Advanced Engineering Technology and Application
An International Journal

http://dx.doi.org/10.12785/aeta/040101

Comparative Analysis of CRC-32 and SHA-1 Algorithms in WEP

Amit Grover[1,*] *and Sukhchain Singh*[2]

[1] Department of Electronics & Communication Engineering, S.B.S State Technical Campus Ferozepur, Punjab, India
[2] Department of Electronics & Communication Engineering, Ferozepur college of Engineering and Technology, Ferozepur, Punjab, India

Received: 1 Jun. 2014, Revised: 28 Jul. 2014, Accepted: 29 Jul. 2014
Published online: 1 Jan. 2015

Abstract: Wireless technology has become an integral part of today's life .WLAN is widely used in many conditions, especially when traditional network is difficult to install. WEP is used to make wireless traffic as secure as wired network traffic .WEP suffers from various weakness i.e. a shared key weakness, 24-bit Initialization vectors (IVs) are too short, and this puts confidentiality at risk , poor key management etc. The CRC called cyclic redundancy check is insecure and does not prevent modification of intercepted packets. To overcome these problems, the existing WEP protocol is modified by replacing CRC-32 with SHA-1 hash function to enhance the security and performance of WLAN systems

Keywords: WEP, CRC-32, SHA-1, Average End to End Delay, Packet Delivery Ratio

1 Introduction

Wireless is a growing area is research and industry. WEP (Wired equivalent privacy) or the 802.11b is the most spread standard. It is designed to provide a same security as that of the wired LAN.WEP gives more security than the wired LAN .WEP gives security by encrypting data and transmit it from one end to other. WEP is based on the RC4 algorithm which is used to provide the confidentiality of wireless data. WEP is not intended to be the only security mechanism but it is very effective in the traditionally security practices .WEP is the wireless security standard for Wi-Fi and it is commonly used on home computer networks. Since wireless network transmit data over the radio waves, it is easy to tamper the data. So our aim is to make wireless network as secure as wired.

2 WEP (Wired Equivalent Privacy)

WEP (Wired Equivalent Privacy) is a wireless security protocol ratified by IEEE. WEP prevents the casual eavesdropping; tampering with transmitted messages .WEP raises the level of security for WEP enabled wireless devices to that of traditional wired networks .Despite the weakness and security flaws, WEP at least provides level of security that can deter casual snooping. Even though WEP has its own weaknesses, it is still relevant in our daily life. In the academic world, WEP has been studied extensively in information security, cryptology and telecommunication fields. Certain small and medium enterprises find it difficult to stop using WEP because the process of replacing their current WEP-compatible telecommunication devices to WPA/WPA2-[1][2] compatible telecommunication devices is too expensive and cumbersome.

3 WEP is designed to achieve three main security goals

1.Access control - Only authorized stations can access the network.
2.Confidentialnality - Communication is protected against eavesdropping.
3.Message Integrity - A message sent over the network cannot be altered during the transmission without the receiver station noticing the manipulation and subsequently discarding the invalid message

* Corresponding author e-mail: amitgrover_321@rediffmail.com

4 WEP Encryption

WEP is typically concerned with the main body. Actually the entire data which need to be encrypted it with [3]. WEP would get encrypted would have Initialization vector (IV), Actual data along with ICV which used the CRC-32 algorithm. Data and the ICV are encrypted and the IV is not encrypted .IV is actually a random 24 bit value which the access point or client uses and it is generated randomly on a per packet basis [4]. WEP key which could be 40, 104 or 232 bit contaminated with 24 bits IV which make it 64,124,256 bit key which goes as seed to the RC4 algorithm. The output of RC4 Algorithm is a random key stream which is used as Encryption by using a IV which is random .If we want to send some data to the client of variable size and we apply the CRC-32 which produces the integrity check value .Data or plaintext is contaminated with Integrity check value .We do the XOR operation of random stream and plaintext along with ICV which produces the cipher text .Cipher text is then transmitted and this is how we do the WEP encryption [5]. We remembered that the access point generated the IV in a random manner and the client only has the WEP key .Client does not know the IV which the access point has generated as the part of the seed to the RC4 algorithm. We take the IV and append it to the cipher text. Figure 1 shows the WEP Encryption.

