IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# EVALUATING PERFORMANCE AND SECURITY OF WPA USING SHA1

Lakhveer Kaur [*], Pawan Luthra
[*] CSE, SBSSTC, Ferozepur, India

## ABSTRACT

Wirelesses Local Area Networks (WLANs) have become more common and are widely used in many places like university campuses etc. With Growing popularity, the security of wireless network has become very important issue .Wi-Fi device needs the security so as to protect it from unauthorized access and data theft. WPA protocol are used for security of wireless network .In this paper evaluation of MAC and SHA-1 is performed by calculating throughput and the results shows improvement of WPA using SHA1.

**General Terms :** Encryption, Message Authentication Code, Throughput

**KEYWORDS:** WPA , SHA1 , MAC , MIC , IV

## INTRODUCTION

**W**i-Fi **P**rotected **A**ccess. The WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP. WPA uses the **T**emporal **K**ey **I**ntegration **P**rotocol (**TKIP**) algorithm for encryption. TKIP is a security protocol used in the IEEE 802.11 wireless networking standard. TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as a solution to replace WEP without requiring the replacement hardware. This was necessary because the breaking of WEP had left Wi-Fi networks without viable link-layer security, and a solution was required for already deployed hardware [6].

### WPA

The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.[3]

WPA also includes a message integrity check, which is designed to prevent an attacker from altering and resending data packets. They required too much mathematical calculation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC [8], [9]

### *MIC*

The term message integrity code (MIC) is frequently substituted for the term MAC,[1] .MAC traditionally stands for Media Access Control address. However, some authors [2] use MIC as a distinctly different term from a MAC; in their usage of the term the MIC operation does not use secret keys. This lack of security means that any MIC intended for use gauging message integrity should be encrypted or otherwise be protected against tampering. MIC algorithms are created such that a given message will always produce the same MIC assuming the same algorithm is used to generate both. MAC algorithms are designed to produce matching MACs only both at sender and receiver side if the same message, secret key and initialization vector are input to the same algorithm.

### Temporal Key Integrity Protocol

WPA's encryption method is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism. WPA provides "strong" user authentication based on 802.1x and the Extensible Authentication Protocol (EAP). WPA depends on a central authentication server such as RADIUS to authenticate each user[10].

TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP related key attacks.[5] Second, WPA implements a sequence counter to protect against replay

attacks. Packets received out of order will be rejected by the access point. Finally, TKIP implements a 64-bit Message Integrity Check (MIC).[6]
To be able to run on legacy WEP hardware with minor upgrades, TKIP uses RC4 as its cipher. TKIP also provides a rekeying mechanism. TKIP ensures that every data packet is sent with a unique encryption key.

