ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

PERFORMANCE AND SECURITY EVALUATION BY USING SHA3 IN WEP

Ashish Kumar, Vishal Arora
Computer Science and Engineering Department
Shaheed Bhagat Singh State Technical Campus
Ferozepur ,India

ABSTRACT

In this paper we have discussed the wireless networks, security issues in wireless networks, and WEP (Wired Equivalent Privacy Protocol) .We have given the details of various limitations of WEP, how they can be eliminated by various cryptographic hash algorithms. We also proposed that how by replacing CRC-32 in WEP with SHA-3 can lead to improvement in the performance of WEP as compare to, when SHA-1 is used in that place.

Keywords: WEP,SHA3,SHA2,CRC-32,SHA,WPA,

Introduction

Wireless network is the mostly available and used in today's environment and life of common. This has become important part of everybody's life from personal to professional .Mobile, Tablets and various other devices are the best examples of it. As this is the era of information and technology, wireless network has the utmost importance. Wireless network is defined as the network of the wireless nodes moving freely in the specified region connected with signals provided by various access points, towers etc. This is a collection of mobile nodes, hubs, switches, base stations, active nodes, sleeping nodes etc. We can classify the wireless network into various types:- WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WWAN (Wireless Wide Area Network) as described in fig-1.

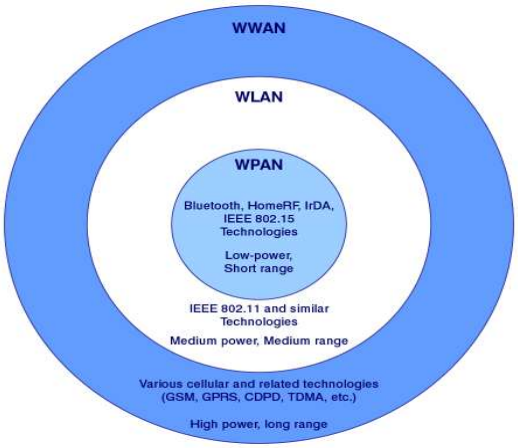

Fig-1

Here, we will emphasis on WLAN that is primarily used by us or an organization. As the use of Wireless network has increased, chance of attacks on it has also increased. As Wireless is openly access as compare to wired networks, threats to security of it has become an important issue. Various kinds of attacks possible on wireless network are shown in following figure, Fig-2.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Fig-2

To resolve all these kinds of attacks various Security protocols have been defined by IEEE for WLAN(Wireless Local Area Network).These are WEP, WPA , WPA2.Here we will focus on WEP, its functioning , weak points in WEP and how it can be resolved out by using various Cryptographic Hash Algorithms and comparing there Performance.

WEP(WIRED EQUIVALENT PRIVACY PROTOCOL)

Wired Equivalent Privacy Protocol was the first of its kind to provide the wireless security to the end user. It makes the use of mainly the two things, Initialization Vector in RC4 algorithm and CRC (Cyclic Redundancy Code).Initialization Vector used in WEP is basically of 24-bit size leading to the 224 bits of keys that can be used for unique identification of the message.CRC (Cyclic Redundancy Check) is used for checking the integrity of the message, that is whether it is the same message being sent by the sender or it has been altered in the mid way. It checks the validity that whether the correct message has been recie3ved on the receiver end or not. If we have to send 64-bit key in a message then 24-bit of the message will be Initialization Vector, and rest of 40-bit will be the message key. If we have to send 128-bit of key, we can send 104-bit of the message key and rest of 24-bit again IV (Initialization Vector).Similarly in a larger case, where we have to send 256-bit of message, We can use only 232 bits-key for message only and rest of 24 bit-key for Initialization Vector).Several weakness have been reported in the WEP ,that lead to the formation of new protocols WPA and WPA2.The main advantages of using WEP are Access control, Confidentiality and integrity. Complete process of WEP can be divided into two Parts: WEP Encryption and WEP decryption.

WEP ENCRYPTION

This is the first part of WEP Protocol, which has main target of encrypting the data into the coded format that can be uploaded on to the network and from there it can be sent to the target receiver. Encryption in WEP takes place in three steps. First, CRC is implemented in Plain text to generated checksum value and then that Checksum value is embedded to the plain text. Second, Initialization Vector (24-bit) is provided to the RC4 Algorithm to generated unique code that confirms the confidentiality of the message .Third, Both embedded Plain text and Key produced by RC4 algorithm is then XORed to produce encrypted message. This is shown in Fig-3.

.

