Wardriving: an experience in the city of La Plata

Javier Díaz, Matias Robles, Paula Venosa, Nicolás Macia, Germán Vodopivec

LINTI, Facultad de Informática, Universidad Nacional de La Plata, La Plata, Buenos Aires, Argentina
{jdiaz, mrobles, pvenosa, nmacia}@info.unlp.edu.ar, vodopivec@cespi.unlp.edu.ar

Abstract

In the last few years, the use of wireless networks has been growing exponentially in many situations of our daily life. They are implemented in very different environments and are used for a wide range of applications. This reality is reflected in the information published in the CISCO barometer [1][2].

The incorporation of wireless technology allows, by taking advantage of broadband connections through xDLS or cablemodem, with the speed these have acquired, the incorporation of wireless devices which extend coverage with lower costs, while providing users with mobility.

With the goal of proving the said growth, and analyzing the characteristics of these networks, we performed a study, using the wardriving technique in the city of La Plata. Similar studies have been performed around the world, some with the main goal of evaluating the security status of these networks [3][4].

This article describes our wardriving experience in the city of La Plata, capital city of the province of Buenos Aires, describing the tasks performed, the tools used and the results obtained.

Keywords: wireless network, wardriving, security, Shared Key, WEP, WPA, GPS

An introduction to wireless networks

In the year 1997, after 7 years of work, the IEEE launched the 802.11[5][6], which is part of its 802 standards suite. This means its architecture is similar to the rest of the networks defined within the said family, especially to the 802.3 standard, which has led many people to call 802.11 networks 802.11 Wireless Ethernet. Like all 802 IEEE standards, 802.11 treats the two lower layers of the OSI model: the physical layer and the data link layer. The network layer protocols should run on a network of this type the same way they do on an Ethernet network.

The original standard, specifically its physical layer, was modified in successive amendments with the idea of giving this type of networks a higher transfer speed. In 1999, they launched the 802.11a revision, which reaches 54 Mbits and works in the 5 Ghz band, and the 802.11b revision, which reaches 11 Mbits using the 2,4 Ghz band. Years later, in 2003, they launched the 802.11g revision, with 54 Mbits which uses the 2,4 Ghz band, making it compatible with 802.11b.

Both in the 2,4 Ghz and in the 5 Ghz band, the frequency range is divided into channels. The 2,4Ghz range was divided into 11 channels (this depends on the country). For every wireless network, the channel can be chosen freely, but there should be some considerations, as the 11 channels are not completely independent from each other – the continuous channels overlap and create noise. In practice, only 3 channels can be used simultaneously (1, 6 and 11).

Wireless networks can be classified into two groups: infrastructure and independent networks. The latter are commonly known as ad-hoc networks. The difference between them is that the former are, generally, permanent and there is a special device called access point (AP) which has control over the network. Unlike them, ad-hoc networks are temporary, created for a specific purpose and whose control is shared between all the participants in the network.

All wireless networks have a name, known as SSID, which differentiates between them and makes it possible for the users to find and use them. The access points are in charge of announcing the networks by sending periodical Beacon messages. Should it be necessary that the wireless network remains hidden, its SSID will be eliminated from these messages. This is generally used as a security measure, though not a particularly strong one.

After finding the desired network, the client must become associated with the access point, after completing an optional authentication step. The original standard defines two authentication methods: Open and Shared Key [6]. The first method allows access to the network for anyone who requests it, the second one requires knowing a key shared by all the users of the network. The posterior interchange of frames can, and should, be encrypted. WEP (Wired Equivalent Privacy) [6], is used for this, and also included in the original document.

