Studding and Analyzing Wireless Networks Access points

Arafat Al-dhaqm, Majid Bakhtiari, Essa Alobaidi, Abdulalem Saleh

Abstract— the purpose of this mini project is to enable the reader to understanding affairs and status of the wireless network in the Perdagangan area (PA) and in the Bangunan Sultan Bazar JB area (BSBJA) in Malaysia. We used wardriving to collect and analyze data to know the encryption technology, authentication scheme, configuration, transmissions speed, network topology and manufacturers which used in these wireless networks. In addition, advantage and disadvantage of the technologies and mechanisms which used to configure the access points of the Wireless.

.

Index Terms --- **Authentication, Configuration, Transmissions, Speed, Network Topology, Manufacturers**

1 INTRODUCTION

Nowadays wireless networks are the most popular way to connect people to the internet in companies, e-markets, cafes and in homes. Therefore, it must be secured against the malicious users who try to damage the confidentiality, authenticity and privacy of it. Although, wireless networks are protected and powered by encryption technologies such as WEP / WPA encryption, but several tools were developed to analyze and crack the encryption keys by setting the wireless adapter to monitoring mode, where it can gather the packets of the targeted wireless access point from the air and start to analyze them and trying thousands of decryption keys to crack the key, and it works fine. The problem is the wireless adapter can sniffed and collected the packets from the air, so if the proper cracking tools, compatible wireless adapter and little experience are available the attacker can crack the encryption key of any wireless access point that uses WEP or WPA encryption keys.

2 Field survey

This is the first time that the data collected in the PA by wardriving. The data which collected about wireless networks were different in term of their network topology, Configuration, authentication, encryption, channels, manufactures and radio types. During the wardriving, 99 and 111 access points captured in the morning and afternoon respectively. The tools which used during the wardriving were Wireless laptop (802.11b/g) card and Wlan scanning software called vistumbler 9.4 (www.vistumbler.net), we did not try to decrypt or intercept any data transmitted, owing to that it is not good ethics, and if they catch you, surely you will be in a critical situation. Figure1 show the data which collected morning in PA. Figure2 show the data which collected after noon in PA. Figure3 show the PA by Google earth.

Figure1: Morning Data Collected in PA

- Arafat Mohammed Rashad Aldhaqm is currently pursuing master's degree program in computer science (Information Security) in University Technology Malaysia. E-mail: arafat_aldoqm@yahoo.com
- Dr. Majid Bakhtiari, **Senior** Lecturer *Faculty* of Computer Science & Information System UNIVERSITY TECHNOLOGY MALAYSIA Skudai, 81310Johore MALAYSIA. E-mail:bakhtiari.majid@gmail.com , bakhtiari@utm.my.
- Essa Zaki Abdulrazzak Alobaidi *is currently pursuing master's degree program in computer science (Information Security) in University TechnologyMalaysia. E-mail:* essazk@hotmail.com
- Abdulalem Ali Mohammed Saleh *is currently pursuing master's degree program in computer science (Information Security) in University Technology Malaysia. E-mail: alm_aldolah@yahoo.com*

Figure2. Night Data Collected in PA

Figure3. PA by Google earth

4 Manufacturers

This part deals with the physical concept of these networks in the PA. The table1 and figure4 below shows the total number of different equipment manufacturers, percentage used. Equipment's from 19 different manufacturers were detected in this area, but unfortunately 37% of equipment manufacturer were unknown. The first five of the manufacturers were as (D-link corporation ,Cisco-Linksys LLC, Green packet Bhd, Belkin International Inc, Tp-Link Technology Co) respectively. The D-link Corporation is the market leader in this area and the (Cisco -Linksys LLC) came in the second rank and so on for other manufacturers.