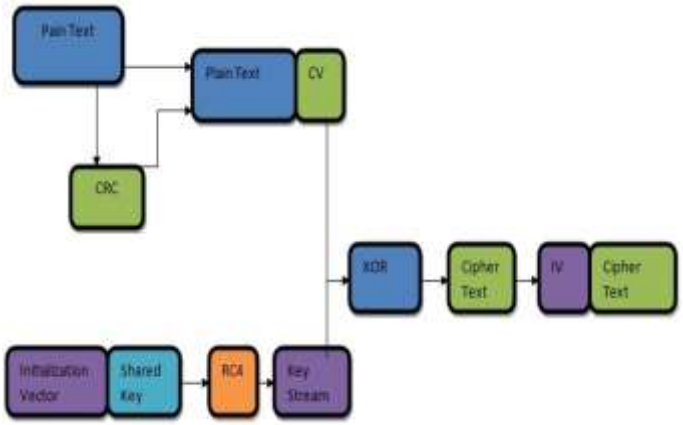

Fig-3

WEP DECRYPTION

As name indicates, it is the decryption part of WEP protocol. Here, the encrypted data is taken by the receiver from the network. The encrypted data along with receiver‘s WEP key for decryption is seeded to RC4 gen. Now, we can divide the coded data again into two parts ,plain data with Checksum Value and RC4 generated data. Checksum valuecalculated on the data by using same CRC-32 algorithm, which is

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

then compared with embedded Checksum Value as shown in fig-4.

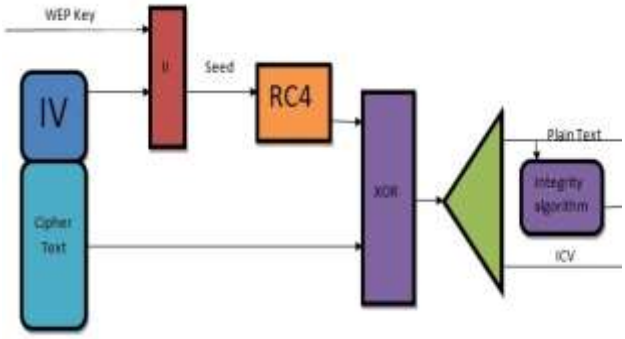

Fig-4

WEAKNESS IN WEP

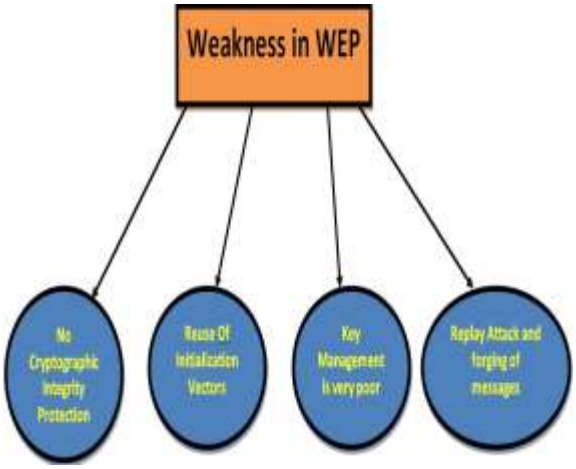

Fig-5

Various weakness have been founded in WEP that are listed above in fig-5.These are as follows, No cryptographic has based integrity algorithm implemented. As combination of stream ciphers with non cryptographic checksum can result into various vulnerabilities in WEP.As there are maximum chances of reuse of Initialization vector, this may lead to higher chances of attack. An attacker who will listen to the network on regular basis will have a higher chance of guessing the initialization vectors and thus can harm WLAN. Along with it, Key management in RC4 in WEP is very poor as there is repeated use of selected keys and ignoring some of the keys for encryption work. Replay attacks are easily applicable on WEP, and not as an independent document. Please do not revise any of the current designations. Means attacker can repeat the packets sent in the network over large number of times so that it can be very helpful for attacker in guessing ciphered text. Packet spoofing/forging the packets/Packet injection is one of major drawback in WEP; it means third party can send their own packets in large quantity in the network that can lead to blockage/disturbance in the network is again.

SHA3

Secure Hash Algorithms are the family of Cryptographic hash algorithm published 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 revert back the data by using only hash values. It has following properties,It is easy find out hash for a given message.It is infeasible to get data back from hash values alone, It is infeasible to change the data without changing hash,making it more secure. Classification of secure hash algorithms are SHA0,SHA1,SHA2,SHA3. SHA3 is easlier 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 is 1600 bits that is in 5x5x64 in 3-D form. The best part of SHA3 is that it has unlimited size of message which makes it more powerfull, It also Prevent varios kind of attacks like image attack and collision attack.