Both Shared Key and WEP were quickly cracked. This led the IEEE to develop new security mechanisms to solve the problems found in the original methods. In 2004 they launched the 802.11i [7], which defined two new methods: a transitory method, called WPA (Wi-Fi Protected Access) by the Wi-Fi Alliance [8], and a definitive one, known as WPA2. Both methods support two modes: Personal and Enterprise. If a shared key is used, the PSK (from Pre-Shared Key) suffix is added, and it is Personal. For Enterprise, however, an authentication server is used, such as Radius. To encrypt, WPA uses TKIP (Temporal Key Integrity Protocol), which is an improved form of WEP, and WPA2 uses AES (Advanced Encryption Standard) [9], also known as Rinjdael, which is the encryption standard adopted by the government of the United States.

Wardriving

We call wardriving to the search of wireless networks from a moving vehicle. To achieve this, aside from the vehicle, the user requires simply a portable device equiped with a wireless card [10] and a special software to detect this type of networks.

Wardriving got its name from wardialing, made popular in the film starring Matthew Broderick, *War Games*, which consists of finding information systems using a modem and a telephone. There are other techniques with the same goal but using other means such as warwalking, warflying, etc.

This activity, as indicated by the FBI, does not constitute a crime so long as the information obtained is not used to steal the service or access data to which the user is not authorized [11]. Some computer scientists also refer to it as a sport [12]. Another argument in defense of wardriving is that the two frequency bands occupied by this type of network, which are known as ISM (Industrial, Scientific and Medical), are not licensed. Neither permition nor payment are needed to use them.

Wardriving is simply the action of moving within a specific geographic area with the goal of determining the population of wireless devices with exclusively statistic purposes. These statistic data may help in determining the way in which this kind of devices is used, such as, for example, whether they implement security, which channel they use, the type of network, etc.

As explained in the prior section, the access points periodically send a frame called Beacon. These frames, as well as carrying the name of the network, include the authentication method and the security configured, the channel number, the transfer speeds it supports, etc. (in an ad-hoc network the Beacon frames are sent, alternatively, by all the devices in the network). The tools used to complete this activity must capture and process these packets which will provide them with a description of the characteristics of each of the networks detected.

All this information may be complemented by a GPS (Global Positioning System) device which gives coordinates of all the wireless devices found and allows locating them on a map. This helps to determine how these devices are distributed and what zones are most densely occupied.

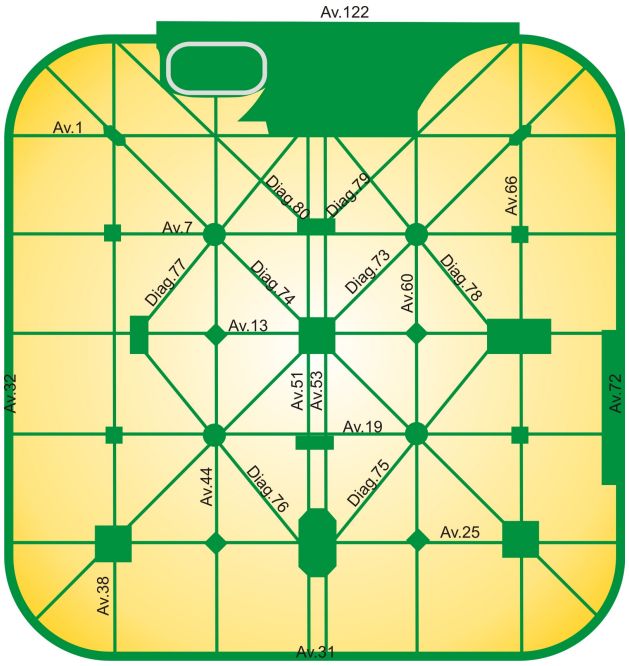
These activities are conducted in many cities of the country and the world. For example, in the city of Buenos Aires, this type of experience has been undergone since year 2005. In particular, in August 2007 a wardriving activity was performed in downtown Buenos Aires, gathering information from a circuit of 53 Km through the main avenues, during a total of three hours and a half [13].

