iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

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

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

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.***

Today 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

Wireless technology has been gaining rapid popularity for some years. Where ever you go, either it's a workplace, coffee shop, library or even a park there is a high chance today that you're able to connect to wireless networks. However, with the rising accessibility of Wi-Fi, this also makes attacks more likely to occur from attackers. There are two types of attackers- Intentional attackers and Non-Intentional attackers. Intentional attackers hacks your network or non-intentional when you connect to the wrong access point. Security is the major issue with the development of wireless networks as it security needs increases. There are number of security issues that make securing a WLAN difficult. Our goal with this report is to show how easy it is to exploit vulnerabilities using easily available software and tools in the wireless networks today.

The existing security protocols are WEP, WPA& WPA2. The main 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 this paper, we will discuss the encryption mechanisms of data protection or security in wireless network. In second section, 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.

A. Wired Equivalent Privacy (WEP)

It is a security algorithm for IEEE 802.11 wireless networks. Introduced as a part of the original 802.11 standard ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network. This security measure is for Wireless LAN and it is a part of the IEEE 802.11 security standard. In the WEP, the Cyclic Redundancy Code (CRC-32) is used for providing data security and integrity, while the RC4 stream cipher is used to provi

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

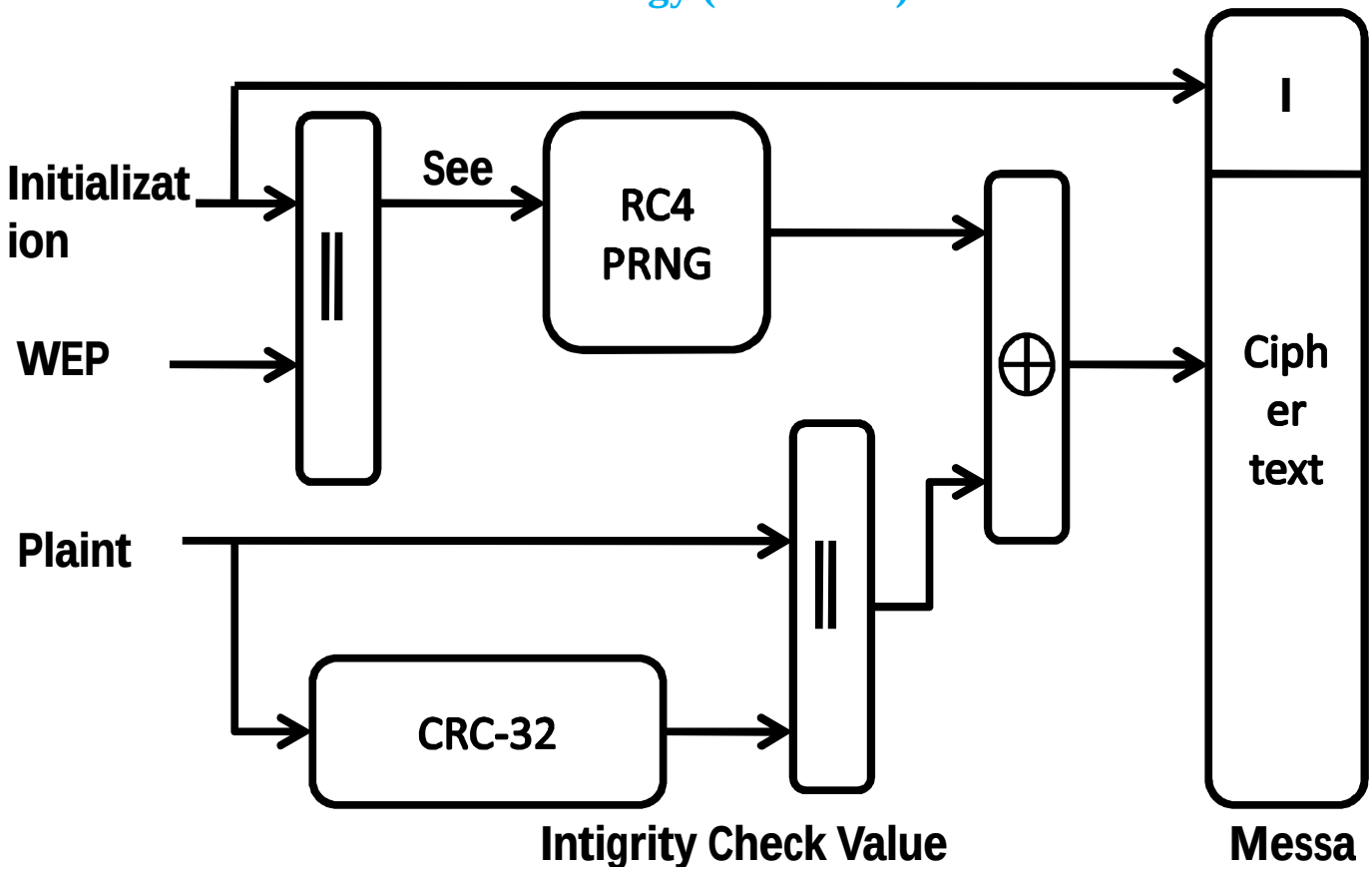


Fig. 1 WEP Encryption

Confidentiality [2][3]. The WEP standard specification supports a 40-bit key length while the non-standard specification provides a 128 and 256-bit key length in data encryption.

1) *Data Encryption and Integrity Protection:* Every data frame send by a station in a WEP protected network is encrypted and integrity protected. Non-data frames, like beacon frames acknowledgment frames and similar frames are not protected by WEP at all. When station sends a packet, the following steps are executed. The station picks a 24 bit value called initialization vector IV. We will later use this value byte wise and write IV [0] || IV [1] || IV [2] for it. Te IEEE 802.11 standard does not specify how to choose this value. Beside some minor modifications, most vendors implemented one of the following two methods. First is the IV is chosen by a pseudo random number generator PRNG independently from all other packets send by this station. Second is the station always remembers that last IV used. When a new IV needs to be chosen, the station interprets the last IV used as a number and adds 1 to this number. When the highest possible number reached, the station starts again with 0. On startup the IV counter either takes a fixed value or a random number is assigned to it. After implementation, the IV is prepended to the root key and forms per packet key K = IV||Rk. A CRC32 checksum of the payload is produced and appended to the payload. This checksum is called Integrity Check Value (ICV). The per-packet key K is feed into the RC4 stream cipher to produce a key stream X of the length of the payload with checksum. The plaintext with the checksum is XORed with the key stream and forms the ciphertext of the packet. The ciphertext, the initialization vector IV and some additional header fields are used to build a packet, which is now send to the receiver.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