SIMULATION AND IMPLEMENTATION OF SHA3 IN WEP

In our research work, we have used SHA3 Algorithm in WEP, in place of CRC32 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 from referenced paper, we have taken values for three different length of message keys i.e. 128,256,512 bits

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Throughput

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 6,7 and 8 represent the values of throughput using SHA3 in WEP with 64, 128, 256 bit length of key.

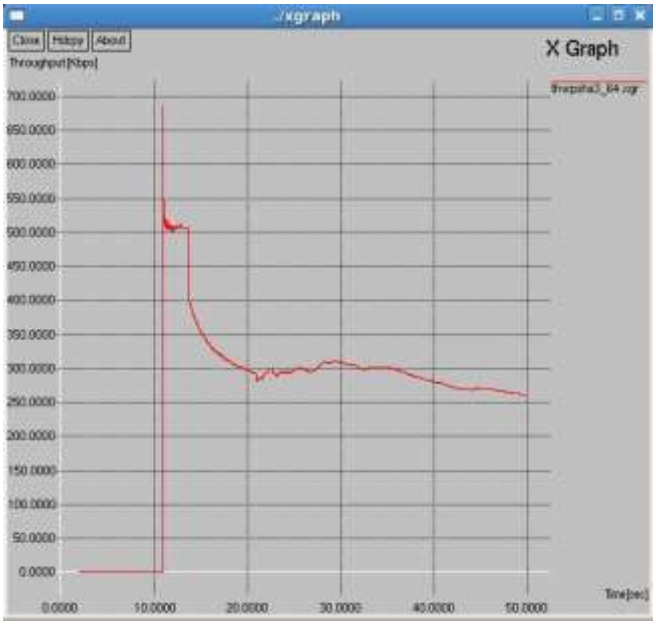

Fig 6:Throughput using SHA3 in WEP with 64 bit length key

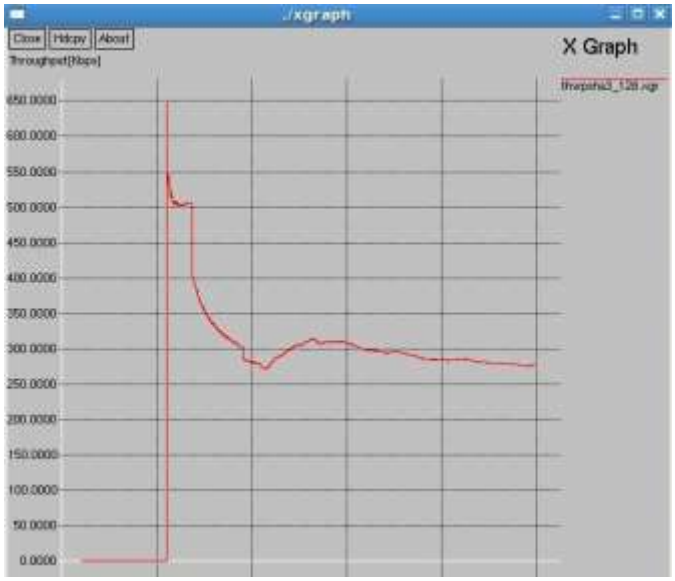

Fig 7: Throughput using SHA3 in WEP with 128 bit length key

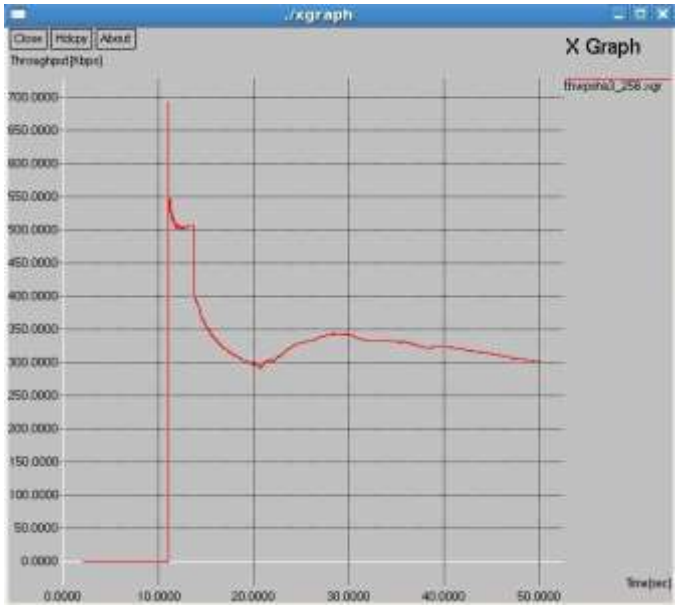

Fig 8: Throughput using SHA3 in WEP with 256 bit length key

We have compared throughput with SHA1 in WEP under similar conditions [2],[3] we found that SHA3 is more secure than SHA1 and also it shows some improvement over SHA1 under some specific conditions. These values are compared in following figure (Fig 9).