Equipment	count	Per-centage
D-link corporation	20	18%
Cisco -linksys,LLC	10	9%
Green packet Bhd	7	6%
Tp-Link Technology Co	7	6%
Belkin International Inc.	5	5%
Aztech System Ltd	3	3%
Zyxel Communication Corporation	3	3%
Shenzhen Gongjin Electronics Co	2	2%
Netgear Inc.	2	2%
Senior International Co	2	2%
Complex Incorporated	1	1%
Altai Technologies Ltd	1	1%
T&W Electronics (Shenzhen) Co,Ltd	1	1%
Smc networks ink	1	1%
Billion electronic co,ltd	1	1%
Hostnet corporation shanghais dare global	1	1%
Abocom	1	1%
3com LTD	1	1%
2WIRE	1	1%
Unknown	41	37%
Total	111	

Table1: Equipment Manufactures in PA

5 Default Configuration

Networks with default configuration are very dangerous, because the attackers can use these default configurations to attack wireless networks easily. The default SSID means that the administrator of the access points has not changed the name of the router. This also may be an indirect indicator of the fact that the administrator account is still using the default password. The internet is full of information about default passwords which are used by different types of networks equipment, and if the attacker knows the origin of the equipment he will be able to take complete control over such a network. The figure4 below shows 8% of access points in this area use default SSID, and 92% of access points use without SSID, this result lead us to believe that most of the people of this area uses a good configuration, because as mentioned in previous paragraph that the default configuration may cause dangerous situations.

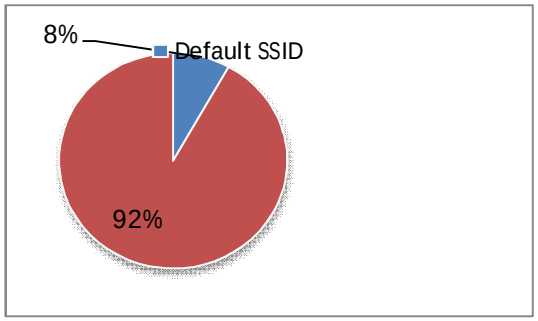

Figure4:- Default Configuration in PA.

6 Network Topology

Wireless networks are either made up access point infrastructure connection or AdHoc node-to-node connections.

In general, the figure5 shows 100% of wireless network access points in the PA are infrastructure network; there was no AdHoc network connection detected. Around 90% of the network worldwide use access point's infrastructure. In my point of view, the Infrastructure networks are better than the AdHoc Network, owing to the serious threats on the AdHoc networks.

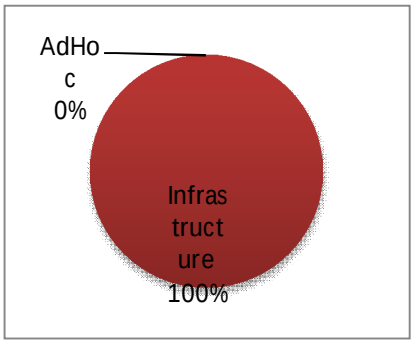

Figure5:- Network Topology in PA.

7 Authentication Technologies

During wardriving in the PA, the Vistumbler program captured data about the authentication scheme which the wireless networks use, and authentication scheme such as (OPEN,WPA-PERSONAL,WPA2-PERSOANL) authentication, open authentication mean that there were no any authentication use to check the client entity or process that wants to connect to network . The figure6 below shows almost of wireless networks in this area use open authentication, 71% of access points use open authentication, 15% of access points use WPA-Personal authentication and also 14% of access points use WPA2-Personal authentication .

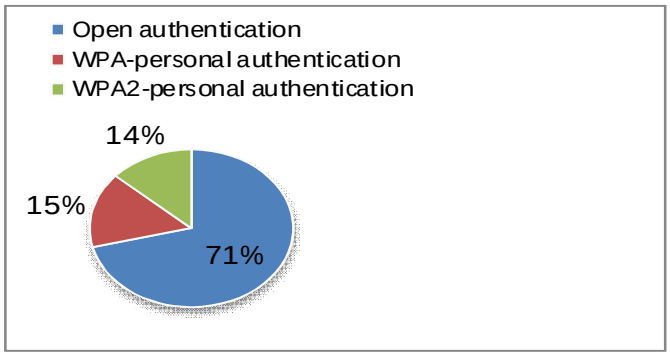

Figure6:-Authentication Mechanism in PA.