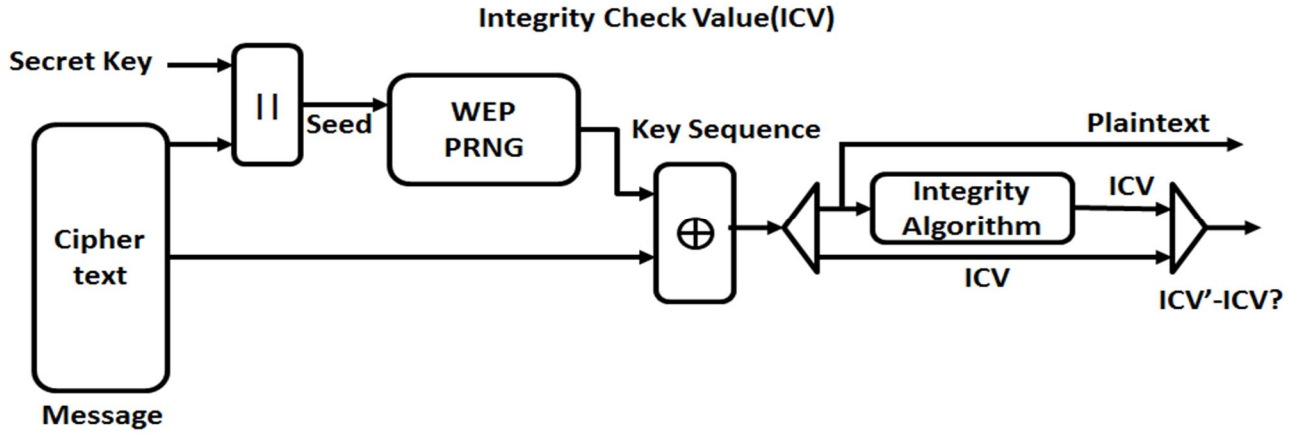


Fig. 2 WEP Decryption

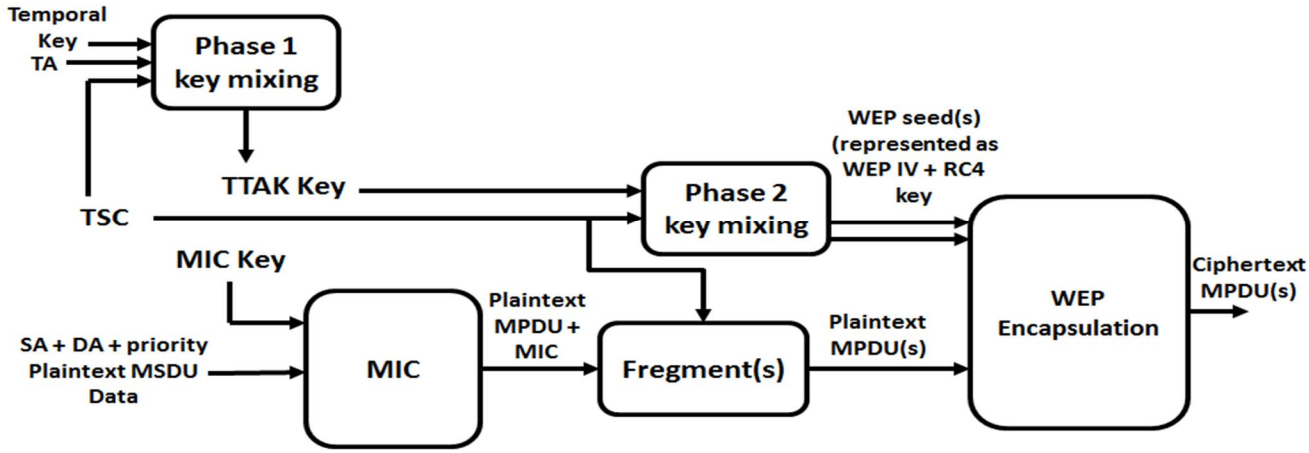


Fig. 3 WPA Encryption Algorithm (TKIP)

2) *Data Decryption and Integrity Protection:* WEP try to use from five operations to decrypt the received side (IV + Ciphertext). At first, the Pre-Shared Key and IV concatenated to make a secret key. Secondly, the Ciphertext and Secret Key go to in CR4 on algorithm and a plaintext come as a result. Thirdly, the ICV and plaintext will separate. Fourthly, the plaintext goes to Integrity Algorithm to make a new ICV (ICV') and finally, the new ICV (ICV') compare with original ICV. The IV of the incoming message is used to generate the key sequence necessary to decrypt the incoming message. Combining the ciphertext with the proper key sequence will give the original plaintext and ICV. The decryption is verified by performing the Integrity Check algorithm on the recovered plaintext and comparing the output of the ICV' to the ICV submitted with the message. If the ICV' is not equal to the ICV, the received message is in error, and an error indication is sent to the MAC management and back to the sending station. The following diagram exhibits how WEP is decrypted.

