WLAN Security and Efficiency Issues based on Encryption Techniques

Riddhi C. Somaiya[1], Dr. Atul M. Gonsai[2], and Rashmin S. Tanna[3]

[1](Ph.D. Scholar in Saurashtra University, Rajkot,Gujarat, India)

[2](Associate Professor, Department of Computer Science, Saurashtra University, Rajkot,Gujarat, India)

[3](Lecturer, Department of Electronics and Communication, A. V. Parekh Technical Institute Rajkot, Gujarat, India)

Abstract: *The first wireless protocol WEP has not been up to the mark as proved by several attacks. The second wireless security protocol WPA is better than WEP in terms of security, throughput and memory utilization. Still it has major weaknesses in terms of security and the protection of integrity of transmitted data. The latest standard WPA2 has shown the best immunity towards these attacks. Hackers are finding newer ways to expose its vulnerability. In order to provide secure service WPA2 has to keep on adapting with this new attacks.in doing so it should not compromise its efficiency. In this paper we reviewed WPA2, some encryption algorithms, their benefits, vulnerabilities and reviewed research papers that tried to modify the encryption algorithms to make the process more secure and efficient.Finally we conclude that many algorithms, mechanisms and standards are developed to secure the WLANs. But in one or other way they failed to provide security and efficiency altogether.*

Keywords: *WPA2, Encryption Algorithms, AES, Blow fish.*

I. INTRODUCTION

Wireless LANs have increased in popularity in recent years. Wireless communication is convenient and plays a prominent role in networking, however security and performance is a major concern. If an unauthorized person is able to get access to this network, he can get access to all the resources and data that are being transmitted on that network.

There are no clear physical borders in WLANs because of spreading of radio waves. So WLAN can be listened by anyone within range (packet sniff) and can be potentially connected to. Encryption keeps WLAN data private so encrypted data can still be overheard, but cannot be understood.

To avoid this insecurity, there are some security standards for wireless LANs those are named as WEP, WPA and WPA2. WEP and WPA are outdated now because of lake of security they provide.WPA2 is considered as most secure standard for wireless networks as of now.

Security specialists must stay busy in the lab concocting new schemes to keepcyber-attacksat bay because they are constantly evolving. It's not 100 percent bulletproof as shown by successful attacks on victims, but without it, you're data is totally accessible.

In this paper we have stated need of the study in section II will discuss about WPA2 in section III and its security loopholes in section IV. Section V gives a brief idea about different encryption algorithms like DES, AES, RC6, blowfish and two fish, and pros and cons to use them keeping in mind some performance parameters like throughput, energy saving, round-trip time, bandwidth, delay, encryption-decryption time, speed. In section VI we have shown performance analysis of different encryption algorithms. Finally section VII and VIII provides conclusion and scope of future work to be done.

Need of the study

As computers and wireless networks are reaching closer to non IT people, the development of strong, efficient and easy to manage security system is strongly needed. Because a small loop hole in the network can cause any big harm by intruders like access control attacks, confidentiality attacks, integrity attacks, authentication attacks etc. These can challenge the person or business financially and socially.

Encryption techniques play a major role in wireless network security. As data is encrypted before sending it through wireless medium, even though any intruder gets the access to the data he/she will not be able to get any meaningful information out of it. So encryption techniques should be strong enough for anyone to decrypt.

We have studied current scenario of wireless networks security and some encryption algorithms with their merits and demerits innext sections. so that we can get closer to the idea of developing a secure and efficient encryption algorithm which can make wireless networks secure enough to transfer confidential information.

WPA2

802.11i (also called WPA2) [1] is designed for wireless networks by Task Group i (TGi). It was standardized in 2004. WPA,its previous version hasn't been broken; this protocol has been designed by IEEE 802.11ibecause of possible flaws according to the WEP weaknesses. WPA2uses Counter Mode with CBC-MAC Protocol (CCMP) to encrypt network traffic. CCMP employs Advanced EncryptionStandard (AES) as encryption algorithm. WPA2 is backwards compatible with WPA but not with WEP.

Security flaws in WPA2

Even though WPA2 provided strong security solution there are some potential flaws in the algorithms adopted by WPA2. For example, Junaid et al. in paper [2] and Khan et al. in paper [3] showed that WPA2 can be subjected to dictionary attacksby predicting the initial counter value used in CCMP. Also, Mitchell and He in [4] mentioned that, in CCMP, management andcontrol frames are neither encrypted nor authenticated by link-layer encryption algorithm. Hencethey are vulnerable to several threats. They also said that CCMP may have some impact on the system's performance as it requires some hardware upgrades.

SamadSalehiKolahiet.al.in [5] compared the network with open system and with wpa2 security and proved that network with wpa2 security gives less throughput then open system.

While enabling WPA2 security against open VPN we have to compromise with performance issues as in [1] enabling WPA2 causes 3 Mbps less TCP throughput and 0.20 ms more TCP RTT than open system for both IPV4 and IPv6 on Fedora 12.

WPA2 has also been successfully hackedeven though it is the most secure compared to others.Some of the known security issues of wpa2 are Brute force attack,weak password, WPS PIN recovery,Wrong offset and sequence, MS-CHAPv2, Sniffing, ARP poisoning, Port scanning, ICMP DoS attack, WPA packet spoofing and decryption, TCP/IP hijacking,Symmetric key attack,Hole196, numbers in IP header.

II. ENCRYPTION ALGORITHMS

Encryption algorithms use computing resources intensively such as memory,CPU time and battery power. Due to encryption algorithms a wireless device, usually with very limited resources, especially battery power, is subject to the problem of energy consumption. In addition, wireless devices commonly transmit and receive data over a wireless link. To keep the data secure from an eavesdropper it is protectedusing an encryption algorithmbefore transmission.

The security in WLAN is based on cryptography. Cryptography is called science and art of transforming messages the way that no one other can read them to make them secure and immune to attacks by authenticating the sender and receiver within the Wireless LAN. The cryptography algorithms are divided into two types: symmetric-encryption algorithms and asymmetric-encryption algorithms. There is a lot of symmetric-encryption algorithms used in WLAN, such as DES, TDES, AES, CAST-256, RC6 etc.

AES

The Advanced Encryption Standard (AES) algorithm as in [12] is a symmetric block cipher that can encrypt and decrypt the plaintext and cipher text of 128-bits using cryptographic keys of 128-bits (AES-128), 192-bits (AES-192), or 256-bits (AES-256). Number of rounds can be 10, 12 or 14 depending on the key size.

DES

DES is a symmetric encryption algorithm as in [13], it needs two inputs: a keyalong with the plaintext. The length of the plaintext is 64 bits, and the key is also 64 bits in length. The basic building block is called a round and is repeated 16 times. For each DES cycle, a sub-key is obtained from the original key using an algorithm known as key schedule. Then DES encrypts the data in 64-bit blocks using a 64-bit key (note that its effective key length is only 56-bit).

TDES

TDES (Triple DES) as in [14] is a block cipher formed from the DES cipher by using it three times. When it was found that a 56-bit key of DES was very small and could be broken, TDES was chosen as a simple way to enlarge the key space without changing the algorithm. The use of three steps Encryption - Decryption – Encryptionis effective against the DES encryption.

Blowfish

Blowfish as described in [7] is a symmetric 64-bit block cipher, invented by Bruce Schneier; optimized for 32-bit processors with large data caches, it is significantly faster than DES on a Pentium/PowerPC-class machine. Key lengths can vary from 32 to 448 bits in length. Blowfish, available freely and intended as a substitute for DES or IDEA, is in use in a large number of products.

RC6

As described in [15]RC6 is more accuratelyspecified as RC6-w/r/b where the word size is w bits, encryption consists of a nonnegative number of rounds r, and b denotes the length of the encryption key in bytes. Since the AES submission is targeted at w = 32 and r = 20, RC6 shall be used as shorthand to refer to such versions. When any other value of w or r is intended in the text, the parameter values will be specified as RC6-w/r. Of particular relevance to the AES effort will be the versions of RC6 with 16-, 24-, and 32-byte keys.

Blowfish is fastest among these algorithms as in [8]. As per experiment in [21] AES is found to be the best in terms of encryption performance and memory utilization [9]. When and experiment of encryption was performed with different data packet sizes it was found that AES tends to perform better than RC4 with a small packet size, but when data packet size was increased the throughput of RC4 was better than that of AES. This proves that RC4 is more efficient than AES when encryption is performed over large data blocks. AES and RC$ tends to have close performance with different key sizes, while RC4 performance is likely independent of the key size.

A performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices is presented in [20].AES, DES, and 3DES, RC6, Blowfish and RC2 were the selected algorithms. From the Experimental results we can conclude that:

(1) In the case of changing packet size with and without transmission of data using different architectures and different WLANs protocols; Blowfish has better performance than other common encryption algorithms used, followed by RC6. As shown in Figure 1 which is taken from [20].

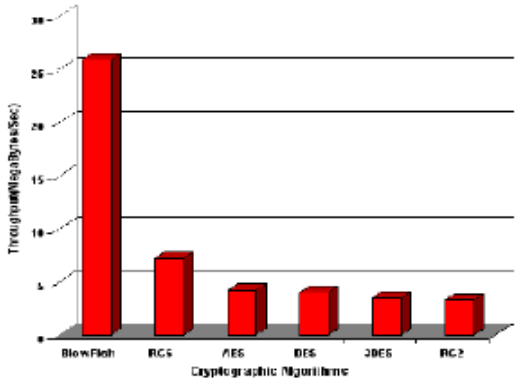

Figure1: Throughput of each encryption algorithm to encrypt different text data (Megabytes/Sec) without data transmission.

(2) In case of changing data type such as audio files, it is found the result as the same as in text and document. In the case of image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption. Also, it is found that 3DES still has low performance compared to algorithm DES. As shown in Figure 2 which is taken from [20].

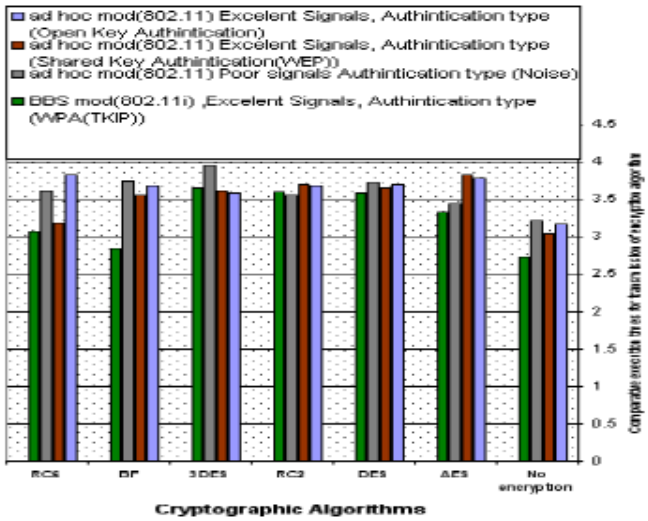

Figure 2: Comparative execution times for transmission of Image files using different algorithms

(3) When the transmission of data is considered there was insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). There is insignificant difference between open key authentications and shared key authentication in ad hoc Wireless LAN connection with excellent signals. In case of poor signal it is found that, transmission time increased minimum by 70 % over open sheered authentication in ad hoc mod.

III. PERFORMANCE ANALYSIS OF DIFFERENT ALGORITHMS

In paper [10] Monika Agrawal and Pradeep Mishra presented a modified version of blowfish algorithm and concluded that the new algorithm isless time consuming as compared to blowfish algorithm. And the encryption time and decryption time for modified blowfish algorithm is almost half to that of blowfish algorithm. Nusrat Jahan Oishi et.al. Has presented a new algorithm [11] by adding a function of RC6 with blowfish, and the outcome was more secure but slower than blowfish but comparatively faster algorithm then existing AES.

P. Prasithsangaree and P. Krishnamurthycompared AES and RC4 for its energy consumption in paper [16]. For experiment, many performance parameters were collected like encryption time, CPU process time, and CPU clock cycles. In this paper they reviewed related literature and also explained the importance of different encryption algorithms.

When comparedsymmetric algorithms like AES takeminimum amount of time to perform encryption and decryption.This enhances 'over the air' safety of informationaccording to a survey [17]. Asymmetric algorithms like RSA and Diffie-Hellmanare secure with respect to their size of the keys. RSA solves the problem of the key agreement and key exchange problem in secret key cryptography. Therefore the feature of public and private keys from RSA algorithm can be combined with AES which provides the advantage of fast encryption/decryption as well as more security. Not only the encryption but also secure transmission of data over the network is mandatory because the cryptographic algorithms can provide security but they cannot guarantee 100% safety.

A new efficient key management scheme to increase security-throughput trade-off performance in wireless networks is shown in the paper [21]. Existing schemes had poor key management for large wireless networks since their implementation was based on symmetric encryption techniquesbut this new scheme has the benefit of being used in encryption, authentication, data integrity and non-repudiation with efficient key management. As per results we can say that "Throughput and security increase as the number of bits used for the block lengths increases". But throughput decreases when key sizes and block lengths of 256 bits or more is used due to modular exponentiation. The new algorithm shows high security level for key sizes of 64, 128 and 256 bits when using three or more convolutional cascaded stages. The security level is far above the traditional 1024-bit RSA which is already vulnerable. The vulnerability of 1024-bit RSA led to the implementation of higher levels such as 2048-bit and 4096-bit. These high level RSA schemes when implemented will greatly compromise throughput due to modular exponentiation. Hence, the usefulness of a scheme such as the one presented in this paper.

