# Wireless Security in Libya: A Survey Paper

Salima Benqdara
University of Benghazi
Benghazi, Libya

Abdelfattah Mahmoud
University of Bright Star
Elbreaga, Libya

## ABSTRACT
Wireless networks have advanced quickly over the most recent of years because of the improvements of new wireless standards and cost-effective wireless hardware. This has prompted broad selection of the innovation in home and private companies. Notwithstanding, the vulnerabilities and threats that wireless networks are exposed to resulted in higher risk for unauthorized users to access the computer networks. This paper assesses the security status of Wireless Local Area Networks (WLAN) use by occupants and coffee houses in two noteworthy city communities of Libya. The objective is to assess the security vulnerabilities that lie underneath the use of WLAN by the general population in Libya. Information will be gathered from different populated locales and will be analyzed to better understand the wireless security awareness among the public.

## General Terms
Security, Wireless LAN

## Keywords
Wireless Network Security, Wireless LAN, SSID, WEP, WPA, WPA2.

## 1. INTRODUCTION
Wireless networks are one a standout amongst the most developing segments of information technology. Due to the adaptability of wireless networks, businesses, educational establishments and households are adjusting this technology which makes it an integral part of recent life. This has prompted across the board reception of the innovation in home and private companies. With the development of wireless networking, security is the main weakness of the whole wireless system, which brought about inappropriate employments of system assets. The sending of wireless networks can conceivably make private networks subject to public use. As wireless access expands, security turns into a significantly more vital issue. War-driving is a typical practice at which an individual furnished with electronic devices, skilled for wireless access, meanders in the boulevards with the aim to locate wireless networks for access to the Internet, either house-based or corporate-based wireless networks, map their existence, and hack them. It's a laptop equipped with a wireless LAN adapter or smart mobile phone, and randomly driving around looking for unsecured wireless LANs.

Maximum network threats originate from the ignorance of users, the inactive attitudes of companies, and the unsuitable implementation of security features by wireless device manufacturers [1]. The lack of adequate learning materials and or funding for users' wireless connections at home, as well as public places wireless access fakes a critical threat to the systems as well as the information these system hosts. Some researchers suggest that with the increased demand for wireless connections, comes a growing concern about the security and protection the wireless networks [2, 3].

Numerous security measures have been proposed to reduce the risk of wireless attacks such as changing the default SSID name, using security algorithms, disabling SSID broadcasting. Nevertheless, a few companies and residents enforce these security measures. In this paper, evaluate the wireless security awareness in Libya. Survey the security of wireless networks in 2 populated parts of the cities of Ajdybia and Elbreaga.

The rest of the paper is organized as follows: Section 2 discusses the related works on the Wireless Security. In section 3 present a brief overview of the wireless local area networks to provide a proper background. Section 4 and 5 present wireless security issues and data collection. The results and discussion of findings are presented in Section 6. Finally, Section 7 concludes the paper.

## 2. RELATED WORK
In an effort to address the network security problems, in this section discuss the published papers have provided solutions in an organizational or technical approach.

Kalbasi et al. (2007) conducted drive in the United Arab Emirates (UAE) with two laptops and with a GPS to locate detected APs. The study explained how SSID provides the channel information. Their study found more than 70% APs using channel 11, which can slow down all the APs in the vicinity of each other. The authors suggested WPA-PSK instead of WEP and consider Media Access Control (MAC) address filtering as a security mechanism.

Chenoweth et al. (2007) Conducted study of users' behavior in a university. The study finds that 9% of 3,331 of personal computers on campus do not have firewalls properly configured on them. Furthermore, 60% of wireless networks did not use any respectable procedure for authentication or encryption according to a survey by panda international. In addition, vulnerability checks indicated that a number of users not having firewalls on their computers. This was attributed to negligence on the part of the users. Therefore, user behavior is important in terms of network security.

Sarkar and Abdullah (2011) conducted a war walking field study of WLAN networks, in Auckland to compare security updates in 2010 with respect to 2004 and 2007. The study found a huge increase, not only in the adoption of encrypted wireless networks, but also in other practices in Auckland. The study suggestes some recommendations for securing communications over WLAN networks. These recommendations include enhanced encryption technology for WALNs, the default SSID should not be used to improve security, WLAN access should be controlled by minimizing MAC addresses and VPN should be used to improve security.