B. Wi-Fi Protected Access (WPA)

Since various security limitations were posed by WEP, the Wi-Fi Alliance discovered Wi-Fi Protected Access (WPA) [3]. WPA uses more complex encryption technology than WEP called Temporal Key Integrity Protocol (TKIP). TKIP utilizes a longer encryption key that can go up to 256 bits than WEP employing a 40 bits key which is relatively weak even when properly implemented. In addition, it is supported by Message Integrity Check (MIC) which helps in contesting bit flipping attack, to which WEP can be easily subjected to. Another improvement which WPA offers over WEP is that any alphanumeric string can be used to negotiate the initial session with the Access Point (AP).

WPA was also made available in two modes: personal and enterprise. WPA-Personal is also referred to as WPA-PSK (Pre-Shared Key) mode. It is designed for SOHO networks and is targeted for domestic use shown in Figure 4. It does not require an

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

authentication server. Each wireless network device encrypts the network traffic using a 256-bit key. Since both the client and the AP already possess this key, WPA provides mutual authentication, and the key is never transmitted over the air. WPA-Enterprise is also referred to as WPA-802.1X, this is designed for enterprise networks as shown in Figure 5. It uses Remote Authentication Dial In User Service (RADIUS) for authentication. Here the RADIUS server puts a check that whether the information is correct while authentication scheme called Extensible Authentication Protocol (EAP) is processing the information.

1) *TKIP Encapsulation Process:* TKIP enhances the WEP encapsulation with several additional functions. When station wishes to transmit an MSDU, the TKIP uses the temporal key to compute the MIC over source and destination MAC addresses and MSDU payload. TKIP appends the MIC to the data field. TKIP fragments the MSDU into MPDUs are needed. Then TKIP assigns each fragment (MPDU) a monotonically increasing TSC (TKIP Sequence Counter). TTAK (TKIP mixed transmit address and key) is produced using the temporal key and source address (Phase I). Employs the key mixing function to create a per-packet encryption key for each fragment, represented as a WEP IV and a base key (Phase II). At this point, the remaining steps are pure WEP, usually implemented in hardware. The system computes and appends the ICV to the data field ICV of each fragment. The encryption consumes the IV and base key, encrypts the data field, including the MIC and ICV, and encodes the IV and the key id of the set of temporal keys into the WEPIV field, completing the encapsulation process. The entire MPDU is now protected and ready to transmit. Figure 3 is a block diagram depicting the process.
2) *TKIP De-capsulation Process:* TKIP enhances the WEP de-capsulation with several additional functions. TSC is recovered from the received packet (MPDU) and is examined to ensure that the packet just received has a TSC value greater than the previously received packet. If it does not, then the packet is discarded in order to prevent potential replay attacks. Then the MPDU's are passed on to WEP for de-capsulation. If WEP indicates ICV check succeeded for every MPDU, Then they are reassembled into MSDU. MIC is calculated on the received and decrypted MSDU and is compared with the received MIC value. If the MIC Value does not match then the packet is discarded, otherwise the MSDU is delivered to the upper layer. The block diagram of De-capsulation Process is shown in Figure 4.

C. *Wi-Fi Protected Access 2 (WPA2)*

As the name suggests, WPA2 is a second, newer version of Wireless Protected access (WPA) security and access control technology for Wi-Fi wireless networking. WPA2 ia available on all certified Wi-Fi hardware since 2006 and was an optional feature on some products before that. It is designed to improve the security of Wi-Fi connections by requiring use of stronger wireless encryption then what WPA requires. The 802.11i is completely implemented in the WPA2. The main change that was done in the WPA2 over the WPA relates to the data encryption algorithm. The counter mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) uses a block cipher which is the Advance Encryption Standard (AES) for data encryption [1]. Most current WPA2 implementations use a pre-shared key (PSK), commonly referred to as *WPA2 Personal*, and *WPA2 Enterprise* uses an authentication server to generate keys or certificates.