No successful attack is noted until now for blowfish other than brute force attack (an exhaustivekey search of every possible key). Serge Vanudenay inpaper "On Weak Keys of Blowfish" [18] explainsthat here is a possibility that the key size can bereduced. Vanudenay states that dynamically creating the S-Boxes can increase the possibility ofaccidental replication such that byte x is equal tobyte x'. This theory was tested and proved to besuccessful through round 8 of Blowfish.Unfortunately,it is not practical in real time. In this paper the author foreknew the S-Box valuesbefore creation; attackers should not have this type of information.

In the paper "Blowfish Survey" authored by Jason W. Cornwell [19], the design, performance analysis and possible vulnerabilities of blowfish is surveyed. This paper explained the design, code and execution of blowfish in brief; also shared some reviews of previous papers and stated its vulnerability i.e. brute force attack. Author concludes that blowfish is currently providing security up to its best and in future it can continue to serve by re-evaluating it time by time.

IV. CONCLUSION

Many algorithms, mechanisms and standards are developed to secure the WLANs. For example, as discussed in earlier sections, algorithms like AES, RSA, DES, TDES, Blowfish are being used for cryptography But in one or other way they failed to provide security and efficiency altogether. This paper reviews the WPA2 and its benefits, drawbacks, as well as some encryption algorithms. We have also reviewed some papers that modified some of these encryption algorithms to make them more power full where algorithms are modified or they are combined with one another like Blowfish + RC6 or AES + RSA to combine the benefits of both the algorithm. The combination of Blowfish and RC6 outcomes in a new algorithm that is faster and securer then existing AES but is slower than Blowfish,Whereas combination of RSA and AES gives more security and takes less time in encryption/decryption but that also cannot guarantee 100% security. Still a lot more research is required in this area

and a better algorithm is yet to be created which satisfies all the requirements of a speedy, secure and highly efficient wireless network.

V. LIMITATIONS AND FUTURE WORK

Limitations of study

Encryption techniques can secure the data passing through wireless medium by encrypting it. But it cannot secure entire network from malpractice. So securing entire network is as well important.

After studying existing scenarios, we can say that process of Encryption and Decryption consumes more time and energy than passing unencrypted data through network. Many researches are held and algorithms are developed to make Encryption-Decryption process fast and energy saving but they are successful up to some extent and cannot reduce consumption of time and energy as much as it is in unencrypted data.

Future Work

In future, we want to create such a new encryption algorithm that can make WPA2 more secure and more efficient taking in consideration the parameters like throughput, energy saving, round-trip time, bandwidth, delay, encryption-decryption time, speed. Test the new algorithm in simulated as well as real environment, compare it with existing scenario and provide statistics and valid reasons to use the new algorithm.

VI. REFERENCES

[1] *Peng Li, Samad S. Kolahi, Mustafa Safdari, and MulugetaArgawe,"Effect of WPA2 Security on IEEE 802.11n Bandwith and Round Trip Time in Peer-Peer Wireless Local Area Networks"Workshops of International Conference on Advanced Information Networking and Applications, pp.777 - 782,22-25 March 2011.*

[2] *M. Junaid, M. Mufti, and M. U. Ilyas, "Vulnerabilities of IEEE 802.11 iwireless LAN CCMP protocol," Trans. Eng., Comput. Technol., vol. 11,pp. 228–233, Feb. 2006.*

[3] *M. A. Khan, A. R. Cheema, and A. Hasan, "Improved nonce constructionscheme for AES CCMP to evade initial counter prediction," in Proc. 9thACIS Int. Conf. SNPD, 2008, pp. 307–311.*

[4] *J. C. Mitchell and C. He, "Security analysis and improvements for IEEE802.11 i," in Proc. 12th Annu. NDSS, 2005, pp. 90–110.*

[5] *SamadSalehiKolahi, Peng Li, MulugetaArgawe, and Mustafa Safdari, "WPA2 Security-Bandwith Trade-off in 802.11n Peer-Peer WLAN for IPv4 and IPv6 Using Windows XP and Windows 7 Operating Systems", Computers and Communications (ISCC), 2012 IEEE Symposium on, p.p. 000575 – 000579, 1-4 July 2012.*

