Studying the Effects of Most Common Encryption Algorithms

Diaa Salama[1], Hatem Abdual Kader[2], and Mohiy Hadhoud[2]
[1]Jazan University, Kingdom of Saudi Arabia
[2,3]Minufiya University, Egypt

Abstract: *Wireless networks play critical roles in present work, home, and public places, so the needs of protecting of such networks are increased. Encryption algorithms play vital roles in information systems security. Those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. CPU and memory usability are increasing with a suitable rates, but battery technology is increasing at slower rate. The problem of the slower increasing battery technology forms "battery gap". The design of efficient secure protocols for wireless devices from the view of battery consumption needs to understand how encryption techniques affect the consumption of battery power with and without data transmission. This paper studies the effects of six of the most common symmetric encryption algorithms on power consumption for wireless devices. at different settings for each algorithm. These setting include different sizes of data blocks, different data types (text, images, and audio file), battery power consumption, different key size, different cases of transmission of the data , effect of varying signal to noise ratio and finally encryption/decryption speed. The experimental results show the superiority of two encryption algorithm over other algorithms in terms of the power consumption, processing time, and throughput .These results can aid in new design of security protocol where energy efficiency is the main focus. 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.*

Keywords: *Encryption techniques, Computer security, wireless network, ad hoc wireless LANs, Basic Service Set (BSS)*

Received November 25, 2009; Accepted February 17, 2010

1. Introduction

In past few years, wireless communications has been fast increasing with many devices like laptops, PDAs, and Pocket PCs. Individuals are using wireless technology for private communications, for mobile, and/or E-commerce, emails and business interactions.

Wireless networking resources have been started as initiatives towards a network of a future world without wires.. Studies indicate that the growth of wireless networks is being restricted by their perceived insecurity [2]. The increasing of wireless systems provides malicious entities greater incentives to step up their efforts to gain unauthorized access to the information being exchanged over the wireless link. Security is important for wireless networks, mainly because the communications signals are openly available as they propagate through the air. Companies and individuals using wireless networks must be aware of the possible issues and applicable countermeasures. The amount of security required by the system may depend on the organization using the wireless network. A financial company would require very strong security techniques to prevent unauthorized users and maintain information confidentiality. The hot-spots networks may require that only legitimate users access the network and may not require confidentiality and data integrity.

The protocols for wireless LAN security are developing to meet the needs of serious users. Until the systems provide verifiable security related to wireless network access would be based on a more careful approach. Due to the time gap between wired and wireless systems and due to wired connectivity, wired systems are inherently more secure than the wireless systems [3]. The eavesdropper is more difficult in a wired LAN and needs to be connected to the LAN. The physical connectivity could come through a current employee, a dial up connection or through the wiring closet of the premise. On the other hand, in the wireless connections, the vulnerabilities to eavesdropping is highly increased. The wireless interface can be easily configured to listen to packets being transmitted in a promiscuous mode. Wireless systems are thus prone to the vulnerabilities of the wired systems along with increased chances of security failure. (WEP) can be hacked in a matter of hours [4], [5].

Security protocols implement mechanisms through which security services can be provided. Security can be implemented at the transmission level through the means of frequency hopping and spread spectrum technologies. Such schemes would prove to be very

expensive for the users and the companies employing such schemes [6].

For cost and simplicity, the method that seems to be gaining acceptance is data encryption. The IEEE 802.11 standard uses the WEP protocol for security. This protocol has been designed for wired systems. In wireless systems, a security protocol should also consider the limited battery power, small memory and limited processing capabilities of the devices and the available bandwidth. In addition, the systems need to be able to supply to the requirements of the wide variety of wireless devices that could be used for connectivity.

The study of the energy consumption of the encryption schemes in wireless devices is essential in design of energy efficient security protocols customized to the wireless environment. A key limitation in wireless devices is the battery capacity, while memory and processor technologies double with the introduction of every new semiconductor generation (roughly every 18 months) [7]; battery technology is increasing at the much slower rate of 5%-10% per year. This is causing a gap to form between the power required and the battery available (Figure 1) [7].