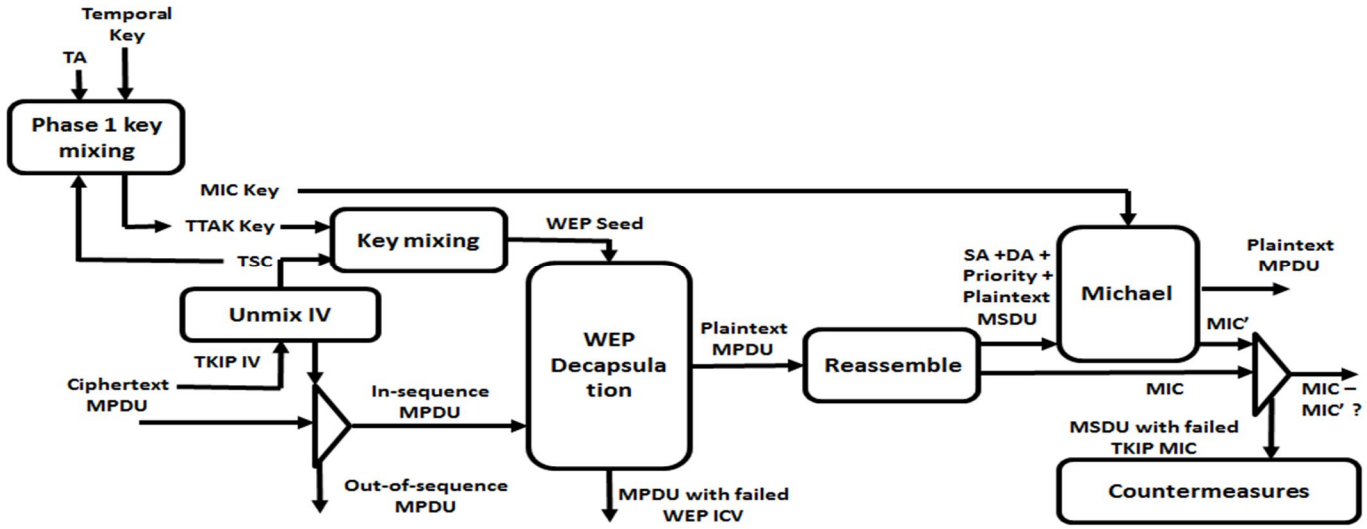


Fig. 4 WPA Decryption Algorithm (TKIP)

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

1) *CCMP Encryption Process:* The AES encryption blocks in both the MIC calculation and the packet encryption use the same temporal encryption key (K in Figure 5). As with TKIP, the temporal key is derived from the master key that was derived as part of the 802.1X exchange. The MIC calculation and encryption proceed along parallel paths as shown in Figure 5. The MIC calculation is seeded with an IV formed by a flag value, the PN and other data pulled from the header of the frame. This IV is fed into an AES block and its output is XORed with select elements from the frame header, which is then fed into the next AES block. This process continues over the remainder of the frame header and down the length of the packet data to compute a final 128-bit CBC-MAC value. The upper 64 bits of this MAC are extracted and used in the final MIC appended to the encrypted frame. The encryption process is seeded by a counter preload also formed from the PN, a flag value, data from the frame header, and a counter value which is initialized to 1. This preloaded value is fed to the AES block and its output is XORed with 128 bits of clear text from the unencrypted frame. The counter value is incremented by 1 and this process is repeated for the next block of 128 bits of clear text. This process continues down the length of the frame until the entire frame has been encrypted. The final counter value is set to 0 and input to an AES block whose output is XORed with the MIC value computed previously before appending to the end of the encrypted frame for transmission.
2) *CCMP data Decryption:* The CCMP de-capsulation process is not shown but is essentially the reverse of the encapsulation process of Figure 5. A final step is added to compare the value of the computed MIC to that received before the decrypted frame is passed on by the MAC.

