iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Comparison and Analysis of Existing Security Protocols in Wireless Networks

Kirti Rana[1], Aakanksha Jain[2]
[1,2,]*Computer Science Department, Deenbandhu Choturam University of Science and Technology*

Abstract: ***Today over the past few years, there has been a rapid growth in the use of wireless networks. Since they have introduced in the mid 1990s, they have proliferated among home users and have taken over organizations whether or not they are authorized. Users want to secure their important information, companies want to transfer their sensible data over WLAN, that's why lots of people are doing research on WLAN to improve the security. For Security purpose different kinds of protocols are available. But fast development in codes, standards and technology gives hackers an opportunity not only to hack and steal the important information but also to change the integrity of transmitted data aver wireless network. In this case, contrast between the usage of wireless networks and security standards show that the security s not keeping up with the growth pace of end user's usage. Lack of rigid security standards has caused many companies to invest millions an securing their wireless networks.***

There exist different kinds of tools and programs inbuilt in operating system. By using them and analysing weaknesses of protocol used, cracking of protocol is easy. Researchers have proposed three main security protocols: WEP, WPA and WPA2 to provide security in wireless networks. This research is going to compare the WEP and WPA encryption mechanism for better understanding of their working principles and security bugs. We will also study in this paper about how security protocols authenticate the users. The major part in this thesis is to show how easy it is to crack the security protocols of wireless networks with a set of software in windows also. For this purpose, we will use the vendor script named aircrack-ng and commview software which helps in showing the procedures for hacking.

Keywords: ***WEP, WPA, WPA2, Wireless, 4-way handshakes, attacks***

I. INTRODUCTION

The existing security protocols in WLAN are wired equivalent privacy (WEP), Wi-Fi protected access (WPA1), and Wi-Fi protected access II (WPA2). WEP is the simplest and uses computationally light cipher. However, it has been shown to be insecure and should no longer be used. WPA1 is stronger than WEP; but, has few security vulnerabilities and was replaced by WPA2. WPA2 is known to be secure since it relies on strong cipher AES. In last paper, we have discussed the encryption mechanisms of data protection or security in wireless network. In this paper, we would try to highlight the weaknesses and authentication procedures of the security protocols: WEP and WPA/WPA2. Finally, with the help of software we would try to show how easy it is to crack the security protocols of wireless networks in Windows also.

II. PROBLEM FORMULATION

Similar to all wireless technologies, security in WLAN is considered one of its main weaknesses. The wireless medium is shared among the users and open access for any malicious attacker. That's because systems become vulnerable to negative forces due to the lack of proper safeguards. There are several vulnerabilities that occur mostly in wireless network because of the very nature of the LAN, which uses radio frequencies (RFs) to permit the transmission of data over the airwaves. One major reason that a number of vulnerabilities occur in SOHO is because uninformed users setup wireless LANs without the prudence necessary to secure these systems from malicious or even accidental events.

In this section we provide a brief description of the weaknesses of the most commonly used security protocols in WLAN. We also learn about the Authentication processes of the security protocols which are WEP and WPA/WPA2.

A. WEP

Now we will give the description of the WEP weaknesses and WEP authentication process (which will give us an idea how it is easy to crack it) in the following way:

1) *WEP Shared Key Authentication:* In this, WEP encryption works between wireless AP and wireless station. At first the wireless station and Access Point shares their secret key which we commonly called as passphrase which is shown in Figure 7. As a first step, a wireless client sends an authentication to the access point. In this step, no data encryption takes place. Then the Access Point responds with an authentication response message consist of challenge text. Now the client uses its secret WEP key to encrypt the challenge text and sends it to the access point. If the access point, successfully decrypt the encrypted challenge and retrieve the original challenge text then it comes to know that the client is also using the same secret key. So responds with a confirmation success message. Finally data transfer takes place.
2) *Security Vulnerabilities in WEP:* In computer, data or network security a proposed solution does not always cover or profile solution to all the areas that have weakness in the corresponding field. The WEP protocol has some security weakness such as:

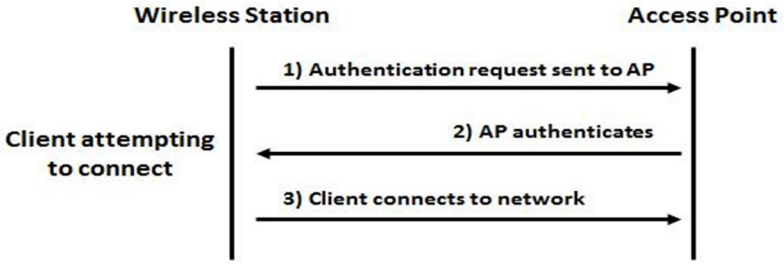


Figure 6: Open System authentication

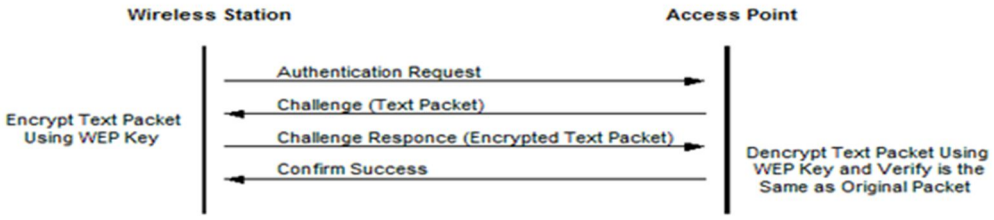


Figure 7: Shared Key Authentication

a) *Weak Cryptography:* Captured network traffic analyzed showed that shared key that is been used by the WEP can be easily decoded analyzing the captured data. This can lead to data manipulation and loss of data integrity.
b) *Absence of Key Management:* The WEP does not have the key management feature to manage different keys in its key table, rather same key is used for a very long period of time and this shows poor quality.
c) *Small Key Size:* The key size of the WEP standard is only 40-bit key. This makes the WEP open to attack especially the brute force attack, because the encryption key is only 40-bit. The brute force attack as form of an offline dictionary mechanism that probes the network with frequently used encryption words and check out the data gotten from the captured traffic to get the secret passphrase.
d) *Reuse Initialization Vector:* WEP reuses the initialization vector. This can lead to the data decryption without the use of the appropriate key, because the IV can be gotten easily and other crypto-app can be used to decrypt the data.
e) *Authentication Issues:* Due to the challenge-response scheme that is used in shared key authentication, a man-in-the-middle attack can be carried out in the WEP. Such kind of attack which posses as the corresponding destination or source of a data in a network in order to gain access to confidential information that is in transit. This lead to sensitive information to be compromised and if possible it can also lead to data loss.
f) *Packet Forgery:* There is no protection against packet forgery in WEP. Data packets can be forged using third-party application and injected into the network, this can lead to data manipulation and loss of data integrity.
g) *Flooding:* This is sending of huge data packets which mean lots of messages to an access point and thereby preventing the legitimate users from gaining access to the network, and also limiting the access point from processing data in the traffic.

B. WPA/WPA2

Now we will give the description of the WPA/WPA2 weaknesses and WPA/WPA2 authentication process (which will give us an idea how it is easy to crack it) in the following way:

1) *Authentication Process of WPA/WPA:* The authentication process is known as 4-way handshake. The authentication process leaves two considerations: the access point (AP) still needs to authenticate itself to the client station (STA), and keys to encrypt the traffic need to be derived. The earlier EAP exchange or WPA2-PSK has provided the shared secret key PMK (Pairwise Master Key). This key is, however, designed to last the entire session and should be exposed as little as possible. Therefore the four-way handshake is used to establish another key called the PTK (Pairwise Transient Key). The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address, and STA MAC address. This is a handshake using PMK. The handshake also yields the GTK (Group Temporal Key), used to decrypt multicast and broadcast traffic. The actual messages exchanged during the handshake are depicted in the figure 8. Firstly, the AP sends a nonce-value to the STA (ANonce). The client now has all the attributes to construct the PTK. The STA sends its own nonce-value (SNonce) to the AP together with a MIC, including authentication, which is really a Message Authentication and Integrity Code: (MAIC). The AP sends the GTK and a sequence number together with another MIC. This sequence number will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection. The STA sends a confirmation to the AP.
2) *Security Vulnerabilities in WPA/WPA2:* While a number of minor weaknesses have been discovered in WPA/ WPA2 since their release, none of them are too dangerous provided simple security recommendations are follows as:

a) *Attack on PMK Key:* The most practical vulnerability is the attack against WPA/WPA2's PSK key. The PSK (Pre-Secret Key) provides an alternative to PMK (Pre-Master Key) generation using an authentication server. It is a string of 256 bits or a passphrase of 8 to 63 characters used to generate such a string using an algorithm. The PTK is derived from the PMK using the 4-Way Handshake and all information used to calculate its value is transmitted in plain text. The strength of PTK therefore relies only on the PMK value, which for PSK effectively means the strength of the passphrase.