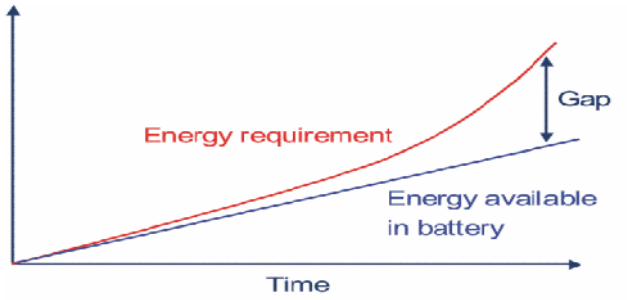

Figure 1. The growing gap between battery technology and power requirements

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 [8-10] while AES uses various (128,192,256) bits keys [11,12]. Blowfish uses various (32-448); default 128bits [13] while RC6 is used various (128,192,256) bits keys [14]. The performance measure of encryption schemes will be conducted in terms of energy for wireless devices, changing data types -such as text or document, Audio files, Video files and images- on power consumption, changing packet size and changing key size for the selected cryptographic algorithms on wireless devices.

The threats of wireless networks are also growing. Due to the discovery of vulnerabilities of WLANs in 2001, many business and governments have temporarily stopped to adopt WLANs in their networks because they increase threats to their businesses [17]. The threats in wireless networks have also been identified as major threats to information security [18, 19].

This paper examines a method for evaluating performance of selected symmetric encryption of various algorithms on power consumption for wireless devices. A wireless device is 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" [15, 16, 20 - 22].We need a way to make decisions about energy consumption and security to reduce the consumption of battery powered devices. 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. Related work is described in Section 2. The proposed experimental design is described in section 3. Experimental results are shown in section 5. Finally the conclusions are drawn section 6.

2. 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 [8] 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 [23] 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 [24] 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 [25] 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.

3. Experimental Design

The setup for the proposed experiment is shown in Figure 2.Two laptops are used in the experiment. The two laptops (sender and receiver) had windows XP professional installed on it. The first laptop (sender) is connected to access point.

Figure 2. Configuration of the Experiment setup.

In the experiments, the first laptop encrypts a different file size for different data types ranges from 321 Kilobytes to 7.139Megabytes for text data (.DOC files), from 33 Kbytes to 8,262 Kbytes for audio data (.WAV files), from 28 Kbytes to 131 Kbytes for pictures and Images (.GIF and GPG files) using .NET environment. Six encryption algorithm that are selected in the experiment are AES (key size:256 bits),DES(key size:64 bits),RC2(key size:64 bits),RC6(key size:256 bits),Blowfish(key size:256 bits),and 3DES(key size:192 bits) . These implementations are thoroughly tested and are optimized to give the maximum performance for each algorithm. The results are checked and tested for AES that supposed to be the best encryption algorithms by a different implementations program to give the maximum performance for the algorithms and make sure the results are the same using multiple platforms. Then for transmission of data, the two laptops are connected wirelessly. Data is transmitted from the first laptop to the second one through the wireless link using TCP/IP protocol. the experiment are applied in two mode of wireless LANs connection (BSS and ad hoc mode).Using IEEE 802.11 standard, data is transmitted using the two different types of authentication. First, data is transmitted using Open System Authentication (no encryption). Second case, data is transmitted using Shared Key Authentication (WEP encryption). Using IEEE 802.11i, data is transmitted using Open System Authentication (no encryption) and data is transmitted using WPA. The effects of different signal to noise conditions and its effect on transmission of data (under excellent signals and poor signals) are studied.

Several performance metrics are measured:

- Encryption time.
- Throughput.
- Battery power.
- Transmission time in many cases.

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 in equation (1).

$$\text{Throughput of encryption} = \frac{Tp(Bytes)}{Et(Second)} \quad (1)$$

where

Tp: total plain text (bytes)
Et: encryption time (second)

The CPU process time is the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU.

The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while operating on encryption operations. Each cycle of CPU will consume a small amount of energy.

The road map for experiment steps are explained in sections 3.1., 3.2. and 3.3.

3.1. Results Comparison

A comparison is conducted between the results of selected different encryption algorithms using different setting such as different data types, different packet size, different key size.