II. LITERATURE REVIEW

In [4], Author explained the structure of WEP in sender and receiver side and described all steps verbally and practically at the same time as a brief about the first generation of wireless security protocols. They have also discussed about the second generation of wireless security as WPA and define the two modes and try to describe all major improvements on WPA such as cryptographic message integrity code or MIC, new IV sequencing discipline, per-packet key mixing function rekeying mechanism then make a whole diagram for WPA encryption and decryption. Finally, they discusses about third generation of wireless security protocol as WPA2/802.11 and define two type of this security as home user and corporate.

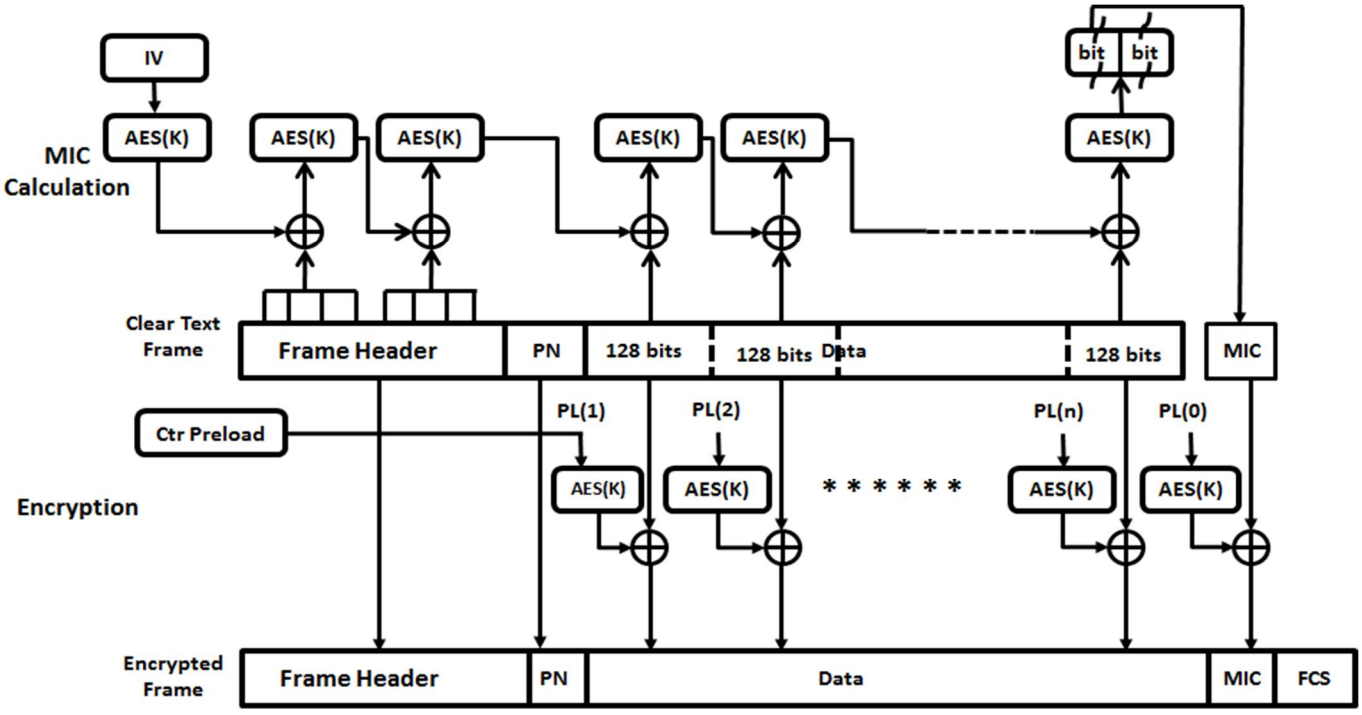


Fig.5 WPA2 Encryption Algorithm (CCMP)

In [5], Author have analysed and compared all the three security protocols of the wireless network, i.e. WEP, WPA and WPA2. They gave the detailed description of these protocols and also discussed how easy it is to crack the security protocols. They tried to perform and check authentication of all 3 protocols by implying the legendary attack vector scripts i.e. Aircrack

set of tools. They have conducted the test on Back Track operating system which is considered as dedicated pen testing operating system. In this testing, they have showed that it is little difficult to crack WPA/WPA2 as compared to the WEP which indirectly proves that the WEP is the weakest protocol in all.