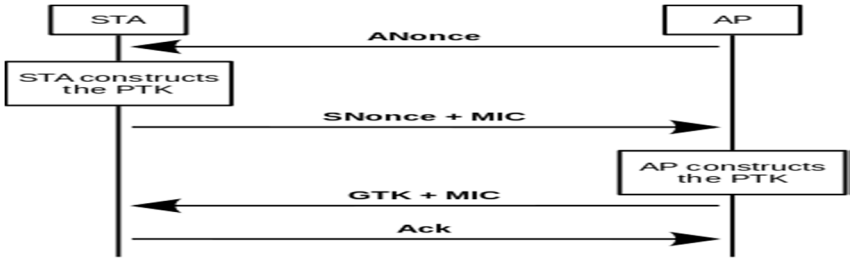


Figure 8: 4-Way Handshake

b) *Communications Interception:* If a user intercepts the user authentication process with a Wi-Fi sniffer called 4-way handshake and cracks the Wi-Fi network password, or rather knows the password, he or she could decrypt the traffic of any other user connected to the Wi-Fi network.

c) *Brute Force Attack:* The second message of the 4-Way Handshake could be subjected to both dictionary and brute force of-fline attacks. To perform this attack, the attacker must capture the 4-Way Handshake messages by passively monitoring the wireless network or using the de-authentication attack to speed up the process.

d) *DoS Attack:* The other main WPA weakness is a Denial of Service possibility during the 4-Way Handshake. It has been noticed that the first message of the 4- Way Handshake isn't authenticated and each client has to store every first message until they receive a valid third (signed) message, leaving the client potentially vulnerable to memory exhaustion. By spoofing the first message sent by the access point, an attacker can perform a DoS on the client if it possible for several simultaneous sessions to exist.

e) *Michael Message Integrity Code:* It also has known weaknesses resulting from its design. The security of Michael hinges on communication being encrypted. While cryptographic MICs are usually designed to resist known plaintext attacks (where the attacker has a plaintext message and its MIC), Michael is vulnerable to such attacks since it is invertible. Given a single known message and its MIC value, it is possible to discover the secret MIC key, so keeping the MIC value secret is critical.

III. IMPLEMENTATION

A. *Breaking and Cracking WEP*

Some flaws in WEP make it easy to crack. The encrypted packet along with IV is sent as plain text. Thus the information which is out in the air ware can be easily cracked by anyone and can hack the secret key. During a few iterations KSA and PRGA leak

information of their algorithm. With the help of XOR which is a simple process used to deduce unknown value if the other two values are known. We need lots of IVs in order to sufficiently crack a real life WEP key of a wireless AP. These IVs are not generated very quickly in normal network traffic. It needs lots of patience to crack the WEP key by simply listening of the network traffic and saving them. The process injection is used to speed up the process. Injection involves resending process again and again very rapidly. Thus in a short period of time we can capture a large number of IVs, after determining the IVs. We use these IVs for determining the WEP key.

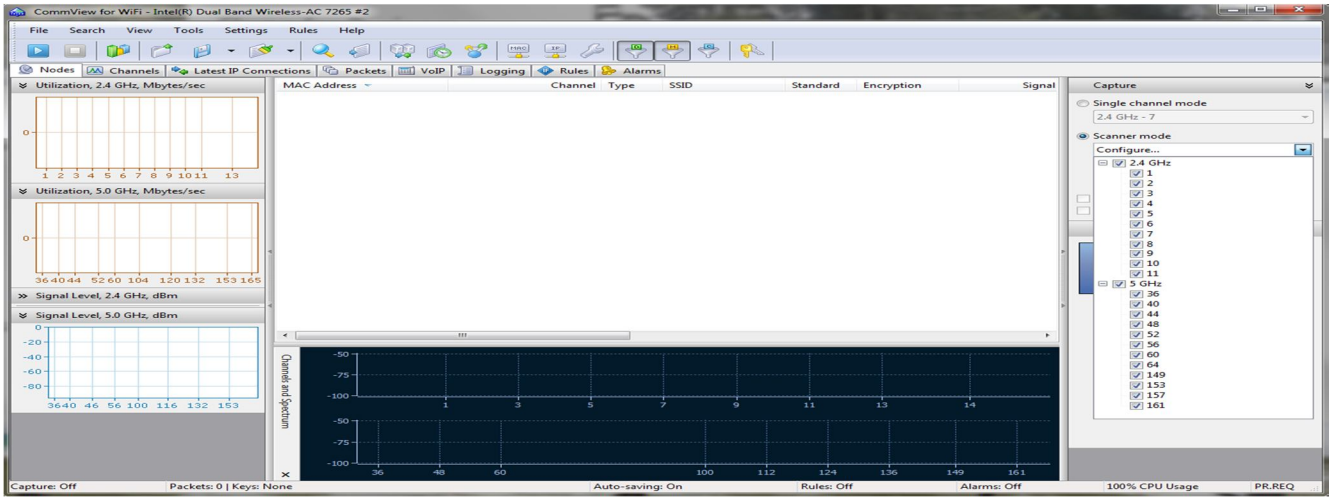


Figure 9: Selecting all the channels of Scanner mode

Open the commview and select the scanner mode from a new channel selection and scanner control. In Figure 9, we select all the channels of both frequencies. So that it scan all the wireless networks of any frequency and channel. Click the play button and scan for the network you want to crack as shown in Figure 10. Once you have found it, drag the channel menu down to the desired channel and again click the play button in Figure 11.