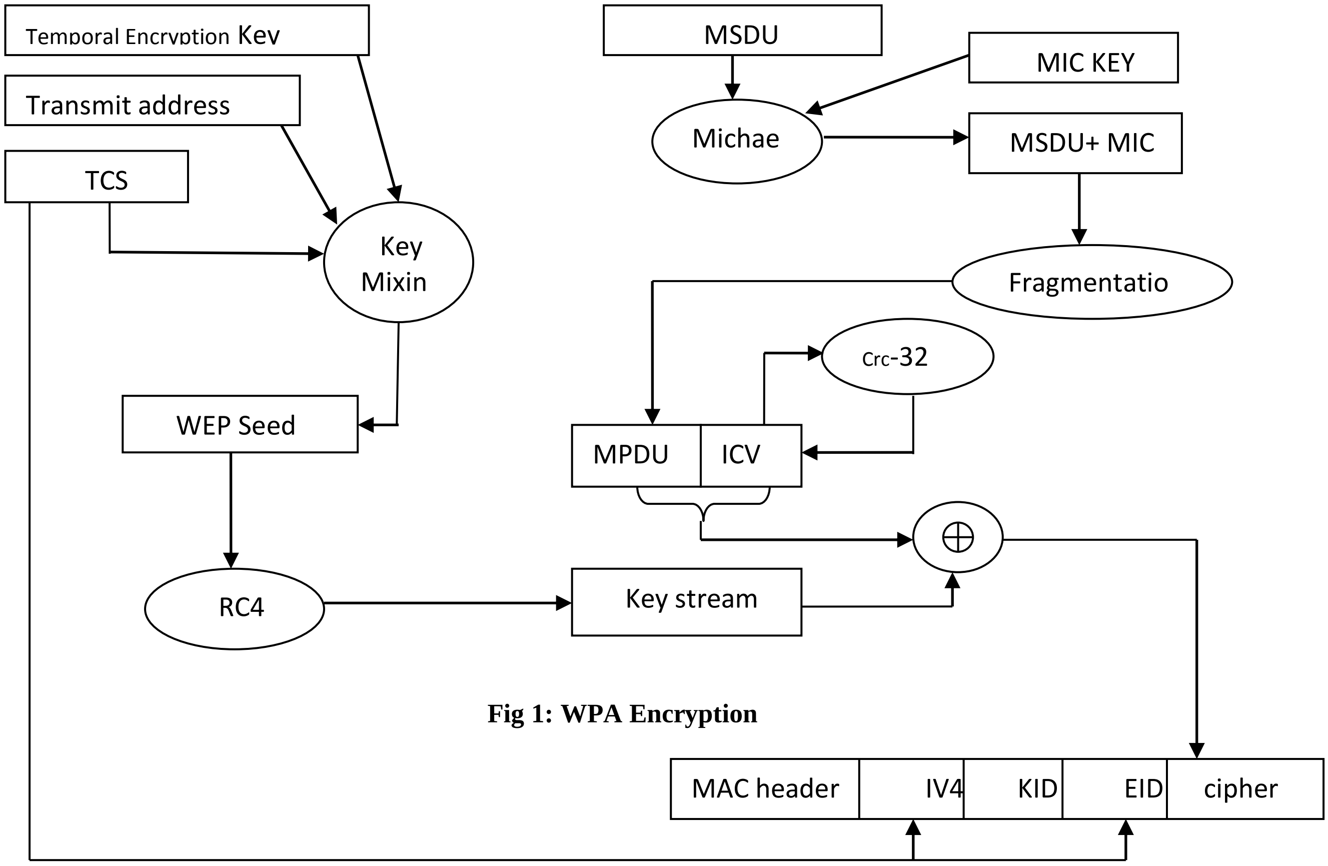


**Fig 1: WPA Encryption**

Key mixing increases the complexity of decoding the keys by giving an attacker substantially less data that has been encrypted using any one key. WPA2 also implements a new message integrity code, MIC. The message integrity check prevents forged packets from being accepted. Under WEP it was possible to alter a packet whose content was known even if it had not been decrypted.

### *2.3 Message Authentication Code*

In cryptography, message **authentication code** (often **MAC**) is a short piece of information to authenticate a message and to provide integrity and authenticity assurances on the message. Integrity assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin.
A MAC is also called a keyed, cryptographic hash function is only one of the possible ways to generate MACs, accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC .

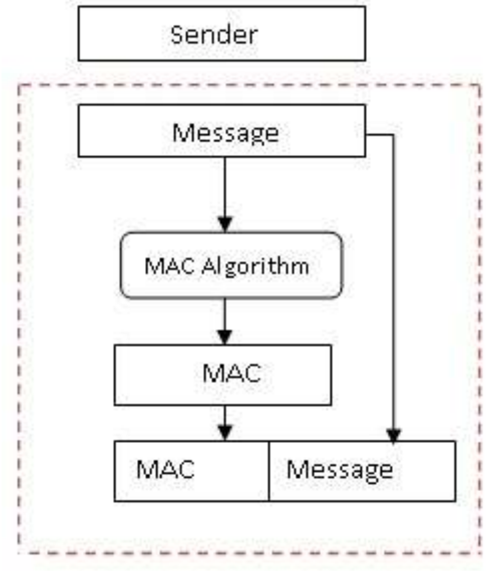


*Fig 2 : Message Authentication Code*

The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers to detect any changes to the message content. the sender of a message runs it through a MAC algorithm to produce a MAC data tag.

