Study and Analysis of Dictionary attack and Throughput in WEP for CRC-32 and SHA-1

Sukhchain Singh
Assitant Professor/ECE
FCET, Ferozepur
Punjab, India

Amit Grover
Assistant Professor/ECE
SBSSTC, Ferozepur
Punjab, India

ABSTRACT
Wirelesses Local Area Networks (WLANs) have become more prevalent and are widely deployed and used in many popular places like university campuses, airports, residences, cafes etc. With this growing popularity, the security of wireless network is also very important. In this work, the evaluation of CRC-32 and SHA-1 is performed by calculating the throughput and by running dictionary attack on both the algorithms. The analysis shows that SHA-1 is more secure that CRC-32.

General Terms
Encryption, Decryption, Dictionary attack, Throughput

Keywords
WEP, CRC-32, SHA-1

1. INTRODUCTION
Wireless is a growing area in research and industry. Wired equivalent privacy (WEP) 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 transmitting 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 also very effective in the traditional 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 ENCRYPTION AND DECRYPTION
WEP Encryption: WEP uses the RC4 engine which is used to produce the random key stream.WEP also uses the CRC -32 for integrity. The entire data which have to be encrypted would have initialization vector which is of 24 bits, data along with integrity check value. Initialization vector (IV)[1][11] is generated randomly on per packet basis which means 1 packet produces 24 bits of initialization vector. Actual key is 40, 104, or 232 bits but when it is combined with the 24 bits IV it becomes 64,128,256 bits key. Both IV and the key will combine with each other and go as input to the RC4 algorithm which produces the random key stream.

Now we apply the CRC-32 on the plaintext data and produce the Integrity check value (ICV). When the plaintext data along with the ICV and the random key stream is XORED it produces the cipher text. As a client only knows the WEP key but does not know the Initialization vector, hence IV is padded with the cipher text. Now the cipher text can be encrypted and transmitted using the WEP technology.

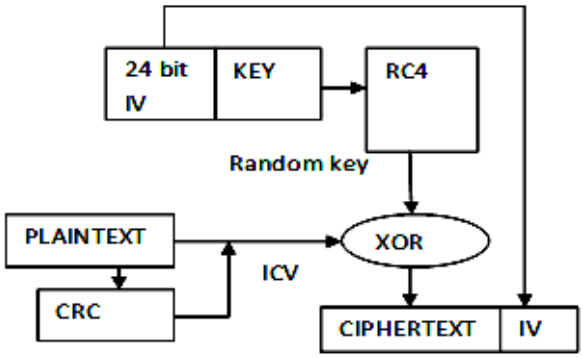

Fig1. WEP Encryption

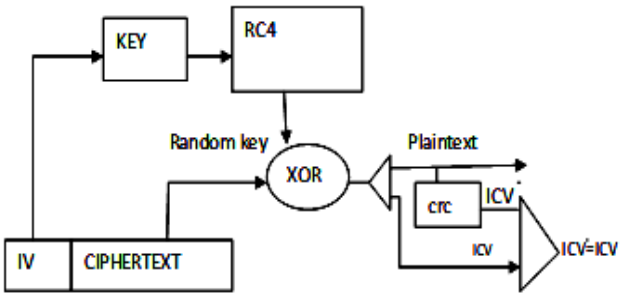

Fig.2 WEP Decryption [2]

WEP Decryption: In this process[11], the IV which is of 24 bits get combined with key and go as seed to the RC4 algorithm which produces the random key .The Cipher text XORED with random key which produce the plaintext. Integrity check value also produces by the CRC. If both the integrated check values are same then there is no error in the data received. Fig. 2 above shows the decryption process.

3. WEP WEAKNESSES
1. Poor key management: Most wireless networks which use WEP have symmetric WEP key shared between access points and client stations. 802.11 standards do not specify any WEP key sizes other than 40 bits [3].

2. The IV is short: WEP's IV which is of size 24 bits provide for 1.6 million different RC4 cipher streams for any size WEP key. Its looks too much but it is too small for cryptographic world .We know that Cipher text along with IV is transmitted and it is reuse at receiver end. If IV is found then it is very easy to decrypt an encrypted data

3. The ICV algorithm is not good: CRC-32 produces ICV that is used for detecting noise and errors in transmission. It is used for small block of messages and it is not a good choice for cryptographic hash

4. CRC-32 (CYCLIC REDUNDANCY CHECK)

CRC32 [4][5] is a hashing algorithm which is very commonly used in data transmission. It is a technique to for detecting errors but not for solving errors. In the CRC method, number of check bits called a checksum, are attached to the message which is being transmitted. At the receiver end if the check bits are matched then there is no error otherwise there should be some errors in the encrypted message. CRC-32 is used only for small block of data.