8.0 Encryption Technologies

The most important factor in wireless networks is the secure the access points. So here before any analysis, let me to give some information about encryption technologies (WEP, WAP, WAP2) briefly._WEP encryption was designed to insure the confidentiality of the data at network layers. It uses the RC-4 encryption algorithm that has key size 40 or 120 bit. The problem with the WEP is that the initialization vector IV address space is too small, and they are not recommended it is due to the serious security flaws. WPA encryption based on the temporal key integrity protocol (TKIP). The length of the initialization vector (IV) equal 48 bits. WPA does not directly utilize the master keys. Instead it constructs a hierarchy of derived keys to be utilized in the encryption process. WPA dynamically cycles keys while transferring data (regularly changed), so it is better and stronger than the WEP encryption, and the attacker has short time to carry out his attack. WPA2, encryption based on the advanced encryption standard (AES). The default configuration utilizes the advanced encryption standard (AES) and the counter mode CBC MAC protocol (CCMP). WPA and WPA2 are stronger than the WEP encryption, but the surprising is that the administrators of these networks already have knowledge about this weakness in WEP and use it in a higher percentage not only in this area but in most of the areas!

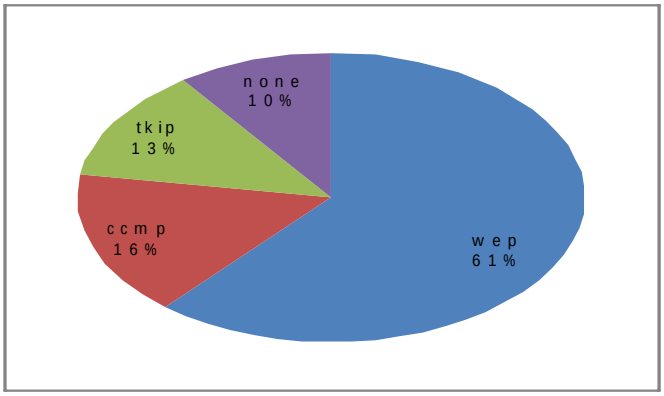

Figure7: Encryption Percentage in PA.

Looking at figure7 above, 61% of access points use wep encryption, and 13% use WPA(TKIP), and 16% of AP use wpa2(CCMP), also 10% of the access point without any encryption. Here the popular encryption technology in this area is WEP encryption; however, it is very weak. In this situation any attacker can attack these networks wireless easily by using a small knowledge and a little tool.

9.0 Radio Types (802.11)

During wardriving in PA the software Vistumbler captured two types of 802.11 protocols (802.11n, 802.11g). The figure8 below shows the radio types which I collected in this area. Only 13% of access point uses the 802.11n, whereas 87% of AP uses 802.11g.

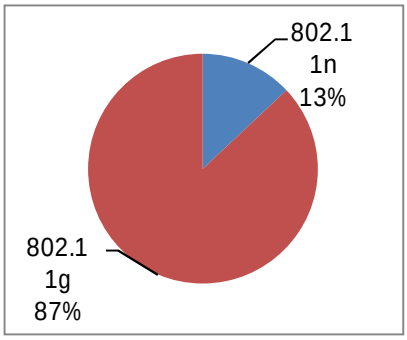

Figure8:- Radio Types in PA.

10.0 Channels Use

The graph below shows the channels that the access point's uses and which is the most popular among these channels. Actually, the channel6 is the most famous among these channels and channel 1 in second in ranks, also channel 11 in third ranks. More than 36% of access points use channel 6, 31% of AP use channel 1, 20% of AP use channel 11 and the other channels are least popular.

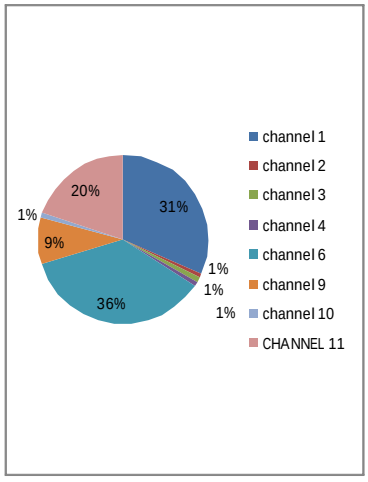

Figure9: Channels in PA

Figure10: Data collected in BSBJA.

This is the additional work (effort personal), another data collected from other place called BSBJA to compare it with data in the main area. Below data which collected during wardriving. More than 300 access points collected.