- In case of changing packet size, (throughput, power consumption in µJoule/Byte and power consumption by calculating difference in battery percentage were calculated) in case of encryption processes to calculate the performance of each encryption algorithms.
- In case of changing data types such as audio, ,(throughput ,power consumption in µJoule/Byte and power consumption by calculating difference in battery percentage were calculated)in case of encryption processes to calculate the performance of each encryption algorithms.

These results lead to second step in section 3.2.

3.2. Calculating With Data Transmission

A comparison is conducted between the results in case of data transmission using BSS and ah hoc wireless network. The main difference between BSS mode and Ad-hoc mode that Ad-hoc mode hasn't access point between sender and receiver

3.2.1 Ad-Hoc Structure

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, the transmission time, and power consumption for encryption are calculated for different packet size and different data types. So that, 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 can be calculated.
- In case poor signals, comparison is conducted using (WEP) .The transmission time and power consumption of encryption are calculated for different packet size and different data types. So that, 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 can be calculated.

3.2.2. BSS mode

In case of BSS 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.

The battery and computational trade-off of encryption schemes under different scenarios are considered in various experimental setups but the original setup remains the same.

Processing in experiment for encryption without data transmission is to read data from the file encrypt the data and put it in another file. In case of encryption with data transmission the data is read from the file encrypted and the send to the second laptop. This is done till the battery drains to 30% of the lifetime left. We stop at 30% because after that the systems alarm and data recovery mechanisms become active and the performance of the schemes change. After a few runs of processing on the file the battery life left and the system time is recorded. The average battery life consumed per run and the time taken to do so is the calculated for the results. It is expected that the computation time would be closely related to the battery requirements; however, since the CPU utilization of power depends on parameters like voltage supply and capacitive load. The capacitive load on the CPU depends on the switching demand, which again depends on the instructions being executed. Hence, measurements for both the parameters are considered.

3.3. Measurement of Energy Consumption

Energy consumption for encryption and decryption can be measured in many ways. These methods as follows:

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 that can computed by equations (2), (3)

The battery life consumed in percentage for one run =

$$\frac{\text{Change in battery life}}{\text{the number of runs}} \quad (2)$$

Average battery Consumed per iteration=

$$\frac{\sum_{1}^{N} BatteryConsumedPerIteration}{N} \quad (3)$$

The second method of security primitives can also be measured by counting the amount of computing cycles which are used in computations related to cryptographic operations. For computation of the energy cost of encryption, we use the same techniques as described in [20], [22] using the following equations.

$$B_{cost\_encryption}\ (\text{ampere-cycle}) = \tau * I \quad (4)$$

$$T_{energy\_cost}\ (\text{ampere-seconds}) = \frac{B_{cost\_encryption}(\text{ampere-cycle})}{F(\text{cycles/sec})} \quad (5)$$

$$E_{cost}\ (\text{Joule}) = T_{energy\_cost}\ (\text{ampere-seconds}) * V \quad (6)$$

Where

Bcost_encryption: a basic cost of encryption (ampere-cycle).

τ: the total number of clock cycles.

I: the average current drawn by each CPU clock cycle.

Tenergy_cost: the total energy cost (ampere-seconds).
F: clock frequency (cycles/sec).
Ecost (Joule): the energy cost (consumed).

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, on average, each cycle consumes approximately 270 mA on an Intel 486DX2 processor [20] or 180 mA on Intel Strong ARM [26]. For a sample calculation, with a 700 MHz CPU operating at 1.35 Volt, an encryption with 20,000 cycles would consume about 5.71 x 10-3 mA-second or 7.7 μ Joule.
So, the amount of energy consumed by program P to achieve its goal (encryption or decryption) is given by

$$E = VCC \times I \times N \times \tau \quad (7)$$

Where N: the number of clock cycles.
τ: the clock period.
VCC: the supply voltage of the system
I: the average current in amperes drawn from the power source for T seconds.

Since for a given hardware, both VCC and τ are fixed, E α I × N. However, at the application level, it is more meaningful to talk about T than N, and therefore, we express energy as E α I × T. Since for a given hardware Vcc are fixed [22]. The Scand and third methods were used in this work.

4. Experimental Results

4.1. The Effect of Cryptographic Algorithms on Power Consumption (Text Files)

4.1.1. Encryption of Different Packet Size

Encryption time is used to calculate the throughput of an encryption scheme. In this section, Encryption throughput (Megabytes/Sec) and power consumption by using two different methods (μJoule/Byte, and Average battery Consumed per iteration) are calculated for encrypting text files (.doc files) without transmission to show which encryption is more powerful than others. The results are shown in (Fig.6, Figure7 and Figure 8) respectively

- Encryption Throughput. Throughput of each encryption algorithm to encrypt different text data (Megabytes/Sec) without data transmission is shown in Figure 6.

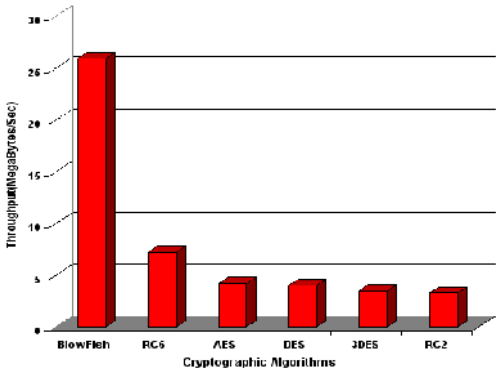

Figure 6. Throughput of each encryption algorithm to encrypt different text data (Megabytes/Sec) without data transmission.

- Power Consumption (μJoule/Byte). The Power consumption to encrypt different text data (.doc files) with a different data block size in micro joule/bytes are shown in Figure 7.

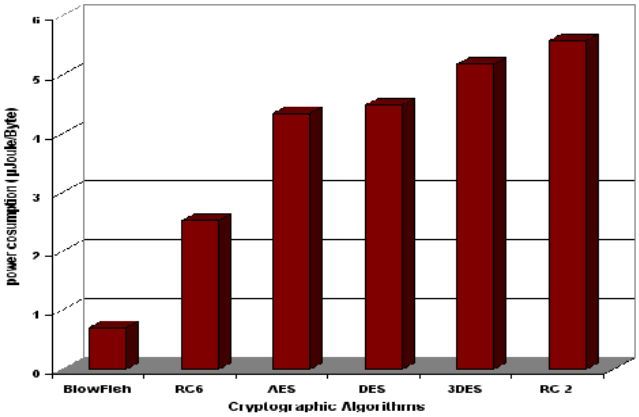

Figure 7. Power consumption (μJoule/Byte) for encrypting different Text document Files without data transmission.

- Power Consumption (Percentage of Battery Consumed).The Power consumption by calculating change in battery left for encryption process for text data (.doc files) with a different data block size are shown in Figure 8.

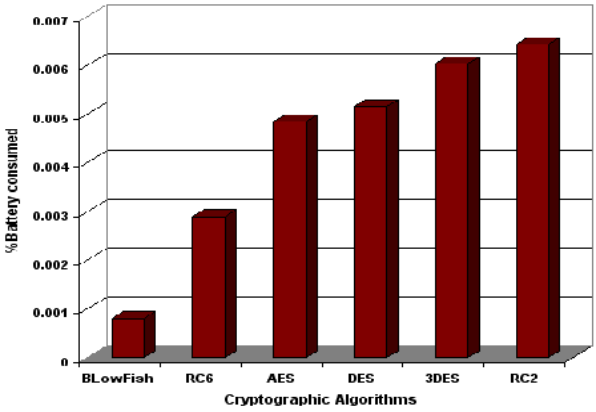

Figure. 8. Power consumption for encrypting different Text document Files without data transmission

4.1.2. Wireless Environment

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 (BSS, and ad hoc mode) are calculated. The results are shown in (table 2 and in Figure 9).

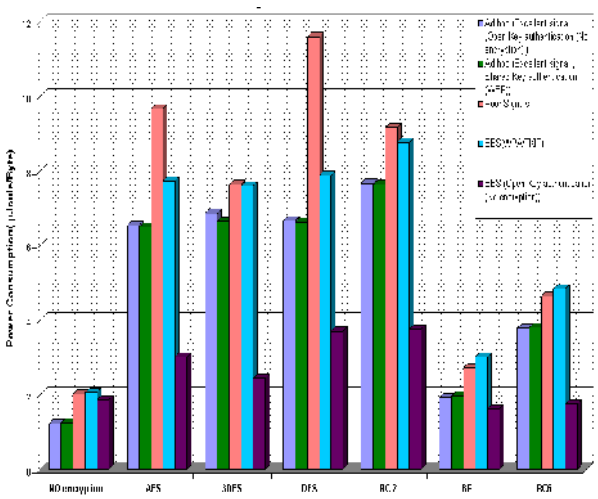

Figure 9. Power consumption for Encrypting different Text document Files in µJoule/Byte with data transmission.

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

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	18.94	18.5	45.93	29.28	25.94
DES	14.38	12.55	21.17	20.72	21.07
RC2	18.82	18.38	61.31	29.29	31.92
3DES	18.05	17.75	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

4.1.3. Results Analysis for Text Data

The results show the superiority of Blowfish algorithm over other algorithms in terms of the power consumption, processing time, and throughput in case of encryption and decryption(when the same data is encrypted by using Blowfish and AES, it is found that Blowfish requires approximately 16% of the power which is consumed for AES and 34% in case of decryption). Another point can be noticed here that RC6 requires less power ,and less time than all algorithms except Blowfish (when the same data is encrypted by using RC6 and AES ,it is found that RC6 requires approximately 58% of the power which is consumed for AES and 87% in case of decryption). A third point can be noticed here that AES has an advantage over other 3DES, DES and RC2 in terms of power consumption, time consumption, and throughput in case of encryption and decryption. A fourth point can be noticed here that 3DES has low performance in terms of power consumption and throughput when compared with DES in both cases. It requires always more time than DES because of its triple phase encryption characteristics. Finally, it is found that RC2 has low performance and low throughput when compared with other five algorithms in spite of the small key size used.

Also, there is insignificant difference in performance of different symmetric key schemes in case of data transmission. 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. When the encrypted data is transmitted by using Blow fish, RC6, and AES, it is found that RC6 and Blow fish require approximately 56% of the time consumption which is consumed for AES in case of ad- hoc architecture (8.2.11 standard using open system authentication and shared key authentication with excellent signals). When the encrypted data is transmitted using Blow fish, RC6, and AES, it is found that RC6 and Blow fish require approximately 68% of the time consumption which is consumed for AES in case of BBS architecture (802.11i using WPA/TKIP with excellent signals). In case of ad hoc mode (poor signal) , it is found that transmission time are increased approximately to double of open and shared key authentication in ad hoc mod using excellent signals.

4.2. The Effect of Changing Data Type (Audio) on Power Consumption

4.2.1. Encryption of Different Audio Files (. Wav files -Different Sizes)

- Encryption Throughput . Now a comparison between other types of data (Audio file) will be made to check which one can perform better than others in this case. Experimental results for audio data type (.wav files) are shown Figure 10 in case of encryption step.

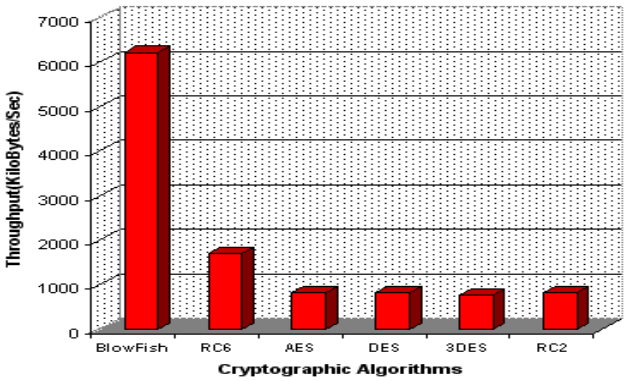

Figure 10. Throughput of each encryption algorithm (Kilobytes/Sec) without data transmission

- Power Consumption (µJoule/Byte). The Power consumption for encryption process by two different methods using a different audio block size without data transmission are shown in Figure 11 and in Figure 12.

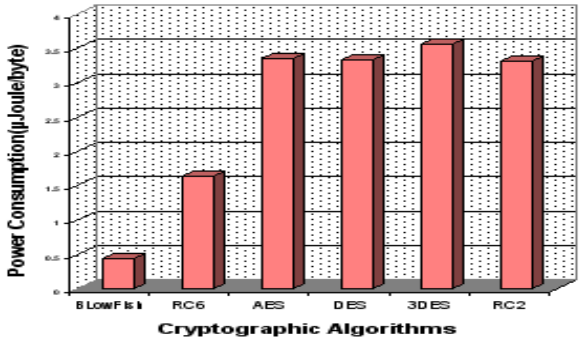

Figure 11. Power consumption for encrypting different Audio Files in µJoule/Byte without data transmission

- Power Consumption (Percentage of Battery Consumed)

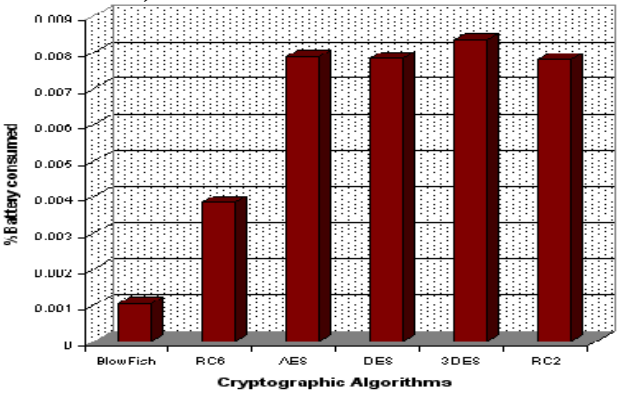

Figure 12. Power consumption for encrypting different Audio Files without data transmission.

4.2.2. Wireless Environment

We consider the effects of changes when transmission of data is taken in consideration under different scenario are considered for audio file. The results are shown in Figure 13 and in table 3.

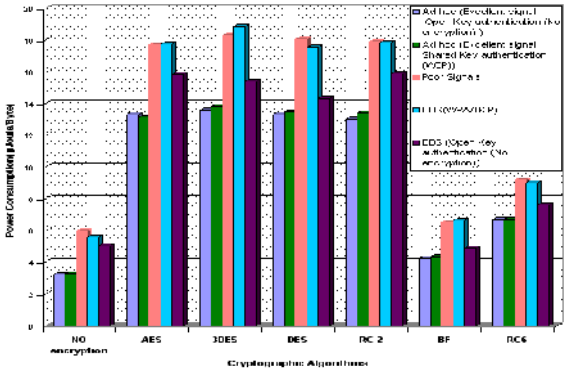

Figure 13. Power consumption for Encrypting different Audio files in µJoule/Byte with data transmission.

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

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	55.37	53.82	93.45	93.59	77.39
DES	54.53	56.48	94.83	99.87	69.97
RC2	55.84	57.2	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

4.2.3. Results Analysis for Audio files

The results show the superiority of Blowfish algorithm over other algorithms in terms of the power consumption, processing time, and throughput in case of encryption and decryption(when the same data is encrypted by using Blowfish and AES, it is found that Blowfish requires approximately 13% of the power which is consumed for AES and 18% in case of decryption). Another point can be noticed here that RC6 requires less power ,and less time than all algorithms except Blowfish (when the same data is encrypted by using RC6 and AES ,it is found that RC6 requires approximately 48% of the power which is consumed for AES and 84% in case of decryption). A third point can be noticed here that AES has an advantage over other 3DES, DES and RC2 in terms of power consumption, time consumption, and throughput in case of encryption and decryption. A fourth point

can be noticed here that 3DES has low performance in terms of power consumption and throughput when compared with DES in both cases. It requires always more time than DES because of its triple phase encryption characteristics. Finally, it is found that RC2 has low performance and low throughput when compared with other five algorithms in spite of the small key size used.

Also, there is insignificant difference in performance of different symmetric key schemes in case of data transmission. 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. When the encrypted data is transmitted by using Blow fish, RC6, and AES, it is found that RC6 and Blow fish require approximately 51% of the time consumption which is consumed for AES in case of ad- hoc architecture (8.2.11 standard using open system authentication and shared key authentication with excellent signals). When the encrypted data is transmitted using Blow fish, RC6, and AES, it is found that RC6 and Blow fish require approximately 52% of the time consumption which is consumed for AES in case of BBS architecture (802.11i using WPA/TKIP with excellent signals). In case of ad hoc mode (poor signal) , it is found that transmission time require approximately 74% of open and shared key authentication in ad hoc mod using excellent signals.

4.3. The Effect of Changing Data Type (Images) on Power Consumption.

4.3.1. Encryption of Different Images Files (.JBG files, .JIF files -Different Sizes)

Experimental results for image data type (JPEG images) are shown (Figure 14, and Figure15) respectively.

- Encryption Throughput

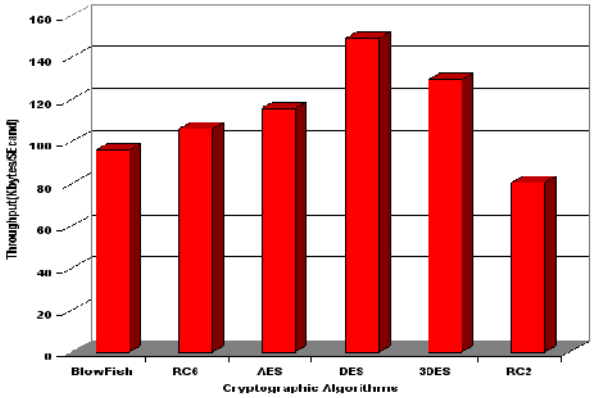

Figure14. Throughput of each encryption algorithm (Kilobytes/Sec).

- Power Consumption (Percentage of Battery Consumed)

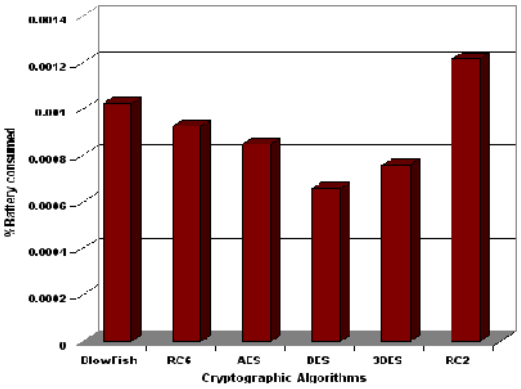

Figure 15. Power consumption for encrypting different Images Files.

4.3.2. Wireless Environment

The effects of changes on results when transmission of data is taken in consideration .The results are shown in Figure 16.

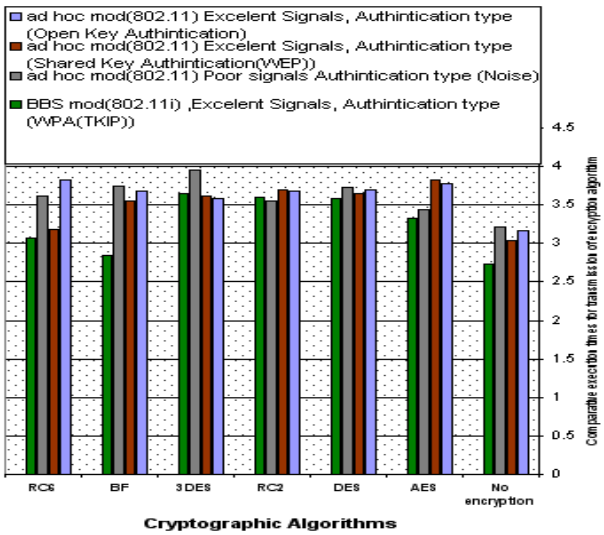

Figure 16. Comparative execution times for transmission of Image files using different algorithms

4.3.3. Results Analysis for Image files

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. It is found that 3DES still has low performance when compared to DES. It is found that there is insignificant difference in performance of different symmetric key schemes in case of data transmission

5. 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 Experimental 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 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. 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 it is found that , transmission time increased minimum by 70 % over open sheered authentication in ad hoc mod.

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] Borison.N (UC Berkeley), Goldbery.I (Zero-Knowledge Systems), and Wagner.D (UC Berkeley) (2001),"Intercepting Mobile Communications: The Security of 802.11,".

[2] Brown.B(2003), "802.11:the security differences between b and i," "Potentials, IEEE Volume 22, Issue 4, pp23-27At: portal.acm.org/citation.cfm?id=383768

[3] Bruce.S.(2008) The Blowfish Encryption Algorithm available http://www.schneier.com/blowfish.html

[4] Chandra.P(2005),"Bulletproof Wireless Security: GSM, UMTS, 802.11, and Ad Hoc Security (Communications Engineering), " ELSEVIER Newnes,.

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

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

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

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

[9] Endey .J, Arbaugh .W.A(2003), "Real 802.11 Security: Wi-Fi protected access and 802.11i ," Addison Wesley.

[10] Fischer.K(2004),. "Embedded wi-fi market undergoing major shift," Web article, 23 Aug.

[11] Gast.M.S (2002),"802.11 Wireless Network: The Definitive Guide," O'REILLY.

[12] Hardjono.T(2005), "Security in Wireless LANS and MANS," Artech House Publishers.

[13] Heinzelman.W.R,Chandrakasan.A,andBalakrishnan.H(2000), "Energy-efficient communication protocol forwireless microsensor networks," in Proceedings of the 33rd Hawaii International Conference on System Sciences, Maui, Hawaii.

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

[15] Karygiannis.T and Owens.L(2002), "Wireless Network Security: 802.11, Bluetooth and Handheld Devices," special Publication 800-48.

[16] Kempf.J(2008),"Wireless Internet Security: Architecture and Protocols," CAMBRIDGE University Press.

[17] Lahiri.K,Raghunathan.A, Dey.S, and Panigrahi .D(2002), "Battery driven system design," a new frontier in low power design.

[18] Li.L and Halpern.J(2001), "Minimum energy mobile wireless networks revisited," in Proceedings of IEEE International

Conference on Communications (ICC), Vol.1,PP.278-283.
[19] McKay.K(2005), "Trade-offs Between Energy and Security in Wireless Networks Thesis," Worcester Polytechnic Institute.
[20] Naik.K,Wei.D.S(2001),Software Implementation Strategies for Power-Conscious Systems," Mobile Networks and Applications - 6, 291-305.
[21] Nadeem. A.,and Javed,M.Y(2006); "A Performance Comparison of Data Encryption Algorithms," IEEEFirst International Conference , PP. 84- 89.
[22] Prasithsangaree.P and Krishnamurthy.P(2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.
[23] Ruangchaijatupon.P, Krishnamurthy.P(2001), "Encryption and Power Consumption in Wireless LANs-N,'' The Third IEEE Workshop on Wireless LANs - Newton, Massachusetts.
[24] Saleh.M.A(2006),"Weakness of Authentication and Encryption Methods Used in IEEE802.11b/g Wireless Networks, "IEEE Alexandria student Branch.
[25] Shih.E, Cho.S, Ickes.N, Min.R, Sinha.A, Wang.A, and Chandrakasan.A(2001), "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks," in Proceedings of The 7th ACM Annual International Conference on Mobile Computing and Networking (MobiCom), Rome, Italy,pp.272-287.
[26] Sinha.A and Chandrakasan.A.P(2001), "Joule Track A Web Based Tool for Software Energy Profiling," in the Proceedings of the 38th Design Automation Conference, Las Vegas, NV, USA, pp.220-225.
[27] Stallings.W (2005), "Cryptography and Network Security 4th Ed," Prentice Hall.

Diaa Abdul-Minaam was born on November 23, 1982 in KafrSakr, Sharkia, Egypt. He received the B.S from Faculty of Computers &Informatics, Zagazig University, Egypt in 2004 with grade very good with honor, and obtains master degree in information system from faculty of computers and information, menufia university, Egypt in 2009 and submitted for PhD from October 2009. He is working in Jazan University,KSA as teaching assistance at Faculty of Computer and informatics .Diaa has contributed more than 15+ technical papers in the areas of wireless networks , wireless network security, Information security and Internet applications in international journals, international conferences, local journals and local conferences. He majors in Cryptography and Network Security. (Mobile: +20166104747; +966548713895 E-mail: ds_desert@yahoo.com)

Hatem 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, and 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.

Mohiy 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 Pro- fessor 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 Pub- lisher. Prof. Hadhoud has published more than 110 pa- pers 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.