Nisbet (2013) conducted a war walking field study of WLAN networks, in Auckland City for more than four hours to cover as many APs as possible. The study describes how the channels may overlap if not kept distant. The study also listed the channel configurations of all the detected APs. The author considers WEP as even worse than an unencrypted channel as

it gives the users a false sense of security and suggested WPA2 which keeps updating the encryption keys periodically.

Nagashree et al. (2014) conducted study of new technology like Near Field Communication (NFC). The study pointed out that new technology, NFC which is based on wireless network technologies could be compromised by a hacker through eavesdropping on the network, thereby leading to stealing of payment credentials because NFC is usually used for contactless payments.

Sebbar et al. (2016) Conducted war driving field study of WIFI networks, in Rabat, the capital of Morocco. The field covers about 10,000 WIFI networks in residential and administrative neighborhoods in Rabat. The study finds that 77% networks use WPA or WPA2, indicating that WIFI security in Morocco is comparable to WIFI security in developed countries. Moreover, 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. The results show that the WiFi situation in the Rabat neighborhoods tested is very encouraging. The authors suggest that users use appropriate tools to identify the appropriate channel to use rather than just use channel 1 or 11. Moreover, the authors propose to offer a customer education program that heightens consciousness around the importance of securing WIFI networks

# 3. WIRELESS LOCAL AREA NETWORKS

WLAN Stands for Wireless Local Area Network, WLAN is basically trying to imitate the structure of the WLAN, using another medium to transfer data rather than cables. This medium is electromagnetic waves which are mainly either infrared frequency (IR) or radio frequency (RF). WLAN consists of two components which are Access Points (AP) and clients or end-user devices. AP functions similar a regular router or switch in wired network for the wireless devices. Furthermore, it denotes a gateway between the wireless devices and a wired network. Clients' are armed with devices which permit the user to use the RF medium to communicate with other wireless devices. The basic structure of a WLAN is called BSS (Basic Service Set). The network contains of an AP and several wireless devices. When these devices attempt to communicate between themselves, they propagate their data through the AP device. In order to form the network, AP keeps broadcasting its SSID (Service Set Identifier) to allow others to join the network.

# 4. WIRELESS SECURITY ISSUES

WLAN media are challenging to secure due to its broadcast nature. This property makes creating a good secured protocol that is similar to wired security modules a very arduous job [10]. WLAN depends on cryptographic technique to enable protection. There are mainly 3 WIFI security algorithms: WEP, WPA, and WPA2.

Wired Equivalent Privacy (WEP). WEP is a security protocol introduced by the WiFi 802.11b standard designed to provide a similar level of security and privacy for a WLAN. It uses a shared key mechanism adopting a stream cipher RC4 with two key sides (40 bits and 104bits) for confidentiality and authentication, and CRC-32 checksum for integrity. This shows that the security of WEP is mainly dependent on the security of shared key mechanism. It is important that whether the key is capable to attack, brute-force attack [11].

Wi-Fi Protected Access (WPA).WPA is a data encryption specification for 802.11 wireless Networks. It is a developed solution to WEP security problems and also an intermediate solution between WEP and WPA2. It adopts dynamic keys, Extensible Authentication Protocol to secure network access, and an encryption method called Temporal Key Integrity Protocol (TKIP) to secure data transmissions [12].

WI-Fi Protection Access 2 (WPA2).WPA2 is an enhanced version of WPA. It is enhances WPA by introducing Counter Mode CBC-MAC Protocol (CCMP) which is a new AES-based encryption mode with stronger security than TKIP. AES 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 [13]. Moreover, WPA2 adopts the same methods as WPA for user authorization and message integrity.

Various measures have been offered to secure wireless networks. Such measures include:

- Disabling SSID broadcasting
- Changing default SSID name
- Using strong encryption methods like WPA-PSK and avoid using the weak WEP encryption method
- Changing default username and password used for the AP configurations
- Using MAC filtering, to grant access for only known clients [14].

