).

Results. Figure 2 plots the cumulative distribution of the number of neighbor WiFi access points per home. Overall, homes may be surrounded by several WiFi access points. The 95th percentile of WiFi access points is 26 overall, 34 in France, and 21 in the United States.

Almost all WiFi access points we detect operate in the 2.4 GHz band. In the United States, 5% of the access points are in the 5 GHz band, whereas this percentage is less than 2% in all other countries. Either only few access points operate on this band, or the WiFi adapters of the end-hosts cannot scan this band. In any case, these results indicate that 5 GHz

Country	Channel						Total
	1	2 – 5	6	7 – 10	11	12 – 14	
France	18%	6%	17%	9%	40%	6%	2547
United States	26%	11%	27%	7%	28%	0%	360
Canada	14%	14%	26%	15%	28%	0%	209
Brazil	20%	6%	37%	13%	20%	1%	145
Italy	37%	3%	26%	4%	27%	2%	96
Overall	20%	7%	20%	9%	35%	5%	3864

Table 8: Percentage of neighbor access points on each channel for the 2.4 GHz band.

WiFi access is not yet widespread. The rest of this section focuses on the 2.4 GHz band. There are only three non-overlapping channels on the 2.4 GHz band. Hence, when there are more than three access points operating on the 2.4 GHz band in a neighborhood, the WiFi may experience some interference. In our measurements, more than 70% of the homes have more than three neighbor WiFi.

We omit results for other countries from Figure 2 for readability, but we do find some differences. The median number of neighboring WiFi access points in French homes is 7, whereas it is 6 in Canada, 5 in the United States, 5 in Brazil, and 4 in Italy. Many reasons could explain these geographical trends: in France, residential ISPs often provide a WiFi-enabled gateway to their users. Also, French cities are often densely populated. Nevertheless, population densities do not explain why Italy ranks lower. Maybe residential ISPs in Italy do not often provide WiFi-enabled gateways.

Table 8 presents the percentage of access points on each channel in the 2.4 GHz band. Channels 1, 6, and 11 are the non-overlapping channels in the 2.4 GHz band and hence are recommended for use. We merge other (overlapping) channels for the 2.4 GHz band (i.e., up to channel 14) into ranges. Interestingly, a large fraction of the neighbor WiFi access points (with the exception of Italy) operate on overlapping channels, which is usually not recommended. Finally, we notice a predominance of access points on channel 11 in France. Our analysis of the vendors of these access points shows that most Free and SFR’s WiFi access points are connected to channel 11.

When we compare the channel selected by the in-home access point to other channels in the neighborhood, we find that 26% of the homes would benefit from switching to another channel—either because the access point is on an overlapping channel or it is on a non-overlapping channel with too many WiFi neighbors.

Takeaway. WiFi neighbourhoods can be crowded and channel selection can be biased in certain locations.

6.3 Received Signal Strength

Along with the channel information, HomeNet Profiler stores the RSSI of each BSSID-ESSID pair.

Results. Figure 3 plots the RSSI of all the neighbor WiFi access points and of the home WiFi network. Although these values are measured by the WiFi adapter and hence can be uncalibrated, the RSSI is an indication of the reception power at the computer running HomeNet Profiler. The

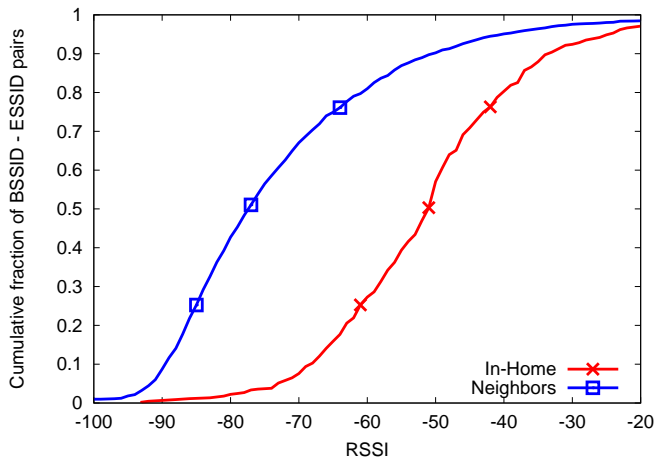


Figure 3: WiFi signal strength of in-home versus neighbor ESSID-BSSID pairs.