In [6], Author has highlighted the data security process and methods of the WEP, WPA and WPA2. They found out that the WPA2 is more secured in data transmission compared to the preceding protocols, although they all have their shortcomings. They have also discussed various data encryption method for securing data before it's been transferred. Some of the data encryption methods that they have detailed are the symmetric and Asymmetric encryption methods, types of data cipher for data encryption such as the block cipher and the stream cipher, where the stream cipher seems more faster in process while block cipher has been slower but more secured.

In [7], Erik Tews had focused over the one of the three main security protocols of wireless network namely WEP. In this paper, he had not only discussed about the encryption process of the WEP but also its working and attacks that can happen on it. He categorized the attacks in two category which attacks that happen on WEP related to RC4 and attacks that happen on WEP which is not related to RC4. Already it is very well known that WEP is the weakest security protocol in all the three which means breaking or attacking on it is very easy. Still he introduced another attack named PTW which requires very less time, say a minute or less, to break the WEP. He showed the attack process with the help of software named Aircrack-ng.

In [8], Author has described the authentication process of WPA standard and a way of cracking WPA. They have first surveyed all the important terms related to the wireless world and then acknowledged the important that is needed to be done in this field. They have also studied the important attacks and their modus operandi. After studying about the authentication protocols, they got the knowledge related to the breaking and cracking of the WPA. They hacked the WPA by using software named "Aircrack" in backtrack operating system.

In [9], Author described many of the vulnerabilities that can exist for home wireless LAN systems, also referred to as small office/home office (SOHO) LAN systems, also referred to as well as for enterprise LAN systems. They surveyed that both LAN types are vulnerable to the same kinds of attacks and errors but they emphasized the details of the larger more complex enterprise wireless LANs. In this paper, they focused first in checking where the vulnerabilities reside, then on methods that can be used to detect them and at last in how to secure them. They have also discussed the tools that hackers used to hack, the security standards and points to consider in planning a wireless LAN for security. The major focus in this paper is given to the security vulnerabilities and some information on current and future trends in Wireless LANs. They have also concluded some security measures that should be taken care of for securing wireless LAN.

In this paper, We have tried to discuss the encryption and decryption process of the security protocols of wireless networks which is WEP, WPA and WPA2. And we have looked on the work that has happened yet. Till now, we have noticed that the authors have worked on security vulnerabilities, cryptographic encryption of security protocols and attacks that can be possible on security protocols using air crack in Backtrack OS. In next paper, our work will be to highlight the process of authentication and attacking the security protocols of wireless networks using the Software: Air crack and Commview in windows.