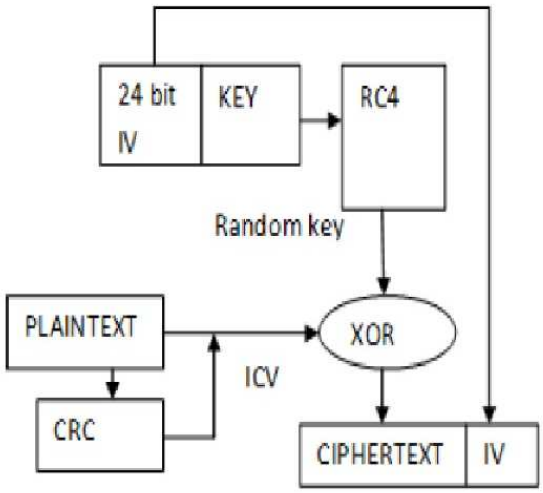


Fig. 1: WEP Encryption

5 WEP Decryption Process

WEP [3]decryption is very straight forward once we understand the Encryption part. Receiver know the WEP key but it does know the IV which is used as a part of the seed .We take the message which is received in the frame .IV and the WEP key contaminated with each other and it will seed to the RC4 PRNG algorithm and key stream is generated .We do the XOR operation on cipher text and key stream to get back the plaintext data. We know that cipher text consists of two things plaintext data and the ICV which has been appended in the end. Now the receiver does the two things it takes the plaintext and calculate the Integrity check value for the plaintext by itself and also looks for the ICV which is there is the packet itself . After decryption it will compare both ICV. If both value matched the data integrity is absolutely okay and there is no error otherwise the data is tempered by someone. Figure 2 shows WEP Decryption.

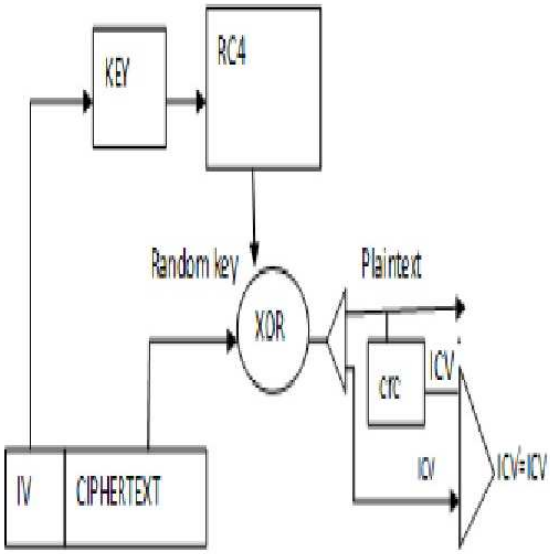


Fig. 2: WEP Decryption

6 CRC-32 (Cyclic Redundancy Check)

CRC [6][7] stands for cyclic redundancy check which is a method of detecting errors. It is used only for detecting errors in encrypted data but not for correcting error. It is used to encode the message or data which is in plaintext by adding fixed length integrity check value. Check value is attached to detect the errors. CRC uses polynomial division method to find the value of CRC which is 32 bit in case of CRC-32.CRC is a good technique to find the random errors in communication. In the CRC , message which is in plaintext is divided by the polynomial and the remainder which will comes out will be the result or the check value which will be attached with the message then we encrypt the message along with check value and send

it . At the receiver end, message along with check value is again divided by the same polynomial and if the remainder becomes zero then it means there is no error in the encrypted data which means data value of both transmitter and receiver matched with each other. CRC-32 is easy to implement but it is used only for small block of data.

7 SHA-1 (Secure Hash Algorithm)

SHA-1[8] is a standard algorithm which produces 160 bit hash or digest of any size of file or data using 512 bit blocks. Hashing is a process of taking high value of data and reduce it into low volume of data .SHA-1 provide message authentication which means it uses a secret value before hashing so that nobody can modify the message .SHA-1 is used in TLS, IP sec etc and it is also used by the law in US Govt. applications .SHA-1 is easy to compute and it also minimize the collisions. It processes a message and produces a condensed presentation called message digest. Message digest is used as a part of the message integrity. After the message digest we provide the digital signature with it then do the encryption. We provide digital signature in SHA-1 for non- repudiation. SHA-1 minimizes the collisions of packets which increases the performance. SHA-1 is called secure because it is very difficult to find two messages which produce the same message digest. Figure 3 shows SHA-1 Algorithm