higher the RSSI, the better the WiFi reception. WiFi reception at home is good: half of the users get an RSSI of at least -51 dBm. The median RSSI for neighbor WiFi access points is -77 dBm, which is much lower than the home WiFi signal. We expected that places like North America with larger homes would get lower WiFi quality. However, our results indicate that the RSSI distribution of the different countries are similar (not shown). These results indicate that the interference with neighbor networks is probably manageable. Nevertheless, 20% of the neighbor BSSID-ESSID pairs have an RSSI above -60 dBm. Moreover, in 44% of the homes, we find that the end-host running HomeNet Profiler detects a neighbor WiFi access point with a better RSSI than the home access point. A WiFi network with a stronger RSSI only interferes with the home WiFi if the two channels overlap. The percentage of homes with a stronger neighbor signal with overlapping channels is 35% and for the same channel is 33%.

Takeaway. WiFi reception is overall good in home networks, but a significant fraction of end-hosts receive at least one neighbor WiFi with a better signal than the home WiFi.

7. RELATED WORK

The interest in home networks has increased in the last few years with the spread of broadband Internet access. We divide the prior work into studies of residential Internet access, which are often large-scale; studies of the home network and its utilization, which often focus on a few homes; and studies of WiFi performance. HomeNet Profiler is the first tool to measure and characterize a broad set of properties from inside a large number of homes.

Access networks. Most prior work has focused on measuring and characterizing residential Internet access from different vantage points: servers connected to the Internet [8, 10], traffic traces collected passively at residential ISPs [15, 18], or inside the home [7, 11, 12, 14, 19]. Vantage points outside the home cannot directly measure devices connected to the home network as we do in this paper. One

study of NAT behavior inferred that 50% of the homes have more than one host [16]. Our study confirms this result and sheds new light on the diversity of devices in home networks.

HomeNet Profiler is inspired by the recent success of research tools to reach a large number of users, many of them at homes [7, 11, 14, 19]. So far, all these studies have focused on access link performance or security issues, not on home network configuration. HomeNet Profiler complements these studies. In fact, we include Netalyzr [14] as a measurement module to later correlate end-to-end performance with home network configuration.

Home networks. Both the networking and HCI research communities acknowledge that home networks are becoming complex and that we need to develop better tools to assist users in managing and troubleshooting home networks [1, 3, 5, 6, 9, 13, 21]. Most studies are developing management and troubleshooting techniques based on detailed data from a few homes and having a close relationship with home users [5, 6, 13]. These studies track the performance and utilization of home networks much closer than we do, but it is hard to know whether the particular homes they measure are representative. The data we collect with HomeNet Profiler and the results presented in this paper should inform the selection of home networks for future studies and the design of management and diagnosis tools for home networks.

WiFi networks. The performance of WiFi networks has received considerable attention in the literature. Closest to our goal of characterizing WiFi in the home is the work by Papagiannaki et al [17]. Their measurements from a testbed of six nodes inside three homes showed that even though home WiFi networks are small, the connectivity is not guaranteed to be good everywhere. In contrast, we study the quality of in-home WiFi with a single measurement from the user’s machine for hundreds of homes. Our results show that most often end-hosts connect with good signal strength. Our result on the number of WiFi neighbors per home is consistent with results from a study of data collected wardriving in some cities in the United States in 2007 [2]. Interestingly, at the time of their study many access points in the United States operated on channel 6, which is no longer the case in our measurements.

8. IMPLICATIONS

HomeNet Profiler gave us a first look inside over a thousand home networks. We now briefly discuss the implications of our findings. First, the diversity of home networks implies that any tool designed for the home has to adapt to a multiplicity of environments. Our results also suggest that building models of the number of devices in a home network is not a simple extrapolation of the number of people in a household. The fact that devices are often powered off also has implications for management and troubleshooting tools, because the home network configuration is often changing. Second, we showed that protocols that were built to help configure and monitor home networks have limited support

from current devices. Hence, although UPnP and Zeroconf can help managing home networks, tools that plan to use these protocols should test for their presence and accuracy beforehand. Finally, our study of WiFi indicates that there is still room for improving channel selection mechanisms.