III.ACKNOWLEDGMENT

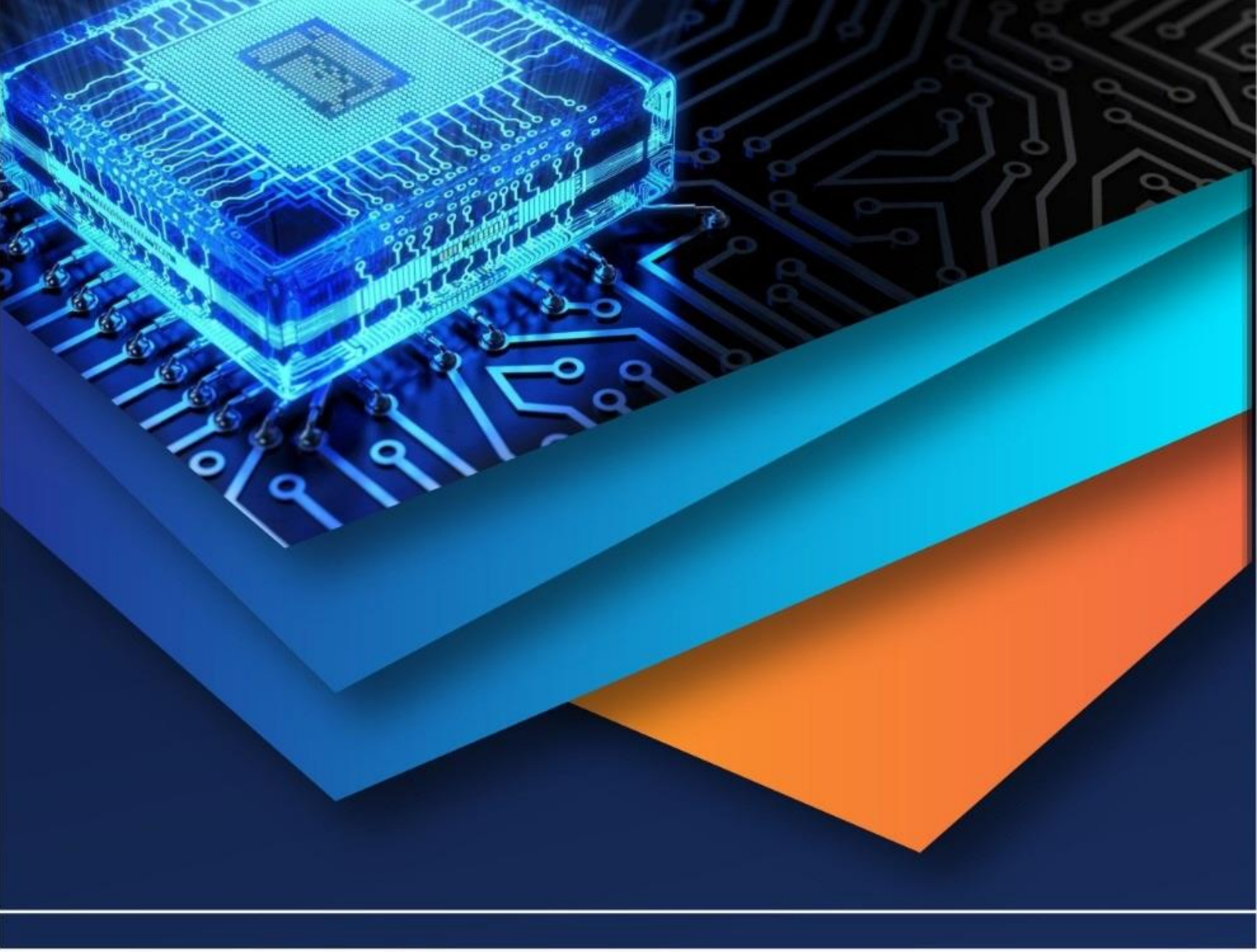
We would like to express our appreciation to our parents and all the teachers and lecturers who help us to understand the importance of knowledge and show us the best way to gain it.

REFERENCES

[1] B. Miler, (2008) WPA2 Security: Choosing the Right WLAN Authentication Method for Homes and Enterprises, Global Knowledg
[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,

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

Feb. 2012.
[9] H.D. Lane, " Security Vulnerabilities and Wireless LAN Technology", GIAC Security Essentials Certification Assignment. Virginia Beach: SANS
[10] Institute InfoSec Reading Room, 2005, Version 1.4c.
[11] (2003) The Tech Republic website. [Online]. Available:
[12] The CISCO website. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch4_Secu.htm
[13] (2008-2013) The Flylib website. [Online]. Available:
[14] The CISCO website. [Online]. Available: https://blogs.cisco.com/smallbusiness/understanding-the-difference-between-wireless-encryption-protocols



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY