ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

REFINEMENT OF WPA USING SHA3

Kashish Monga, Vishal Arora
Shaheed Bhagat Singh State Technical Campus, Ferozepur, India

ABSTRACT

Wireless communication is the base of this generation. Reliable and fast communication has become the need of the day. Any person or industry which want to grow with the speed need wireless communication. Mobile networks, wireless broadband ,3G,4G has become an essential part of the today's life. With growth in Wireless communication, there has been increase in the need of it security. So, Wi-Fi alliance has provided us with WEP(Wired Equivalent Privacy) and WPA(Wi-Fi protected Access) protocols. In this paper we will analyze the weakness of WPA and will make improvement by using SHA3(Secure Hash Algorithm-3) in it. The results will be displayed in the graph and in comparison with SHA1

KEYWORDS: WEP,WPA,SHA1,SHA3,3G,4G,Wi-fi

INTRODUCTION

The wireless communication is one of the best invention and gift to the mankind .Wireless communication can be defined as the communication of the data and information without the use of wires/cables or any electrical conductors. The distance of communication can vary from few meters(e.g.TV remote Control) to Kilometers(e.g. Radio Communication using satellite).It is evident that major communication are now being done using wireless equipments like mobiles, GPS units, Wireless computer Accessories, Satellite phone and TVs. With the increase in the use of wireless, there is increase in security breaches that should be resolved that too quickly. To resolve all these kind of issues Wi-Fi Alliance has provided us with various Protocols like WEP,WPA,WPA2,that work in both areas safety of th data as well as authorization problem. In this paper firstly , we will discuss Wireless Communication ,then WPA. Later on we will focus on how refinement can be done in WPA to make it more secure and Powerful. We will prove this with the help of results. In last part, we will compare refined WPA with WPA using SHA1.

.

WIRELESS COMMUNICATION

A. Wireless Communication

Wireless communication can be defined as communication or information exchange between two or more points(wireless devices) connected to each other wirelessly. These include radio signals transmissions e.g. Radio waves, TV remote Signals,2G service by cellular companies

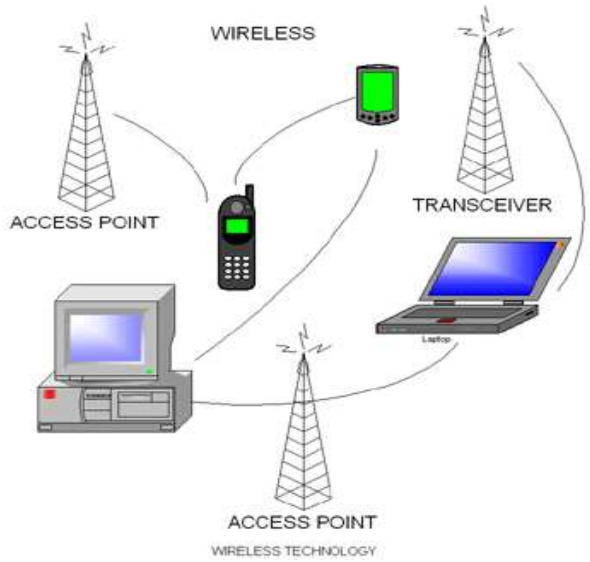

FIGURE-1:VARIOUS MODES OF WIRELESS COMMUNICATION

B. Types of wireless Communcaiton

We can classify the wireless communication in various categories depending on the area and its usage .These are as follows:

1.WPAN(wireless Personal Area Network)
2.WLAN(wireless Local Area Network)
3.WMAN(wireless Metropolitan Area Network)
4.WWAN(Wireless Wide Area Network)

WPAN is meant to be used for personal use only like using personal Bluetooth/Infrared Communication .WLAN is used by the organization/large local area,so that persons lyin in that area can easily access it like in college campus or organization area.WMAN is meant to work for a wide area like a city/twon ,bigger than LAN.A detail aboiut all this can be easily figured from the following table-1.

In this paper, our emphasis will be on WLAN, that is being primarily used in the organization. As the use of wireless network has increased, the probability of the attacks on it has also increased. As wireless is open to all in comparison to wired where only targeted user will get the information. The security has evolved out as one of the major issues. To resolve these issues WEP,WPA and WPA2 has been proposed. Specifically our area of work will be WPA and its weakness.

Type	Coverage	Performance	Standards	Application
WPAN	within reach of person	Moderate	IEEE 802.15/Bluetooth	Cable replacement for peripherals
WLAN	In Building or campus	High	IEEE 802.11,Wi-Fi ad Hiper LAN	Mobile extensions of wired networks
WMAN	In City	High	IEEE 802.16 and Wi-MAx	Fixed wireless in home and business
WWAN	Worldwide	Low	CDPD and Cellular 2G,3G,4G	Mobile access to net from anywhere in the city

Table-1-comparision of different wireless network on various parameters

WPA

WPA is a security protocol and security certification program developed by Wi-fi alliance to secure wireless computer networks.It was devloped in response to serious loophole in WAP.It became available in 2003.The WPA protocol implements much of IEEE 802.11i standard, specifically Temporal Key Integrity Protocol(TKIP), whereas 40-bit /104-bit encryption keys were used by WEP(previous security protocol) for encrypting the data which remained same for every packet, TKIP makes a dynamic encryption key scheme. This was a major change in WPA. The second important part of WPA was to replace the CRC Checksum method used in WEP with message integrity check(MIC) algorithm called Michael. The purpose of MIC algorithm is to prevent an attacker from changing and resending data packets. Michael is much stronger than CRC.WPA has two versions and either can be installed depending on customer needs, WPA-Personal and WPA-Enterprise.

WPA-Personal: It is also known as WPA-PSK(Pre-shared key)mode. It is mostly designed for home and small office networks because it doesn't require an authentication server. In this, the network traffic is encrypted using a 256-bit key by every device as shown in Figure

Figure-2:Working of WPA-Personal

WPA-Enterprise: It is also known as WPA-802.1X mode RADIUS-Authentication server is required and designed for enterprise networks. In this, Extensible Authentication Protocol are used for authentication as shown in Figure-4.

Figure-3-Working of WPA-Enterprise

Working of WPA

The working of WPA can be explained by explaining two important parts i.e. MAC and TKIP.

MAC(Message Authentication Code): The concept of MAC is quite similar to that of a message digest. However, there is one difference. A message digest is simply a fingerprint of a message. There is no cryptography process involved in case of message digest. In contrast, a MAC requires that sender and receiver should know a shared secret key, which is used in preparation of MAC. Thus, MAC involves cryptographic processing.

Let us assume that sender A wants to send a message M to a receiver B. How the MAC processing works:

1. sender and receiver share a secret key, which is not known to anyone else. sender calculates the MAC by applying key to the message ,as shown in Figure-4

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

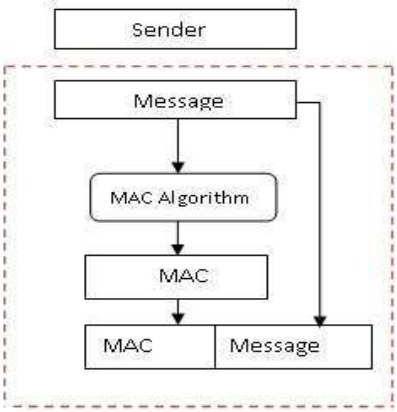

Figure-4-Working of MAC algorithm on sender side

2. Sender then sends the original message M and MAC to receiver.
3. When receiver receivers the message, receiver also uses Key to calculate its own MAC over Message.
4.Receiver now compares both MAC values. If two match , receiver concludes that message has not been changed during transmit. If values are not equal, receiver rejects the message, realizing that message was changed during transmit, as shown in Figure-5.

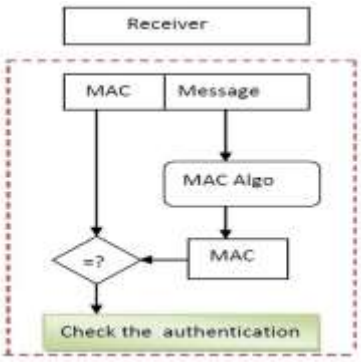

Figure-5-Working of MAC algorithm on receiver side

TKIP(Temporal Key Integrity Protocol): The encryption protocol included as part of the IEEE802.11i standard for WLANs is temporal key integrity protocol. Its purpose is to provide more secure encryption as compared to WEP.TKIP includes four additional algorithm to increase key strength :To protect packets, a cryptographic message integrity check is used, An IV sequencing mechanism, To increase Cryptographic strength, per-packet key-mixing function is used, to provide key generation every 10,000 packets ,a re-keying mechanism is used. Three new security features implemented in TKIP to resolve security problem faced in WEP. First, TKIP Implements a key mixing function that combines a secret root key with IV before passing to the RC4 initialization Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of the order will be rejected by access point. Third, TKIP implements a 64-bit Message integrity check. The following figure-7 depicts TKIP Encapsulation and de-capsulation are shown in following figures.

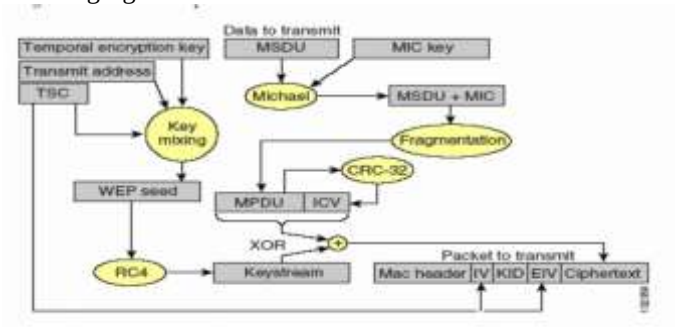

Figure-6-TKIP Encapsulation

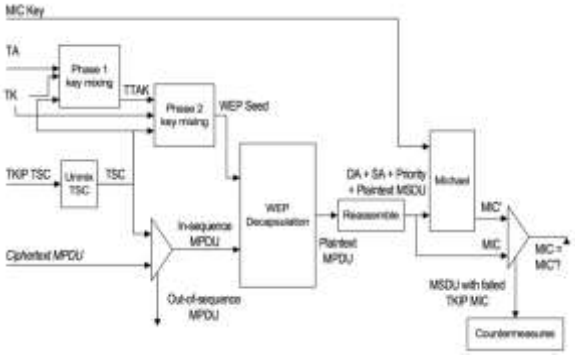

Figure-7-TKIP De-capsulation

Attacks on WPA

It is possible to have Recovery attack on temporal key .The idea of the attack is to brute forcing two different RC4-keys with 104-bit in each and then applying attack to recover 128-bit Temporal key and Message Authentication key of 64-bit. Thus the loss of few RC4-keys give permission to the attacker to easily recover Temporal Key and the contents of compromised packets. The attacker may get all secret keys the user have. So WPA doesn't provide any forward secrecy since the attacker can use earlier formed RC4keys and can generate the new ones. There are various kind of attacks have been found, that performed on WPA, and provide us the various loopholes of WPA. Generating the need of advance version of WPA. These can be explained as follows:-

- Beck-Tews attack
- Royal Holloway Attack

Both of these attacks only could decrypt small portions of data, compromising confidentiality, A

single ARP frame would take around 14-17 minutes to get the plain text..

Beck- Tews Attack: The attack is an extension of the chop- chop attack on WEP.TKIP implements MIC &so if two MIC failures are observed within 60 seconds then both client and access point are shut down and then TKIP session key is rekeyed. Thus the attacker waits for 60 seconds to avoid countermeasures in case of a failure. Packet can be decoded at a rate of one byte per minute with the help of this attack. After plaintext has been retrieved by attacker, he has access to MIC and key stream of packet. This can be used to construct and transmit a new packet on network which enables attacker to execute of Denial of service attacks. This attack can be executed only against TKIP and not against WPA implementing AES.

Royal Holloway Attack: TKIP uses a similar key structure to WEP with low 16-bit value of a sequence counter being expanded into 24-bit 'IV' and this sequence counter always increment on every new packet. An attacker can use this key structure to improve existing attacks on RC4.

SHA-3(Secure Hash Algorithm-3)

Secure Hash Algorithms belongs to the family of Cryptographic hash algorithm stated by NIST(National Institute of Standard and Technology).Cryptographic hash algorithms are those hash function which are used for encrypting and decrypting the data. It is considered to be impossible to get back the data by using only hash values. It has following properties,

1. It will be easy to find out hash for a given message.
2. It will be infeasible to get data back from hash values alone,
3. It will be infeasible to change the data without changing hash, making it more secure.

Classification of secure hash algorithms are SHA0,SHA1,SHA2,SHA3. SHA3 was earlier known as Keccak, chosen after public competition.SHA3 comes in different variants as SHA3-224,SHA3-256,SHA3- 384,SHA3-512 depending on the number of output bits being used in different variants are 224,256,384,512.Internal state size in SHA3 uses 1600 bits that is in 5x5x64 in 3-D form. SHA3 has unlimited size of message which makes it more powerful, It prevent various kind of attacks e.g. image attack and collision attack.

Simulation and implementation of SHA3 in WPA

In our work for research, we have used SHA3 Algorithm in WPA, in addition to TKIP to provide Cryptographic integrity. Our simulation environment is NS-2; here we will take a test bed of 50 nodes with 64,128 and 256-bit message key. We will take various parameters for evaluation e.g. Throughput and End to end delay. For better clearance of result and comparing it with data taken for SHA-1 from referenced paper.

Throughput: It can be defined as the number of packets received at the destination in fixed time period. It is measured in Kbps.

Throughput=N/T

N:total number of packets received

T:time taken

The figures 8,9 and 10 represent the values of throughput using SHA3 in WEP with 64, 128, 256 bit length of key.

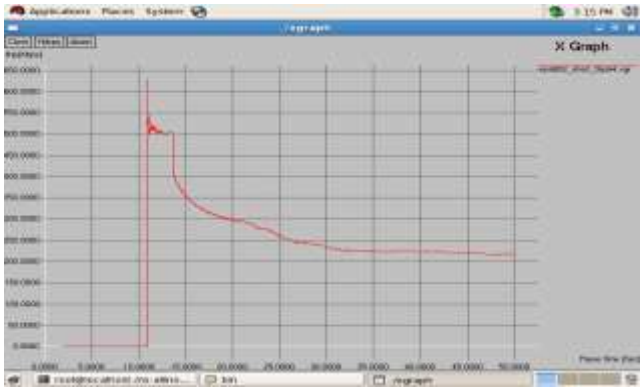

Figure-8- Throughput using SHA3 in WPA with 64 bit length key

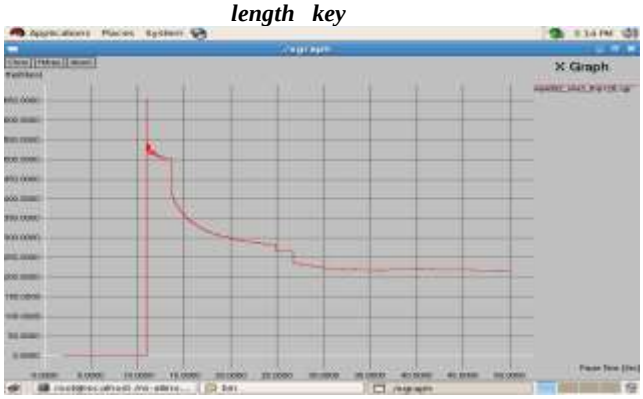

Figure-9-Throughput using SHA3 in WPA with 128 bit length key

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

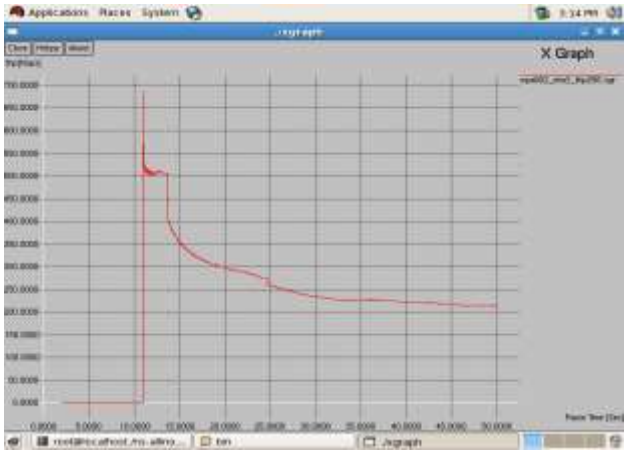

Figure-10-Throughput using SHA3 in WPA with 256 bit length key

We have compared throughput with SHA1 in WPA under similar conditions [2],[3] we can easily say that SHA3 is more better than SHA1 and also it shows improvement over SHA1 with 64-bit and 256-bit. These values are compared in following figure (Figure-11)

Figure-11-Compariion of throughput using different size keys with SHA-1 and SHA-3

End to End delay

It is the total time taken by the data packets from source to destination. The data packets successfully delivered only considered. It is measured in milliseconds.

End to End Delay=T1-T2/n;

T1=Time at which data packets were received
T2=Time at which data packets were sent
n = Total number of data packets

The figures 12,13 and 14 represent the values of end to end delay using SHA3 in WEP with 64, 128, 256 bit length of key.

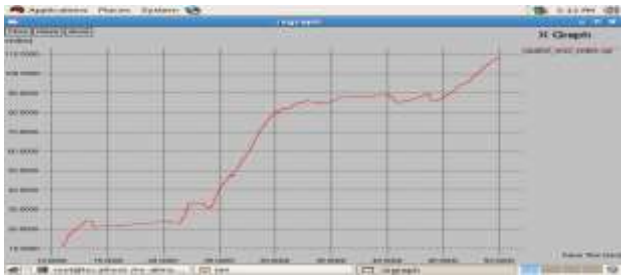

Figure-12-:End to End Delay using SHA3 in WPA having 64 bit length key

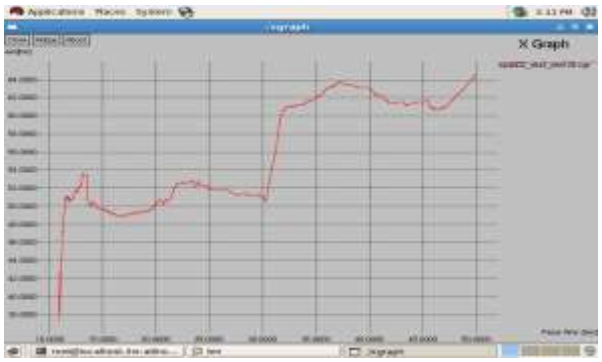

Figure-13-End to End Delay using SHA3 in WPA having 128 bit length key

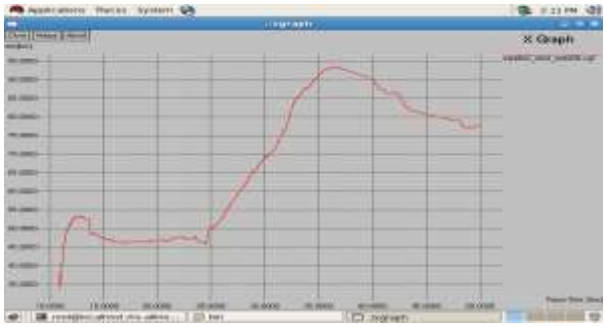

Figure-14-End to End Delay using SHA3 in WPA having 256 bit length key

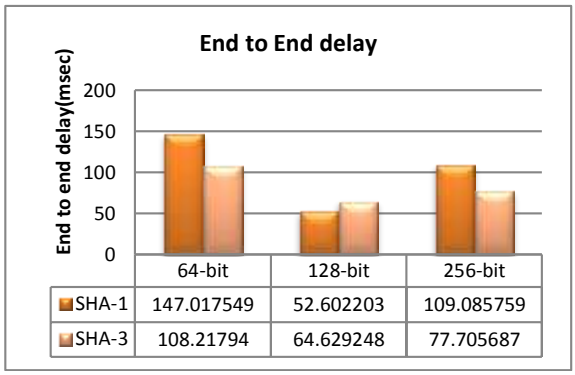

Figure-15-End to End Delay compariion using diferent lenght of keys with SHA-1 and SHA-3

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

CONCLUSION AND FUTURE SCOPE

Weakness is there in WPA that lead to formation of new protocols but by implementing SHA3 in place of CRC-32 in WPA, there can be improvement in the performance as well as in the security. Comparing the value of throughput with SHA1 under similar atmosphere, we realized that the security and performance improves better when we are using the message length of 128-bit.In future, various other parameters can be engaged for same scenario to generate more clear view of performance enhancement .We can also implement SHA3 in both WPA and WPA-2 too.

REFRENCES

[1] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)
[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[3] I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
[4] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[5] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.