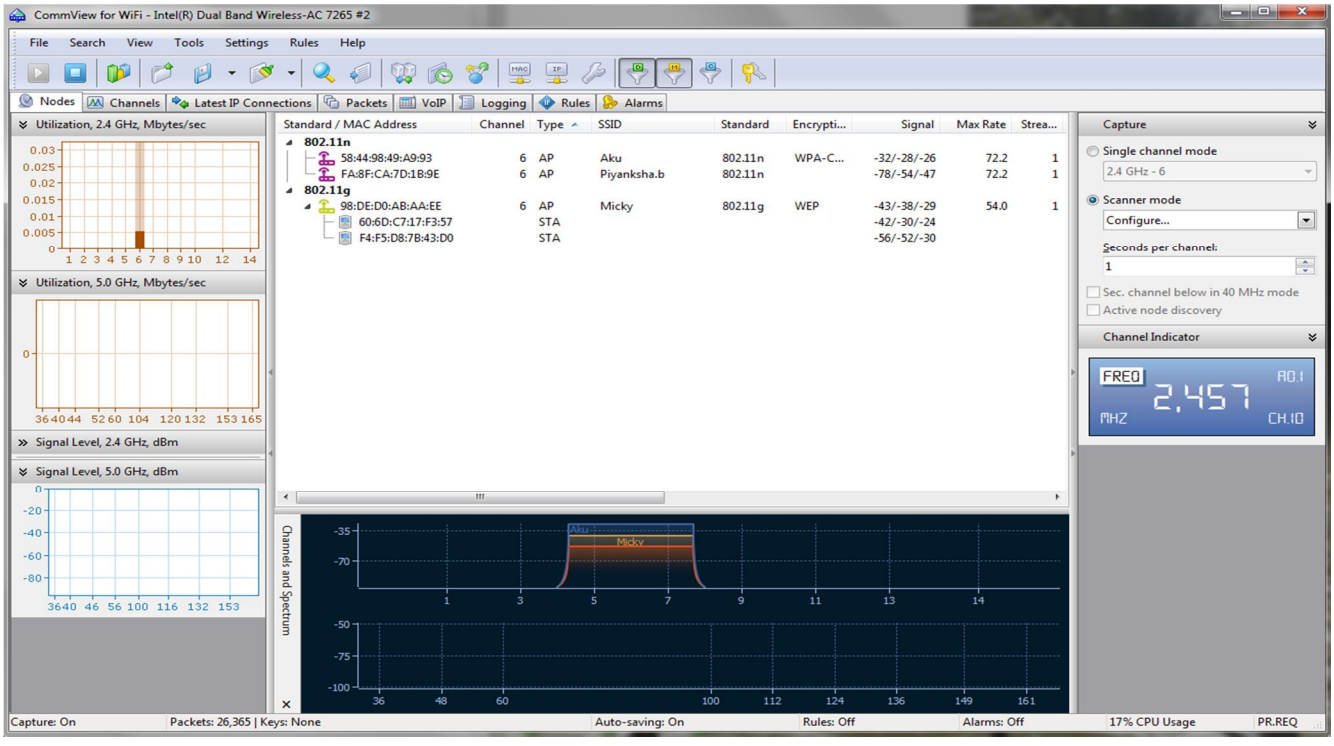


Figure 10: Play the Scanner Mode

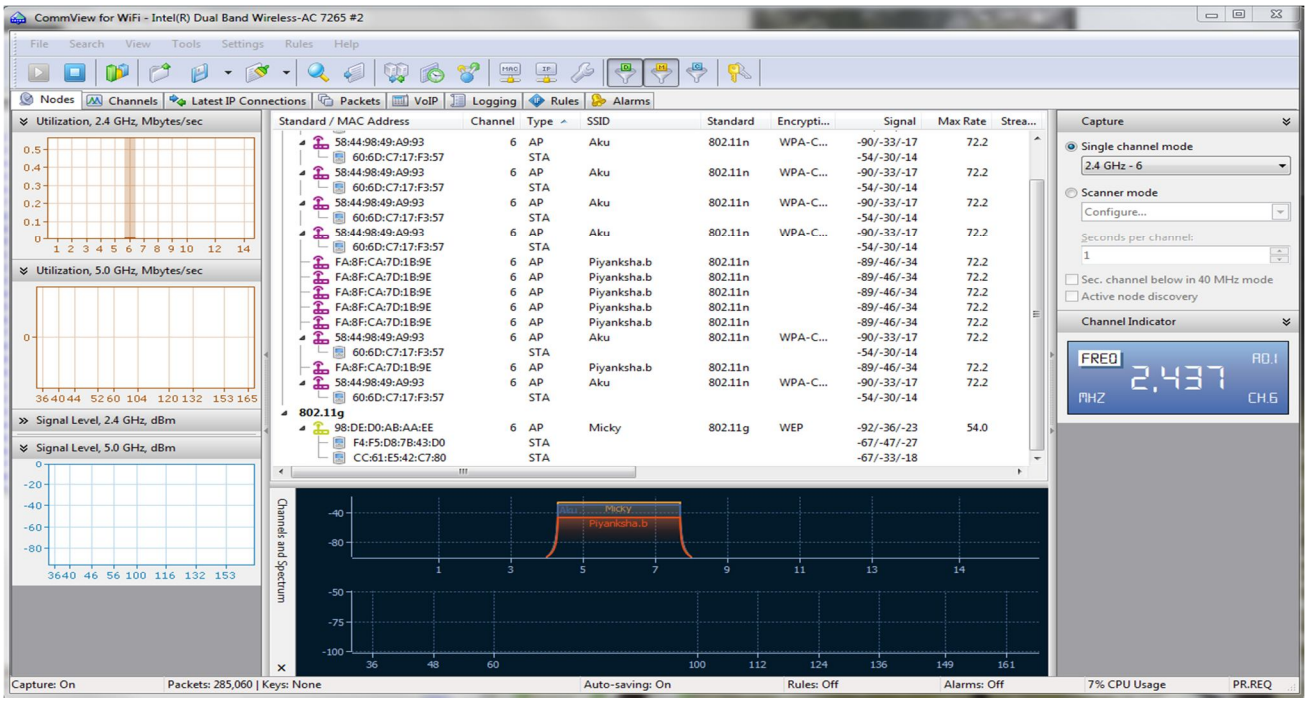


Figure 11: Play the Single Channel Mode

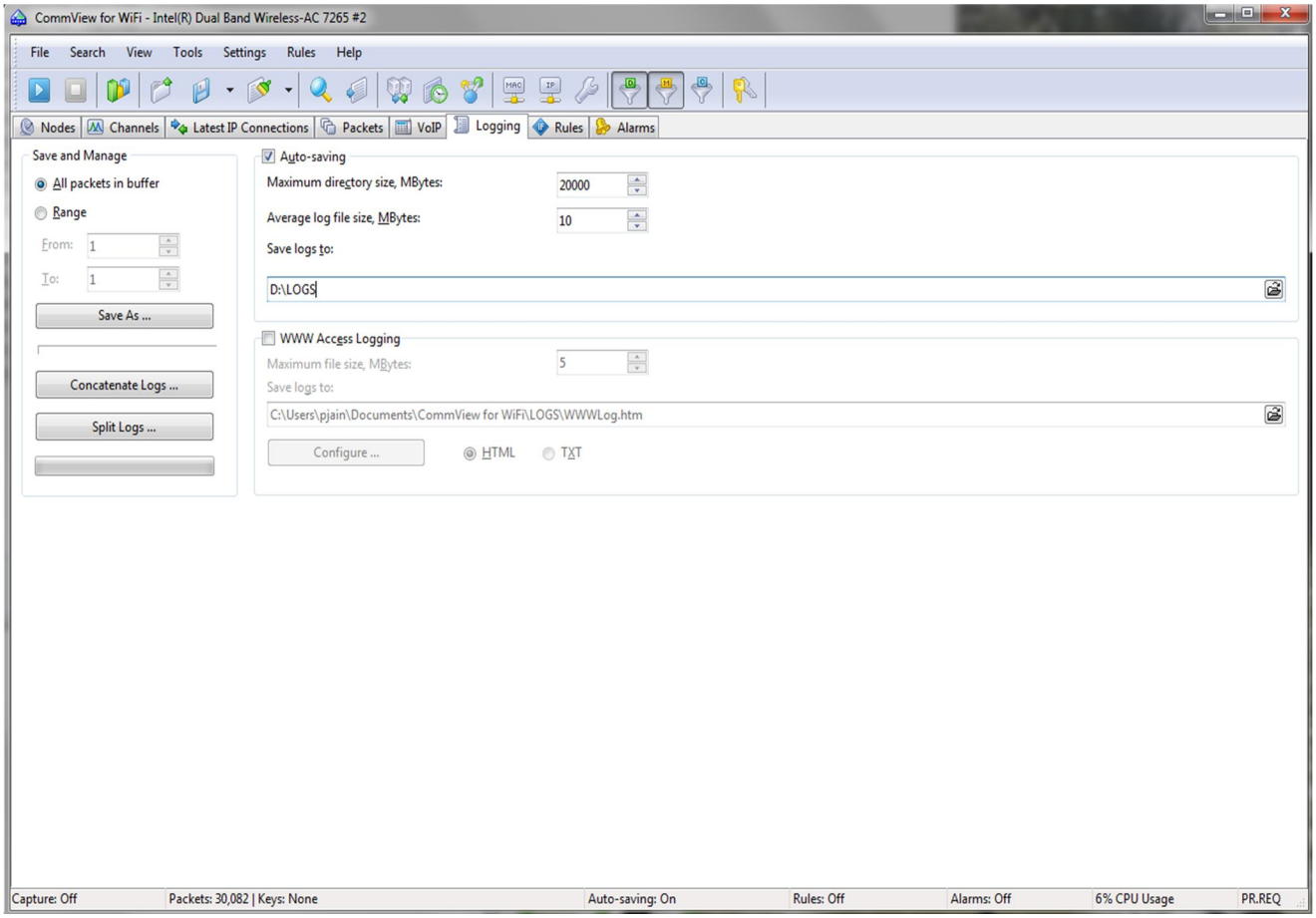


Figure 12: Set the Logging Tab

Open the logging program interface, check on the Auto-saving and change the "Maximum Directory Size" to 20000 MB and "Average Log File Size" to 30 MB. Also set the location in "Saves Logs To" where you want to save the logs in Figure 12. Then come back to the home page and select the packets tab. Here all the packets are collecting. When there will be traffic on that network, more packets will be collected. The more packets we receive the more probability of hacking success will be in Fig 13. When the packets in lakhs collected then open the file and choose the "Load Commview Logs" from file. It will load all the received packets in Figure 14.