[6] *G.Ramesh, Dr. R .Umarani, "UR5:A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation",International Journal of Advanced Research in Computer Science and Software Engineering,vol 2, April 2012.*

[7] *B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.*

[8] *AamerNadeem, Dr M. YounusJaved, "A Performance Comparison of DataEncryptionAlgorithms",International Conference on Information and Communication Technologies, p.p. 84 – 89,27-28 Aug. 2005.*

[9] *S. S. Gautam, ShivlalMewada, Pradeep Sharma, "Classification of Efficient Symmetric Key Cryptography Algorithms", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 14, No. 2, Feb 2016.*

[10] *Monika Agrawal, Pradeep Mishra, "A Modified Approach for Symmetric KeyCryptography Based on Blowfish Algorithm",International Journal of Engineering and Advanced Technology (IJEAT), vol-1, August 2012.*

[11] *NusratJahanOishi, Md.ArafinMahamud,Asaduzzaman, "Short Paper: Enhancing Wi-Fi Security Using aHybrid Algorithm of Blowfish and RC6",International Conference on Networking Systems and Security (NSysS), p.p. 1-5, 7-9 Jan. 2016.*

[12] *HaeyoungRha and Hae-wook Choi, "Efficient pipelined multistream AES CCMP architecture for wireless LAN", International Conference on Information Science and Applications, p.p. 1-5, 23-25 May 2012.*

[13] *ZhouYingbing, LI Yongzhen, "The Design and Implementation of a Symmetric Encryption Algorithm Based on DES", Software Engineering and Service Science (ICSESS), 2014 5th IEEE International Conference on, p.p. 517 – 520, 27-29 June 2014.*

[14] *Jose A. Jaramillo- Villegas, Esteban M Correa-Agudelo, Rene Gomez-Londono, "TDES Implementation in a Reconfigurable Computing Enviroment", Programmable Logic, 2008 4th Southern Conference on, p.p. 191 – 195, 26-28 March 2008.*

[15] *KirtiAggarwal, "Comparison of RC6, modified RC6 & enhancement of RC6", Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in", p.p. 444 – 449, 19-20 March 2015.*

[16] *Prasithsangaree, Phongsak, and Prashant Krishnamurthy. "Analysis of energy consumption of RC4 and AES algorithms in wireless LANs." Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE. Vol. 3. IEEE, 2003.*

[17] *Thambiraja, E., G. Ramesh, and Dr R. Umarani. "A survey on various most common encryption techniques." International journal of advanced research in computer science and software engineering 2.7 (2012).*

[18] *Serge Vaudenay (1996) (postscript). On the Weak Keys of Blowfish. Retrieved 2009-08-23.*

[19] *Cornwell, Jason W., and G. A. Columbus. "Blowfish survey." Department of Computer Science. Columbus: GA Columbus State University (2012): 1-6.*

[20] *Salama, Diaa, HatemAbdual Kader, and MohiyHadhoud. "Studying the Effects of Most Common Encryption Algorithms." International Arab Journal of e-Technology 2.1 (2011): 1-10.*

[21] *Sone, Michael Ekonde. "Efficient key management scheme to enhance security-throughput trade-off performance in wireless networks." Science and Information Conference (SAI), 2015. IEEE, 2015.*

About Authors:

- **Riddhi Somaiya**: is a Ph.D. Scholar in Saurashtra University, Rajkot,Gujarat, India. She has received her M.C.A. degree in 2012 from the Department of Computer Science, Saurashtra University, Rajkot, Gujarat, India and B.C.A degree in 2009 from the same university. Her area of research is security in wireless LANS.

- **Dr. AtulGonsai**: is an Associate Professor, Department of Computer Science, Saurashtra University, Rajkot,Gujarat, India. He has received his Ph. D degree in the field of Computer Science from the same University. He has also completed Master of Computer Applications (MCA) from the same Department in April 2000. He has total teaching experience of Sixteen years. He has been awarded the "CAREER AWARD FOR YOUNG TEACHERS" from ALL INDIA COUNCIL FOR TECHNICAL EDUCATION (AICTE) New Delhi with amount of Rs. 10.5 lakhs.

- **Lect. RashminTanna**: is a lecturer, department of Electronics and Communication, A. V. Parekh Technical Institute Rajkot, Gujarat, India affiliated with Gujarat Technical University, Chandkheda, Gujarat, India. He has received his BE degree in the field of Electronics and communication in 2009 from Saurashtra University. His fields of interest are wireless networks security, robotics and embedded systems.