An Empirical Study of WIFI Security and Performance in Morocco -WarDriving in Rabat

A. Sebbar, SE. Boulahya, G. Mezzour, M. Boulmalf
Computer Science & Logistic Faculty
International University of Rabat
{*anass.sebbar, salaheddine.boulahya, ghita.mezzour, mohammed.boulmalf*}*@uir.ac.ma*

***Abstract*—Morocco is an important regional ICT player that offers interesting investment opportunities to many national and international companies. It is important for these companies to have a good understanding of network performance and security in Morocco. Unfortunately, however, most prior work on network performance and security is interested in countries other than Morocco.**

In this paper, we perform a field study of WIFI networks in Rabat, the capital of Morocco, using wardriving. Our study covers about 10,000 WIFI networks in residential and administrative neighborhoods in Rabat. We find that 77% networks use WPA or WPA2, indicating that WIFI security in Morocco is comparable to WIFI security in developed countries. We also find a balanced use of channels 1, 6, and 11 indicating that network operators are aware of high interferences that can occur on channel 6 and therefore act to minimize interferences. Overall, our results indicate that WiFi situation in the Rabat neighborhoods examined is very encouraging.

KEYWORDS: WARDRIVING, Security Access point, WEP-WPA-WPA2 , Rabat.

1. Introduction

Morocco is a key regional ICT and economical player. For example, Morocco has a 60% Internet penetration, one of the highest in Africa. Moreover, Morocco has attracted investments by many international companies such as Amazon, Microsoft, IBM, Renault, Airbus, and Bombardier.

In Morocco, WIFI is a favorite way to connect to the Internet because of its ease of use and flexibility. Many corporations, cafés, parks, hotels, and houses in Morocco have WIFI networks. The use of WIFI, however, comes with major cyber security threats and degraded performance risks. WIFI, unlike its wired network counterpart where the data remains in the cables connecting the end devices, the transmission in a wireless network takes the form of broadcast radio frequency (RF) signals, which uses the open air as a medium for its movements. Hence the broadcast nature of WLAN introduces a greater risk from intruders who may gain unauthorized access to, or even corrupt, the transmitted data. Although technologies such as WPA and WPA2 are available to secure WIFI networks, such technologies are not always used, mainly due to a lack of security awareness. In terms of performance, the growth of WIFI use raises serious questions about possible high interference levels that may arise from automatic channel assignment. WIFI networks can operate on multiple transmission channels (1 to 11), but often use channel 6 because 6 is the default channel configured by vendors in routers. Such high usage of channel 6 causes major unnecessary interferences.

It is important to conduct a large scale study of WIFI performance and security in Morocco in order to inform local and international organizations interested in conducting business in the country. Unfortunately, however, most large scale studies on WIFI networks are interested in countries other than Morocco.

In this paper, we perform a field study of WIFI networks [24] performance and security in Rabat, the Moroccan capital. We collect data about almost 10,000 WIFI networks in between the Hay Riad and Hay Nahda district through wardriving [18]. These districts are considered the main artery of the moroccan capital. In other words these districts contain residences as well as head quarters of large companies such as service provider in Morocco. More specifically, we collect information about the use of encryption, the channel quality, and the WIFI vendor.

Our team went to areas with large amounts of wireless activity and used inSSIDer to passively collect data from wireless networks. We found more than 10,000 different Access Points in the city and some of them are clearly 13% not secured at all and 77% is secured networks use WPA or WPA2.We also find a balanced use of channels 1, 6, and 11.we also finding Thomson Telecom is the leader vendor with 26%.

The remaining of the paper is organized as follows. We discuss related work in Section 2 and provide background in Section 3. We present our methodology in Section 4 and

978-1-4673-8469-8/16 $31.00 © 2016 IEEE

our results in Section 5. We concluding by conclusion & Perspectives in Section 6.

2. Related Work

In this section, we discuss the fixed wardriving approaches that were previously employed for urban WiFi characterization and equipment used in this study.

Recent years have seen tremendous research efforts at Wi-Fi localization [11]. To localize the Wi-Fi clients, various machine learning-based methods have been proposed. Among them, AP localization is one important topic, which employs various position-bearing information (such as GPS, RSSI, Channels, Vendors) to obtain AP position estimate.