11 Comparison Data in the Both Areas

11.1 Network Equipment Manufacturers

The data which collected on network equipment manufacturers in PA were different significantly from data that collected in the BSBJA. The table2,figure11 and figur12 bellow shows the total number of different equipment manufacturers which detected in both areas and the percentage use for each manufacturers, and which manufactures is the most famous and most common in these areas. In total, equipment from 51 different manufacturers was detected in both areas. At the PA, equipment from 19 different manufacturers was detected, and at the BSBJA, equipment from 32 different manufacturers was also detected. First five manufactures were found be the most widespread in both area (D-link corporation ,Cisco-Linksys LLC,Green packet Bhd, Belkin International Inc, Tp-Link Technology Co) respectively. Equipment from 41 manufacturers was in an unknown case in PA, and 110 equipments were an unknown manufactures in BSBJA. So the manufacturer D-link Corporation is leader in the market in both areas.

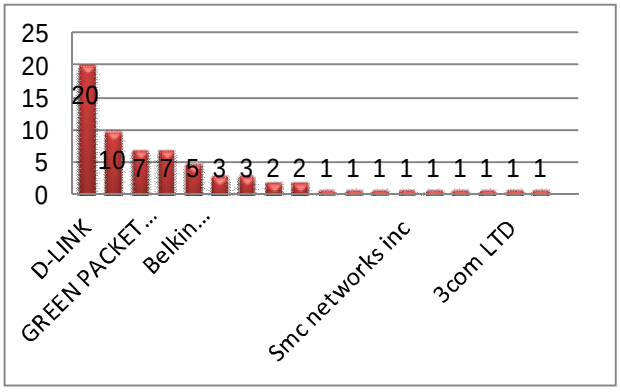

Figure11: Equipment Manufacturers in PA.

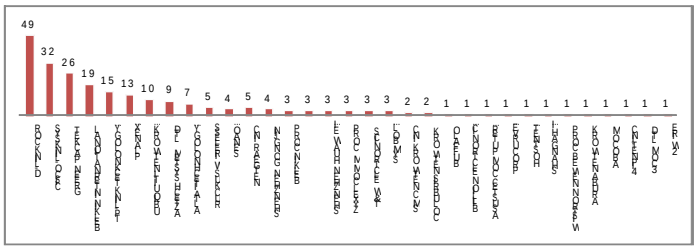

Figure11:- Equipment Manufacturers in BSBJA.

Equipment	Count in PA	Percentage BSBJA	Count	Percentage
D-link corporation	20	18%	49	14%
Cisco -linksys,LLC	10	9%	32	9%
Green packet Bhd	7	6%	26	8%
Belkin International Inc	5	5%	19	6%
Tp-Link Technology Co	7	6%	15	4%
Planex Communications	0	0	13	4%
Ubiquiti Networks Inc	0	0	10	3%
Aztech System Ltd	3	3	9	3%
Altai Technologyies Ltd	1	1	7	2%
Ruckus Wireless	0	0	5	1%
Senao International Co	1	1%	4	1%
Netgear Inc	2	2%	5	1%
Shenzhen Gongjin Electronics Co	2	2%	4	1%
Belkin Corporation	0	0	3	1%
Complex Incorporated	1	1%	3	1%
Shenzhen Hawei Communication	0	0	3	1%
Zyxel Communication Corporation	3	3%	3	1%
T&W Electronics (Shenzhen) Co,Ltd	1	1%	3	1%
Symbol Technologies Wholly owned	0	0	3	1%
Smc networks inc	1	1%	2	1%
Colubris networks	0	0	2	1%
Buffalo	0	0	1	0
Billion electronic co,ltd	1	1%	1	0
Asustek computer inc	0	0	1	0
Procurve networkingn by HB	0	0	1	0
Hostnet corporation shanghais	1	1%	1	0
Wistron neweb corp.	0	0	1	0
Aruba network	0	0	1	0
Abocom	1	1%	1	0
4ipnet,INC	0	0	1	0
3com LTD	1	1%	1	0
2WIRE	1	1%	1	0
Unknown	41	37%	110	32%
Total	111		343	