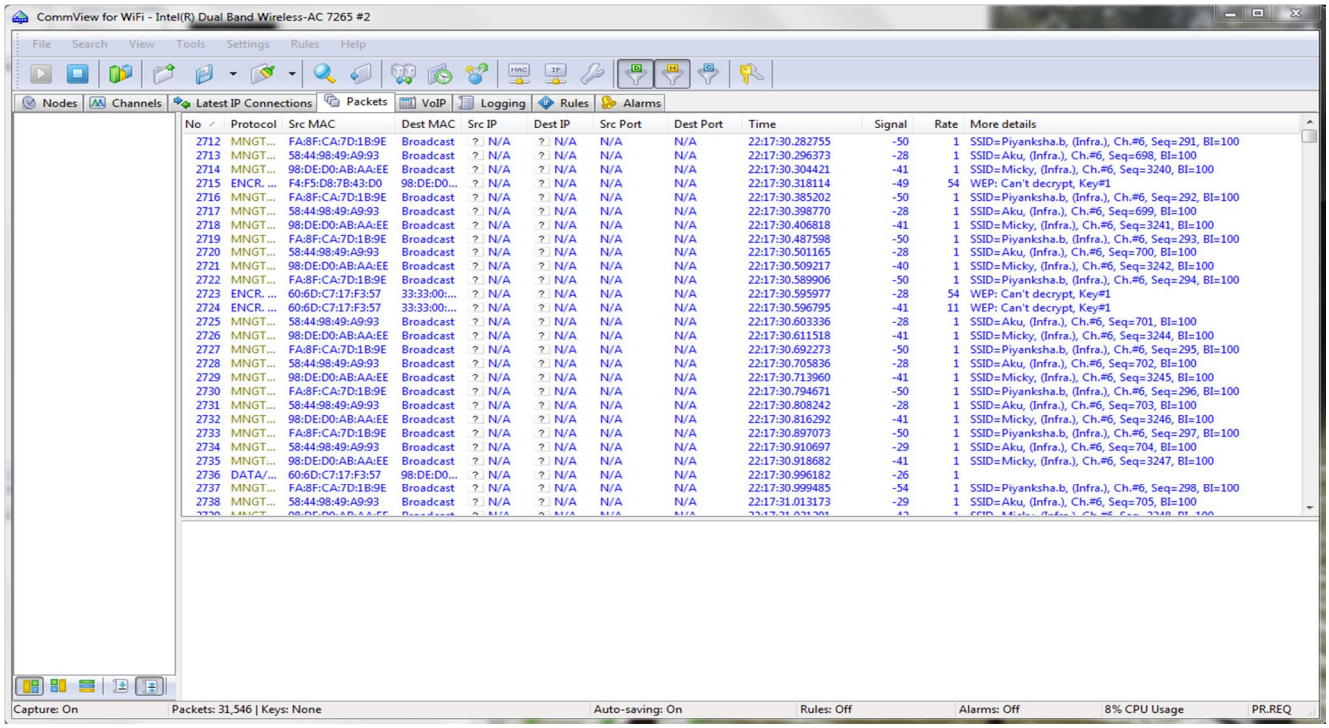


Figure 13: Check the Captured Network Packets

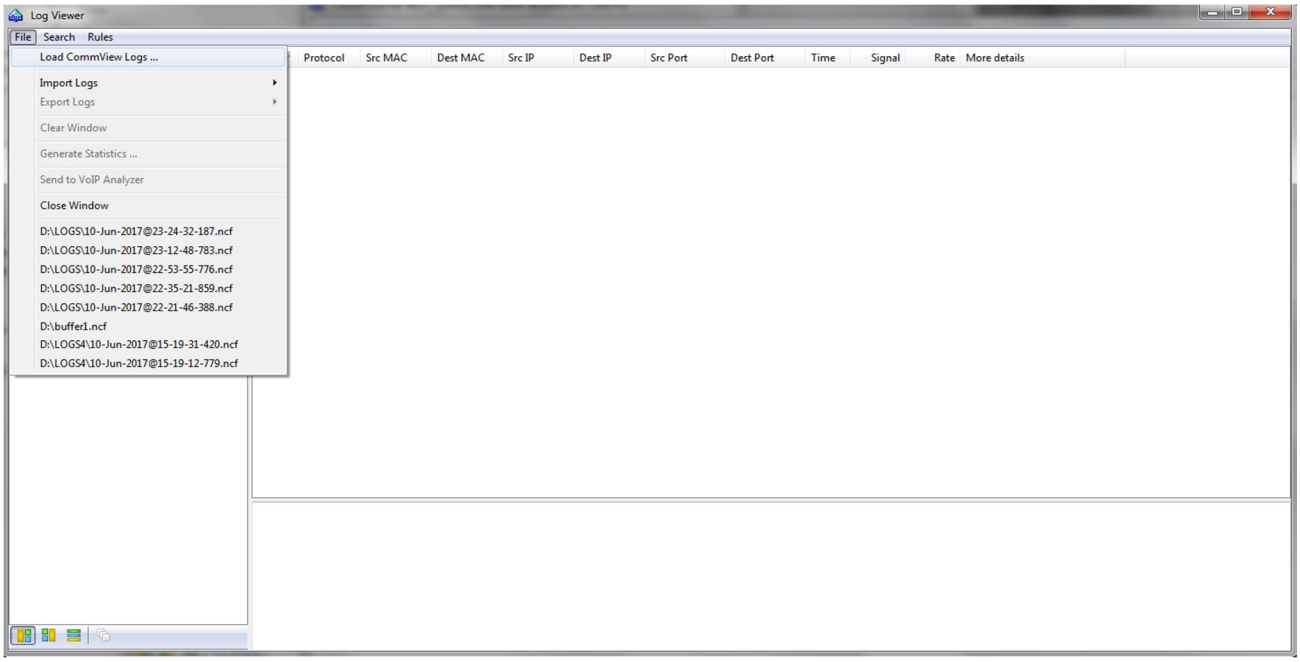


Figure 14: Load the Connection Logs

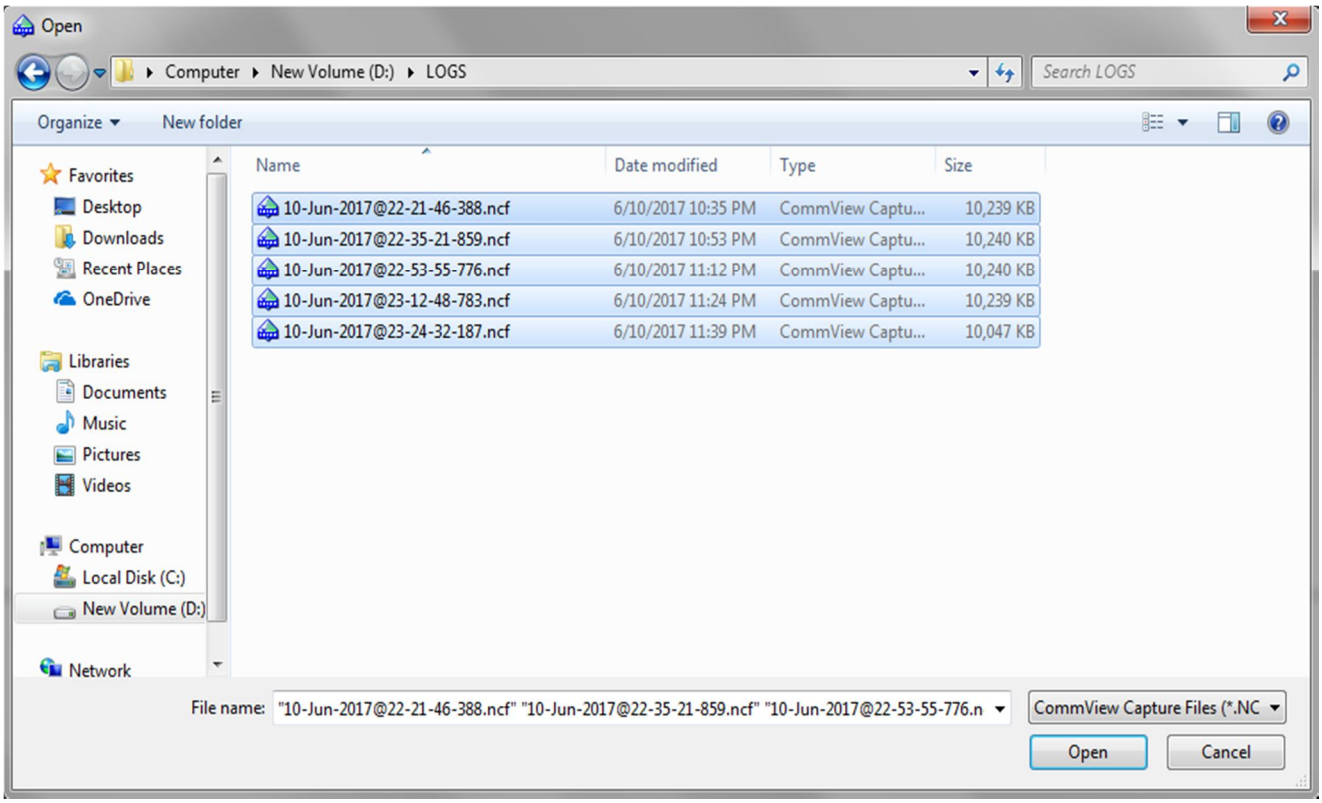


Figure 15: Save the Loaded Connection Logs in NCF Extension

Save the loaded file to the location which we have specified in the logging tab in ncf extension. After again select the file in "Packets" tab and select "Export Logs" in which some further options will be given. There select "Wireshark/tcpdump Format". Now save the file at the location you want to in tcp extension as shown in Figure 16.