The first worldwide wardrive was carried out in 2002 and took place in many American cities including Boston, San Diego and Des Moines as well as in Norway, Barcelona and Johannesburg. 32 areas in nine countries was surveyed in totale. The first survey found 9374 wireless access points, more than 30% of which did not have basic encryption turned on [4]. "Seattle WiFi Map Project" provides AP location maps (data last updated in 2005), showing 45% of WEP enabled networks. The results were published in [7]. The same test, discovering 802.11b/g networks was performed in Perth, Australia in 2004 [27].Over 700 infrastructure networks were discovred while driving 26 km path through city.

The research was conducted between April 24th and April 26th, 2007 in the London business districts of Canary Wharf and City, as well as other areas of the city. During our wireless tour, they collected data on 800 hotspots. No attempts were made to intercept or decrypt traffic on any wireless networks [20]. But wardriving in Limassol, Cyprus at 2010, in this city they found that 31% of all WiFi networks dont have any traffic encryption [3].

3. Background

IEEE 802.11 is the main protocol for Wireless Local Area Network (WLAN). Actually, it is a set of protocols which including 802.11a, 802.11b, 802.11d, 802.11g, 802.11h, 802.11i, 802.11j, etc [1].

3.1. WIFI security

There are mainly 3 WIFI security algorithms: WEP, WPA, and WPA2. WEP started to be used in 802.11b standard in 1999 and is considered broken nowadays. WPA and WPA2 were introduced in 802.11i for solving the secure issues of WEP in 2003 and 2004, respectively.

Wired Equivalent Privacy (WEP). WEP is the abbreviation of Wired Equivalent Privacy which is an encryption algorithm aiming to provide a secure communication over radio signals between two end users in a WLAN. It uses shared key mechanism adopting stream cipher RC4 with two key sides: 40 bits and 104 bits for confidentiality and authentication, and CRC-32 checksum for integrity. This indicates that the security of WEP is mainly dependent on the security of shared key mechanism. It is important that whether the key is able to resist brute-force attack [12], [26].

Wi-Fi Protected Access (WPA). WPA is an improved solution to WEP security problems and also an intermediate solution between WEP and WPA2. It adopts Temporal Key Integrity Protocol (TKIP) instead of RC4, which uses a static 40-bit or 104-bit encryption key that has to be manually entered on wireless access points and devices. TKIP is able to prevent the types of attacks that inflict WEP because it employs a per-packet key by generates dynamically a new 128-bit key for each packet. [15]

Moreover, WPA uses a stronger message integrity check algorithm called Message Integrity Code (MIC) for replacing CRC-32 of WEP to verify the integrity of the packets and provides two additional certification programs which are WPA-Enterprise and WPA-PSK for different types of users, the former adopts 802.1x protocol and Extensible Authentication Protocol (EAP) while the latter only uses pre-shared key (PSK) [16]. Although WPA is much more secure than WEP, it is better to use WPA2 to replace it if the hardware of a WLAN could support WPA2.

802.11i (WPA2). Wi-Fi Protection Access, Version 2 (WPA2), also known as IEEE 802.11i-2004, enhances WPA by introducing Counter Mode CBC-MAC Protocol (CCMP) which is a new AES-based encryption mode with stronger security than TKIP. AES, abbreviation of Advanced Encryption Standard, is a symmetric-key algorithm that uses the same key with a length of 128 bits, 192 bits or 256 bits for both encrypting and decrypting data. [21] Additionally, WPA2 adopts the same methods as WPA for message integrity and user authorization.

3.2. WIFI channels

There are a total of 14 channels defined for use by Wi-Fi. In most cases, the channels used for WIFI are separated by 5 MHz, but it is essential to have a bandwidth of 22 MHz as shown in Figure 1. As a result, it is possible that up to three channels (for example channel 1, 6 and 11) can be seen without overlap. If only two channels are used, the more efficient is the farthest from each other. It is found that when the interference exists, the system throughput is reduced. As a result, it pays to reduce the levels of interference to improve the overall performance

of the WLAN equipment.