9. REFERENCES

- [1] B. Aggarwal, R. Bhagwan, T. Das, S. Eswaran, V. N. Padmanabhan, and G. M. Voelker. NetPrints: Diagnosing Home Network Misconfigurations Using Shared Knowledge. In *Proc. NSDI*, Apr 2009.
- [2] A. Akella, G. Judd, S. Seshan, and P. Steenkiste. Self Management in Chaotic Wireless Deployments. *Wireless Networks Journal (WINET), Special Issue on Selected Papers from MobiCom 2005*, 13(6):737–755, Dec 2007.
- [3] K. L. Calvert, W. K. Edwards, N. Feamster, R. E. Grinter, Y. Deng, and X. Zhou. Instrumenting Home Networks. In *ACM SIGCOMM workshop on Home networks*, Aug 2010.
- [4] S. Chesire. Zero Configuration Networking. <http://www.zeroconf.org/>.
- [5] M. Chetty, R. Banks, R. Harper, T. Regan, A. Sellen, C. Gkantsidis, T. Karagiannis, and P. Key. Who’s Hogging The Bandwidth?: The Consequences Of Revealing The Invisible In The Home. In *Proc. ACM CHI*, May 2010.
- [6] M. Chetty, D. Halsem, A. Baird, U. Ofoha, B. Summer, and R. E. Grinter. Why Is My Internet Slow?: Making Network Speeds Visible. In *Proc. ACM CHI*, May 2011.
- [7] D. R. Choffnes, F. E. Bustamante, and Z. Ge. Crowdsourcing Service-Level Network Event Monitoring. In *Proc. ACM SIGCOMM*, Aug 2010.
- [8] D. Croce, T. En-Najjary, G. Urvoy-Keller, and E. Biersack. Capacity Estimation of ADSL links. In *Proc. CoNEXT*, Dec 2008.
- [9] L. DiCioccio, R. Teixeira, and C. Rosenberg. Impact of Home Networks on End-to-End Performance: Controlled Experiments. In *ACM SIGCOMM workshop on Home networks*, Aug 2010.
- [10] M. Dischinger, A. Haeberlen, K. P. Gummadi, and S. Saroiu. Characterizing Residential Broadband Networks. In *Proc. IMC*, Oct 2007.
- [11] Grenouille. Grenouille. <http://www.grenouille.com/>.
- [12] D. Han, A. Agarwala, D. G. Andersen, M. Kaminsky, K. Papagiannaki, and S. Seshan. Mark-and-Sweep: Getting the Inside Scoop on Neighborhood Networks. In *Proc. IMC*, Oct 2008.
- [13] T. Karagiannis, E. Athanasopoulos, C. Gkantsidis, and P. Key. HomeMaestro: Order from Chaos in Home Networks. Technical Report MSR-TR-2008-84, MSR, Redmond, WA, USA, May 2008.
- [14] C. Kreibich, N. Weaver, B. Nechaev, and V. Paxson. Netylizr: Illuminating the Edge Network. In *Proc. IMC*, Oct 2010.
- [15] G. Maier, A. Feldmann, V. Paxson, and M. Allman. On Dominant Characteristics of Residential Broadband Internet Traffic. In *Proc. IMC*, Oct 2009.
- [16] G. Maier, F. Schneider, and A. Feldmann. NAT Usage in Residential Broadband Networks. In *Proc. IMC*, Oct 2011.
- [17] K. Papagiannaki, M. Yarvis, and W. S. Conner. Experimental Characterization of Home Wireless Networks and Design Implications. In *Proc. IEEE INFOCOM*, Apr 2006.
- [18] M. Siekkinen, D. Collange, G. Urvoy-Keller, and E. Biersack. Performance Limitations of ADSL Users: A Case Study. In *Proc. PAM*, Apr 2007.
- [19] S. Sundaresan, W. de Donato, N. Feamster, R. Teixeira, S. Crawford, and A. Pescapè. Broadband Internet Performance: A View From the Gateway. In *Proc. ACM SIGCOMM*, Aug 2011.
- [20] UPnP Forums. UPnP Specifications. <http://www.upnp.org/>.
- [21] J. Yang and W. K. Edwards. A Study on Network Management Tools of Householders. In *ACM SIGCOMM workshop on Home networks*, Aug 2010.