Wardriving in La Plata

With the purpose of mapping the wireless networks of the city of La Plata and consulting their current status, we underwent a experience of discovery of wireless networks in the city of La Plata, Province of Buenos Aires, Argentina, using the wardriving technique.

Before starting wardriving, we defined the geographic area to be covered, and planned the circuit. Taking the particular design of the city into consideration, the following plan was decided on: covering the main avenues and diagonals of the city between avenues 1 and 31 and avenues 32 and 72. And, in particular, a more detailed tour of the rectangle delimited by avenues 1, 19, 44 and 60. This area is where the commercial centre of the city is as well as most public and governmental organizations.

The following graphic displays the design of the city of La Plata, showing the circuit toured.



We also defined the hardware and software resources to be used, including both the tools necessary to capture and those needed to form the map out of the information obtained. Details of these tools can be found in the following section.

Another matter to be defined was which data we wished to obtained from the achieved captures, in such a way to characterize the networks of the city and provide statistic information about them. We decided to extract from each network: the norm it uses (A, B or G), the channel it works on, the network density by area, whether each network implements a security mechanism and, if they do, which one (WEP, WPA, WPA2).

With all the points defined and agreed on the wardriving took place, fully covering the area presented above. For this, we took a total of 4 tours of 3 hours each approximately, between 16 and 19.30 hrs, at an average speed of 20 kms per hour. The results obtained are described in the present article. It also includes the resulting map in which the location of each of the wireless networks is indicated together with the corresponding security level.

Description of the tools used for wardriving

A wide range of applications and tools were used in the process of wardriving. Next, we list the ones chosen for this investigation:

Notebook: necessary to move through the city. We used a notebook executing the NetStumbler program. For the purpose of this work, we used the model Vostro 1500 by Dell, equiped with an Intel PRO/Wireless 3945ABG wireless card. The operating system used was Windows XP.

Network Stumbler (NetStumbler) [14]: an application compatible with Windows. It detects

WLANs of many standards: 802.11a, 802.11b or 802.11g.

It is completely free and very easy to use. The main inconvenient it could present is an incompatibility with the WI-FI card of the notebook or the card not allowing the configuration of monitor mode. A card is in monitor mode when it can capture frames from all the wireless networks within its reach but is not associated to any access point or ad-hoc network.

A GPS receiver [15]: to allow marking the location of the found networks in a map of the city using coordinates, latitude and longitude.

Fluke Etherscope S2 LAN WLAN SX Fiber, Model ES2-PRO-SX/I: it is a wired and wireless network analyzer, which facilitates to professionals the tasks of measuring network performance, installing wired and wireless LANs, validating LAN instalations and solving LAN and WLAN problems [16].

The GPS receiver, connected by jeans of Bluetooth technology to the notebook executing the NetStumbler application, was used to obtain the coordinates of each of the networks detected. Each time the NetStumbler detected a new network, it obtained the said coordinates from the GPS. Using this information we were able to place them in a map. It is important to mention that we only included access points and wireless bridges in the graphic. Although we detected mobile clients and ad-hoc networks in the circuit, we did not process them due to their temporal character.

Other data which can be obtained using NetStumbler are the SSID of the networks, the channels used, the MAC of the wireless nodes and the security, among others. As regards security, the application only detects whether the networks implement it or not. If they do, it shows them as WEP. It cannot distinguish between the different security methods available for wireless networks (WEP, WPA, WPA2).

As differentiating between the different security mechanisms enabled in each access point was essential to understand how wireless networks are used, we had to run another application which could distinguish them. For this purpose, we used Fluke Etherscope. As is expected, in a later process, the resulting files were combined to gather all the information in one only file. Although both programs may generate output files with XML extension, they do so with different formats. The key field used to combine them was BSSID, which is the MAC address of the access point and appears in Beacon frames, and whose purpose is to differentiate between wireless networks. We successfully combined all this information using tools such as Awk [17] and Sed [18].