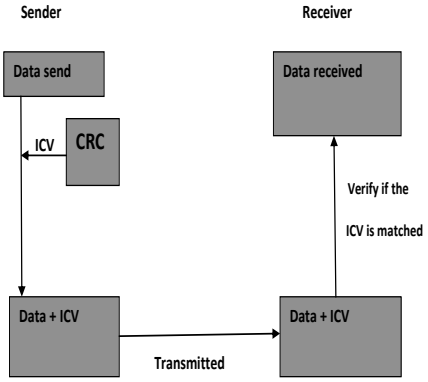

Fig. 3 CRC process

5. SHA-1 (SECURE HASH ALGORITHM)

SHA-1[6] 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.

Simulation Results and Performance Comparison:
Evaluation performance of CRC-32 and SHA-1 using NS-2 on the basis of Dictionary attack and throughput is as follows:

6. DICTIONARY ATTACK

It is a method of breaking a password-protected computer or server by entering every word in a dictionary as a password. A dictionary attack is also used to find the key which is necessary to decrypt an encrypt data. Dictionary attacks work because a lot of computer users using ordinary words as passwords.

Results of dictionary attack on CRC-32 and SHA-1 at 64 bit, 128 bit and 256 bit key.

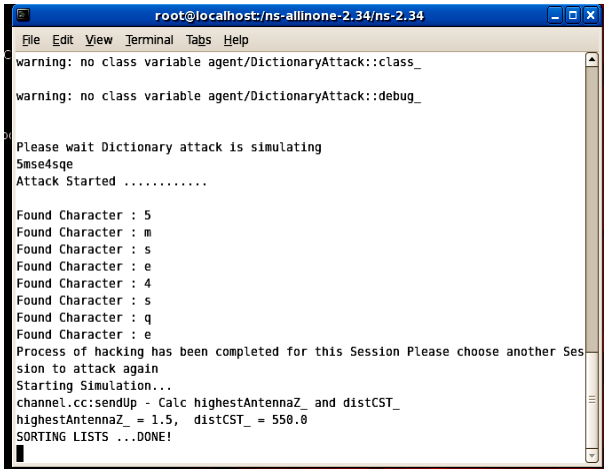

Fig.4 Dictionay attack on WEP with CRC at 64 Bit Key

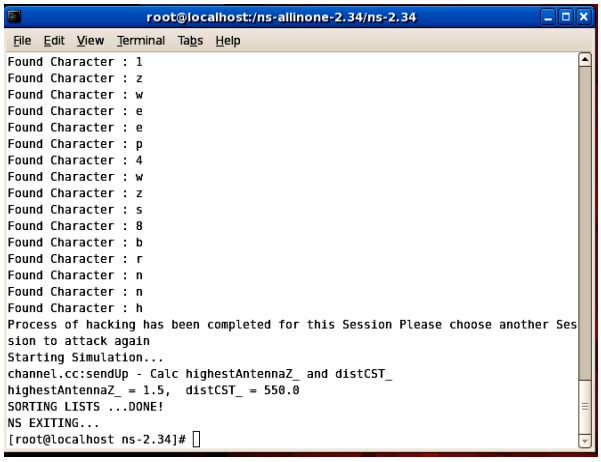

Fig.5 Dictionay attack on WEP with CRC at 128 Bit Key

When implemented dictionary attack on the CRC-32, it runs which is shown in the figure 4 that character of 64 bit key found. This illustrates that CRC-32 at 64 bit key is not secure because dictionary attack implemented on it. Similarly, dictionary attack implement on the traditional WEP with CRC-32 at 128 bit key and 256 bit key which is shown in the figures 5 and 6 respectively but dictionary attack does not run on the SHA-1 which illustrates that it is more secure than CRC-32 shown in the figure 7.

