Wi-Fi Deployment in Dublin: A Twenty Year Comparison

David Malone
Hamilton Inst./Dept. of Mathematics and Statistics
Maynooth University, Ireland.

Niall R. Murphy
CEO
Stanza Systems

Ken R. Duffy
Hamilton Institute
Maynooth University, Ireland

***Abstract*—We will present the results of two Wi-Fi surveys conducted in Dublin in 2002 and 2022. We will describe the methods used for the surveys and the results, highlighting changes in tools, technology and uptake. We see an increase of over five hundred times in the level of observed deployment.**

***Index Terms*—Wi-Fi, IEEE 802.11, network measurement**

I. Introduction

Over the last twenty years, 802.11, or Wi-Fi, networks have been both widely deployed and widely studied. Indeed, searching Google Scholar for *802.11 widely deployed* returns over 60,000 articles and searching for *802.11* returns over half a million results, some of which have tens of thousands of citations (e.g. [1]). While this steady growth in Wi-Fi has been evident in our day-to-day lives, the aim here is to give a crude quantification of this growth by looking at a sample of Wi-Fi networks in Dublin, and their change between 2002 and 2022.

Between May and July of 2002 we conducted a survey of wireless networking deployment in Dublin, Ireland [2]. The survey covered more than a thousand kilometers of Dublin streets, including parts of the city center, university campuses, industrial estates and residential areas. The survey was conducted by car, bicycle and on foot. As deployment at the time was relatively sparse, areas were often convenience sampled, rather than exhaustively covering an area. The Clontarf suburb of Dublin, however, was comprehensively surveyed, including a number of traffic routes towards the city center.

In August 2022, we repeated the comprehensive survey of Clontarf, following broadly the same routes as previously and, in particular, covering all areas where Wi-Fi networks had previously been found. The new survey was conducted using a combination of bicycle, foot and public transport.

II. Method

We outline both our original survey method here, and the more recent one. The original method involved a patchwork of tools. However, interest in surveying wireless networks for security and research purposes has improved the situation, particularly with the availability of projects such as WiGLE (Wirelss Geographic Logging Engine) providing software tools and a database engine [3].

Our aim is to collect the location, hardware identifier (BSSID) and name (ESSID) for each network. At the same time, we may get additional information such as the channel, use of encryption or the signal strength (RSSI).

A. Equipment

The 2002 comprehensive survey was performed with iStumbler on Mac iBook, with an Apple Airport Card, which supported 802.11b in the 2.4GHz band. New SSIDs were announced using Mac OS's speech synthesis features. GPS was collected manually with a waypoint on Palm Pilot (Handspring Visor) with GPS unit[1]. Logs for iStumbler were combined with the manually collected GPS data.

The 2022 survey was performed with a Galaxy Tab A 10.1 (SM-T510) using the WiGLE app. The tablet has integrated Wi-Fi (802.11b, 802.11a, 802.11g in 2.4GHz and 5GHz bands) and GPS (actually supporting multiple GNSSs). The WiGLE app can use Google Speech Services to announce new networks and exports a CSV file, via Google Drive, for analysis. Data can also be uploaded to the WiGLE project.

Battery performance of devices has significantly improved since the original survey. For the original survey, laptop battery life was a few hours and the palm pilot and associated GPS unit had their own batteries that required monitoring and management. The battery of the tablet used for the 2022 survey never went below 95% during any survey runs.

B. Scanning Method

The method used by the software in both surveys for scanning is similar: both ask the OS for a a list of available networks. It seems that iStumbler announced networks quite promptly after they were detected. This may be because scanning was relatively simple in 2002 — a device listened for Beacon frames on each channel or could send a Probe Request and await a Probe Response frame. Also, for the 2002 survey, only the 2.4GHz channels had to be scanned (at most channels 1–13).[2]

The scanning method provided by modern Wi-Fi equipment is often more sophisticated, allowing background scanning where beacons can be passively observed while remaining connected to a Wi-Fi network. In addition, to both enhance privacy and improve battery life, the rate at which scans

[1]Magellan GPS companion, see https://www.cnet.com/roadshow/reviews/magellan-gps-companion-review/.

[2]The use of 802.11a (in the 5GHz band) in Europe was not clearly permitted by regulations in 2002, and, in practice, little equipment was available at that time. See https://www.cnet.com/tech/mobile/wi-fi-spelling-europe-with-an-a/ and https://en.wikipedia.org/wiki/IEEE_802.11a-1999 for discussion of the introduction of 802.11a in Europe.

are permitted and reported by the OS to the software are throttled on more recent Android releases.[3] The WiGLE app also adjusts its request rate depending on the speed of the device reported by GPS.

Initially the 2022 scan was attempted with the default settings, but was it was clear that there were periods where no networks were reported. The Galaxy tablet was put into Android Developer Mode, and throttling was disabled for the remainder of the survey. This improved the situation significantly, however networks appeared to still be reported in batches, possibly at the end of a full scan of all 2.4GHz and 5GHz channels.