Results obtained

Once all the information was combined in a single file, we proceded to generate the necessary file to show the networks in a map of the city of La Plata. We generated a file with kml extension, which is the format the application Google Maps [19] can process. This file contains only the coordinates of each one of the networks process, reason for which the only information shown in the map is the location of the access points and Bridges, and the security configured in each of them. This last is achieved by showing the devices with different colors according to the type of security configured. The rest of the data, such as SSID, was obviously omitted.

The map of the city of La Plata, shown below, displays the location of the wireless devices

and the type of security each implements. Color green depicts wireless networks with no security mechanism configured, color green shows those implementing WEP, yellow corresponds to WPA and blue to WPA2.

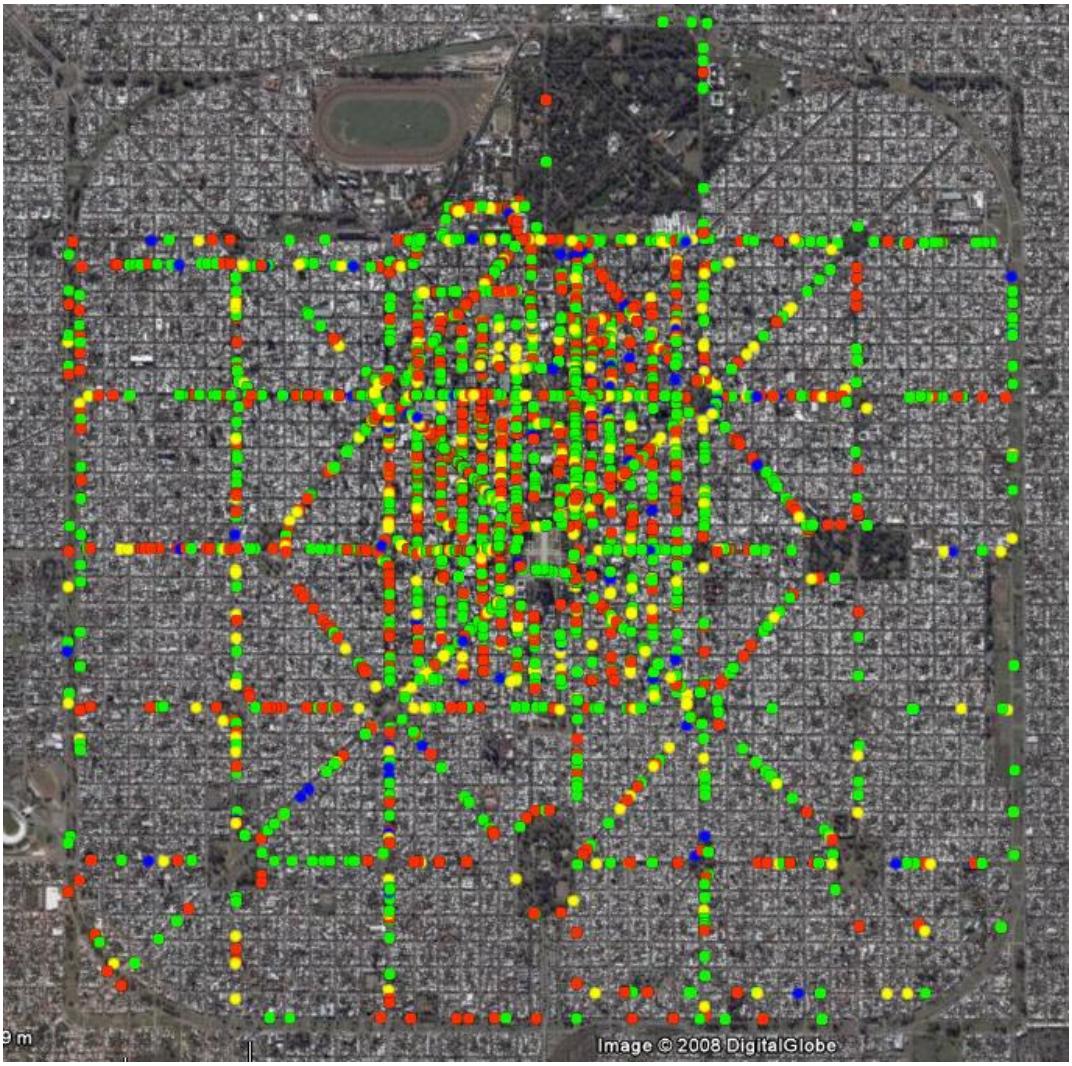


Figure 1. La Plata wireless network map

As expected, the highest network density can be found in the rectangle previously described. This superposition of wireless networks is highly detrimental for the performance of this kind of networks but there is no way to avoid it.

The total of the networks found goes amounts to 2440. From the data gathered we concluded that 44% of the wireless networks do not utilize any security mechanism, while 33% implement WEP, which is a poor security mechanism we discourage users from employing.

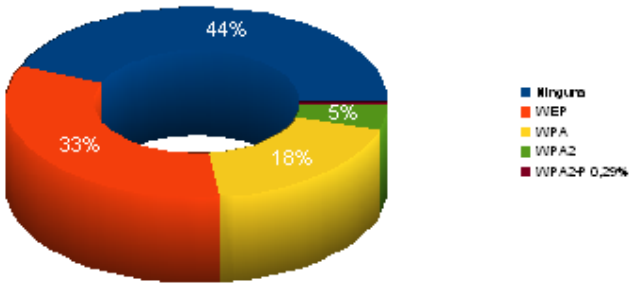


Figure 2. Security mechanisms implemented in La Plata wireless network

It is important to point out that in certain cases the administrators cannot configure the network with a better security than WEP. This is due to the devices, access points or wireless cards, being too old and not supporting the newer mechanisms. Cases of this type should not amount to a significant number if we take into account that the wireless boom occured in the last two years and WPA and WPA2 already existed.