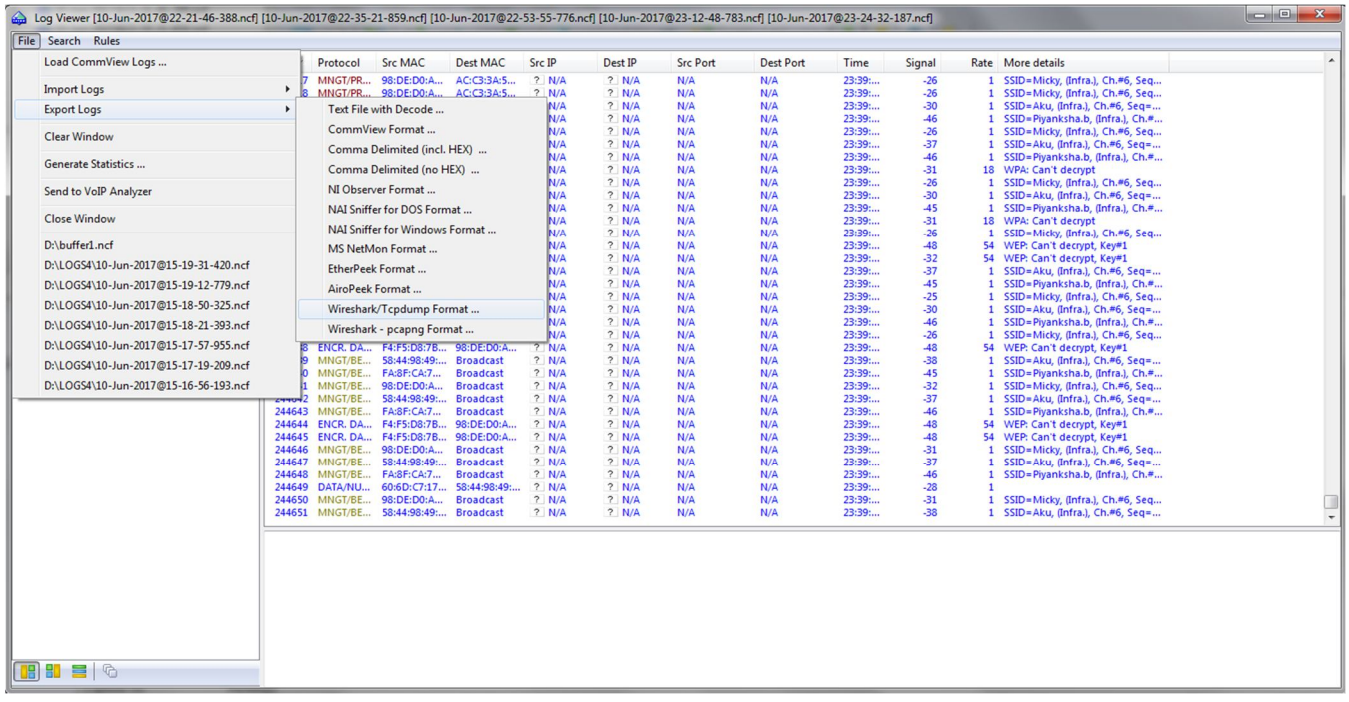


Figure 16: Export the Logs

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

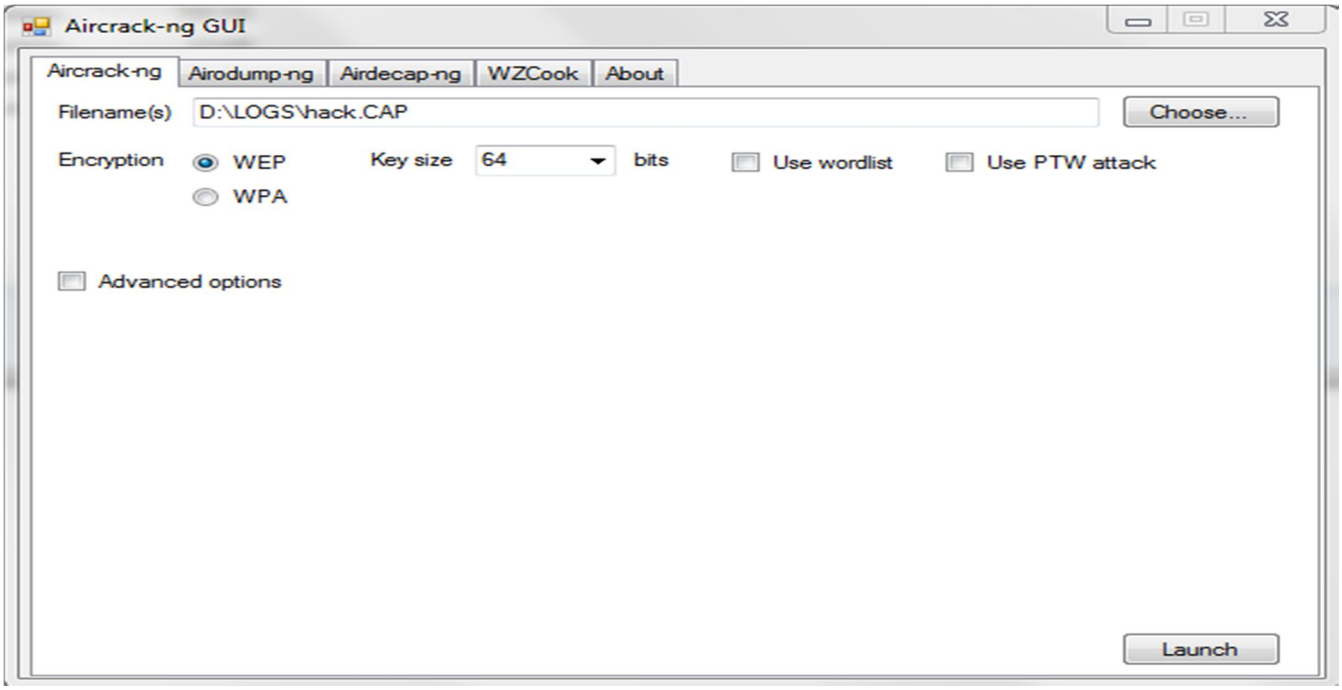


Figure 17: Upload the Log File

Open aircrack-ng-GUI that can be found in the map “bin”. Select the files you saved in cap extension, set the encryption to WEP and change to key size as you desired. Then click on launch in Figure 18. Look at the list of IV’s you have, and select the network you want to crack from the list of all identified networks, choose the one for which you have captured the IVs to hack the network in Figure 19.