## 4.1 Wireless Security Risks

- Data confidentiality: Meanwhile the data traded between the access point and the clients are transmitted through clear air, unauthorized individuals can listen and read the data. The data security risk can have a serious effect on the client if the transmitted information contains individual information or vital passwords like the ones used in bank accounts. The data security risk still holds if the client empowered a weak encryption algorithm such as WEP, since WEP encrypted networks can be cracked today in an average of 10 minutes [14].
- Unauthorized internet access: Unauthorized access can be gained by any user if the AP is broadcasting its SSID name and doesn't filter legitimate clients. Hackers might use the internet, access to initiate attacks on other hosts and hide their identity [15].
- User privacy: Since users of WLAN has the freedom of choosing the SSID name, some of them include personal or business information which can be used as an indication for hackers to direct their attacks. In most cases, the default SSID name represents the AP brand. If the user doesn't change the SSID name, hackers can recognize the AP brand, obtain an exploit for the AP, and brake into it [15].

## 5. DATA COLLECTION

Data collection was planned to be done about existing wireless networks in different Libya areas. The tests were simply conducted using Sony VGN-S18GP laptop equipped with Intel pro wireless 2200 BG card, Toshiba A100-709 laptop equipped with Intel pro wireless 3945 ABG card. The test was performed in two major cities in Libya; Ajdybia and Elbrega. Network Stumbler and Kismet software were used to collect the wireless data. Network Stumbler was used as a sniffer to detect the APs in Ajdybia and Elbrega. Kismet was used for the purpose of detecting networks that don't broadcast their SSID names. The locations that were covered are king Street road and Internet city in Ajdabiya and the Area3 in Elbrega.

## 6. RESULTS

### 6.1 1Wireless Network Security in Elbrega

During perform the test in the Area3 in Elbrega, the team was able to recognize 271 access points (APs). Through the data collection, a path longer than 3 Km was traveled to make sure the area is covered properly and accurate information is collected. The yellow shaded area in the Figure 1 shows the surveyed region around Area3 in Elbrega. The area has mostly residential apartments, offices, clinics, and markets.

**Fig. 1. The surveyed in Area3 in Elbrega city**

Data collected shows that several APs broadcast their default SSID name and mostly without encryption. Furthermore, the study, which involved about 8 hours in Elbrega, only two APs were found to disable their SSID broadcasting. Table 1 summarizes the identifying APs with their corresponding SSID names and WEP encryption status. Table 1shows that 221 of APS used the non-default SSID names and only 122 (55%) of the 221 APS enabled WEP encryption. In terms of APs with default SSID names, 4 of APS used the default SSID names and 2 (50%) of the 4 APS enabled WEP encryption. According to the results, high number of the tested wireless networks are unsecured and the security of the networks needs to be further enhanced to protect those networks.

**Table 1: Access points with their SSID names and their encryption status in the Elbrega area3**

| Elbreaga Area3 | | |
|---|---|---|
| SSID | NUMBER OF APS | WEP enabled (%) |
| Linksys | 14 | 5(36%) |
| speedstream | 12 | 2(17%) |
| 3Com | 6 | 3(50%) |
| USR9106 | 5 | 0(0%) |
| Default | 4 | 2(50%) |
| Others AP brands | 9 | 3(33%) |
| Non-default | 221 | 122(55%) |

Figure 2 illustrates the results on the level protection of WLAN networks in Elbrega city. The figure shows that 51% of the networks are found to be using low level protection (wep). The figure also shows that 49% of WLAN networks use no encryption. The survey indicates that the security standard is low due to lack of awareness in IT community in Elbrega city and the security of the networks needs to be further enhanced .Moreover, the wireless network that is using WEP are more vulnerable then network that using the recent configuration (WPA2), because the WEP 24-bit initialization vector and weak authentication. To secure the wireless network need Implement sophisticated password and configure the encryption to WPA2. These networks are either open because people who configure them lack security awareness or because these people leave them intentionally open.

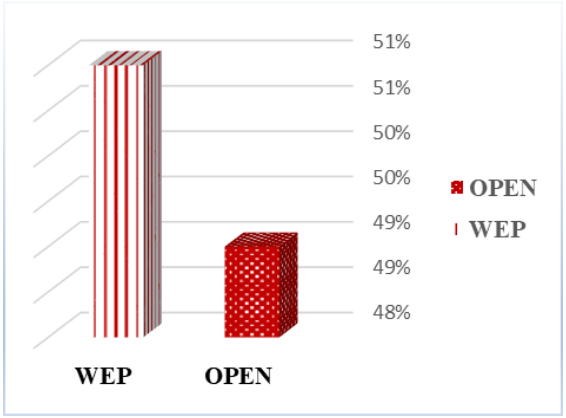


**Fig. 2. WLAN encryption status in Elbrega area3**

figure 3 illustrates the results on the percentage of networks that use default SSID and non-default SSID names in Ajdabiya city. The figure shows that 221 (82%) of the networks are using Non default SSID names. The figure also shows that 2 (1.4%) of networks use default SSID names. The survey shows that the majority of WIFI networks in the area covered using Non default SSID. However, the security standard is low due to lack of awareness in IT community in Elbrega city and the security of the networks needs to be further enhanced. To secure the wireless network need change default SSID, Implement sophisticated password and using high level protection.