Table2: Equipment Manufactures in Both Areas

11.2 Default Configuration or Network SSID in Both Areas.

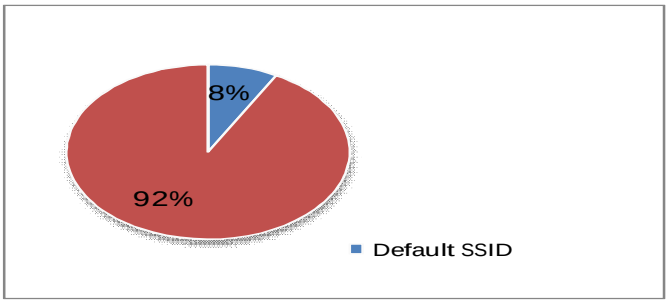

Figure13: Configuration in the PA

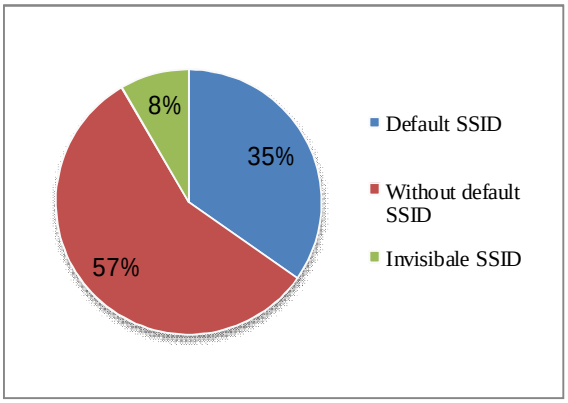

Figure14:- Configuration in BSBJA

Looking at the two figure13, figure14 above, 35% of the access points in the BSBJA retained their default configuration, and this is different from the situation at PA which was better - only 8% of the access points uses the default SSID, on the other hand, the BSBJA was better in different configuration 8% of access points were invisible their default SSID whereas, no any access points in the PA use the invisible SSID. 57% of access points without default configuration in the BSBJA, whereas 92% without default configuration in the PA. This gave us an impression that the configuration in the PA is better than the configuration in the BSBJA. On the other hand, in order to avoid attacks, one of the best ways of protecting a network against Wardriving or sniffing is to disable broadband spreading of the network identifier SSID as we see in the BSBJA, 8% of the networks, their SSID were invisible. The administrators should define the SSID instead of using the default. In addition, it is not good to use an SSID related to the company's name, department, or any other information related to the owner of the network. The SSID could be a generic name meaningful only to the administrators or to other users in order to identify the access points for those who need connect.

11.3 Network Topology in Both Areas

In general, the Data which collected in both areas are around 97% of wireless network were composed of AP access point's manufacturer's connections and 3% of Wireless network were composed of AdHoc connection in the BSBJA. 100% of wireless network access points are infrastructure connection in the PA.

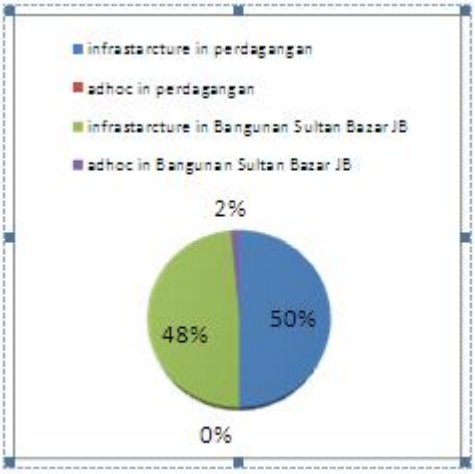

Figure15:- Network Topology in both Area.

11.4 Authentication Schemes

As part of the security, an authentication scheme is a very important part to protect data and prevent attacks on the network layers. Here I will compare the authentication which uses in both areas, and also which area is better than the other authentication. Figure16 and figure17 below are showing us this difference between the authentication schemas in both areas. Around 71% of the access points use open authentication in both areas, 15% of the access points use the WPA-Personal authentication in both areas too, also 14% of the access points use the WPA2-Personal authentication in both areas, but there is one of the access points which uses the WPA-Enterprise authentication in the BSBJA. Basically, open authentication is not recommended, due to the serious weakness and flaws in it. Finally, almost all of the access points uses are open authentication in the both areas. Actually, I have a big question for the administrators in these areas who installed the access points. Why have they used the weak authentication so far?

