International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October, 2009
1793-8201

Analyzing the Energy Consumption of Security Algorithms for Wireless LANs

Diaa Salama Abdul. Elminaam, Hatem M. Abdul Kader and Mohie M. Hadhoud

***Abstract*—Security in wireless networks is of paramount importance. Due to the broadcast nature of the wireless radio signals, wireless networks are implicitly vulnerable to several network attacks. Anyone within the wireless transmission range of a device (including malicious users or attackers) is able to passively listen to or eavesdrop on the signals and could potentially access information from the signals. It is also possible to actively transmit signals that can attack the network. Encryption algorithms play good roles in information security systems (ISS). Those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. Wireless devices are powered by a battery which is a very limited resource. It implicitly says that the power of computing will grow exponentially. However, the capacity of batteries is growing linearly, and this introduces a "power gap" which is the difference between the power required by computing and the battery capacity. Thus, battery power tends to be a very seriously limited resource for small wireless devices, and a security protocol should utilize energy to the minimum extent possible. This aspect is the primary focus of this dissertation. This paper illustrates the key concepts of security, wireless networks, and security over wireless networks. It provides evaluation of six of the most common encryption algorithms on power consumption for wireless devices A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption**

***Index Terms*—Computer security, wireless network, ad hoc wireless LANs, Basic Service Set (BBS), Cryptographic algorithms**

I. Introduction

Both security and wireless communication will remain an interesting subject for years to come. Wireless networks fall into several categories, depending on the size of the physical area that they are capable of covering. The following types of wireless networks satisfy different user requirements: Wireless Personal-Area Network (PAN), Wireless Local-Area Network (LAN), Wireless Metropolitan-Area Network (MAN) and Wireless Wide Area Network (WAN). Encryption algorithms play major roles for protecting data. Those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. CPU and memory are increasing and need for power, but battery technology is increasing at a much slower rate. Collisions and retransmissions lead to additional consumption of power the design of energy efficient secure protocols for wireless devices needs to understand how encryption affects the consumption of battery power with and without data transmission.

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric Asymmetric keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. Strength of Symmetric key encryption depends on the size of key used. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key .DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys [1-4] while AES uses various (128,192,256) bits keys [5-6]. Blowfish uses various (32-448); default 128bits [7] while RC6 is used various (128,192,256) bits keys [8].

Asymmetric key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [1].

This paper examines a method for evaluating performance of most common symmetric encryption of various algorithms on power consumption for wireless devices which are limited in resources such as less memory, less processing power and limited power supply (battery). Battery power is subjected to the problem of energy consumption due to encryption algorithms. Battery technology is increasing at a slower rate than other technologies. This causes a "battery gap" [9], [10]. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types(text, images, and audio file, different cases of transmission of the data has been studied, and Effect of varying signal to noise ratio .finally, encryption/decryption speed.

The major contributions of this work are energy-security trades off then, some suggestions for design of secure communications systems to handle the varying wireless environment have been provided to reduce the energy consumption of security protocols.

This study evaluates six different encryption algorithms used or suggested for wireless local area network (WLANs) namely; AES, DES, 3DES, RC6, Blowfish, and RC2.

This paper is organized as follows. A wireless network overview is explained in section 2.Related work is described in Section 3. A view of simulation and experimental design is given in section 4. Simulation results are shown in section 5. Finally the conclusions are drawn section 6.

II. OverView of Wireless Networks

Wireless networks have spread between home users and companies in an increasing fashion. The main reason behind this fast adaptation is due to the nature of wireless networks where it provides the flexibility and freedom that wired networks lack. With wireless networks, radio frequency (RF) and light signals have the job of carrying information invisibly through the air. the main standard in the wireless world are :802.11 which describes the Wireless LAN architecture, and 802.16 which describes the Wireless MAN architecture.

A. *Wireless LANs*

Wireless LANs supply high performance within and around office buildings, factories, and homes. Wireless LANs consist mainly of two entities: clients or end-user devices and Access Points. The basic structure of a Wireless LAN is called infrastructure WLAN or BSS (Basic Service Set), in which the network consists of an access point and several wireless devices [11]. If the BSS did not have an access point device, and the wireless devices were communicating with each other directly, this BSS is called an Independent BSS and works in mode called "ad hoc mode" [12].

a . Security in WLANs (IEEE 802.11 Standards)

The IEEE 802.11 standard specifies a common medium access control (MAC) and several physical layers for wireless LANs.

To allow clients to access the network they must be go through two steps: getting authenticated by the access point, then getting associated. There are two types of authentications used in IEEE 802.11 standard: Shared Key Authentication and Open System Authentication [13],[14].

b. Data Encryption and Authentication Protocol

The first data encryption and authentication protocol used in WLANs was called Wired Equivalent Privacy (WEP). WEP doesn't provide enough security for most enterprise wireless LAN applications. Because of static key usage, it's fairly easy to crack WEP with off-the-shelf tools [15-16]. Wireless Fidelity (Wi-Fi) alliance, released a new Security protocol standard in 2002, and called Wi-Fi Protected Access (WPA), which aims to fix the flaws [17]. A year later, another version of the WPA standard, WPA version 2 (WPA2) [17], was released to provide advanced security services [19]. The 802.11i standard provides two data encryption services called Temporal Key Integrity Protocol (TKIP) and Counter Mode (CTR) Encryption with AES Cipher (CTR-AES), and two data authentication services called Michael and Cipher Block Chaining Message Authentication Code (CBC-MAC). The WPA standard is composed of the use of TKIP and Michael together to provide data encryption and authentication services while WPA2 is composed of CTR-AES and CBC-MAC. Together with CBC-MAC and CTR-AES, it is called CCMP (Counter Mode CBC-MAC Protocol). 802.11i specifies three protocols: TKIP, CCMP and WRAP. TKIP (Temporal Key Integrity Management) was introduced as a "band-aid" solution to WEP problems. One of the major advantages of implementing TKIP is that you do not need to update the hardware of the devices to run it. Unlike WEP, TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism. TKIP ensures that every data packet is sent with its own unique encryption key. TKIP is included in 802.11i mainly for backward compatibility. WRAP (Wireless Robust Authenticated Protocol) is the LAN implementation of the AES encryption standard introduced earlier. It was ported to wireless to get the benefits of AES encryption. WRAP has academic property issues [20]. CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol) is considered the optimal solution for secure data transfer under 802.11i. CCMP uses AES for encryption. The use of AES will require a hardware upgrade to support the new encryption algorithm. HiperLAN/2 is a European-based standard that is unlikely to compete heavily with 802.11. Table.1 summarizes the WLAN security protocol standards.

TABLE I: WLAN SECURITY PROTOCOL STANDARD

Mode	Service	IEEE 802.11	WPA	WPA2
Enterprise	Authentication	WEP	IEEE 802.1x	IEEE 802.1x
	Encryption	WEP	TKIP/Michael	AES-CCMP
Personal	Authentication	WEP	PSK	PSK
	Encryption	WEP	TKIP/Michael	AES-CCMP

III. RELATED WORK

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources.

It was shown in [1] that energy consumption of different common symmetric key encryptions on handheld devices. It is found that after only 600 encryptions of a 5 MB file using Triple-DES the remaining battery power is 45% and subsequent encryptions are not possible as the battery dies rapidly.

It was concluded in [20] that AES is faster and more efficient than other encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes. Increasing the key size by 64 bits of AES leads to increase in energy consumption about 8% without any data transfer. The difference is not noticeable.

A study in [22] is conducted for different secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data.

In [23] a study of security measure level has been proposed for a web programming language to analyze four Web browsers. This study consider of measuring the performances of encryption process at the programming language's script with the Web browsers. This is followed by conducting tests simulation in order to obtain the best encryption algorithm versus Web browser.

A study in [24] is conducted for different popular secret key algorithms such as RC4, AES, and XOR. They were implemented, and their performance was compared by encrypting for real time video streaming of varying contents. The results showed; encryption delay overhead using AES is less than the overhead using RC4 and XOR algorithm. Therefore, AES is a feasible solution to secure real time video transmissions.

IV. Experimental Design

For our experiment, we use a laptop IV 2.4 GHz CPU, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 321 Kilobytes to 7.139MegaBytes for text data, from 33 Kbytes to 8,262 Kbytes for audio data , and from 28 Kbytes to 131 Kbytes for pictures(Images) .For our experiment , we studying the effects of cryptographic algorithms on power consumption for wireless devices in case of data transmission and with out data transmission.

In first step

Firstly; studying the effects of changing packet size ,(CPU work load, throughput ,power consumption in micro Joule/Byte and power consumption by calculating difference in battery percentage were calculated)in case of encryption and decryption processes to calculate the performance of each encryption algorithms.

Secondly;; in case of changing data types such as audio, video , and image ,(CPU work load, throughput ,power consumption in μJoule/Byte and power consumption by calculating difference in battery percentage were calculated)in case of encryption and decryption processes to calculate the performance of each encryption algorithms.

These results lead to second step (calculating with data transmission)

In second step, a comparison is conducted between the results in case of data transmission using BBS and ah hoc wireless network. The main difference between BBS mode and Ad-hoc mode

Firstly, in case of Ad-hoc structure with excellent signals (distance between two laptops less than 4 meters and there are any application running except data transmission) and poor signals (distance between two laptops is greater than 50 meters contains walls in the distance between two laptops).

In case excellent signals, comparison is conducted using two different types of authentication (Open Key Authentication (no encryption), and Shared Key Authentication (WEP)).for each type of authentication, we calculated the transmission time, and power consumption for encryption for different packet size and different data types. So that, we can calculate the performance for each cryptographic algorithms in case of data transmission and with out data transmission for two different type of authentication in Ad-hoc structure using excellent signals between sender and receiver.

In case poor signals, comparison is conducted using (WEP). We calculated the transmission time, and power consumption for encryption for different packet size and different data types. So that, we can calculate the performance for each cryptographic algorithms in case of data transmission and with out data transmission in Ad-hoc structure using poor signals between source and destination.

Secondly, in case of BBS mode, comparison is conducted with excellent signal between sender and receiver the studying the effects of transmitted data using IEEE 802.11i (Open Key Authentication (no encryption), and WPA/TKIP) by calculating transmission time and power consumed for transmission between the two entities for different packet size and different data types.

Several performance metrics are collected:

1- *Encryption time and throughput.*
2- *Power consumption (Micro joule/bytes)*
3- *Power consumption (Percent of battery consumed)*

The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time which can consider as a good indicator for power consumption [25].

The first method used to measure energy consumption is to assume that an average amount of energy is consumed by normal operations and to test the extra energy consumed by an encryption algorithms. This method simply monitors the level of the percentage of remaining battery. The experiments note the number of iteration or runs over the file and the battery life. Change in battery life divided by the number of runs gives the battery life consumed in percentage for one run. The second method for computation of the energy cost of encryption, we use the same techniques as described in [26]. We present a basic cost of encryption represented by the product of the total number of clock cycles taken by the encryption and the average current drawn by each CPU clock cycle. The basic encryption cost is in unit of ampere-cycle. To calculate the total energy cost, we divide the ampere-cycles by the clock frequency in cycles/second of a processor; we obtain the energy cost of encryption in ampere-seconds. Then, we multiply the ampere-seconds with the processor's operating voltage, and we obtain the energy cost in Joule. By using the cycles, the operating voltage of the CPU, and the average current drawn for each cycle, we can calculate the energy consumption of cryptographic functions. For example, in average, each cycle consumes approximately 270 mA on an Intel 486DX2 processor or 180 mA on Intel Strong ARM [27]. Since for a given hardware Vcc are fixed.

V. Simulation Results

A. The effect of changing packet size for cryptography algorithm on power consumption (text files)

a. Encryption of different packet size

1. Encryption throughput

Experimental results for this compassion point are shown Fig. 1

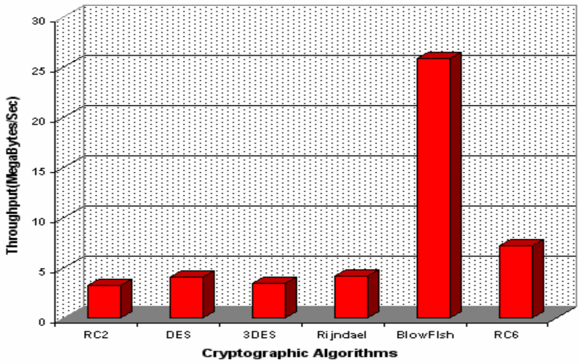

Fig. 1 Throughput of each encryption algorithm to encrypt different text data (Megabytes/Second)

2. Power consumption (Micro joule/Byte)

Experimental results for this compassion point are shown Fig. 2

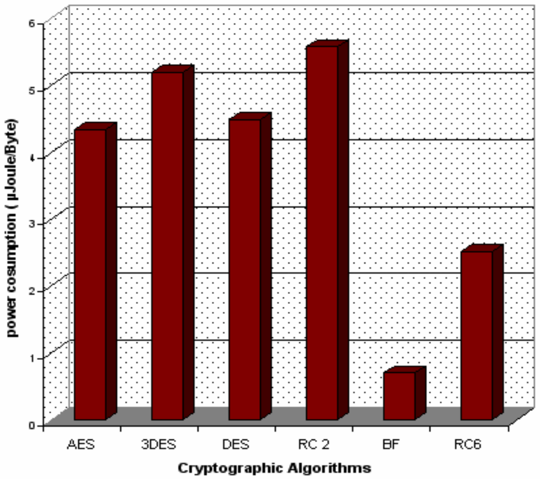

Fig. 2 Power consumption for encrypt different Text document Files

3. Power consumption (Percentage of battery consumed)

Experimental results for this compassion point are shown Fig. 3

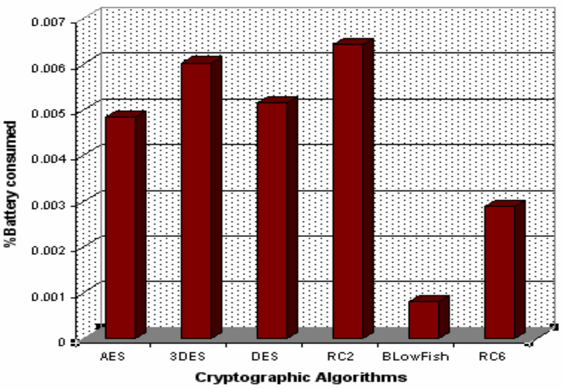

Fig. 3 Power consumption for encrypt different Text document Files with out data transmission

b. Decryption of different packet size

1. Decryption throughput

We calculated the Throughput of each encryption algorithm to decrypt different text data (Megabytes/Second) with out data transmission. Experiment results for this compassion point are shown Fig 4.

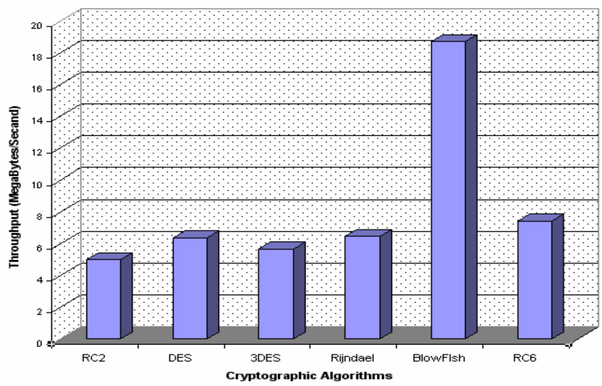

Fig .4 Throughput of each decryption algorithm (Megabyte/Second) for text data with out data transmission

2. Power consumption (Micro Joule/Byte)

We calculated Power consumption (µJoule/Byte) for decrypt different Text document Files with out data transmission. Experiment results for this compassion point are shown Fig.5.

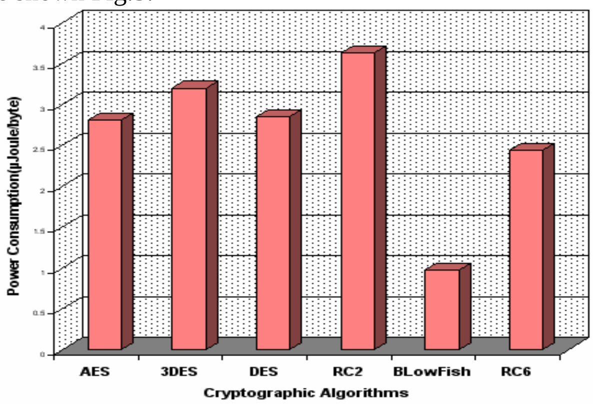

Fig. 5 Power consumption for Decrypt different Text document Files (Micro Joule/Byte) with out data transmission

c. Wireless Environment

we calculated the effect of changes when transmission of data is taken in consideration under different scenario such as transmission of data by using two different architectures (BBS, and ad hoc mode).also we studied the effect of noise ratio on signals (using excellent signals and poor signals).in case of using IEEE 802.11 standard (ad hoc architecture) , we calculated the duration time for transmission using the two different types of authentication (open system authentication (no encryption) , and shared key authentication(WEP)) .in case of IEEE 802.11i (BBS architecture) , we calculated we calculated the duration time for transmission using WPA protocol(TKIP encryption).also in BBS architecture, we calculated the duration time for transmission with out using any encryption techniques.

The results as shown in table.2 and Fig. 6

Text Data					
Data to be transmitted	ad hoc mod(802.11standard)			BBS mod	
	Excellent signals		Poor	Excellent signals	
	WLANs Security Protocol				
	No Encryption(Open System Authentication)	WEP(Shared Key Authentication)	Noise(Poor Signals)	IEEE 802.11i (WPA(TKIP))	No Encryption(Open System Authentication)
	Duration Time in Seconds				
No encryption	10.57	10.76	17.35	17.71	16.1
AES	18.5	18.94	45.93	29.28	25.94
DES	12.55	14.38	21.17	20.72	21.07
RC2	18.38	18.82	61.31	29.29	31.92
3DES	17.75	18.05	30.87	27.47	32.45
BF	10.68	10.93	17.49	19.98	13.93
RC6	10.84	11.13	18.26	20	15.09

Table 2 Comparative execution times for transmission of text data using different encryption algorithms

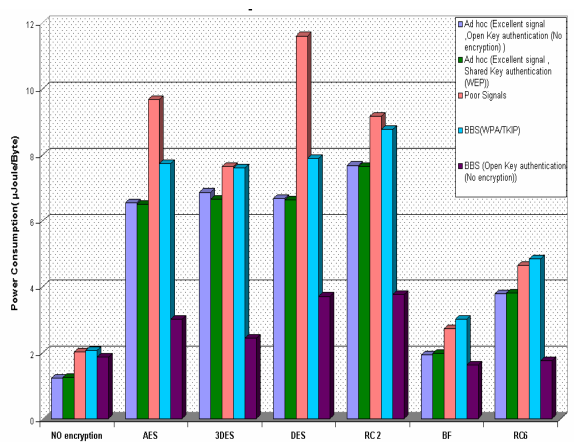

Fig. 6 Power consumption for Encrypt different Text document Files (Micro Joule/Byte) with data transmission

In case of encryption time without transmission, the results show the superiority of Blowfish, and RC6 algorithms over other algorithms in terms of the processing time, throughput and power consumption. When we encrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 16% of the power which is consumed for AES. When we encrypt the same data by using RC6 and AES, we found that RC6 requires approximately 58% of the power which is consumed for AES. Anther point can be noticed here; that AES has an advantage over other 3DES, DES and RC2 in terms of time consumption, throughput, and power consumption. A third point can be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics. A fourth point can be noticed here; that RC2 has low performance and low throughput when compared with other five algorithms in spite of the small key size used. In case of data transmission, we found, there is insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). Even under the scenario of data transfer by using the two architectures -BBS architectures and ad hoc architectures - it would be advisable to use Blowfish and RC6.in case of ad hoc architecture (8.2.11 standard using open system authentication and shared key authentication with excellent signals), when we transmit the encrypted data by using Blow fish, RC6, and AES, we found that RC6 and Blow fish require approximately 56% of the time consumption which is consumed for AES. In case of BBS architecture (802.11i using WPA/TKIP with excellent signals) when we transmit the encrypted data by using Blow fish, RC6, and AES, we found that RC6 and Blow fish require approximately 68% of the time consumption which is consumed for AES. In case of ad hoc mode (poor signal) , we found transmission time increased approximately to double of open shared authentication in ad hoc mod using excellent signals.

B. The effect of changing data type (Images) for cryptography algorithm on power consumption.

a. Encryption of different packet size

In the previous section, the comparison between encryption algorithms has been conducted on text and document data files. We found that Blowfish and RC6 has a performance greater than other the other five types' .Now we will make a comparison between other types of data (Images) to check which one can perform better in this case. Experimental results for image data type (JPEG images) are shown Fig. 7,and Fig 8 respectively.

1.Encryption throughput

Experimental results for this compassion point are shown Fig.7.

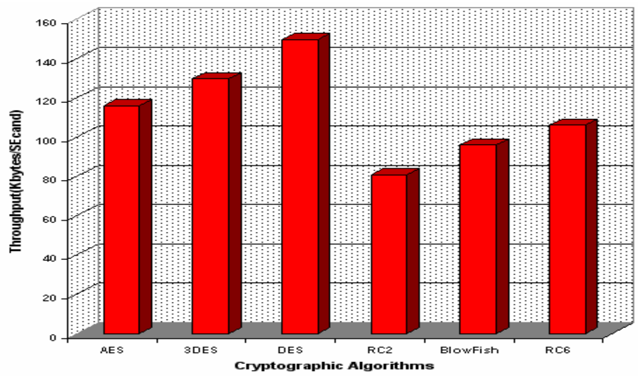

Fig.7 Throughput of each encryption algorithm (Kilobytes/Second)

2.Power consumption

Experimental results for this compassion point are shown Fig. 8

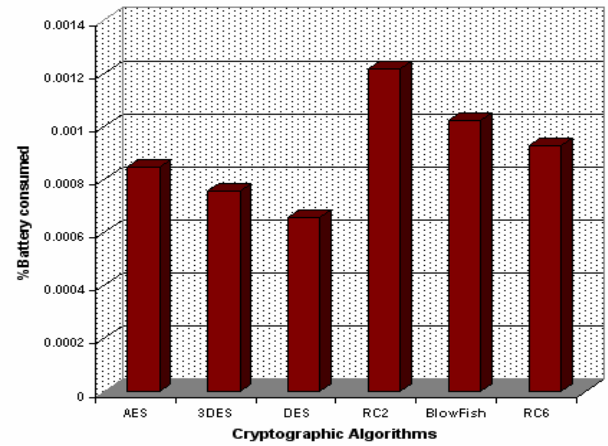

Fig. 8 Power consumption for encrypt different Images Files

b. Decryption of different Images files (different sizes)

1. CPU work load

Experiment results for this compassion point are shown Fig.9 to decrypt different text data with a different data block size with out data transmission.

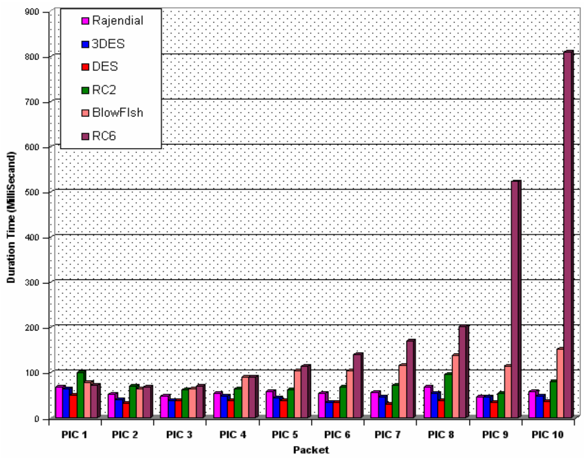

Fig. 9 Time consumption for decrypt different images (Millisecond)

c. Wireless Environment

As we performed in text files we done in Images file. We consider the effect of changes on results when transmission of data is taken in consideration .The results as shown in fig 10

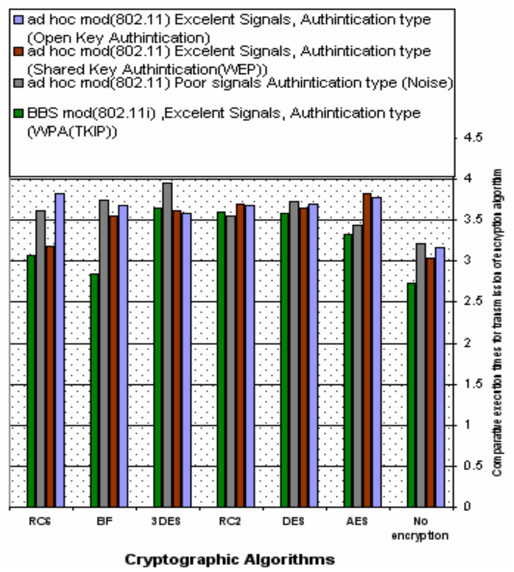

Fig. 10 Comparative execution times for transmission of Image files using different algorithms

From those results, it is easy to observe that RC2 still has disadvantage in encryption process over other algorithms in terms of time consumption and serially in throughput and power consumption. On the other hand, it is easy to observe that RC6 and Blowfish have disadvantage in encryption process over other algorithms in terms of time consumption and serially in throughput and power consumption. We find that 3DES still has low performance when compared to DES. When the transmission of data is considered, we found there is insignificant difference in performance of different symmetric key schemes. In case of data transmission, we found, there is insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation).

C. The effect of changing data type (Audio files) for cryptography algorithm on power consumption.

a. Encryption of different Audio files (different sizes)

1. Encryption throughput

Now we will make a comparison between other types of data (Audio file) to check which one can perform better in this case. Simulation results for audio data type are shown Fig.11 at encryption.

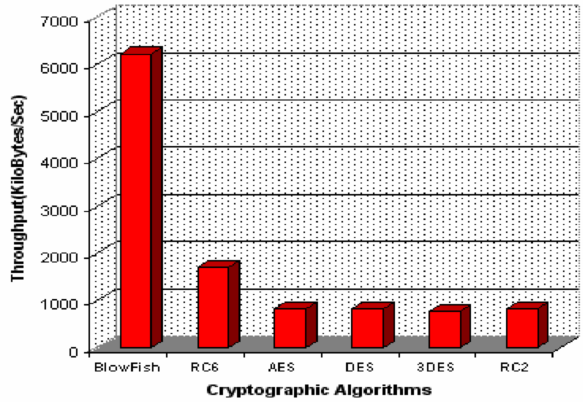

Fig. 11 Throughput of each encryption algorithm to encrypt different Audio files (Kilobytes/Sec)

2. Power consumption (Micro Joule/Byte)

Experimental results for this compassion point are shown Fig. 12

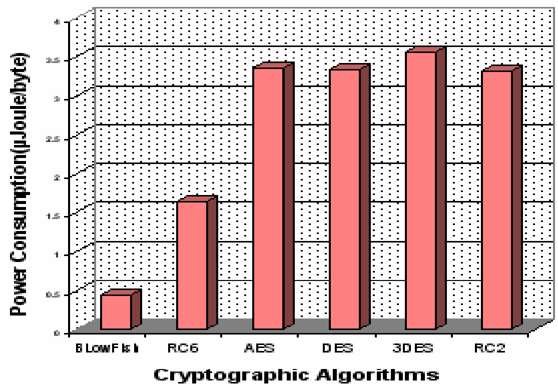

Fig. 12 Power consumption for encrypt different Audio Files (micro joule/byte)

3. Power consumption (percent of battery consumed)

In Figure 13, we show the performance of cryptography algorithms in terms of power consumption. With a different audio block size

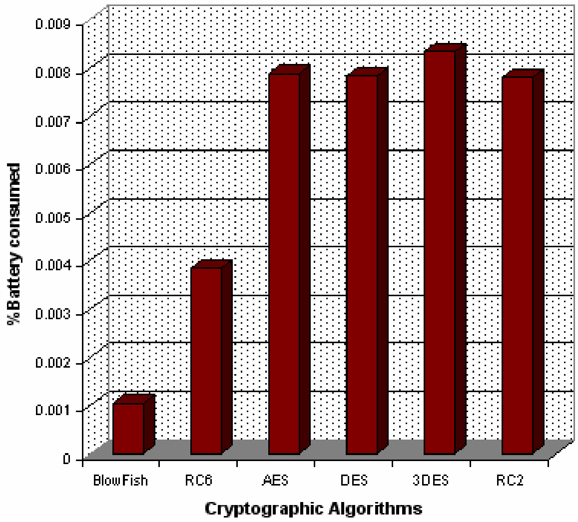

Fig. 13 Power consumption for encrypt different Images Files

b. Decryption of different Audio files (different sizes)

1. Decryption throughput

Experimental results for this compassion point are shown Fig.14

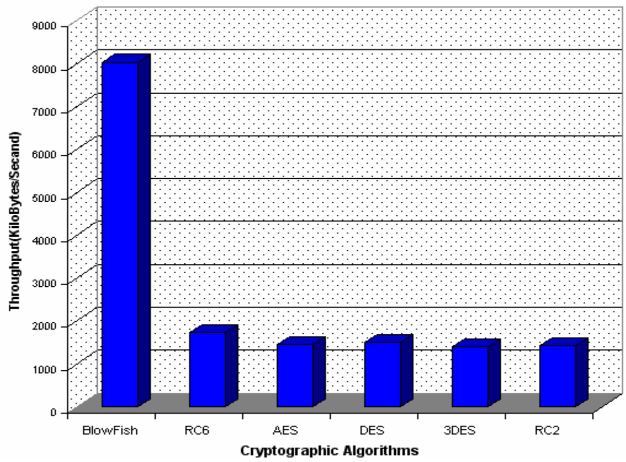

Fig. 14 Throughput of each Decryption algorithm (Kilobytes/Second)

2. Power consumption for decryption

Experimental results for this compassion point are shown Fig. 15.

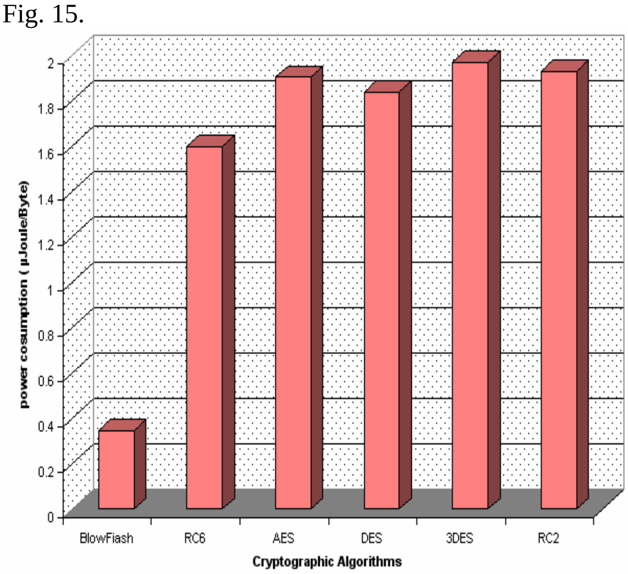

Fig. 15 Power consumption for decrypts different Audio Files (Micro Joule/Byte)

c. Wireless Environment

As we perform in text files , we did in Audio files. We consider the effect of change when transmitted of data is taken in consideration under different scenario the results as shown in table 3 and in Fig16

Audio files					
Data to be transmitted	ad hoc mode(802.11 standard)			BBS mode	
	Excellent signals		Poor	Excellent signals	
	WLANs Security Protocol				
	No Encryption(Open System Authentication)	WEP(Shared Key Authentication)	Noise(Poor Signals)	IEEE 802.11i (WPA(TKIP))	No Encryption(Open System Authentication)
	Duration Time in Second				
No encryption	27.67	28.22	51.14	48.12	43.24
AES	53.82	55.37	93.45	93.59	77.39
DES	54.53	56.48	94.83	99.87	69.97
RC2	57.2	55.84	96.79	92.4	64.52
3DES	53.85	56.93	95.66	95.02	78.25
BF	28.73	29.36	48.11	49.56	34.22
RC6	28.74	28.82	50.26	48.71	36.65

Table 3.Comparative execution times for transmission of audio data using different encryption algorithms

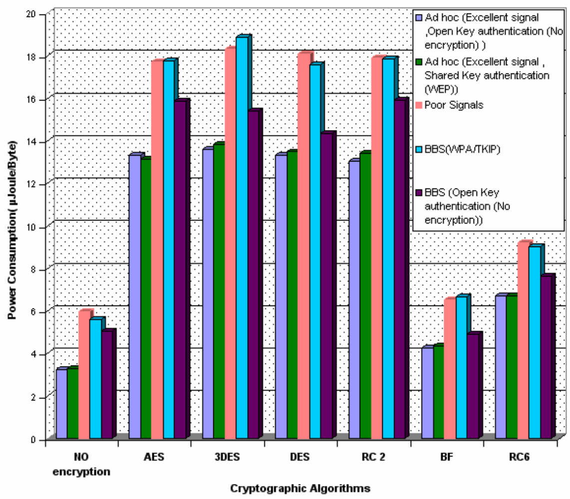

Fig. 16 Power consumption for Encrypt different Audio files (Micro Joule/Byte) with data transmission

From the results we found that the result is the same as in encryption process for audio files. When we decrypt the same data by using Blowfish &AES, we found that Blowfish requires approximately 18% of the power which is consumed for AES. When we decrypt the same data by using RC6 &AES, we found that RC6 requires approximately 84% of the power which is consumed for AES .In case of data transmission, we found, there is insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). Even under the scenario of data transfer by using the two architectures -BBS architectures and ad hoc architectures - it would be advisable to use Blowfish and RC6.in case of ad hoc architecture (8.2.11 standard using open system authentication and shared key authentication with excellent signals), when we transmit the encrypted data by using Blow fish, RC6, and AES, we found that RC6 and Blow fish require approximately 51% of the time consumption which is consumed for AES. In case of BBS architecture (802.11i using WPA/TKIP with excellent signals) when we transmit the encrypted data by using Blow fish , RC6, and AES, we found that RC6 and Blow fish require approximately 52% of the time consumption which is consumed for AES. In case of ad hoc mode (poor signal) , we found transmission time increased approximately by 74% over open shared authentication in ad hoc mod using excellent signals.

VI. Conclusions

This paper presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. The selected algorithms are AES, DES, and 3DES, RC6, Blowfish and RC2. Several points can be concluded from the simulation results. First; in the case of changing packet size with and with out transmission of data using different architectures and different WLANs protocols, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Second; 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, we find that 3DES still has low performance compared to algorithm DES. Third point; 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 we found transmission time increased minimum by 70 % over open sheered authentication in ad hoc mod. Finally -in the case of changing key size – it can be seen that higher key size leads to clear change in the battery and time consumption.

For our future work, we will suggest three approaches to reduce the energy consumption of security protocols: replacement of standard security protocol primitives that consume high energy while maintaining the same security level, modification of standard security protocols appropriately, and a totally new design of security protocol where energy efficiency is the main focus.

References

[1] P. Ruangchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs-N,'' The Third IEEE Workshop on Wireless LANs - September 27-28, 2001- Newton, Massachusetts.