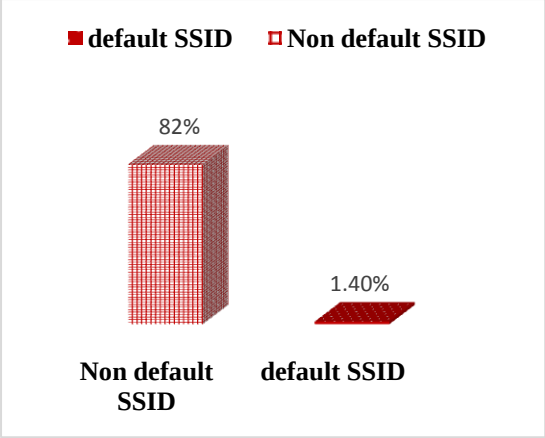


**Fig. 3. SSID Configuration in Elbrega area3**

## 6.2 Wireless Network Security in Ajdabiya

In Ajdabiya city, decided to perform the survey on King Street, road and the Tripoli Street. Both locations named (downtown) have a great number of offices, hotel, residential buildings and university. In the survey, the team identified (1576) access points APs correspondingly. To provide complete coverage of the areas, all service streets were visited. The turquoise lined area in the Figure 4 shows the surveyed region on king street road. The area has local offices, residential apartments, hotel, shops and cafes.

During the survey, 1576 APs were found with disabled SSID broadcasting in Ajdabiya city. Table 2 summarizes the identifying APs with their corresponding SSID names and WEP encryption status. Table 1shows that 22 of APS used the default SSID names and 3 (14%) of the 221 APS enabled WEP encryption. In terms of APs with non-default SSID names, 1169 of APS used the non-default SSID names and 684 (59%) of the 4 APS enabled WEP encryption. According to the results, high number of the tested wireless networks are unsecured and the security of the networks needs to be further enhanced to protect those networks.

**Fig. 4. The surveyed area in Ajdabiya city**

Figure 5 illustrates the results on the level protection of WLAN networks in Ajdabiya city. The figure shows that 47% of the networks are found to be using low level protection (WEP). The figure also shows that 53% of WLAN networks use no encryption. The survey indicates that the security standard is low due to lack of awareness in IT community in Ajdabiya city and the security of the networks needs to be further enhanced. Moreover, the wireless network that is using WEP are more vulnerable then network that using the recent configuration (WPA2), because the WEP 24-bit initialization vector and weak authentication. To secure the wireless network need Implement sophisticated password and configure the encryption to WPA2. These networks are either open because people who configure them lack security awareness or because these people leave them intentionally open.

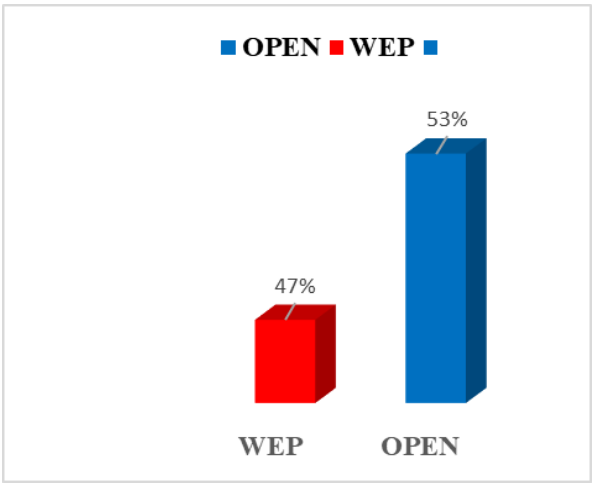


**Fig. 5. WLAN encryption status in Ajdabiya city**

figure 6 illustrates the results on the percentage of networks that use default SSID and non-default SSID names in Ajdabiya city. The figure shows that 22 (1.4%) of the networks are using default SSID names. The figure also shows that 1169 (74%) of networks use Non- default SSID names. The survey shows that the majority of WIFI networks in the area covered using Non -default SSID. However, the security standard is low due to lack of awareness in IT community in Elbrega city and the security of the networks needs to be further enhanced. To secure the wireless network need change default SSID, Implement sophisticated password and using high level protection.