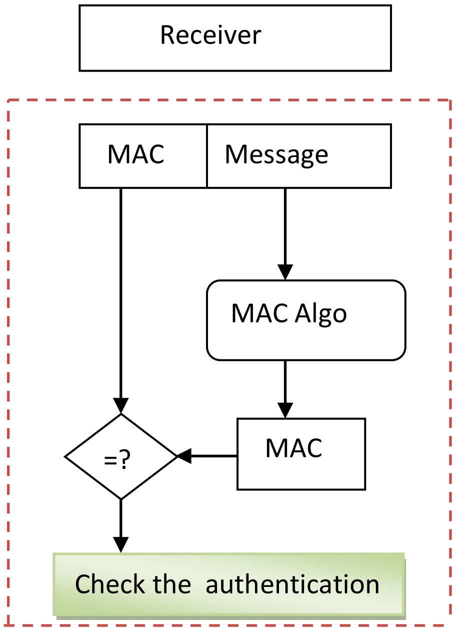


*Fig:3 Check the authentication at receiver side*

The message and the MAC tag are sent to the receiver. The receiver in turn runs the message portion of the transmission through the same MAC algorithm using the same key, producing a second MAC data tag. The receiver compares the first MAC tag received in the transmission to the second generated MAC tag. If they are identical, the receiver will safely assume that the integrity of the message is not compromised, and the message was not altered or tampered with during transmission.

### *RC-4 ALGORITHM*

A well-known flaw of stream ciphers is that encrypting two messages under the same IV and key can reveal information about both messages .The RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce a cipher text. The receiver has a copy of the same secret key, and uses it to generate identical key stream . XOR ing the key stream with the cipher text yields the original plain -text. This mode of operation makes stream ciphers vulnerable to several attacks. If an attacker flips a bit in the cipher text, then upon decryption, the corresponding bit in the plaintext will be flipped. Also, if an eavesdropper intercepts two cipher texts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts.

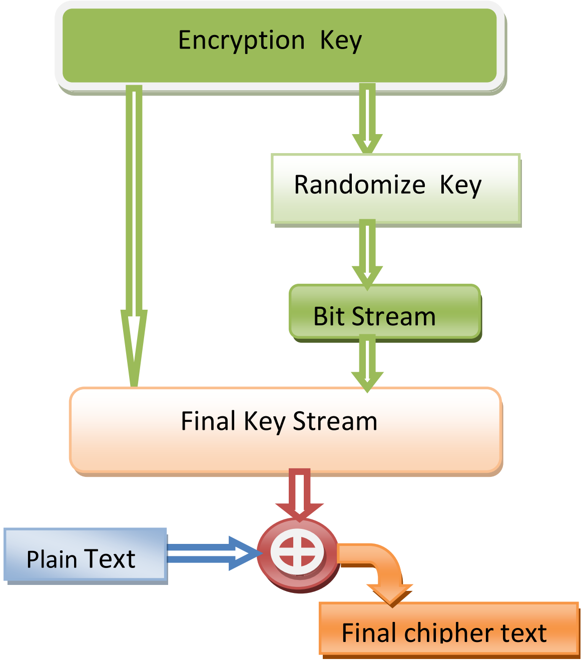


***Fig:4 RC Encryption algorithm***

The statistical attacks become increasingly practical as more cipher texts that use the same key stream are known. Once one of the plaintexts becomes known, it is trivial to recover all of the others.

### SHA-1 (Secure Hash Algorithm)

SHA-1 is a hashing algorithm designed by the United States National Security Agency and published by NIST. It is currently used in TLS, SSL, IP sec etc. It used to provide data integrity and authentication. It takes a variable block of data, and gives a fixed-size output which is called the hash value or message digest. In SHA-1, message is first hashed or digest by various steps and then message with hash is transmitted by applying digital signatures to it.Sha-1 is used for Integrity checking such as The sender hashed the data and signed the hash before sending so that the sender can prove that the message has not been tampered with anyone then send it to the recipient. The recipient will check if the hashes match. If it matched then the data is not modified or tampered. SHA-1
is called secure because it is very difficult to find two messages which produce the same message digest.[2]

The SHA1 is used to compute a message digest for a message or data file that is provided as input. • The message or data file should be considered to be a bit string. • The length of the message is the number of bits in the message (the empty message has length 0). • If the number of bits in a message is a multiple of 8, for compactness we can represent the message in hex. • The purpose of message padding is to make the total length of a padded message a multiple of 512. • The SHA1 sequentially processes blocks of 512 bits when computing the message digest

## Simulation and Implementation of SHA1 in WPA

In our research work, we have used SHA1 Algorithm in WPA to provide Cryptographic integrity. Our simulation environment is NS-2.34; here we have taken a test bed of 50 nodes. We have taken a parameter for this evaluation, Throughput. For better clearance of result and comparing it with data taken for SHA-1, we have taken values for three different length of message keys i.e. 64,128,256 bits

## Throughput

The Throughput is defined as the number of successfully received packets in a unit time and it represented in Kbps .throughput is calculated using awk scripted which processes the trace file and produces the result.
It is defined as the total number of packets received at the destination per unit time. It is measured in Kbps.