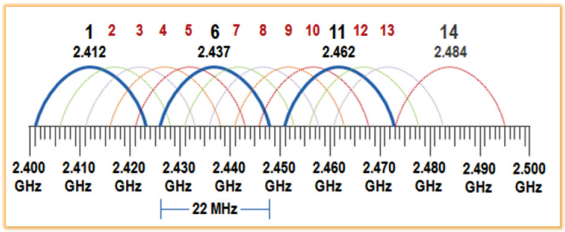

Figure 1. WIFI channels (Source: [13]).

4. Methodology

We perform wardriving on Rabat starting from HayNahda and arriving at Hay Riad as depicted in Figure 2. As shown in Figure 2, the trajectory contains an administrative area that contains many administrations and headquarters of large companies, a rich district with mainly large and luxurious houses, and an urban district with mainly apartment buildings. In other words we performed a 20km path passing by Hay Sinaii, Zair street, Mahaj Riyad, and Annakhil street. In this study, we collect data about 9888 WIFI networks.

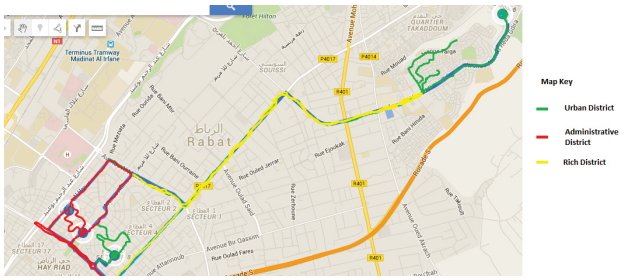

Figure 2. Map showing path performed during collect the data between HAY Nahda and Hay Nahda [19].

Figure 3 contains a diagram of the set up we use to perform wardriving [9], [22]. We use a laptop that runs inSSIDer, a WIFI troubleshooting software that collects data WIFI networks' performance and security level. To that laptop, we connect a 7bB omnidirectional antenna and place the antenna outside our vehicle. Using a 7dB antenna allows covering a large geographical area. We drive at a speed less than 11 km/h in order to minimize the consequences of the Doppler effect on our results.

It is worth noting that wardriving typically involves using a GPS that collects the location of the WIFI networks studied. We choose not to use a GPS because the Moroccan law 09-08 prohibits systematically collecting personally-identifiable data.

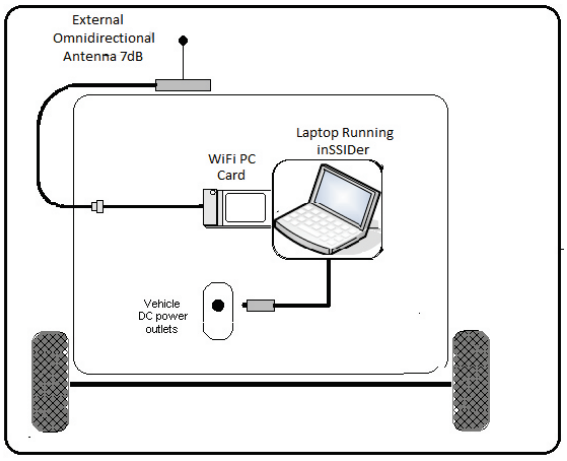

Figure 3. Wardriving Diagram

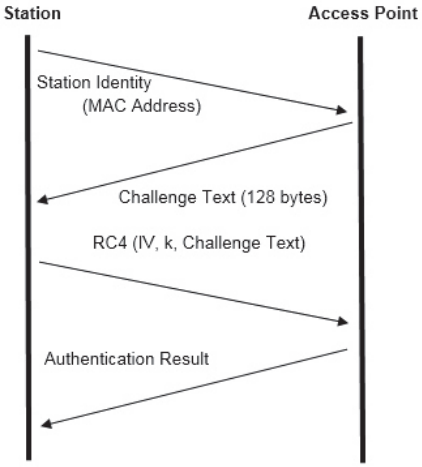

Figure 4. The four steps of an 802.11 shared key authentication [17]

We now explain how the antenna and inSSIDer collect data about surrounding networks. The 802.11 specification defines two methods that a station (Figure 4) can use to look for points surrounding 802.11b / g access. The first is based on Beacon frames which are periodically sent by access points to announce their presence to neighboring stations. In the second method, the station broadcasts a request frame and waits for Probe for executives Probe Response unicasted by access points that received the request. When a station tries surrounding access points, it performs an analysis: the station cycles successively from one channel to the other to report the available access points on all channels of fourteen 802.11b/g. For each access point, inSSIDer displays data that include:

Security- inSSIDer will list the following security settings: Open, WEP, WPA and WPA2,Configuration, Wi-Fi Protected or open (Insecure).

Channel - This is the channel on which a wireless

network operates. Channels 1-14 are in the frequency range of 2.4 GHz, while the channels 30-160 are in the 5 GHz range.

RSSI- Abbreviation for "received signal strength indication" is a measure of the power received in the signal. The RSSI inSSIDer reports is the RSSI seen by our laptop's wireless card.

Vendor - inSSIDer display the hardware vendor to an access point.

5. Results

5.1. WIFI Security

Figure 5 shows the percentage of networks that use no encryption, WEP, and WPA/WPA2. The figure shows that the vast majority (77%) of networks use either WPA or WPA2[1]. This result is comparable to the security level in more developed cities in to the world For example, the percentage of WIFI networks that use appropriate security is 76% in London [5] and is 64% in Dubai [10], [2]. This indicates that the vast majority of WIFI networks in the area covered use appropriate encryption algorithms. In other words, technicians or end-users that configure these networks have sufficient security awareness to be able to choose an appropriate security level.

The figure also shows that a small percentage (10%) of networks use WEP. WEP is an old encryption algorithm, that is known to be broken nowadays. These networks may have been configured in the past when WEP was still considered secure. Alternatively, these networks may have been configured recently by a person who wants to secure their network, but is unaware of the fact that WEP is broken.

Finally, the figure shows that 13% of networks use no encryption. These networks are either open because people who configure them lack security awareness or because these people leave them intentionally open. WIFI in some public places are left intentionally open to allow customers or visitors to connect to the Internet.

We now examine how WIFI security [8], [14] varies by district type. According to Figure 6, the percentage of WIFI networks that use WPA/WPA2 in the administrative district (88%) is higher than in the rich residential district (75%), which in turn than in the urban residential district (64%). WIFI security is higher in the administrative district probably because professional IT personnel configure WIFI access points in administrations, whereas end-users configure WIFI networks in residential areas. The difference between the rich and the urban residential district may be due in a difference in security awareness across the two districts.