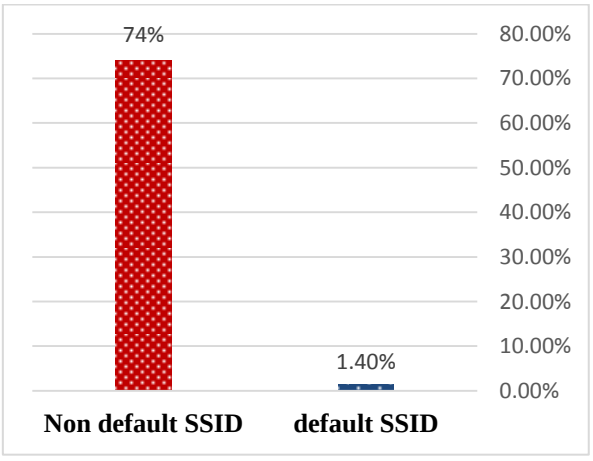


**Fig. 6. SSID Configuration in Ajdabiya city**

## 6.3 Comparison Results in Elbrega and Ajdabiya City

Figure 7 illustrates the results on the list of WLAN channels used in Elbrega city and Ajdabiya city. The figure shows that the majority of networks used channel 11 in Elbrega and Ajdabiya with an average rate of 79 % and 68%, respectively. The figure also shows that 10.6% of networks used channel 6 in Elbrega city and 17.3% used channel 6 in Ajdabiya city. Moreover, 2% and 5.6% used channel 1 in Elbrega and Ajdabiya respectively. The result indicated that high usage of channe11, whereas 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.

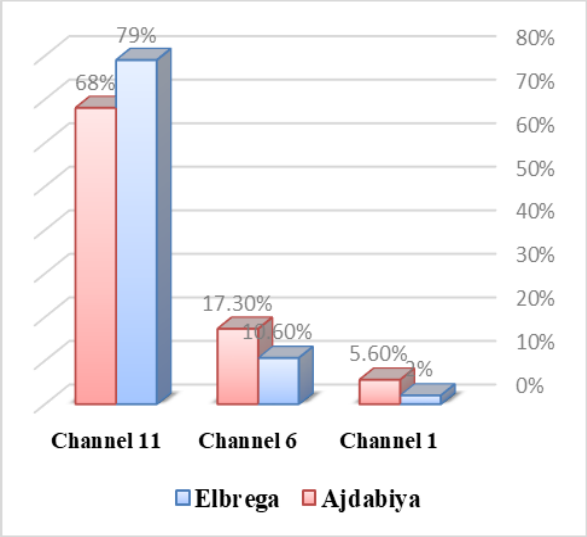


**Fig. 7. Comparison of WLAN Channel Usage in Elbrega and Ajdabiya**

Figure 8 illustrate the comparison in terms of WLAN Security in Elbrega and Ajdabiya city. The comparison result show that 55% of the wireless networks are secured with WEP encryption in Elbrega city. The figure also shows that 59% of the wireless networks are secured with WEP encryption in Ajdabiya city. Furthermore, the figure shows 81% of wireless networks used non-default SSID name in Elbrega city and 74% of wireless networks used non-default SSID name in Ajdabiya city. The results shown that the security in Ajdabiya city better than Elbrega city due to the majority of wireless networks using Non default SSID and enable WEP encryption .Ajdabiya city the fact that more offices are found in the downtown road and Internet centers. However, the security standard is low due to lack of awareness in IT community in that particular city. Moreover, the wireless network that is using WEP are more vulnerable then network that using the recent configuration (WPA2), because the WPE 24-bit initialization vector and weak authentication. To secure the wireless network need change default SSID Implement sophisticated password and configure the encryption to WPA2. Alternatively, these networks are either open because people who configure them lack security awareness or because these people leave them intentionally open.

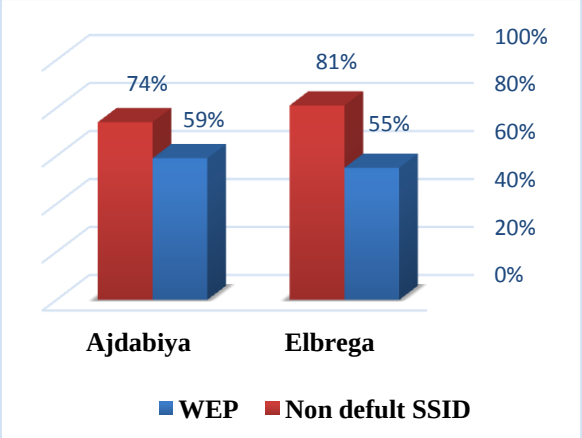


**Fig. 8. Wireless network statistics in Elbrega and Ajdabiya**

## 7. CONCLUSION

In this paper, security issues of wireless local area networks in Elbrega and Ajdabiya were surveyed and analyzed. The results indicate that the security standard is low due to lack of awareness in IT community in that particular city. The survey shows that the wireless network that are using WEP are more vulnerable then network that using the recent configuration (WPA2), because the WPE 24-bit initialization vector and weak authentication. To secure the wireless network need change default SSID Implement sophisticated password and configure the encryption to WPA2

## 8. REFERENCES

[1] Loo, A. W., "Illusion of Wireless Security," Advances in Computers, Volume 79, (2010), 119-167.

[2] Bulbul, H. I., Batmaz, I., and Ozel, M. (2008). Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected protocols). First international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop (e-Forensics '08), ICST, Brussels, Belgium, Belgium.

[3] Zadig, Sean, M and Tejay, G. (2010). Securing IS assets through hacker deterrence: A case study. In the proceedings of conference on Anti-Phishing Working Groups 2nd Annual e Crime Researchers Summit-eCrime,. 1-7, 2010.

[4] Kalbasi, A., Alomar, O., Hajipour, M., Aloul, F. (2007). Wireless security in UAE: A survey paper. In: Proceedings of the 4th IEEE-GCC Conference; IEEE, Manama, Bahrain.

[5] Chenoweth, T., Minch, R and Tabor, S. "User security behavior on wireless networks: An empirical study", (2007), IEEE.

[6] Sarkar, N., Abdullah, AH. (2011). Exploring wireless network security in Auckland City through war walking field trials. In: Proceeding of the 13th International Conference on Advanced Communication Technology, IEEE. Gangwon-Do, South Korea. 685-689.

[7] Nisbet, A. A. (2013). Study of wireless network security in New Zealand: Are we there yet. In: Proceedings of the 11th Australian Information Security Management Conference, Edith Cowan University, 75-82. Perth, Australia.

[8] Nagashree, R N., Vibha, Rao. ,Aswini, N,"Near Field Communication", IJWMT, VOL.4(2), (2014),20-30, 2014.DOI: 10.5815/ijwmt.

[9] Sebbar, A. SE., Boulahya, G., Mezzour, M., Boulmalf. (2016). An Empirical Study of WIFI Security and Performance in Morocco -WarDriving in Rabat, 2nd International Conference on Electrical and Information Technologies ICEIT.1-6.

[10] Ho, J. T., Dearman, D., Truong, K. N, "Improving Users' Security Choices on Home Wireless Networks", ACM, (2010). DOI=10.1145/1837110.1837126. [online]. Available :http://doi.acm.org/10.1145/1837110.1837126

[11] Vishal, K., Akhil ,T., Pawan ,T., Ashish, G. and Seema, S., "Vulnerabilities of wireless security protocols (wep and wpa2) ", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), VOL 1(2), ( 2012),34–38.

[12] Mike, M. (2004).Network Guide to Managing & Troubleshooting Networks Lab Manual. McGraw-Hill, Inc., Wi-Fi Protected Access (WPA). Thomas, M. (2004). "Network Security First-Step".Cisco Press, Indiana, USA. ISBN: 1-58720-099-6. p315.

[13] William, S. and Lawrie, B., "Computer security", Principles and Practice, 2008.

[14] Conklin, W., Williams, D., White, G., Davis,R. and Cothern, C. "Principles of Computer Security," McGraw Hill Technology Education, (2004).

[15] Air, M. Inc., "Managing WLAN Risks with Vulnerability Assessment: A Technical Whitepaper", October 2005.