Throughput=N/T;

N=total number of packets received
T=time taken

The figures 5,6 and 7 represent the values of throughput using SHA1 in WPA with 64, 128, 256 bit length of key.

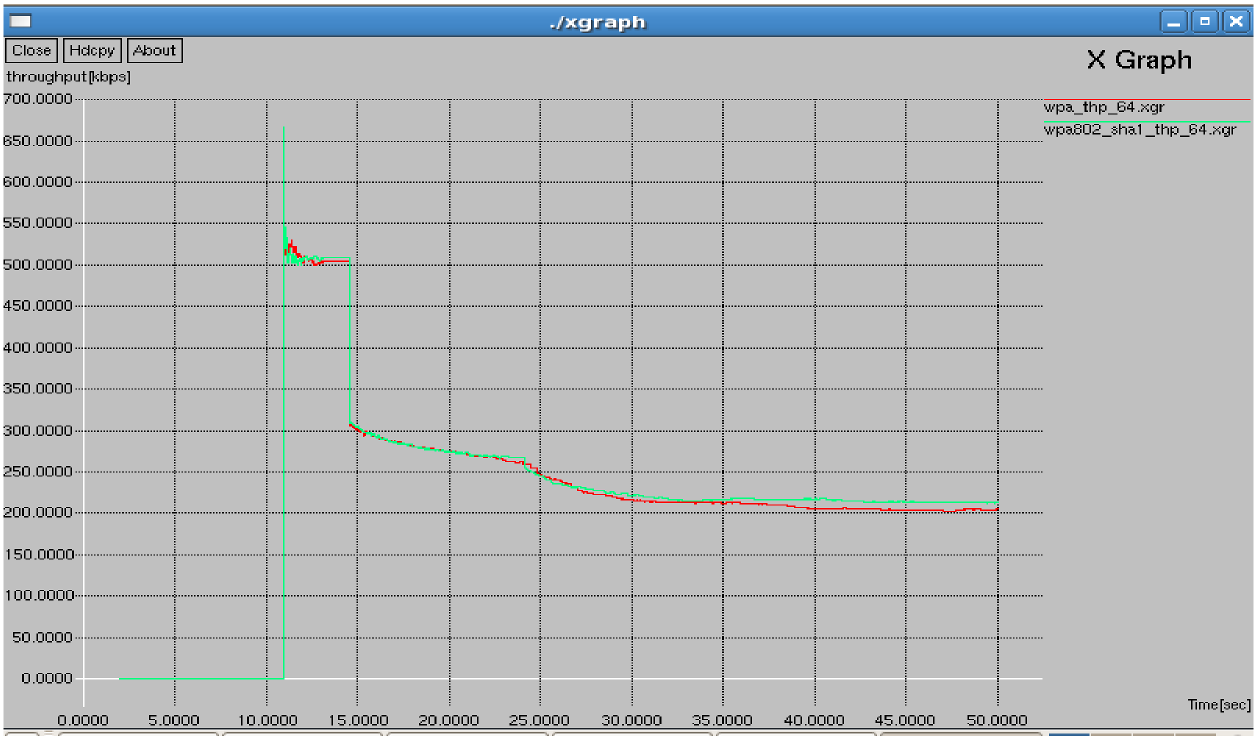


*Fig 5 : Throughput using SHA1 in WPA with 64 bit length Key*

As shown in Fig:5 of throughput [Kbps] and pause time [sec]of MAC and SHA-1, comparison is done between the two algorithms at 64 bit key. According to the graph, MAC has lower throughput than SHA-1.

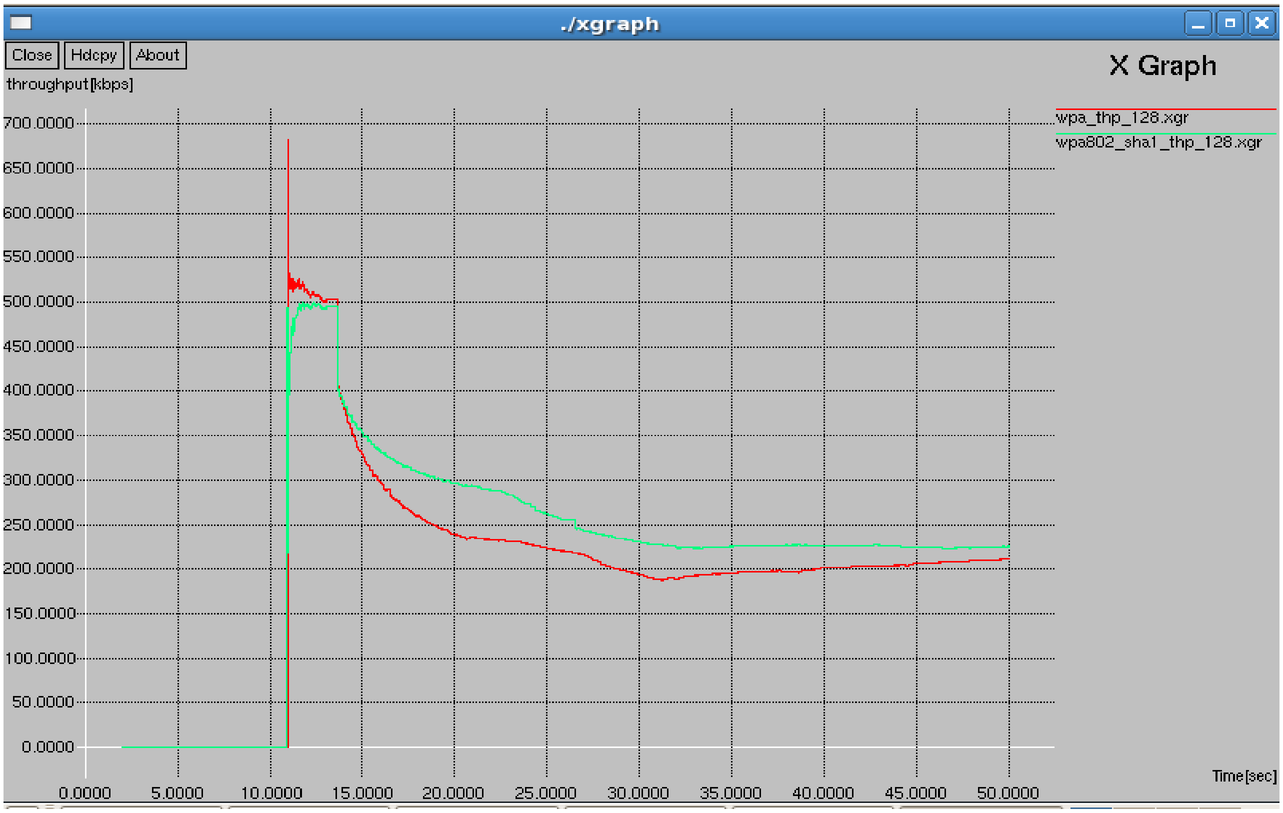


***Fig 6: Throughput using SHA1 in WPA with 128 bit length key***

As shown in Fig: 6 throughput [Kbps] and pause time [sec]of MAC and SHA-1, comparison is done between the two algorithms at 128 bit key. According to the graph, MAC has lower throughput than SHA-1.

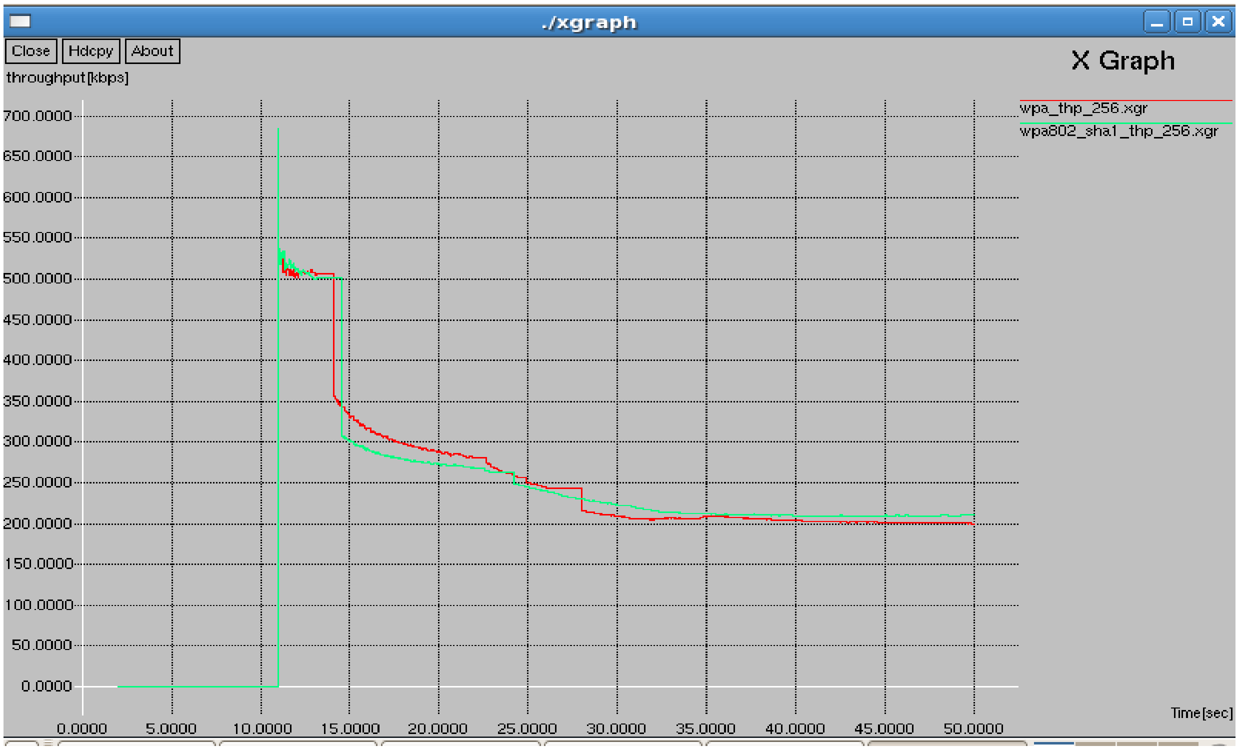
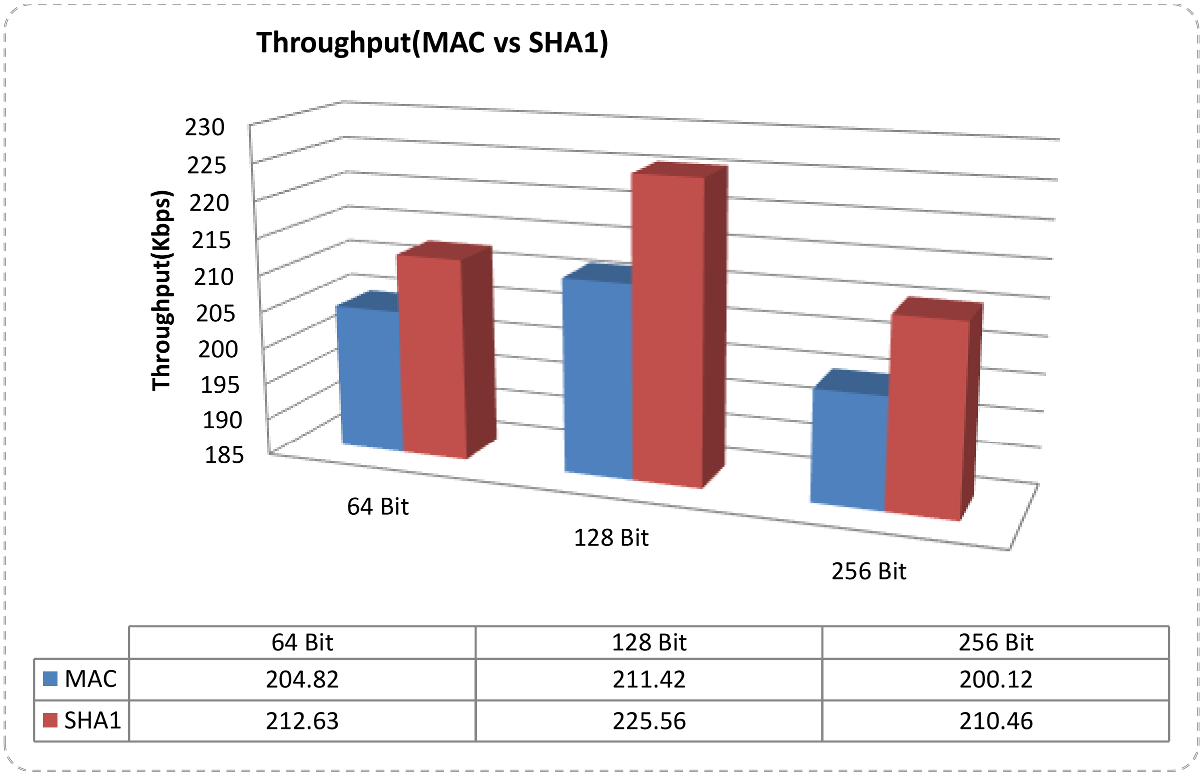


***Fig 7: Throughput using SHA1in WPA with 256 bit length key***

As shown in Fig: 7 throughput [Kbps] and pause time [sec] of MAC and SHA-1, comparison is done between the two algorithms at 256 bit key. According to the graph, MAC has lower throughput than SHA-1.
We have compared throughput with SHA1 in WPA under similar conditions [2],[3] we have found that SHA1 is more secure than MAC and also it shows some improvement over MAC under specific conditions. These values are compared in following figure (Fig 8).



| | 64 Bit | 128 Bit | 256 Bit |
|---|---|---|---|
| 🟦 MAC | 204.82 | 211.42 | 200.12 |
| 🟥 SHA1 | 212.63 | 225.56 | 210.46 |

*Fig-8: Comparison of Throughput with 3 different length of keys*

## CONCLUSION

WPA has its own weaknesses but, it is still applicable in our daily life. While implementing and comparing MAC and SHA-1 algorithms based on throughput, the performance of SHA-1 is better in terms of throughput also. While considering the future scope of the proposed work, more hash algorithms can be implemented on existing WPA that will provide more security to the network. We have compared throughput with SHA1 in WPA under similar conditions, we concluded that SHA1 is more secure than MAC and also it shows some improvement over MAC under some specific conditions.

## REFERENCES

[1] Maocai Wang, Guangming Dai, Hanping Hu, Lei Pen "Security Analysis for IEEE802.11" IEEE 2008, pp. 1-3
[2] Amit Keswani and Vaibhav Khadilkar "THE SHA-1 ALGORITHM" Lamar University Computer Science Department, Beaumont, TX 77710, USA
[3] P. Manickam, T. Guru Baskar , M.Girija , Dr.D.Manimegalai "Performance Comparison of Routing Protocols in Mobile ad hoc networks" International Journal of Wireless & Mobile Networks (IJWMN) ,Vol. 3, No. 1, February 2011, pp. 98-106
[4] Songhe Zhao and Charles A. Shoniregun "Critical Review of Unsecured WEP" IEEE 2007, IEEE Computer society , pp. 1-7
[5] Tarik Guelzim, M. S. Obaidat, Fellow"A New Counter Disassociation Mechanism (CDM) for 802.11b/g Wireless Local Area Networks" IEEE 2009, pp. 251-259

[6] Longjun Zhang,TianqingMo A Signcryption Scheme for WEP in WLAN Based on Bilinear Pairings 201O International Conference on Computer Application and System Modeling (ICCASM 2010)

**[7]** Swati Sukhija, Shilpi Gupta "Wireless Network Security Protocols A Comparative Study" International Journal of Emerging Technology and Advanced Engineering Website,Volume 2, Issue 1, January 2012, pp. 258-264

[8] Arash Habibi Lashkari, F. Towhidi, R. S. Hoseini, "Wired Equivalent Privacy(WEP)", ICFCC Kuala Lumpur Conference, 200

[9] Arash Habibi Lashkari, Masood Mansoori, Amir Seyed Danesh;"Wired Equivalent Privacy(WEP) versus Wi-fi Protected Access",ICCDA Singapore Conference, 2009

[10] Donggang Liu, P. N., "Security for Wireless Sensor Networks",Springer., November, 2006

[11] Kempf, J., "Wireless Internet Security: Architecture and Protocols ",Cambridge University Press. October, 2008

**[12]** Hani Ragab Hassan, Yacine Challal, "Enhanced WEP: An efficient solution to WEP threats", IEEE 2005