Also to be considered is the fact that many networks are installed in public places such as bars, restaurant, etc, and, generally, they are not provided with any kind of security.

However, the percentages of networks without security or with WEP are quite high, which shows that security is of no concern to those who install and/or maintain this type of networks, which constitutes a crass error. Instead of it, most administrators configure MAC filtering (this is not defined in any standard, it is a mechanism introduced by fabricants) to secure their networks. This method, as we all know, is easy to crack by means of techniques such as “MAC Spoofing”, especially, in wireless networks in which MAC addresses can be obtained by simply locating oneself within the coverage area of the access point.

There is yet another thing to consider at the time of configuring a wireless network and that is channel assignation. In general, wireless devices come factory configured with one of the channels which do not overlap: 1, 6 or 11. The administrator has the freedom to select the channel they wish to use. Some access point models have the capacity to analyze the channels and select the least busy one.

As regards the channels detected, most of the wireless networks use channel 6 – over 50% of the networks are configured in this channel. We can also see that many use channel 11 and 1. It is obvious that channel 6 is completely saturated and so, it presents the following problem. Due to channel overlapping, any network which does not use channels 1 or 11 and whose coverage area is overlapping with a network using channel 6 may suffer interference.

The following graphic shows the distribution of the networks in the different channels. It is worth mentioning that channel 0 does not exist. This is a network which was detected but the channel it belonged to could not be obtained.

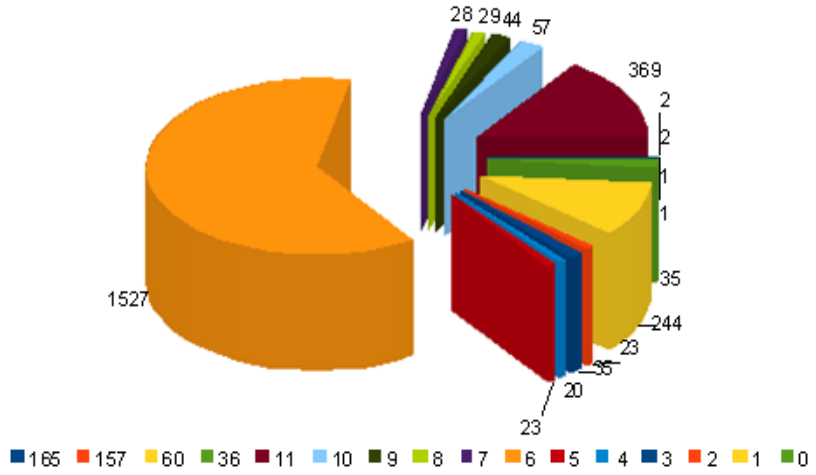


Figure 3. Chanels used in La Plata wireless network

Channels 36, 60, 157 and 165 are used by the norm 802.11a. As explained above, 802.11a occupies the 5 Ghz band, reason for which it doesn not overlap with norms 802.11b and 802.11g. Due to the saturation we can observe in the band of 2,4 Ghz, users are starting to use this band. We can observe that the amount of 802.11a networks is quite inferior to the existing in the other two norms.

Conclusions

Once all the data had been processed, it was posible to obtain the conclusions we present below.

The amount of wireless networks detected in the city of La Plata is surprising, most of which are located in the city center. If the circuit had included all the city streets it is logical to assume the total amount of networks of this type found would have reached 3000.

For security reasons, the SSIDs of the networks detected were not published. In some cases, the name of the network makes reference to their being part of a public or private organization, in which confidential information is likely to be handled. This constitutes an attack vector for the organization. It is convenient that the SSID does not reveal any information of the network to a possible attacker.

One of the greatest disadvantages of wireless networks is security. As shown above, 44% of the networks does not have any type of security configured. Although in certain locations, where free Internet access is offered to users, this is intentional, in other places this situation is caused by the lack of knowledge of the users.

The percentage of use of WEP as a security method is also very high. However, users are discouraged from this due to the vulnerabilities found for the said mechanism. If the equipment allows it, the security implemented shoud include at least WPA. And cases which require the highest degree of security should implement WPA2 Enterprise, which allows the best authentication methods, such as the use of certificates, and the AES encryption standard.

Another problem present due to this proliferation of gíreles networks is the saturation of the channels. Of the 11 channels available, over 50% of the networks use channel 6.

In conclusion, wireless networks have had a great level of acceptance by the users but it is worth noting that their use may be dangerous if the corresponding security measures are not taken.

References

[1] http://www.paisdigital.org/node/625
[2] http://www.cnc.gov.ar/indicadores/archivos/ResultadosBarometroArgentinaQ22007.pdf
[3] http://www.aloul.net/Papers/faloul_ws_gcc07.pdf
[4] http://dspace.icesi.edu.co/dspace/bitstream/item/841/1/estudioWARX.PDF
[5] IEEE Part 11: Wireless LAN Mediem Access (MAC) and Physical Layer (PHY) Specification
[6] OReilly - 802.11 Wireless Networks - The Definitive Guide
[7] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements
[8] http://www.wi-fi.org
[9] http://www.nist.gov/aes
[10] http://en.wikipedia.org/wiki/Wardriving
[11] http://www.syngress.com/book_catalog/291_WarDriving/sample.pdf
[12] http://www.net-security.org/review.php?id=144
[13] http://www.cybsec.com/upload/Estadisticas_WarDriving_Wireless.pdf
[14] http://www.netstumbler.com/
[15] http://en.wikipedia.org/wiki/Global_Positioning_System
[16] http://www.flukenetworks.com/fnet/es-es/products/Etherscope+Series+II/MOA.htm
[17] http://www.softpanorama.org/Tools/awk.shtml
[18] http://www.cornerstonemag.com/sed/
[19] http://maps.google.com/