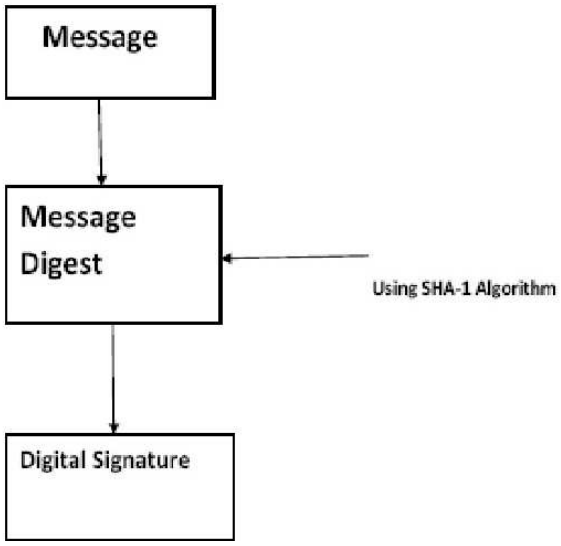


Fig. 3: SHA-1 algorithm

8 Simulation Results and Performance Comparison

The performance evaluation of the Protocol using NS-2 has been considered with the parameters, End to End delay and Packet delivery ratio.

8.1 End to End delay

It is the average time taken by the data packet to reach the destination. Only the data packets that successfully delivered are counted.

$$\sum(arrivetime - sendtime) / \sum Numberofconnections \quad (1)$$

If the value of end to end delay is lower it means the performance of the protocol is better.

8.2 Graphical representation of end to end delay of CRC-32 and SHA-1 at 64,128,256 bit key

The Figures 4,5 and 6 represents the comparison of average End to End Delay for CRC-32 and SHA-1 at 64 ,128, 256 bit key with respect to pause time respectively. From Figure 4, 5 and 6, it has been evaluated that SHA-1 performs better at 64 bit and 128 bit key as it have less end to end delay which illustrates that it will give better performance.

Fig. 4: End to End delay of CRC-32 and SHA-1 at 64 bit key

Fig. 5: End to End delay of CRC-32 and SHA-1 at 128 bit key

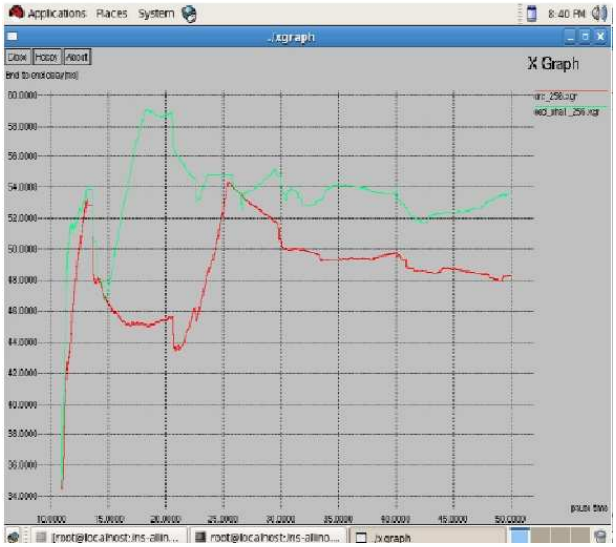


Fig. 6: End to End Delay of CRC-32 and SHA-1 at 256 bit key

8.3 Packet Delivery Ratio

It is the ratio of the number of packet receives to the number of packet send [10].

$$\sum Numberofpacketreceive / \sum Numberofpacketsend \quad (2)$$

If the value of packet delivery ratio is high it means the performance of protocol is better.

End to End Delay		
	CRC-32	SHA-1
64 bit key	55.75764 ms	33.546609 ms
128 bit key	47.714954 ms	59.653347 ms
256 bit key	55.757064 ms	53486611 ms

Fig. 7: Simulation results of CRC-32 and SHA-1

Fig. 8: Packet delivery ratio of CRC-32 and SHA-1 at 64 bit key

8.4 Graphical representation of Packet Delivery Ratio of CRC-32 and SHA-1 at 64,128,256 bit key

The Figures 8, 9 and 10 represents the comparison of Packet Delivery Ratio for CRC-32 and SHA-1 at 64, 128, 256 bit key with respect to pause time respectively. From Figure 8, 9 and 10, it has been evaluated that Packet delivery ratio and reliability of SHA-1 at 128 and 256 bit key is better which illustrates that it will give more accuracy.

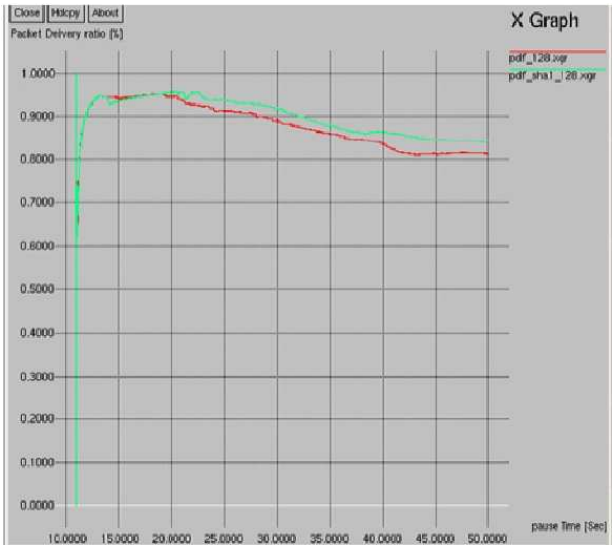


Fig. 9: Packet delivery ratio of CRC-32 and SHA-1 at 128 bit key

Fig. 10: Packet delivery ratio of CRC-32 and SHA-1 at 256 bit key

9 Conclusion

WEP has its own weakness but it is still extensively used in our daily life. In this article implementation and comparison of two algorithms: CRC-32 and SHA-1 has been considered. After evaluation, it has been concluded that CRC-32 is not so good because of its high end to end delay and low packet delivery ratio as compared to SHA-1.SHA-1 is cryptographic hash function which provides better results and security. Finally after running the experiment, it has been concluded that SHA1 is more suitable algorithm than CRC-32.

Packet delivery ratio		
	CRC-32	**SHA-1**
64 bit key	**0.7525**	**0.7169**
128 bit key	**0.8131**	**0.8411**
256 bit key	**0.7525**	**0.8846**

Fig. 11: Simulation results of CRC-32 and SHA-1

References

[1] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne, "Vulnerabilities of wireless security protocols (wep and wpa2)," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 1, no. 2, pp. 34–38, 2012.

[2] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi," in *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*. IEEE, 2007, pp. 46–51.

[3] Y. Wang, Z. Jin, and X. Zhao, "Practical defense against wep and wpa-psk attack for wlan," in *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on*. IEEE, 2010, pp. 1–4.

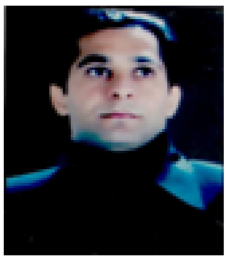
[4] M. Wang, G. Dai, H. Hu, and L. Pen, "Security analysis for ieee802. 11," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*. IEEE, 2008, pp. 1–3.

[5] W. Liu, H.-x. Duan, P. Ren, and W. Jian-ping, "Weakness analysis and attack test for wlan," in *Green Circuits and Systems (ICGCS), 2010 International Conference on*. IEEE, 2010, pp. 387–391.

[6] K. Wada, "Checksum and cyclic redundancy check mechanism," in *Encyclopedia of Database Systems*. Springer, 2009, pp. 328–329.

[7] F. Enns and J. P. O'Hare, "Packet framing using cyclic redundancy checking," Dec. 10 1991, uS Patent 5,072,449.

[8] A. Keswani and V. Khadilkar, "The sha-1 algorithm."



Amit Grover became a Member (M) of Association ISTE in 2006, a Senior Member (SM) of society SELCOME in September 2009, and a Project-In charge (PI) in august 2011 and in September 2012. The author place of birth is Ferozepur, Punjab, India on 27th, September 1980.The author received his M. Tech degree in Electronics and Communication Engineering from Punjab Technical University, Kapurthla, Punjab, India in 2008 and received his B. Tech degree in Electronics and Communication Engineering from Punjab Technical University, Kapurthala, Punjab, India in 2001. Currently, he is working as an Assistant Professor in Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India. The author is a Reviewer of many Reputed International Journals. His area of interest includes signal processing, MIMO systems, Wireless mobile communication; high speed digital communications, 4G Wireless Communications and VLSI Design.

Sukhchain Singh received his B. Tech degree in Electronics and Communication from Adesh Institute of Engineering and Technology, Faridkot, Punjab, India. The Author has been pursuing his research work under the guidance of Mr. Amit Grover, Assistant Professor (ECE), SBSSTC, Ferozepur, Punjab, India. Currently he is working as an Assistant Professor at Ferozpur college of Engineering and Technology. His research Interest includes computer network security, Digital Image Processing, Wireless Networks. He has a teaching experience of 5 years.