1. 60.34% of networks use WPA2 and 16.89% use WPA

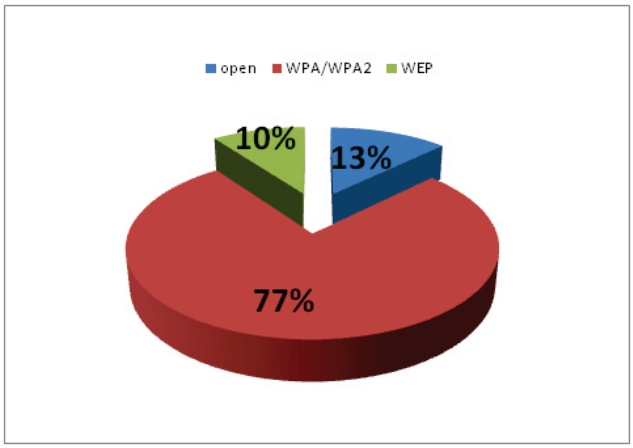

Figure 5. Use of WIFI Encryption

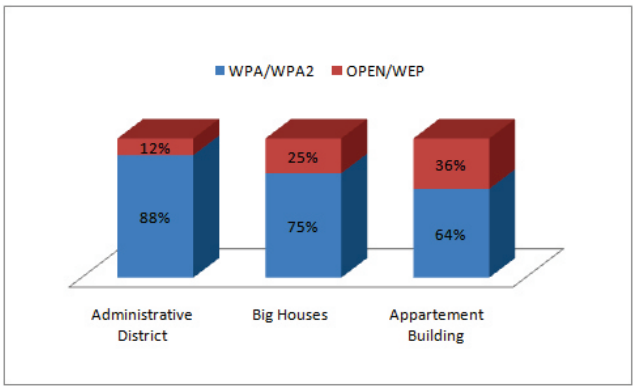

Figure 6. WIFI Security Across Districts

5.2. WLAN Channels

Figure 7 shows the list of WIFI channels used. The figure shows that the majority of networks (27 %) use channel 1. The figure also shows that 23% of networks use channel 6 and 23% use channel 11. The high usage of channel 1 is surprising given that channel 6 provides the best quality. This result may be due to awareness about high interferences that can occur on channel 6 when everybody chooses that channel. Such awareness may have caused network technicians to choose different channels, namely channels 1 and 11. This in turn has caused high interferences on channels 1 and 11. We note that the best method to find the channel to use is through tools such as Nirsofts WifiInfoView [6].

5.3. Signal Strength

The RSSI values we collect represent WIFI signal strength. RSSI [25] is measured in decibels (db) where 0 db represents maximum strength, whereas smaller values represent a smaller strength. Through the RSSI, we can

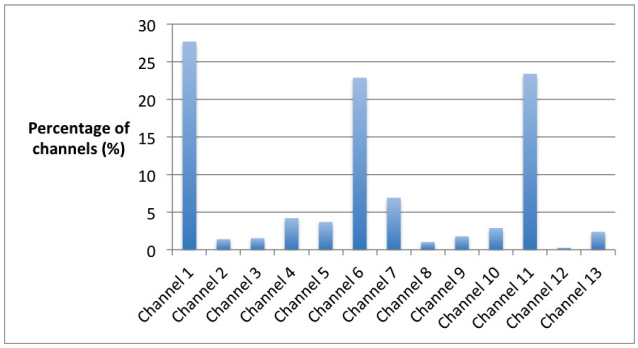

Figure 7. WIFI Channel Usage

TABLE 1. RELATIONSHIP BETWEEN THE RSSI AND THE SIGNAL QUALITY (SOURCE: [23])

RSSI	Signal quality
-51db to -61db	Excellent
-63db to -73db	Good
-75db to -85db	Fair
-87db to -97db	Poor
-99db to -109db	Very poor
-111db to -113db	No signal

assess the signal's quality according to the guidelines in Table 1.

Figure 8 shows the distribution of the signal quality levels according to guidelines in Table 1. The figure shows that the majority of WIFI networks have a usable quality. A considerable number of networks have a low quality. Finally, a small number of networks have a medium quality or a high quality.

It is worth noting that the signal strength that our wireless antenna perceives is typically lower than the signal strength perceived close to access points. One reason for that is the large distance between our wireless card and the access point. Another reason is the Doppler effect, the frequency shift of a wave observed between measures for transmission and reception between the access points and the receiving antenna, when the distance between transmitter and receiver varies over time.

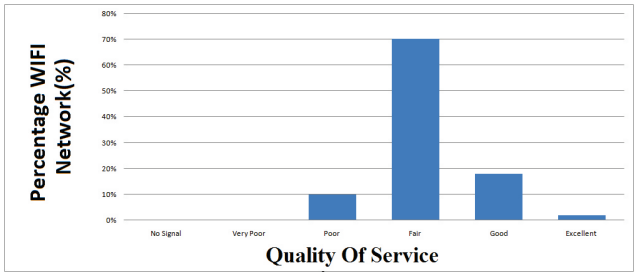

Figure 8. Connection Quality Between Access Points and our Antenna

5.4. WIFI Vendors in Rabat

The interest is the distribution of access points by vendor (figure 9) is the configuration of the latter. A large percentage of Aps is always found that the default configuration is provided by the manufactures, the default name AP and SSID broadcast. Usually only 77% of access points were (WEP, WPA, WPA2) and activated until the majority have left their AP Default SSID. Thomson Telecom is the leader with 26% because it's access points formed by the service provider in Morocco that particularly the only market that vendor APs with identical configurations greatly facilitate a type of ad hoc roaming. The figure below shows access points of vendor in Morocco by order.

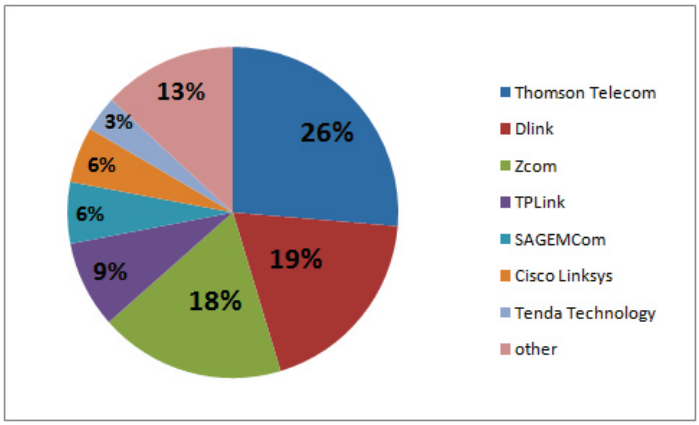

Figure 9. Types of wifi vendors in Rabat

6. Conclusion & Perspectives

First of all, the research was conducted in the two districts (Hay Riad and Hay Nahda). Two districts are not enough for the researcher to get a detailed idea of the security of the access points available in Rabat. In future work, we intend to cover other districts in Rabat and other cities.

In addition, since the inSSIDer tool might give useful information about the access points that we scanned; it seems not to provide the exact location of the access points on the map to locate if this access point belongs to a certain company in the map. The access points were only located in the road area of the map.

Wardriving has many uses, people generally use it to collect data as well as to gather statistics on what types of security used. Wardriving can also be used in order to map out neighborhoods with wireless activity. It is the act of passively collecting data from wireless networks . It is usually done in a vehicle, which allows a person to scan for surrounding WIFI networks.

This paper provides an overview of the state of Wi-Fi networks in Hay Nahda and Hay Riad in Rabat. Our work shows that 77% of the access points discovered use either WPA or WPA2. This is comparable to the security level in more developed cities Dubai and London. In order to increase the percentage of WIFI secured, we believe that there is a need for a consumer education program that raises awareness about the importance of securing WIFI networks.

We also find that many people have moved to channel 1 probably out of awareness about high interferences that can occur on channel 6. This has unfortunately, causes high interferences on channel 1. We suggest that users use appropriate tools to identify the appropriate channel to use rather than just use channel 1 or 11.

We note that our results may not generalize to other neighborhoods in Rabat and other cities in Morocco because of socio-economic and educational differences. As future work, we intend to cover more neighborhoods in Rabat and more cities in Morocco.

Acknowledgments

The authors would like to thank students of the Information Security Master program at the Université Internationale de Rabat.

References

[1] IEEE 802.11. IEEE standards. http://standards.ieee.org, 2008. [Online; accessed January-2016].

[2] Fadi A Aloul. Information security awareness in uae: A survey paper. In *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*, pages 1–6. IEEE, 2010.

[3] Mohammed Boulmalf, Ezedin Barka, and Abderrahmane Lakas. Analysis of the effect of security on data and voice traffic in wlan. *Computer Communications*, 30(11):2468–2477, 2007.

[4] Bob Brewin. Worldwide'war drive'exposes insecure wireless lans. *ComputerWorld*, 2002.

[5] Alexander Gostev. The Wardriving Wardriving in London. https://securelist.com/analysis/publications/36135/wardriving-in-london-2007/, 2007. [Online; accessed January-2016].

[6] LOWELL HEDDINGS. Change Your Wi-Fi Router Channel to Optimize Your Wireless Signal. http://www.howtogeek.com/howto/21132/change-your-wi-fi-router-channel-to-optimize-your-wireless-signal/, 2013. [Online; accessed January-2016].

[7] Kristi Heim. Seattle's packed with wi-fi spots. *The Seattle Times.–2005, Feb*, 18, 2007.

[8] Hanwei Hsiao, Tienhe Chang, and ChihChe Chang. Wireless security analysis using wardrive investigation in kaohsiung areas. In *The 3rd International Workshop on Intelligent Data Analysis and Management*, pages 111–121. Springer, 2013.

[9] Biju Issac and Lawan A Mohammed. War driving and wlan security issuesattacks, security design and remedies. *Information Systems Management*, 24(4):289–298, 2007.