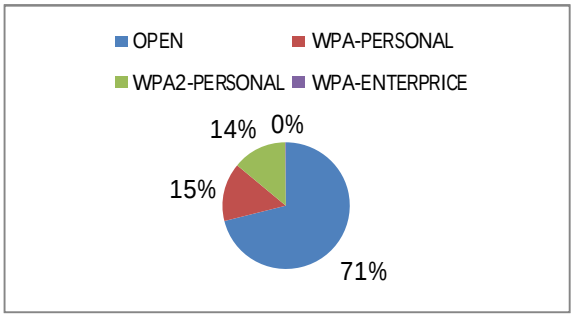

Figure16: Authentication percentage in the PA

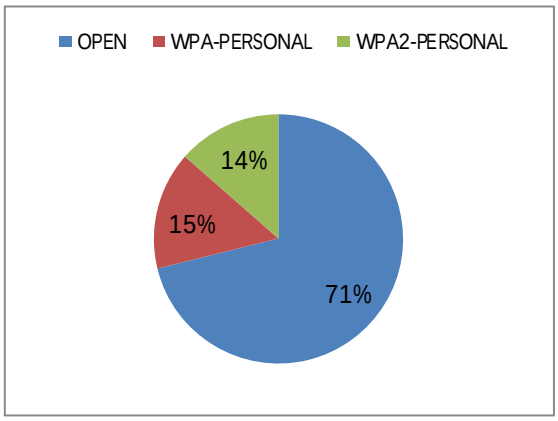

Figure17: Authentication Percentage in BSBJA.

11.7 Encryption Technologies

As mentioned in previous paragraphs, that the protection data is a very important field to prevent the corruption data and malicious users. This section will compare which area has a good encryption than other. Figure18 and figure19 below display the percentage of encryption in both areas.

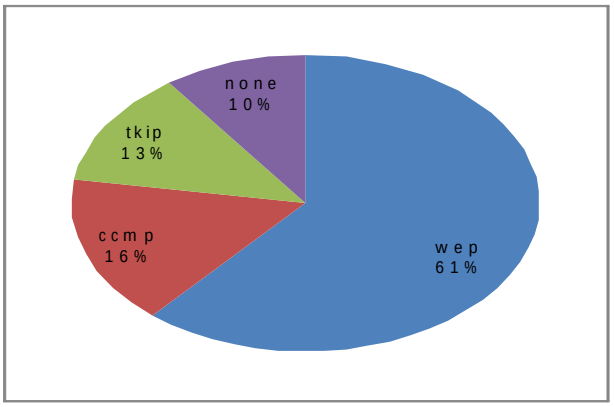

Figure18: PA.

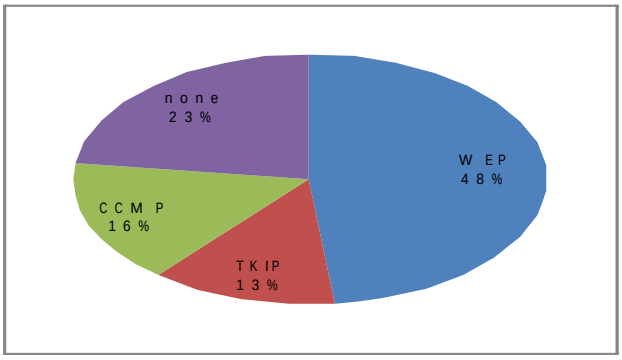

Figure19: BSBJA

Through these figures above, 61% of the access points were in the PA, 48% of the access points in the BSBJA uses WEP en-

cryption, 13% of the access points in the both areas use WPA (TKIP), and 16% of the access points use WPA2 (CCMP) in both areas too, also I found 23% of the access points in BSBJA were without any type of encryption, as well as 10% of the access points in the PA without any encryption. This means that the encryption in the PA is better than the encryption in the BSBJA, owing to more than 20% of the access points in the BSBJA were without any encryption.

11.5 Channels

As compare to channels from the graphs below in both areas, we can see that they were shared in many channels.
The figure20 and figure21 below shows the channel 06 which is the most popular among of other channels, it has many access points than the other channels in both areas, this is because they are often used by these channels as the default when they are configure to the access point equipment. Channel 1 came in second rank; also the channel 11 came in third rank respectively. And the others channels were different from each other. This comparison show us which channel is most common in both areas and overcrowded.

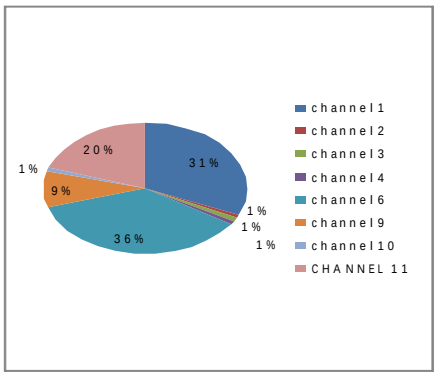

Figure20: channels in the PA.