[2] Hardjono, "Security in Wireless LANS and MANS," Artech House Publishers 2005.

[3] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005, PP. 58-309.

[4] D. Coppersmith, "The Data Encryption Standard (DES) and Its Strength against Attacks." IBM Journal of Research and Development, May 1994, pp. 243 -250.

[5] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."D r. Dobb's Journal, March 2001, PP. 137-139.

[6] K. Naik, D. S.L. Wei, Software Implementation Strategies for Power-Conscious Systems," Mobile Networks and Applications - 6, 291-305, 2001.

[7] Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008,http://www.schneier.com/blowfish.html

[8] N.El-Fishawy," Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, Nov. 2007, PP.241–251.

[9] K. McKay, "Trade-offs Between Energy and Security in Wireless Networks Thesis," Worcester Polytechnic Institute, April 2005.

[10] R. Chandramouli, "Battery power-aware encryption - ACM Transactions on Information and System Security (TISSEC)," Volume 9, Issue 2, May. 2006.

[11] " Wireless Networks First-Step".

[12] W. Kaerygiannis , "Wireless Network Security 802.11, Bluetooth and handheld devices", NIST.

[13] "Wireless Security Handbook," Auer Bach Publications 2005

[14] " Shared vs. Open authentication method",Retrieved October 25, 2008, http://www.startawisp.com/index2.php?option=com_content&do_pdf=1&id=147

[15] J. Walker, "Unsafe at any key size: an analysis of the WEP encapsulation," Tech. Rep. 03628E, IEEE 802.11 committee, March 2000.Retrieved October 25,2008, http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zi%p.

[16] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[17] "Wi-Fi protected access," Wireless Fidelity (Wi-Fi), http://www.weca.net.

[18] "Wi-Fi Protected Access - Wikipedia," Retrieved October 25, 2008, http://en.wikipedia.org/wiki/WiFi_Protected_Access.

[19] Wireless LAN Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security, April 2004, IEEE Standard 802.11i.

[20] "802.11: the security differences between b and i," "Potentials, IEEE Volume 22, Issue 4, Oct-Nov 2003, pp 23-27

[21] S.Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," university of Pittsburgh, April 9, 2003. Retrieved October 1, 2008, At: portal.acm.org/citation.cfm?id=383768

[22] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP. 84- 89.

[23] S.Z.S. Idrus, S.A.Aljunid, S.M.Asi, "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008, PP 20-25.

[24] W.S.Elkilani, H.m.Abdul-Kader, "Performance of Encryption Techniques for Real Time Video Streaming, IBIMA Conference, Jan 2009, PP 1846-1850

[25] A.A. Tamimi, "Performance Analysis of Data Encryption Algorithms. Retrieved October 1, 2008 From http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.html

[26] K. Naik, D. S.L. Wei, "Software Implementation Strategies for Power-Conscious Systems," Mobile Networks and Applications, 6, 291-305, 2001.

[27] A. Sinha and A.P. Chandrakasan, "Joule Track A Web Based Tool for Software Energy Profiling," Proceedings of the 38th Design Automation Conference, DAC 2001, Las Vegas, NV, USA, pp. 220-225.

Diaa Salama Abdul. Elminaam was born on November 23, 1982 in Kafr Sakr, Sharkia, Egypt. He received the B.S from Faculty of Computers &Informatics, Zagazig Univeristy, Egypt in 2004 with grade very good with honor. He is working in Higher Technological Institute, 10th of Ramadan city as Demonstrator at Faculty of Computer and informatics. He majors in Cryptography and Network Security.(e-mail: ds_desert@yahoo.com;mobile:+20166104747)

Dr. H. M. Abdul-kader obtained his B.S. and M.SC. (by research) both in Electrical Engineering from the Alexandria University , Faculty of Engineering , Egypt in 1990 and 1995 respectively. He obtained his Ph.D. degree in Electrical Engineering also from Alexandria University, Faculty of Engineering, Egypt in 2001 specializing in neural networks and applications. He is currently a Lecturer in Information systems department, Faculty of Computers and Information, Menoufya University, Egypt since 2004. He has worked on a number of research topics and consulted for a number of organizations. He has contributed more than 30+ technical papers in the areas of Neural networks, Database applications , Information security and Internet applications .

Prof. Mohiy Mohamed Hadhoud, Dean, Faculty of Computers and Information, head of Information Technology Department, Menoufia University, Shebin Elkom, Egypt. He is a member of National Computers and Informatics Sector Planning committee, University training supervisor. He graduated, from the department of Electronics and Computer Science, Southampton University, UK, 1987. Since 2001 till now he is working as a Professor of Multimedia, Signals and image processing and Head of the department of Information Technology (IT), He was nominated by the university council for the national supremacy award, years 2003, and 2004. He is the recipient of the university supremacy award for the year 2007. He, among others are the recipient of the Most cited paper award form the Digital signal processing journal, Vol. 18, No. 4, July 2008, pp 677-678. ELSEVIER Publisher. Prof. Hadhoud has published more than 110 papers in international journals, international conferences, local journals and local conferences. His fields of Interest: Digital Signal Processing, 2-D Adaptive filtering, Digital Image Processing, Digital communications, Multimedia applications, and Information security and data hiding.