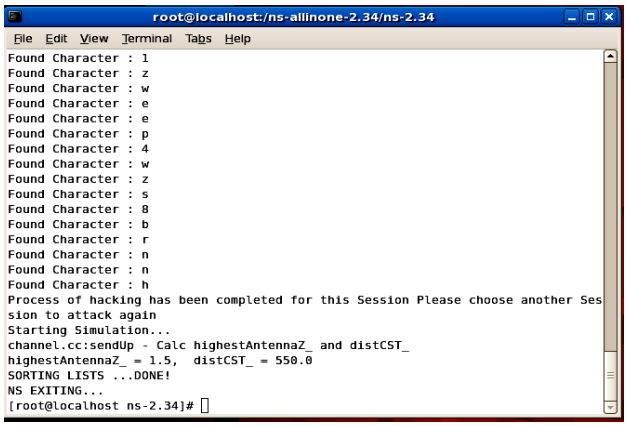

Fig.6 Dictionay attack on WEP with CRC at 256 Bit Key

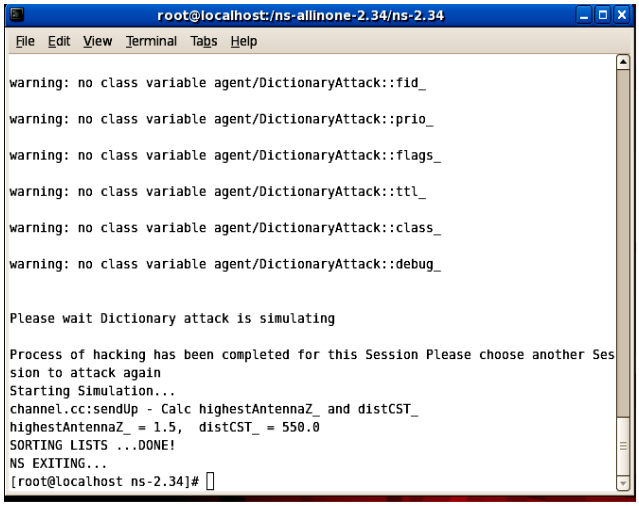

Fig.7 Dictionay attack on WEP with SHA-1 at 64 Bit Key

7. THROUGHPUT

Throughput [7] is the total number of packets delivered over the total simulation time or we can say it is the rate of successful message delivery over a communication channel. The throughput is measured in kbps, mbps and so on .It is the total data transferred from one end to another or processed in a specified amount of time.

Results and graphical representation of Throughput of CRC-32 and SHA-1 at 64 , 128 , 256 bit key .

In graphs shown in Figures 8, 9 and 10 respectively, X axis represents the pause time and Y axis represents the throughput in ms.These graphs compare the CRC-32 and SHA-1 algorithm.

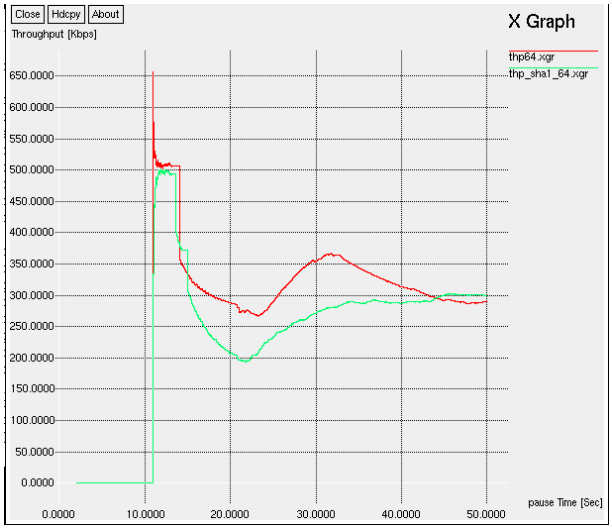

Fig.8 Throughput of CRC-32 and SHA-1 at 64 bit key

According to the graph of throughput vs. pause time of CRC-32 and SHA-1, comparison is done between the two algorithms at 64 bit key. According to the graph, CRC-32 has lower throughput than SHA-1. Results are shown below:

Results of Throughput for CRC-32 at 64 bit key is 290.89

Results of Throughput for CRC-32 at 64 bit key is 299.37

Fig.9 Throughput of CRC-32 and SHA-1 at 128 bit key

According to the graph of throughput vs. pause time of CRC-32 and SHA-1, comparison is done between the two algorithms at 128 bit key which is shown in figure 9. According to the graph, CRC-32 has lower throughput than SHA-1. Results are shown below:

Results of Throughput of CRC-32 at 128 bit key is 260.95

Results of Throughput of CRC-32 at 128 bit key is 295.88

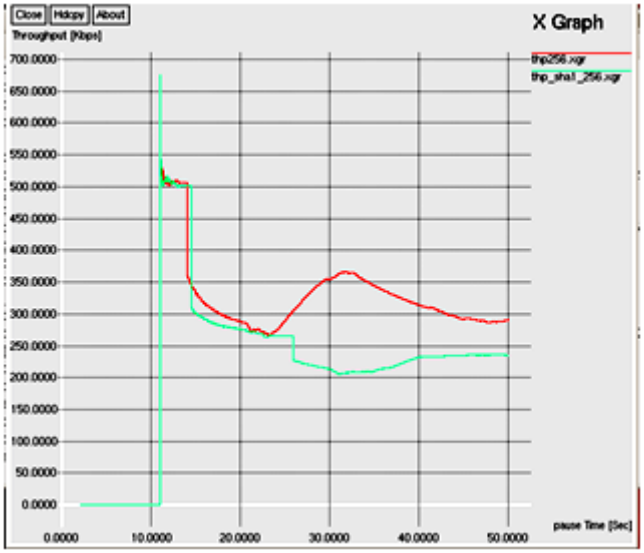

Fig.10 Throughput of CRC-32 and SHA-1 at 256 bit key

According to the graph of throughput vs. pause time of CRC-32 and SHA-1, comparison is done between the two algorithms at 256 bit key. According to the graph, CRC-32 has higher throughput than SHA-1. Results are shown below:

Results of Throughput for CRC-32 at 256 bit key is 290.89 kbps

Results of Throughput for CRC-32 at 256 bit key is 235.25kbps

8. CONCLUSION

Even though WEP have its own weaknesses but, it is still relevant in our daily life. While implementing and comparing CRC-32 and SHA-1 algorithms based on throughput and dictionary attack, it has been found that the dictionary attack runs on CRC-32 which indicates that SHA-1 is more secure algorithm. 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 WEP that will provide more security to the network.

9. REFERENCES

[1] Maocai Wang, Guangming Dai, Hanping Hu, Lei Pen "Security Analysis for IEEE802.11" IEEE 2008, pp. 1-3

[2] Ying Wang, Zhigang Jin, Ximan Zhao, "Practical Defence against WEP and WPA-PSK Attack for WLAN" IEEE 2010 6th International Conference on WiCOM, pp-1-4

[3] LIU Wu, DUAW Hai-xin,REN Ping, wu Jian-ping "Weakness Analysis and Attack Test for WLAN" IEEE 2010, pp. 387-391.

[4] Jyoti Wadhwani, Prof. Nitin Narkhede "Implementation of communication using Cyclic Redundancy" International Journal of Emerging Technology and Advanced Engineering , Volume 3, Issue 7, July 2013 , pp. 229-232

[5] Hasan Md. Mohtarim ,Ayesha Zaman,Nowrin Hoque "An approach for a Standard Polynomial for Cyclic Redundancy Check" International Journal of Computer Applications ,Volume 35– No.2, December 2011, pp. 1-4

[6] Amit Keswani and Vaibhav Khadilkar "THE SHA-1 ALGORITHM" Lamar University Computer Science Department, Beaumont, TX 77710, USA

[7] 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

[8] Songhe Zhao and Charles A. Shoniregun "Critical Review of Unsecured WEP" IEEE 2007, IEEE Computer society , pp. 1-7

[9] 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

[10] 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)

[11] Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, Seema Shrawne " Vulnerabilities of Wireless Security protocols (WEP and WPA2)" International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 2, April 2012 , pp. 35-38..

[12] 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

[13] Orest Kavka, Iurii Garasym, Valerii Dudykevych "The Analyses if wireless Communication Encryption Technologies. Modificated WEP Protocol" TCSET'2010, February 23-2010, Lviv-Slavske, Ukraine. pp. 186

[14] Ondiwa Nashon Odhiambo , E. Biermann & G. Noel, "An Integrated Security model for WLAN" IEEE AFRICON 2009 23 - 25 September 2009