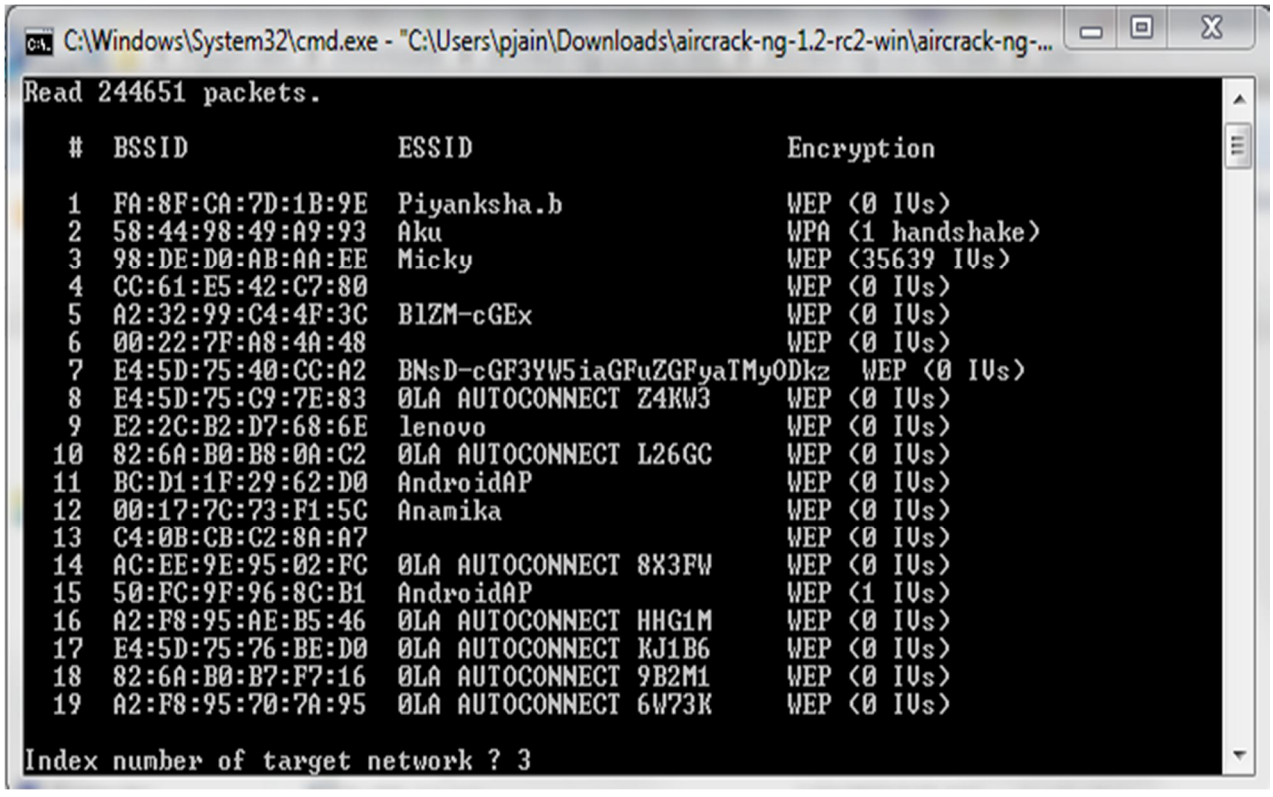


Figure 18: Packets Ready for Interjection

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

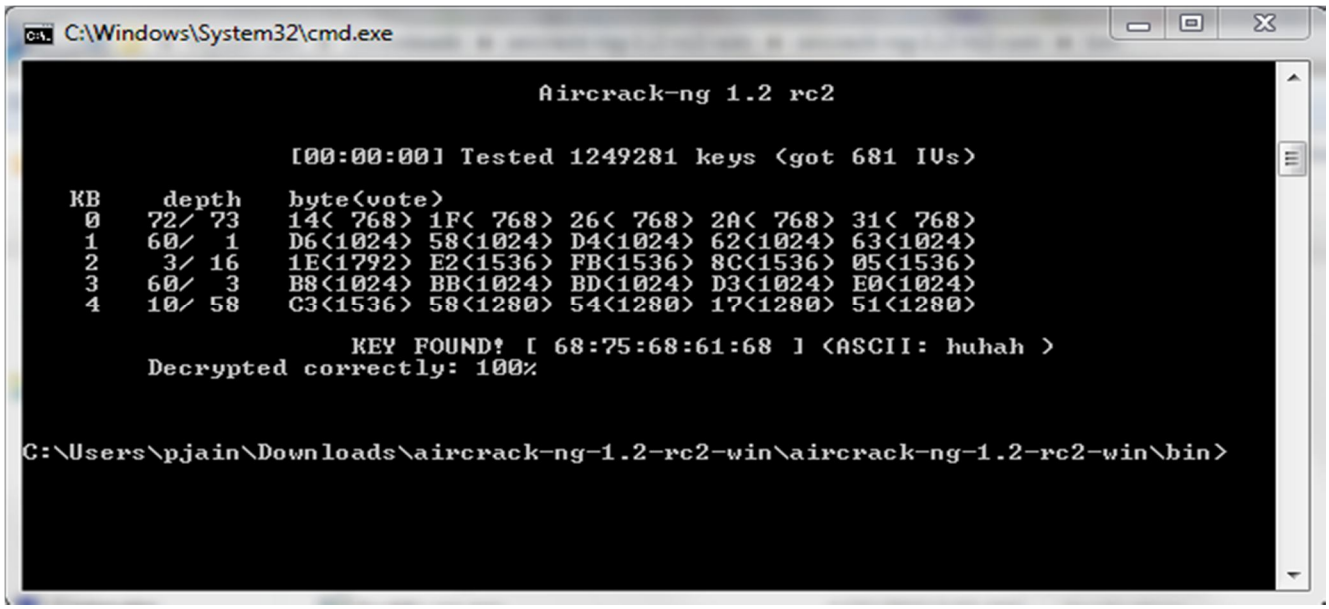


Figure 19: Cracking is Successful

When it shows KEY FOUND, it means hacking is successful. You are now connected to the desired network.

B. Breaking and Cracking WPA/WPA2

To successfully crack WPA/WPA2, we first need to be able to set the wireless network card in "monitor" mode to passively capture packets without being associated with a network. This can be done using commview. This NIC mode is driver-dependent. One of the best free utilities for monitoring wireless traffic is done by the commview and cracking of WPA-PSK/WPA2-PSK keys is done by the aircrack-ng suite. It has both Linux and Windows versions (provided your network card is supported under Windows). Here we will use commview version 7 and aircrack-ng version 1.2 on a Windows OS on Dell latitude E7450 laptop, using the built-in Intel network card. 4-Way Handshake is a way through which cracking can be done which is related to wireless network. The information in the first two messages is enough for password cracking. Even though it is enough, it is important to eavesdrop the whole 4-Way handshake to be sure that the handshake was successful and that the information in the first two messages is valid.
The procedure of capturing of IV is exactly same using CommView as it is for WEP as shown in Figure 9 to Figure 17. Open aircrack-ng-GUI that can be found in the map “bin”.

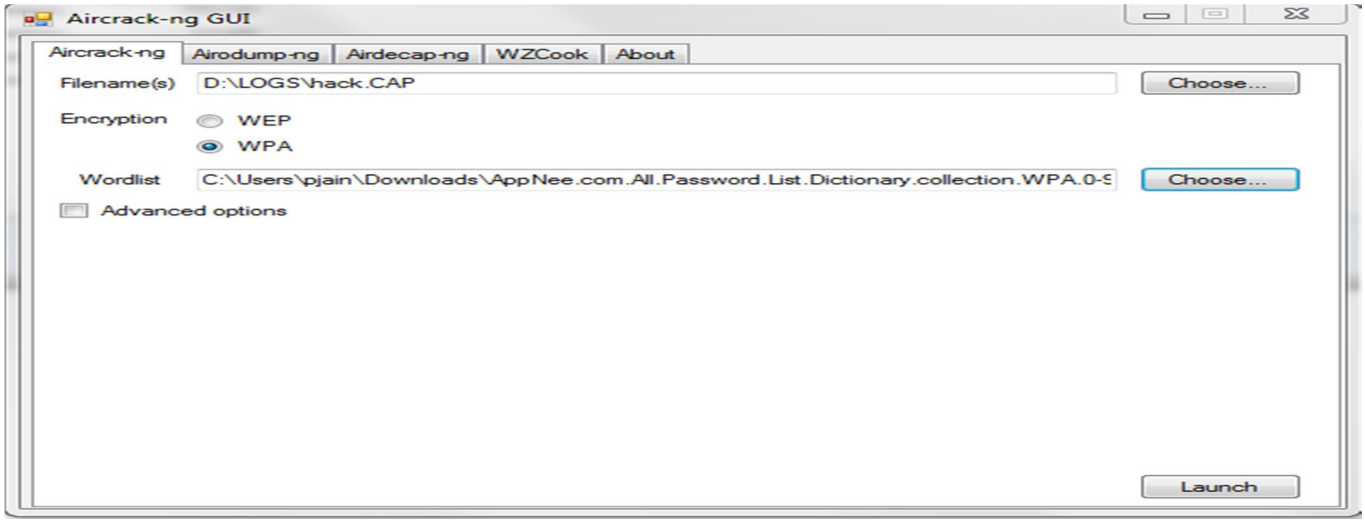


Figure 20: Select the Log File and Wordlist

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Select the file you saved in CAP extension, set the encryption to WPA and choose the wordlist. Then click on launch as shown in Figure 20. Look at the list of handshakes you have, and select the network you want to crack from the list of all identified networks, choose the one for which you have captured the IVs to hack the network in Figure 21. Through Wordlist, it is trying to find a password in Figure 22. When it shows KEY FOUND, it means hacking is successful. You are now connected to the desired network in Figure 23.