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

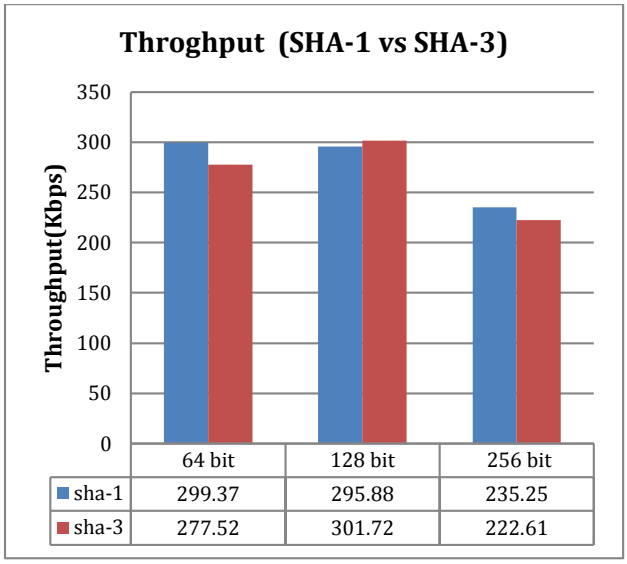

Fig-9: Comparison of Throughput with 3 different length of keys

CONCLUSION AND FUTURE SCOPE

Weakness is there in WEP that lead to formation of new protocols but by implementing SHA3 in place of CRC-32 in WEP, 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.

REFERENCES

[1] Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker, "Security flaws in 802.11 data link layer protocol", COMMUNICATIONS OF THE ACM May 2003/Vol. 46, No. 5

[2] Amit Grover and Sukhchain Singh, "Study and Analysis of Dictionary attack and Throughput in WEP for CRC-32 and SHA1", International Journal of Computer Applications (0975 – 8887) Volume 96– No.17, June 2014

[3] Amit Grover and Sukhchain Singh, "Comparative Analysis of CRC-32 and SHA1 Algorithms in WEP" Advanced Engineering Technology and Application, No. 1, 1-6 (2015)

[4] Laxmi Mounika.Nannaka , Hepzybah.Singarapu & Ramadevi.Puli, "Remodelling RC4 Algorithm for Secure Communication for WEP/WLAN Protocol" Global Journal of researches in engineering Electrical and electronics engineering, Volume 12 Issue 5 Version 1.0 April 2012

[5] ARASH HABIBI LASHKARI, MASOOD MANSOORI, AMIR SEYED DANESH, "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)", 2009 International Conference on Signal Processing Systems

[6] Mr. S.M.K.M. Abbas Ahmad, Dr. E.G. Rajan and Dr. A. Govardhan: "Attack Robustness and Security Enhancement with Improved Wired Equivalent Protocol" ACEEE Int. J. on Network Security , Vol. 03, No. 02, April 2012

[7] Dr.Satya Prakash Singh, Ramveer Singh: "Security Challenges in Mobile Adhoc Network" International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.7 No.11 (2012)

[8] Tomas ONDRASINA, Maria FRANEKOVA: "Attacks to Cryptography Protocols of Wireless Industrial Communication System" INFORMATION AND COMMUNICATION TECHNOLOGIES AND SERVICES VOLUME: 8 /NUMBER: 3 /2010/ SEPTEMBER

[9] 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

[10] ONDIWA NASHON ODHIAMBO , E. BIERMANN & G. NOEL, "AN INTEGRATED SECURITY MODEL FOR WLAN" IEEE AFRICON 2009 23 - 25 SEPTEMBER 2009

[11] P. MANICKAM, T. GURU BASKAR , M.GIRIJA , DR.D.MANIMEGALAI "PERFORMANCE

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

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

[12] LIU WU, DUAW HAI-XIN,REN PING, WU JIAN-PING "WEAKNESS ANALYSIS AND ATTACK TEST FOR WLAN"