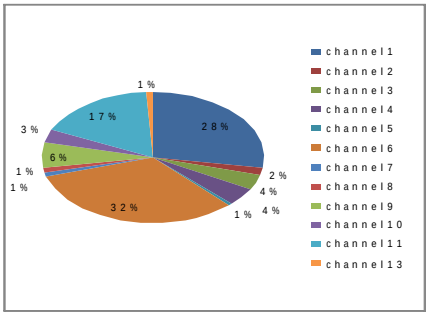

Figure21: channels in the BSBJA.

11.6 Radio Types

During wardriving in both areas, the program vistumbler captured many types of radio type (802.1n, g, and b), which the wireless networks used. These two graphs below display these data and compared it. Figure22 and figure23 below shows that almost all access points in both areas uses 802.11g protocol this mean that the transmission speed for these networks are very fast, 54mbp/s.

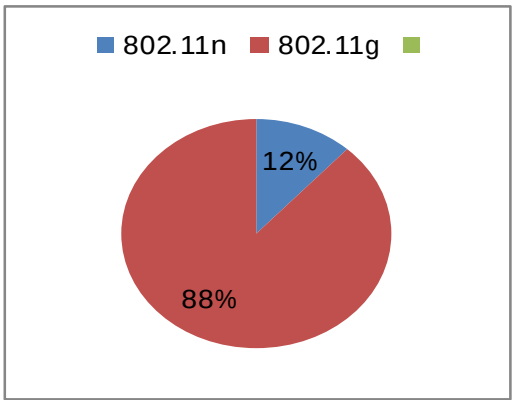

Figure22:- Radio Type in PA.

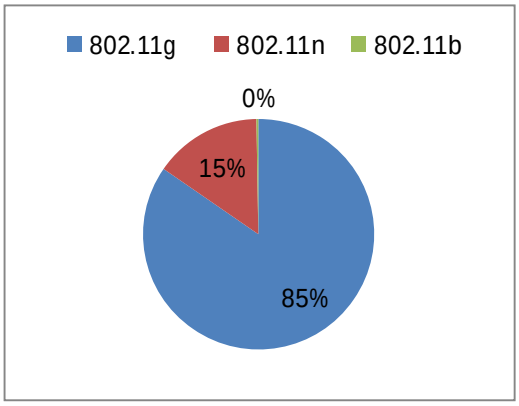

Figure23: Radios Type in BSBJA.

12.0 Recommendations

We know that there is not yet completed ways to protect against attacks on wireless networks, but prevention is better than cure. Therefore, to reduce the possibility of access to wireless networks, I recommend the following:

1- I highly recommend modifying and hiding or disabling the SSID network identifier when the wireless network is setup; do not let it be a default SSID.
2- If you have been using the WEP encryption technology so far, you must change it now and replace it to WPA, WPA2 encryption technologies, owing to the WEP encryption are very weak and any attacker can exploit it easily.
3- Do not use the channel 6 when you planning to a new network, due to the fact that is always overcrowded as I mentioned in the channels section.

4- Limit the MAC address to connect to the network and use a virtual private network for added security.

13.0 Conclusion

During wardriving in both areas, 99 and 111 access points which collected in the PA respectively, and 343 access points in the BSBJA, almost all it were infrastructure connection. These access points are different in terms of authentication, encryption, configuration, manufacturers, channels, transmission speed and radio type. Unfortunately, almost of these wireless networks have a poor security. More than 65% of the access points use the weak security standard such as an open authentication and wep encryption which are not recommended, whereas 15% were distributed among other authentications and encryption standard (WAP, WAP2) and 20% did not have any type of encryption. In addition, there is 15% of the access point which uses the default SSID. Among types of wireless network equipment which the manufacturers used in both areas were D-Link Corporation and Cisco-Linksys respectively. On the other hand, channel 6 is the most popular channel in both areas, which is usually preset by the manufacture. On the other hand, more than 85% of Wi-Fi equipment in both areas uses the wireless network card (802.11g) protocol which allows speed up to 54mbps. Only 15% of all equipment uses the 802.11n protocol.

14.0 References

[1] www.vistumbler.net