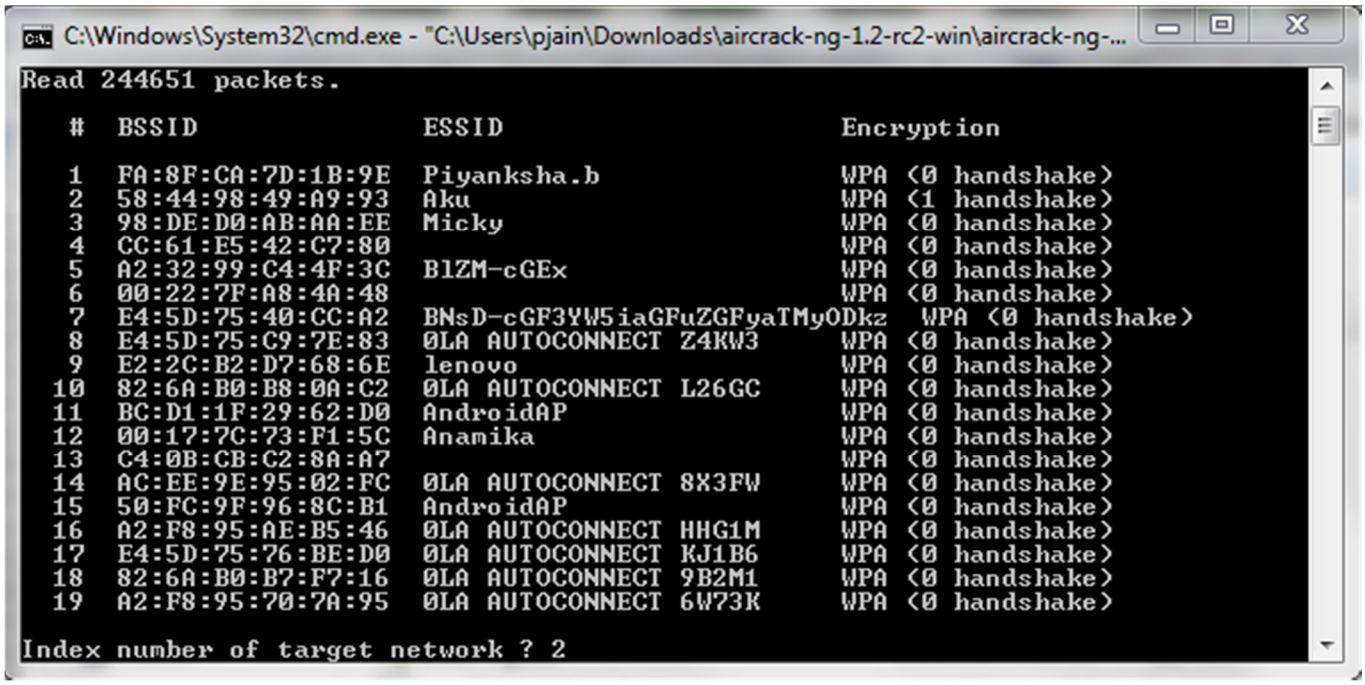


Figure 21: Handshake Happened and Packets Ready for Interjection

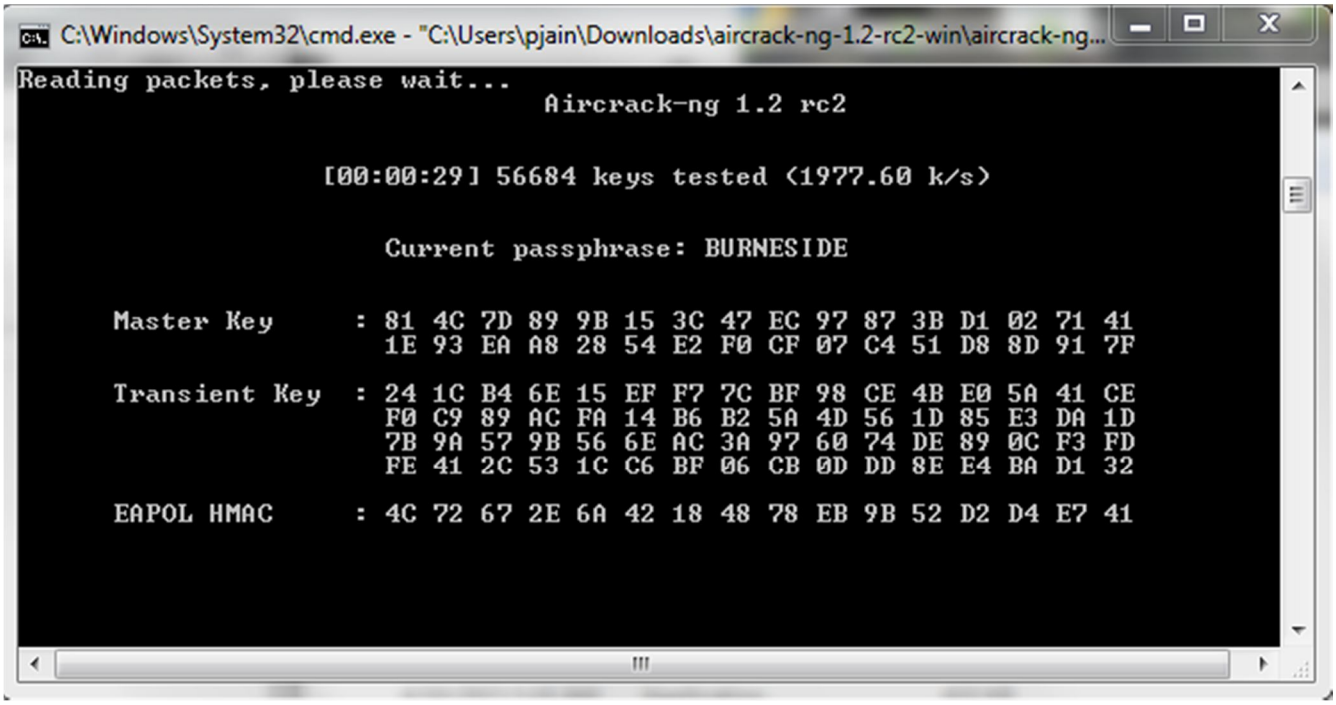


Figure 22: Through Dictionary Searching a Password

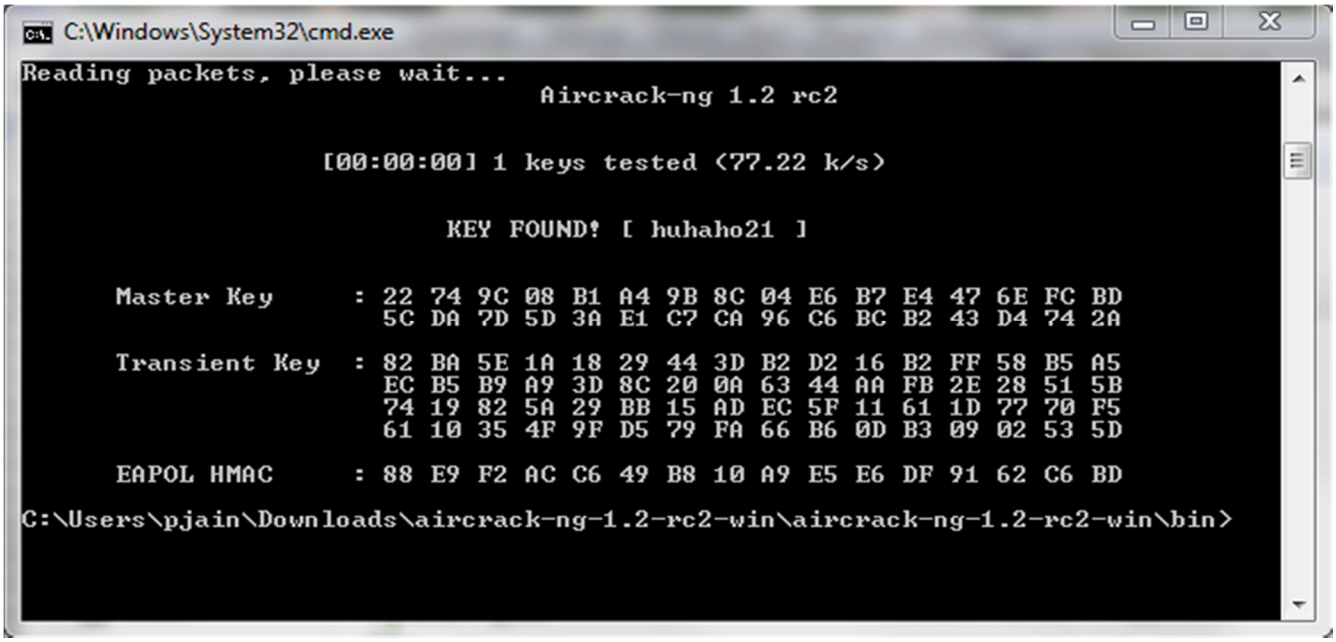


Figure 23: Cracking is Successful, Password Found

IV. CONCLUSIONS

Today the most successful technology that has spread over the world is wireless networks. The development of wireless network is the unique and outstanding in the technology world because of its various advantages, portability and convenient to end user. As all the communication that happens is through the airwaves because of which data get compromised, altered, and stolen always. In this paper we have focused on protocols WEP and WPA/WPA2. The overall detailed description of these protocols has been examined and later the implementation of cracking of these protocols is showed in this paper. The study of authentication protocols led us to knowledge of WEP and WPA/WPA-PSK breaking and cracking. This study may lead us to harden our protocol system and making it resistant to cracking tools. It is clear that WEP encryption does not provide sufficient wireless network security and can be easily cracked within a minutes using some set of software in windows. WPA and WPA2 is a secure solution as cracking is not that much easy and takes lot of time.

