A Study on the Security, the Performance and the Penetration of Wi-Fi Networks in a Greek Urban Area

Savvas Mousionis, Alex Vakaloudis, Constantinos Hilas

A Study on the Security, the Performance and the Penetration of Wi-Fi Networks in a Greek Urban Area

Savvas Mousionis, Alex Vakaloudis, and Constantinos Hilas

Department of Informatics and Communications,
Technological Educational Institute of Serres,
Terma Magnisias, 62124, Serres, Greece
{mousioniz@hotmail.com,avakaloudis@hotmail.com,chilas@teiser.gr}

Abstract. This paper presents a study on the expansion of urban Wi-Fi networks and the degree of users' awareness about their characteristics. It involves an experiment contacted at the area of Serres, a Greek city of around 70,000 inhabitants. The findings revealed that although the number of Wi-Fi networks is quite high, their owners are unaware of their technical settings. As a result many networks remain either unlocked or with WEP encryption while many adjacent networks use the same channel thus reducing their performance.

Keywords: Wi-Fi networks usage, wireless security, war driving, urban networks.

1 Introduction

It has been around seven years since the introduction of Asymmetric Digital Subscriber Line (ADSL) as a high speed Internet access service in Greece. Despite the initial reluctance by home users to upgrade their previous dial-up connections to ADSL, currently a large number of Greek homes or enterprises connect to the internet through ADSL. It is a mainstream practice for providers to supply a wireless modem/router/access point for every new connection, mainly in the form of a subscription gift. This has gradually filled Greek cities with Wi-Fi networks. These devices typically use the 802.11b/g protocols with a 100mW antenna at 2.4 GHz. Transmission occurs in one of 13 overlapping channels [1].

The present paper explores the use of the resulted Wi-Fi networks which in turn provides clues for the degree of user awareness on wireless security. The main tool used in this research is the method of war driving [2]. War Driving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle using a Wi-Fi equipped computer, such as a laptop or a PDA. It is similar to using a radio scanner, or to the ham radio practice of DXing.

War driving is a play of words on the older term war dialing, which is automatically calling various telephone numbers to look for any that have a modem attached. War dialing, in turn, comes from the 1983 movie War Games now

written in the cult lore of computer geek circles. In the movie a young cracker (Matthew Broderick) is using war dialing to look for games and bulletin board systems. However, he inadvertently ends up with a direct connection to a high-level military computer that gives him control over the U.S. nuclear arsenal [3].

The paper proceeds as follows. The next section defines the hypotheses of the experiments, its subjects, methods and materials and the problems that occurred during its execution. Section 3 lists the results, while in the last section the outcomes of our work along with suggestions for improvements and future work are discussed.

2 Description of the Experiment

2.1 Motivation and Hypotheses

The survey discussed in this paper has two objectives. The first one is to investigate the penetration of Wi-Fi networks considering the provincial city of Serres as a case study. The outcome may not only be used to demonstrate their wide spread but also to confront the reluctance of home users to operate a wireless network due to health considerations. Measurements of the Signal-to-Noise Ratio (SNR) will confirm that the whole city is covered by a number of wireless networks. Therefore, if someone is surrounded by neighbors owning Wi-Fis, she is already exposed to some RF radiation anyway. Moreover, this RF exposure is normally thousands of times below international standards [4].

Our second objective is to examine the manner of usage of Wi-Fi networks and to demonstrate the ignorance of their owners when it comes to simple security of performance settings. The knowledge, for example, to choose the type of encryption or to adjust the Wi-Fi channel is important for the good operation of a network, yet the vast majority of wireless access point (WAP) users are either oblivious or inconsiderate when it comes to their network.

Although WiFi technology security vulnerabilities are well known, the extent of these vulnerabilities may be surprising. War driving may identify many potential points of entry [5].

2.2 Subjects

Serres is the capital of the Serres Prefecture located in the Central Macedonia Periphery of Greece. The city has a population of around 70,000 inhabitants (56,145 in the last official census of 2001) and is an important trade centre for tobacco, grain, and livestock. In our view, it represents a sound choice for an experimental subject since it reflects the average situation regarding wireless networks in Greece. It is situated in a location which is neither near the cutting-edge capital (Athens) nor one found in less developed places. For the better interpretation of results, we divided the city into the following areas:

– City centre: The area where mainly commercial shops or companies exist. Wireless networks in this area are expected to have been setup by professional technicians.

- Around the city centre: A residential area with few shops or companies.
- Suburban and densely populated: A residential area with block of flats of four to six floors.
- Suburban and sparsely populated: The outskirts of the city, a residential area with houses.
- Student area: The area around the technical university (T.E.I. of Serres) populated with students. Some of them study in the Informatics and Communications Department, hence a higher degree of technical expertise and involvement is expected from them.
- Difficult to approach: The area consisting of the hills around the old part of the city with old houses and narrow roads.

2.3 Methodology and Tools

The method used to carry out the experiment is war driving, in other words, driving around the city and stopping regularly to discover wireless networks. The density of these stops is specified by:

- The surrounding area: In densely populated areas stops are every 10–15m since networks of the top floors must be discovered and the number of expected networks is high. On the other hand, in sparsely populated areas the scheduled stops are around 20–30m.
- The surrounding environment: Parked coaches and large trees hinder the discovery of networks.

The tool used is Network Stumbler which is a widely used tool that provides all required information [6]. This is the WAPs MAC address and SSID which were used to identify unique networks, the communication channel, the encryption standard, the type of the device, e.g. WAP or station, and the SNR.

Regarding the first objective of our experiment we measure:

- The number of unique Wi-Fi networks at each stop. The uniqueness requires checking if a network has appeared in adjacent measurements.
- The SNR of each network and the maximum SNR for each point of measurement.

For the use of Wi-Fi networks we examine the following parameters:

- The encryption used, i.e. no encryption, WEP, WPA and WPA2. In the case of unencrypted networks we also try to login to the administration console to check if the user has changed the default username and password
- The SSID used, i.e. if it is the default one or it has been altered
- The Wi-Fi channel to which the network is adjusted.

From a legal perspective, there is no restriction of examining wireless networks broadcasting in a public place, especially for academic purposes. Moreover, we have just searched for the existence of wireless networks in a non-intrusive way, with no ulterior motive. Adding to this, no attempt was made to interfere

or jam the wireless traffic nor did we try to correlate the networks or their traffic with specific persons. We, also, do not publicize the exact location and owner of the individual insecure APs. What is illegal is the unauthorized access to a wireless network in order to steal internet access, steal information, alter the network's configuration or commit other computer crimes. As a result, for networks that were found unlocked, our action stopped to the point of examining whether the user still uses the default security settings. We want to stress out that this may not always be legal in other countries.

2.4 Problems

Although war driving seems to be a time-consuming, yet straightforward process, a number of issues appeared during its execution. Stopping even for one minute in the city centre is not always permitted or it may cause the annoyance of other drivers. Consequently, it may take a few attempts to take a single measurement. Likewise, a stop on a street with parked cars on each side causes interruption of the traffic. Furthermore, some streets are one-way traffic which increases the time needed to reach a desired point. Finally in the difficult to approach section, driving must be very cautious to avoid damaging the car. There were cases where war driving turned out to be war walking.

Since the experiment took place during the summer, the leaves of the trees were a source of reduced SNR values. Hence, the measurement should not take place at points below or nearby large trees.

Finally, an updated map had to be used since the city is expanding and an outdated map was inconsistent with the real picture; for instance there were sections of roads that had been widened or even replaced by squares or roundabouts.

All the above, while solvable, increased the expected time planned for each session of war driving.

3 Results

The war driving part of the experiment took place over the three summer months of 2010. It took 14 sessions of 10 hours each to cover the whole city. The processing of the results included printing the screenshots of Network Stumbler, identifying unique networks along with their maximum SNR.

Overall, 1021 measurements were made and 5374 Wi-Fi networks were found (Table 1). From the 677 (12.6%) unlocked ones, 268 had retained the default access to the administration console. As regards the use of encryption 840 (15.6%) networks were using WEP, 3782 WPA and just 75 WPA2. 3728 were still using the default SSID and the rest 1646 had changed their SSID. The average SNR for each measurement point was 34.2 dB. Considering that WEP encryption is only little better than no encryption we see that almost one third of the networks are susceptible to eavesdropping.

The channels used for Wi-Fi are separated by 5 MHz in most cases but have a bandwidth of 22 MHz. As a result channels overlap and it is possible to find a maximum of three non-overlapping channels. Therefore, if there are adjacent pieces of WLAN equipment that need to work on non-interfering channels, there is only a possibility of three.

Table 1. Number of Wi-Fi networks found at each of the areas described in subsection 2.3

Area	Unlocked	WEP	WPA	WPA2	Default SSID	Altered SSID	Total
City Centre	103	68	521	52	459	285	744
Around City Centre	181	276	1186	13	1199	457	1656
Densely populated	167	235	820	10	867	365	1232
Sparsely populated	64	63	217	0	258	86	344
Student Area	41	81	211	0	1199	457	1656
Difficult to approach	121	117	827	117	730	335	1065
Total	677	840	3782	75	3728	1646	5374

In Table 2 the channel usage of the surveyed networks is shown. Channels 1, 6 and 11 do not overlap with each other and are the preferred choices when setting up a WAP. Channel 6 is usually the default factory setting. The findings in Table 2 coincide with the common practice. Interestingly, there are WAPs set up to work on channels other than the three most common.

Table 2. Active networks per channel

1	2	3	4	5	6	7	8	9	10	11	12	13
1575	40	34	38	45	2296	50	45	57	42	1107	12	33

In Fig. 1 the position of the discovered networks in the city is depicted. The number of identified networks at each location is visualized by means of spheres of variable sizes. The size of each sphere correlates to the number of networks at the point. In Fig. 2 the SNR measurements at each position are visualized. One may observe that the city seems covered with Wi-Fi signals. In Fig. 3 the findings of Table 2 are further clarified. The bar chart displays the possibility two or more adjacent networks to use the same Wi-Fi channel.

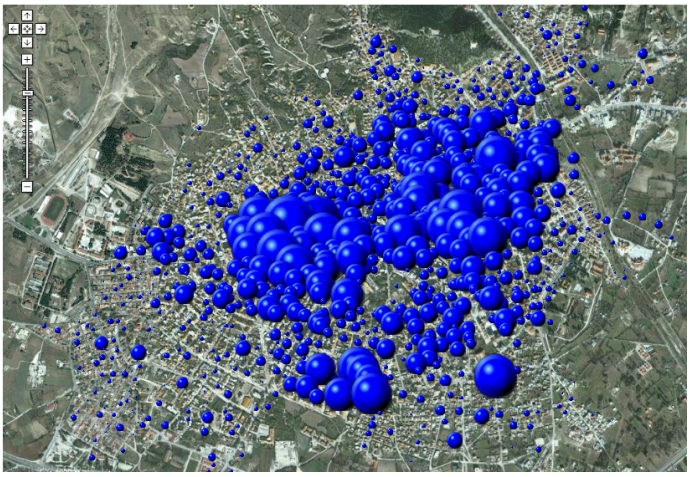

Fig. 1. Positioning and population of Wi-Fi networks. The size of the spheres correlates to the number of networks.

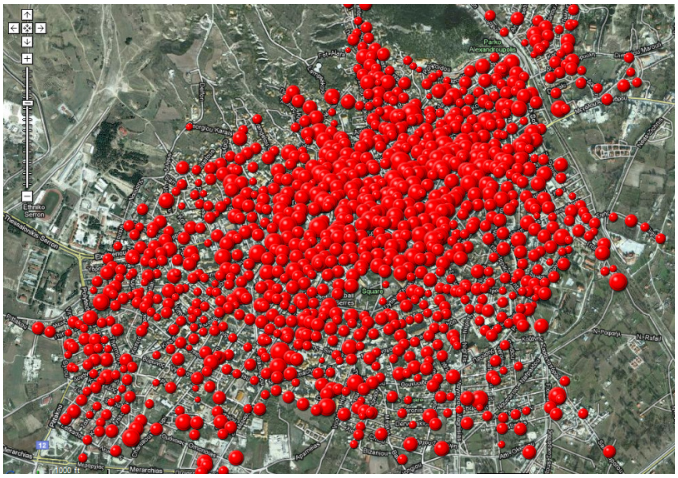

Fig. 2. Wi-Fi coverage of the city. Measured SNR values are visualized by the size of the sphere.

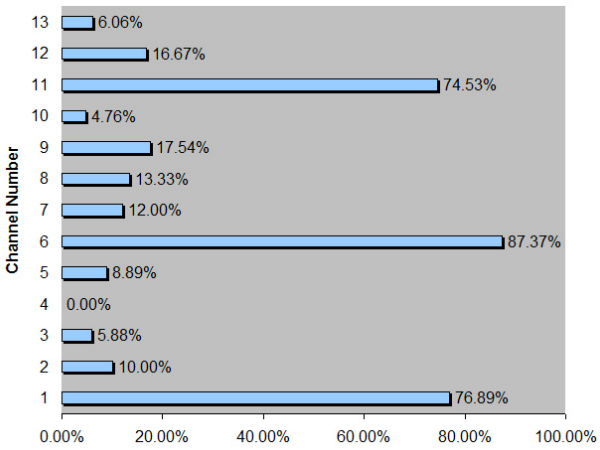

Fig. 3. Percentage (per channel) of neighboring networks that were found using the same channel.

4 Conclusions and Discussion

4.1 Interpretation of Results

This experiment demonstrated that a medium-sized city (for Greek standards of population) is almost fully covered by Wi-Fi networks. The only blank points where squares or the outer limits of the city. The number of unique networks discovered is translated to one network per around 11 inhabitants. This indicates a good penetration of the wireless technology plus that there is still room for more networks to be added. It also illustrates a wide-spread interest of people in Greece for wireless internet access.

As the number of base stations and local wireless networks increases, so does the RF exposure of the population. Recent surveys have shown that the RF exposures from base stations range from 0.002% to 2% of the levels of international exposure guidelines, depending on a variety of factors such as the proximity to the antenna and the surrounding environment. This is lower or comparable to RF exposures from radio or television broadcast transmitters [4].

Our measurements of the SNR also confront the fear of not installing a home wireless network because of health risk concerns [7]. If a specific apartment is surrounded by Wi-Fi networks, it is already susceptible to their electromagnetic radiation. However, considering the very low exposure levels and research results collected to date, there is no convincing scientific evidence that the weak RF signals from wireless networks cause adverse health effects [4].

An important question, left to be answered, is whether users actually access the Internet over a wireless and not over a wired medium. In other words, we can not be sure whether all the discovered networks serve their purpose or are idle.

On the issue of configuring a Wi-Fi network, our evaluation of the experiment's results is carried out under the perspective that the performance and security of wireless networks are topics of general interest, regularly brought up in ordinary discussions. Users are concerned with security and desire faster internet access.

At the same time, the basic configuration of a wireless access point is a procedure that does not require advanced technical expertise or understanding of the wireless technology. In addition, most devices are shipped, by the ISPs, with manuals detailing simple settings alterations e.g. how to change the channel or to apply encryption. And while encryption or Wi-Fi channel numbers are notions whose exact meanings are unknown to the common user, the provided web-based interfaces are simple enough to facilitate their management.

Nevertheless, our survey revealed that despite the importance of security and the easiness for its application, very few users are confident enough to change their WAP settings. As a result, only 1.4% encrypts their data with WPA2. The only exception to this rule is the city centre where 7% of the networks use WPA2. Even though this can be explained by the higher number of business related networks, these are usually setup by specialized technicians and hence this percentage should have been much higher. No WAP using WPA2 was found in the student populated area which took us by surprise as we expected to find more technically competent users there.

It was found that around 70% of Wi-Fi networks are encrypted with WPA. We assume that this is because WPA is the default encryption for the devices preset by Greek ISPs in the last couple of years. Older subscribers still use the unsecured WEP or no encryption at all.