[10] Amir Kalbasi, Omar Alomar, Mohammad Hajipour, and Fadi Aloul. Wireless security in uae: A survey paper. In *Proc. of the IEEE GCC Conference*, 2007.

[11] Swarun Kumar, Stephanie Gil, Dina Katabi, and Daniela Rus. Accurate indoor localization with zero start-up cost. In *Proceedings of the 20th annual international conference on Mobile computing and networking*, pages 483–494. ACM, 2014.

[12] Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, and Seema Shrawne. Vulnerabilities of wireless security protocols (wep and wpa2). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 1(2):34–38, 2012.

[13] Valeria Magoni. Wi-Fi Cloud Management and Remote Monitoring. http://blog.tanaza.com/blog/how-to-pick-right-channel-deploying-social-wifi/, 2014. [Online; accessed January-2016].

[14] Ahmad S Mashhour and Zakaria Saleh. Wireless networks security in jordan: A field study. *International Journal of Network Security & Its Applications*, 5(4):43, 2013.

[15] Mike Meyers. *Mike Meyers' Network+ Guide to Managing & Troubleshooting Networks Lab Manual*. McGraw-Hill, Inc., 2004.

[16] Mike Meyers. *Mike Meyers' Network+ Guide to Managing & Troubleshooting Networks Lab Manual*. McGraw-Hill, Inc., 2004.

[17] Arunesh Mishra, Nick L Petroni, William A Arbaugh, and Timothy Fraser. Security issues in ieee 802.11 wireless local area networks: a survey. *Wireless Communications and Mobile Computing*, 4(8):821–833, 2004.

[18] Piotr Sapiezynski, Radu Gatej, Alan Mislove, and Sune Lehmann. Opportunities and challenges in crowdsourced wardriving. In *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, pages 267–273. ACM, 2015.

[19] Sebbar. The Wardriving results show in google maps. HTTPS://www.google.com/maps/d/editedit?hl=fr\&authuser=0\&mid=z5hCz5dnO7bI.kdQ_qla2DvbQ. [Online; accessed January-2016].

[20] Faisal Karim Shaikh, Bhawani Shankar Chowdhry, Habib M Ammari, Muhammad Aslam Uqaili, and Assadullah Shah. *Wireless Sensor Networks for Developing Countries: First International Conference, WSN4DC 2013, Jamshoro, Pakistan, April 24-26, 2013, Revised Selected Papers*, volume 366. Springer, 2013.

[21] William Stallings and Lawrie Brown. Computer security. *Principles and Practice*, 2008.

[22] Arkadiusz Stopczynski, Vedran Sekara, Piotr Sapiezynski, Andrea Cuttone, Mette My Madsen, Jakob Eg Larsen, and Sune Lehmann. Measuring large-scale social networks with high resolution. *PloS one*, 9(4):e95978, 2014.

[23] SuperUser. RSSI value of wifi connection - how to interpret? http://superuser.com/questions/21827/rssi-value-of-wifi-connection-how-to-interpret, 2011. [Online; accessed January-2016].

[24] Di Wu, Qiang Liu, Yuan Zhang, Julie McCann, Amelia Regan, and Nalini Venkatasubramanian. Crowdwifi: efficient crowdsensing of roadside wifi networks. In *Proceedings of the 15th International Middleware Conference*, pages 229–240. ACM, 2014.

[25] Rong-Hou Wu, Yang-Han Lee, Hsien-Wei Tseng, Yih-Guang Jan, and Ming-Hsueh Chuang. Study of characteristics of rssi signal. In *Industrial Technology, 2008. ICIT 2008. IEEE International Conference on*, pages 1–3. IEEE, 2008.

[26] Sen Xu, Manton Matthews, and Chin-Tser Huang. Security issues in privacy and key management protocols of ieee 802.16. In *Proceedings of the 44th annual Southeast regional conference*, pages 113–118. ACM, 2006.

[27] Suen Yek and Chris Bolan. An analysis of security in 802.11 b and 802.11 g wireless networks in perth, wa. In *Australian Computer, Network & Information Forensics Conference*, pages 117–124. Citeseer, 2004.