Even with this improvement, it still may be harder to detect modern networks, because of the more modern PHY rates. In 802.11b, the PHY rates used for management frames was often 1Mbps or 2Mbps. In 802.11a or 802.11g, the base rate could be the OFDM-based 6Mbps rate, or faster. The 6Mbps rate is actually less robust than the 802.11a 11Mbps rate (and consequently the 2Mbps and 1Mbps rates) [4], meaning that it may be harder to decode management frames in modern networks, particularly if they are remote from the receiver.

C. Mapping

In 2002, mapping options were relatively limited. While Microsoft's Terraserver had recently launched, online mapping services were specialist and we manually handled the coordinate mapping between the GPS records and satellite images of Dublin, kindly provided by ERA Maptec.

In 2022, the options for mapping data have improved considerably, particularly with the availability of OpenStreetMap [5], under the Open Database Licence. We used the `leaflet.js` open source framework to map our results.

The location of a network is taken to be a weighted average of the positions reported in the log files from the survey, where weights are generated from the signal strength. The locations of networks have jitter by a few meters applied before plotting, primarilly to break up clusters of networks reported at similar locations in the 2022 survey.

III. Results

The results of the 2002 comprehensive survey are shown in Fig. 1. The northmost network was an ad-hoc mode Wi-Fi network with a BSSID in the locally allocated range that changed regularly. Consequently, we counted it as just one network, even though we observed multible BSSIDs. This gave a total of 21 networks in the 2002 survey.

The results of the 2022 survey are shown in in Figure 2. Here we show networks identified that are in ESS mode and that do not have a blank network name (ESSID). This will cover Wi-Fi networks that are in the most common configurations. Using these criteria, we found 13,570 networks.

There is a large change in the use of encryption. In 2002, just three of the 21 networks used the WEP encryption mechanism. In 2002, the WEP was known to be flawed, but was the only standardised mechanism available. In 2022, most of the 13,570 networks use the more modern standards of WPA or WPA2 (12,982). Of the remaining networks, 566 network use no encryption, though many of these are public networks, such as those available in shops or on public transport. Amazingly, 22 networks were still using the flawed WEP system.

[3]See https://developer.android.com/guide/topics/connectivity/wifi-scan for details of the restrictions imposed by Android.

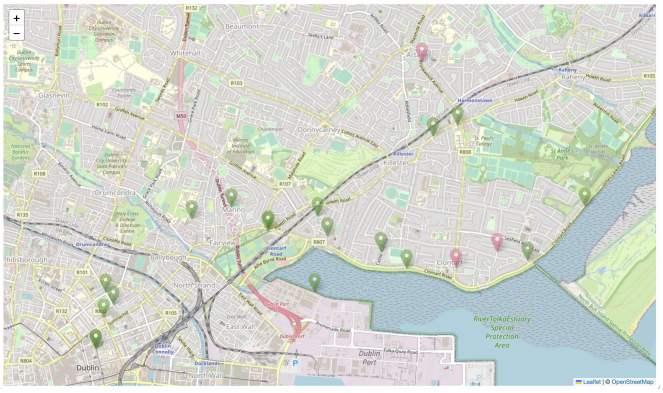

Fig. 1. Networks detected in the Clontarf area in 2002. Green denotes unencrypted networks, red denotes networks using WEP.

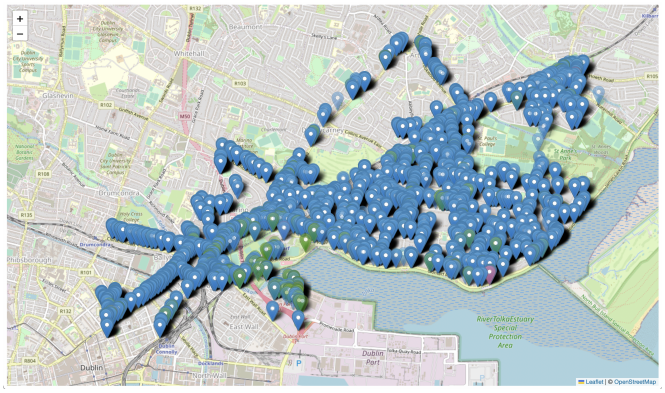

Fig. 2. Networks detected in the Clontarf area in 2002 (left) and 2022 (right). Green denotes unencrypted networks, red denotes networks using WEP and blue denotes networks using WPA/WPA2.

IV. Conclusion

In the presentation, we will present the results of our survey above, and also highlight other findings from our surveys.

References

[1] G. Bianchi, "Performance analysis of IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, March 2000.

[2] N. Murphy, D. Malone, and K. Duffy, "802.11 wireless networking deployment survey for Dublin, Ireland," Tech. Rep., 2002. [Online]. Available: https://www.maths.tcd.ie/~dwmalone/p/wardrive02.pdf

[3] P. WiGLE, "Wireless geographic logging engine," 2001. [Online]. Available: https://wigle.net/faq

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

[5] J. Bennett, *OpenStreetMap*. Packt Publishing Ltd, 2010.