Another evidence of security unaware users is the number of default SSIDs found. Keeping the default SSID can not be considered as a security risk on its own, but it prompts a potential hacker to try to penetrate to such a network. Default SSIDs provide clues about the apparatus model and imply that there is a good possibility that the default administration authentication has also been kept.

The ignorance of users is further exposed when it comes to channel collisions, i.e. the use of the same Wi-Fi channel by many neighboring networks. It is found that when interference exists, the throughput of the system is reduced. It therefore pays to reduce the levels of interference to improve the overall performance of the WLAN equipment. Although users crave for faster internet access they do not take the corresponding actions. Our survey shows that in 87% of the cases another nearby network was using the same channel. This causes interference among such networks and reduces their throughput.

4.2 Relation to Other Works

To our knowledge no similar experiment has been contacted in Greece. A study on war driving in Dartmouth college campus is published in [8], while the Professional Information Security Association (PISA) of Hong Kong reports the findings of war driving in Hong Kong and Macau [9].

The first one is a survey that focus primarily on the accuracy of the WAP position estimation and the impact it has on pervasive-computing applications that depend on knowledge of user location. The article also comments on the effect of using estimated WAP locations in computing AP coverage range and estimating interference among WAPs.

The findings of the second survey are similar to ours, although it was made 3 years earlier (2007). An increasing adoption of encryption settings was identified although 72% of the encrypted sites used WEP. Also, more that 40% of the WAPs kept the default SSID settings while 20% of the rest used individual/family names or organization names as their SSID.

Also, RSA, the security division of EMC^2 Corporation, has commissioned annual research over the past seven years, as part of its campaign to promote and improve best practices in wireless security [10].

4.3 Impact for Practitioners

The fact that Wi-FI APs come with WPA encryption on their default settings has improved the overall security of home networks. We propose a similar approach to be adopted regarding the Wi-Fi channel setting. Randomizing the assigned channel per WAP will reduce the probability of interference and thus will improve performance.

It should be noticed that although all manufacturers provide advanced security measures in their appliances such as modifiable network identifier names and passwords, address filtering, firewalls and WPA to protect wireless networks, it is the consumer who must make the final steps in order to install, configure and adjust all features for maximum security. Thus, it would be very helpful to spare a few pages in user manuals with detailed step-by-step guides on security and performance.

The ignorance or fear to manipulate device settings seems to be apparent in the behavior of professional technicians as well and this is a situation that has to be addressed.

4.4 Research Agenda

The same experiment will be repeated next year to examine changes in the penetration of networks and the use of channels/encryption so as to find out any progress in these issues. We also plan to perform similar experiments in other cities in order to compare the relation of the public to wireless networks in different areas. The parameter of checking MAC filtering will also be added.

References

1. IEEE: IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Available online http://standards.ieee.org/about/get/802/802.11.html (2007)

2. Wireless LAN Security, 802.11/Wi-Fi Wardriving and Warchalking, Available online: http://www.wardrive.net/
3. Brown, S.: WarGames: A Look Back at the Film That Turned Geeks and Phreaks Into Stars, Wired Magazine, 16, 08, (2008).
4. World Health Organization: Electromagnetic fields and public health, Base stations and wireless technologies, Fact sheet N304, (2006)
5. Berghel, H.: Wireless infidelity I: war driving, Communications of the ACM, Volume 47 Issue 9 (2004)
6. Network Stumbler web site http://www.netstumbler.com/
7. Bale, J.: Health fears lead schools to dismantle wireless networks, The Times, November 20, (2006)
8. Minkyong, K., Fielding, J. J., Kotz, D.: Risks of Using AP Locations Discovered Through War Driving, in In: Fishkin, K.P., Schiele, B., Nixon, P., Quigley, A. (eds.) PERVASIVE 2006. LNCS, vol. 3968, pp. 67–82, Springer, Heidelberg (2006)
9. Fong, K.K.K., and Ho, Al.: PISA & WTIA's Hong Kong & Macau War-Driving Report 2007, Professional Information Security Association Seminar: Live! Wi-Fi Attack and Defense, (2008)
10. RSA wireless security surveys, Available online: http://www.rsa.com/node.aspx?id=3268