While hacking one need to very patient as sometimes cracking WPA / WPA2-PSK takes lots of time. We did the breaking procedure by means of dictionary which means if word is there in the wordlist then and then only cracking can be done. At last, we concluded that the WPA / WPA2-PSK is possible to crack but not easy to hack as compare to WEP.

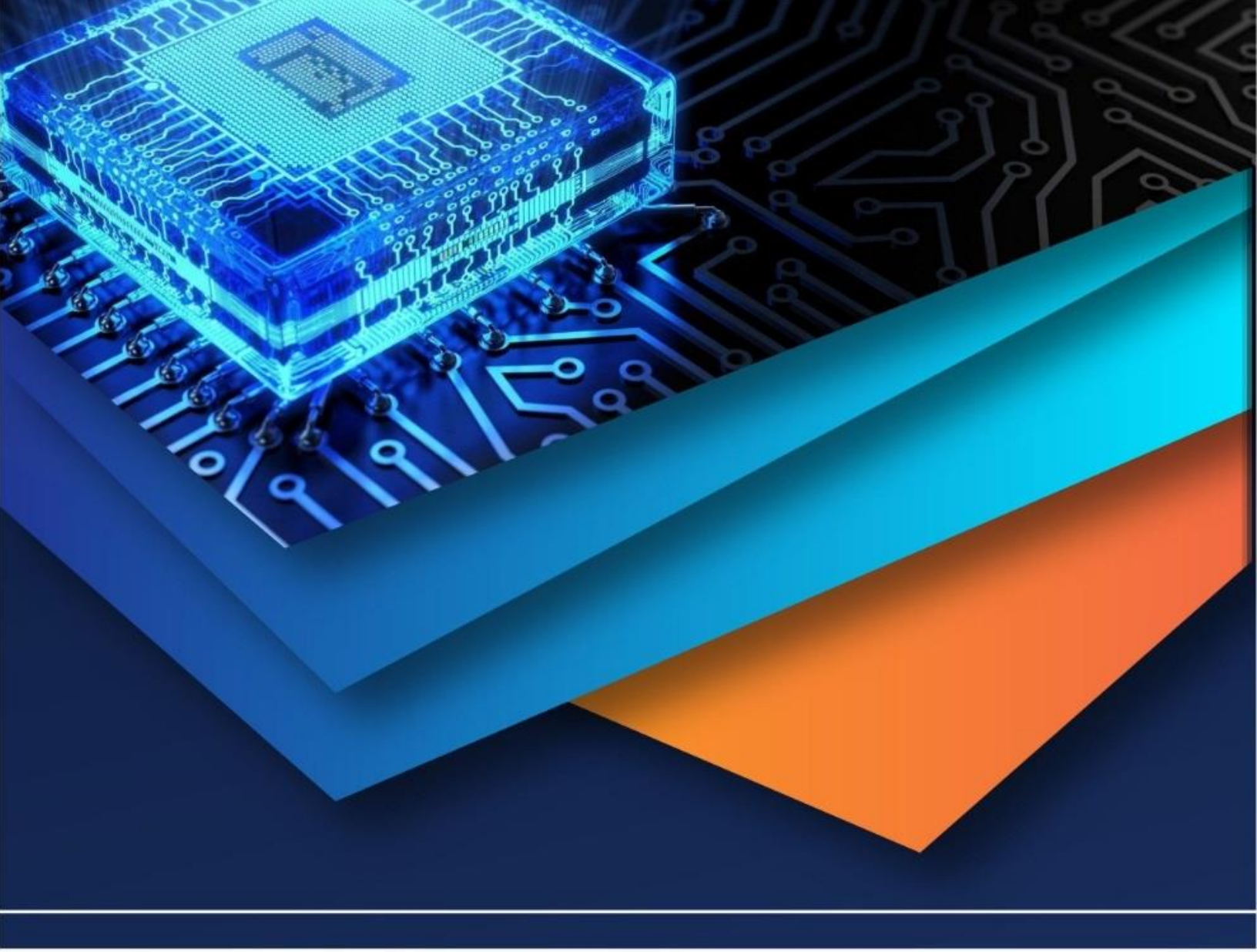
V. ACKNOWLEDGMENT

We would like to express our appreciation to our parents and all the teachers and lecturers who help us to understand the importance of knowledge and show us the best way to gain it. I would also like to thank my husband, Piyush Jain, for helping and supporting me to achieve the goal of the project.

REFERENCES

[1] Miler, (2008) WPA2 Security: Choosing the Right WLAN Authentication Method for Homes and Enterprises, Global Knowledge.
[2] A. Sari, (2012) Impact of Determinants on Student Performance towards Information Communication Technology in Higher Education. International Journal of Learning and Development, 2, 18-30.
[3] Benton, K. (2010) The Evolution of 802.11 Wireless Security. INF 795, April 18th, 2010. UNLV Informatics, Spring
[4] A.H. Lakshkari, M.M.S.Danesh and B. Samandi, " A Survey on Wireless Security Protocols (WEP, WPA and WPA2/802.11i)", Computer Science and Information Technology, 2009.
[5] V. Poddar, H. Choudhary, A Comparitive Analysis of Wireless Security Protocols (WEP and WPA2), Jaipur, Rajasthan: International Journal on AdHoc Networking Systems (IJANS), Vol. 4, July 2014
[6] A. Sari, M. Karay, Comparative Analysis of wireless Security Protocols: WEP Vs WPA, Int. J. Communications, Network and System Sciences. Kyrenia, Cyprus: Scientific Research Publishing Inc., 2015.
[7] E. Tews. (2007), Attacks on the WEP Protocol. [online]. Available: http://eprint.iacr.org/2007/471.pdf

[8] P.S. Ambavkar, P.U. Patil and P.K. Swamy, "Exploitation of WPA Authentication", IOSR Journal of Engineering (IOSRJEN), Vol. 2 Issue 2, pp. 320-324, Feb. 2012.
[9] H.D. Lane, " Security Vulnerabilities and Wireless LAN Technology", GIAC Security Essentials Certification Assignment. Virginia Beach: SANS Institute InfoSec Reading Room, 2005, Version 1.4c.
[10] (2003) The Tech Republic website. [Online]. Available: http://www.techrepublic.com/article/what-the-tkip-protocol-is-all-about/
[11] The CISCO website. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch4_Secu.html
[12] (2008-2013) The Flylib website. [Online]. Available: http://flylib.com/books/en/2.519.1.49/1/
[13] The CISCO website. [Online]. Available: https://blogs.cisco.com/smallbusiness/understanding-the-difference-between-wireless-encryption-protocols
[14] How to Geek website. [Online] Available: http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters
[15] The Research Center website [Online] Available: https://researchcenter.paloaltonetw orks.com/2013/09/risks- to-wireless-networks-attacks-on-wpawpa2/
[16] The Aircrack Tutorial Website [Online] Available: https://www.aircrack-ng.org/doku.php?id=simple_wep_crack
[17] The Tamos Website [Online] Available:http://www.tamos.com/htmlhelp/commwifi/aboutcvwifi.htm
[18] R. Bhatnagar, V. Kumar Birla "Wi-Fi Security: A Literature Review of Security in Wireless Network" IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET), Vol. 3, Issue 5, pp. 22-30, May 2015.
[19] C. Maple, H. Jacobs and M. Reeve, "Choosing the right wireless LAN security protocol for the home and business user", in IEEE Computer Society ,2006, p. 1025-1032
[20] Heather D. Lane (2005) SANS Institute Reading Room site. [Online]. Available: https://www.scribd.com/document/175725803/Evolution-Wireless-Security-80211-Networks-Wep-Wpa-80211-Standards-1109
[21] The CISCO Website [Online]. Available: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1300/12-2_15_JA/configuration/guide/o13wep.html
[22] The StopSpam.Org Website [Online]. Available: http://www.stopspam.org/hacking-prevention-hacking-wpa-and-wep-wi-fi/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY