Wireless Network Security Has no Clothes

Hatem M. Abdual-Kader[1], Diaa Salama Abdul Minaam[2] ,and Mohiy Mohamed Hadhoud[3]
(Corresponding author: Diaa Salama Abdul Minaam)
Faculty of Computers and Information, Minufiya University[1]
hatem6803@yahoo.com [1]
mmhadhoud}@yahoo.com [3]

Higher Technological Institute 10th of Ramadan City[2]
Elbetrol st., Elsalam Area, Kafr Sakr, Sharkia, Egypt
ds_desert@yahoo.com[2]

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 video files), 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. So that current wireless network security protocols has no clothes according to power consumption

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

I. INTRODUCTION

In past few years, wireless communications has been fast increasing with many devices like laptops, PDAs, and Pocket PCs.

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 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 (Fig. 1) [7].

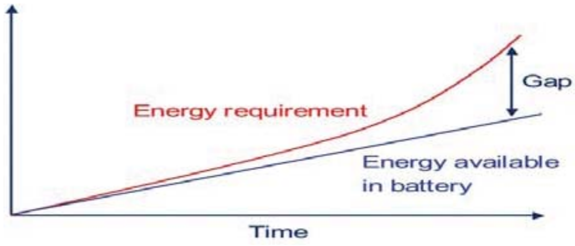

Fig 1. The growing gap between battery technology and power requirements

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 [18-22].

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].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.

II. 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.

In [24] 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.

For more details about previous work are found in [25-32]

III. EXPERIMENTAL DESIGN

The setup for the proposed experiment is shown in Fig. 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.

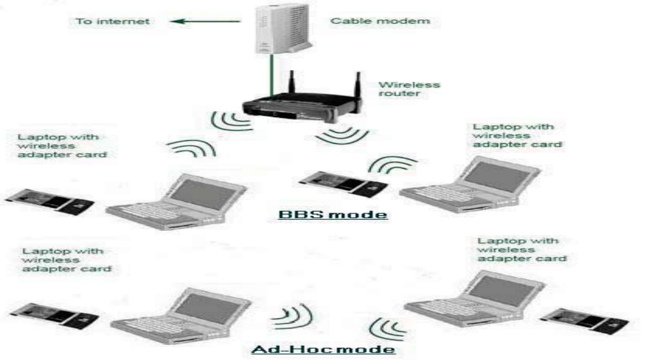
To internet
Cable modem
Wireless router
Laptop with wireless adapter card
Laptop with wireless adapter card
BBS mode
Laptop with wireless adapter card
Laptop with wireless adapter card
Ad-Hocmode

Fig 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 28 Kbytes to 131 Kbytes for pictures and Images (.GIF and GPG files) and from 4,006 Kbytes to 5,073 Kbytes for video files (.WAV 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[27].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:

1- Encryption time.
2- Throughput.
3- Battery power.
4- 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).

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

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 computation of the energy cost of encryption will be discussed in the next section.

The road map for experiment steps are described in the

III-1, a comparison is conducted between the results of selected different encryption algorithms using different setting such as different data types, different packet size, and different key size

Firstly; 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.

Secondly; in case of changing data types such video , and image ,(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 (calculating with data transmission)

III-2, 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

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, 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.

Secondly, 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.

IV. Measurement of Energy Consumption

Energy consumption of security primitives 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 =

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

Average battery Consumed per iteration=

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

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 [30], [32] using the following equations.

Bcost_encryption (ampere-cycle) = τ * I (4)

Tenergy_cost (ampere-seconds) =

$$\frac{B_{\text{cost\_encryption}}(\text{ampere - cycle})}{F(\text{cycles/sec})} \qquad (5)$$

Ecost (Joule) = Tenergy_cost (ampere-seconds)*V (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 [30] or 180 mA on Intel Strong ARM [31]. 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

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

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 [32]. The Scand and third methods were used in this work.

V. Experimental Results

5.1. The Effect of Cryptographic Algorithms on Power Consumption (text files)

➢ *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.3, Fig.4 and Fig. 5) respectively

- *Encryption Throughput*

Throughput of each encryption algorithm to encrypt different text data (Megabytes/Sec) without data transmission is shown in Fig 3.

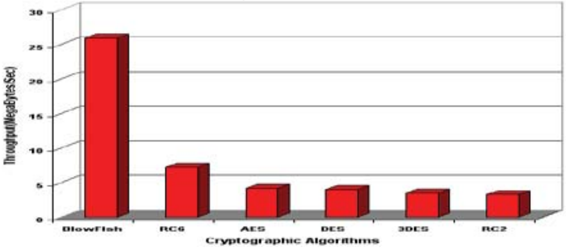

Fig 3. Throughput of each encryption algorithm to encrypt different text data (Megabytes/Sec) without data transmission

- *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 Fig 4 .

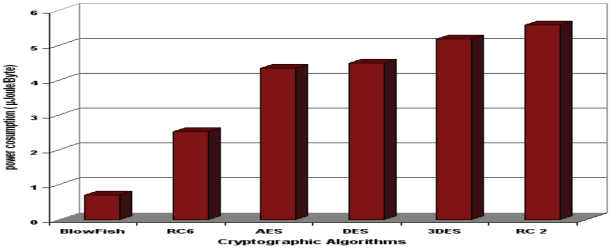

Fig 4. Power consumption (µJoule/Byte) for encrypting different Text document Files without data transmission

- *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 Fig 5.

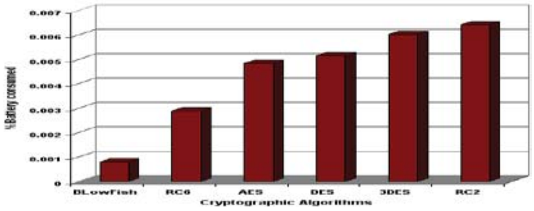

Fig 5. Power consumption for encrypting different Text document Files without data transmission

➢ *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 .1 and in Fig .6).

TABLE .1

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

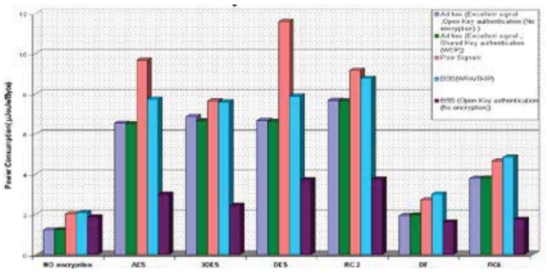

Fig 6. Power consumption for Encrypting different Text document Files in µJoule/Byte with data transmission

➢ *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.

5. 2. The Effect of Changing File Type (video) on Power Consumption.

➢ *Encryption of Different Video Files (.wav files - Different Sizes)*

- *Encryption Throughput*

Experimental results for video data type are shown Fig .7 at encryption.

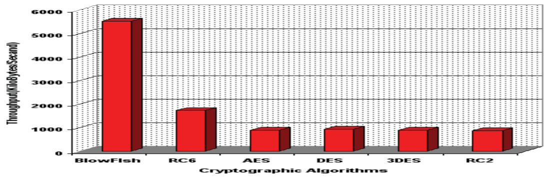

Fig 7. Throughput of each encryption algorithm (Kilobytes/Sec) without data transmission

- *Power Consumption (µJoule/Byte)*

The Power consumption for encryption process using a different video block size in µJoule/Byte are shown in Fig 8

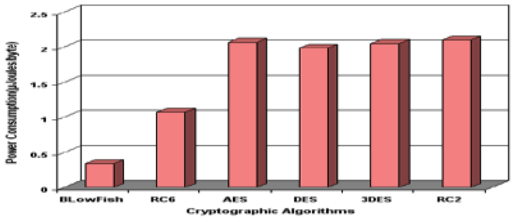

Fig 8. Power consumption for encrypting different Video Files in µJoule/Byte without data transmission

- *Power Consumption (Percentage of Battery Consumed)*

The Power consumption for encryption process by Battery consumed per iteration for different video block size are shown in Fig .9.

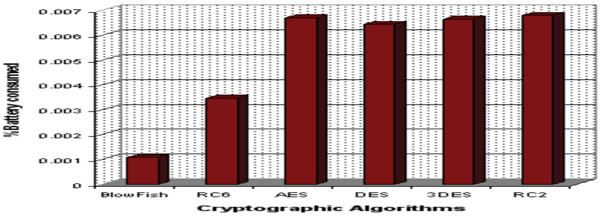

Fig 9. Power consumption for encrypting different Video Files in µJoule/Byte without data transmission

➢ *Wireless Environment*

The effects of change when data transmission is taken in consideration under different scenario are considered. The results are shown in table .2 and Fig 10

TABLE 2

COMPARATIVE EXECUTION TIMES FOR TRANSMISSION OF VIDEO DATA USING DIFFERENT ENCRYPTION ALGORITHMS

Video Streaming					
Data to be transmitted	ad hoc mod (802.11 standard)			BSS 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 Systems Authentication)
	Duration time in second				
No encryption	8.27	8.35	19.39	13.7	12.21
AES	14.89	16.24	26.84	27.1	21.47
DES	16.66	16	26.72	26.4	22.7
RC2	15.18	16.3	26.5	26.6	25.5
3DES	16.85	16.4	26.77	26.7	22.5
BF	9.3	8.78	16.17	14.2	12
RC6	8.49	9.36	14.13	13.9	12.68

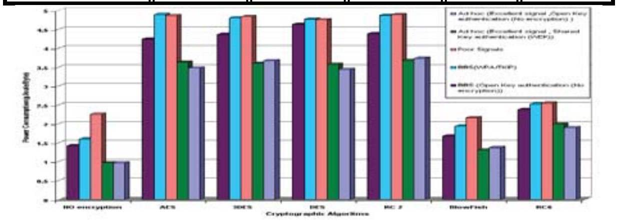

Fig 10. Power consumption for Encrypting different Video Files in µJoule/Byte with data transmission

➢ *Results Analysis for Video 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 24% of the power which is consumed for AES and 16% 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 51% of the power which is consumed for AES and 93% 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 57% 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 51% 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 71% of open and shared key authentication in ad hoc mod using excellent signals.

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

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

Experimental results for image data type (JPEG images) are shown (Fig. 11,and Fig.12) respectively.

- *Encryption Throughput*

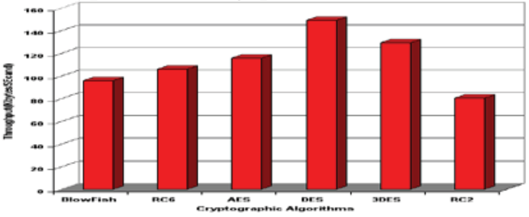

Fig 11. Throughput of each encryption algorithm (Kilobytes/Sec)

- *Power Consumption (Percentage of Battery Consumed)*

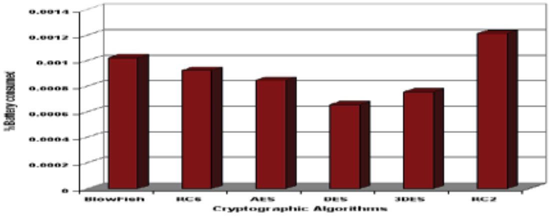

Fig 12. Power consumption for encrypting different Images Files

➢ *Wireless Environment*

The effects of changes on results when transmission of data is taken in consideration .The results are shown in Fig 13

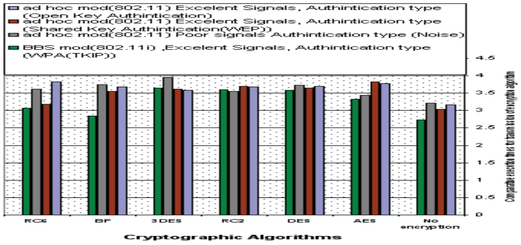

Fig 13. Comparative execution times for transmission of Image files using different algorithms

➢ *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. 4. The effect of changing key size of AES, and RC6 on power consumption.

The last performance comparison point is the changing different key sizes for AES and RC6 algorithm. In case of AES, We consider the three different key sizes possible i.e., 128 bit, 192 bits and 256 bit keys. The simulation results are shown in Fig. 14 and Fig.15.

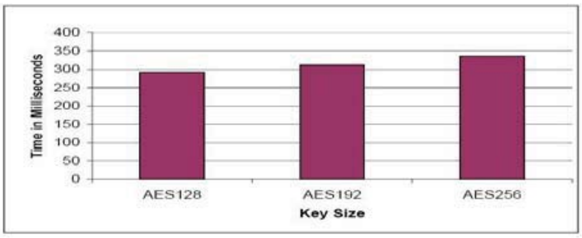

Fig 14. Time consumption for different key size for AES

In case of AES it can be seen that higher key size leads to clear change in the battery and time consumption. It can be seen that going from 128 bits key to 192 bits causes increase in power and time consumption about 8% and to 256 bit key causes an increase of 16% [15].

Also in case of RC6, We consider the three different key sizes possible i.e., 128 bit, 192 bits and 256 bit keys. The result is close to the one shown in the following figure

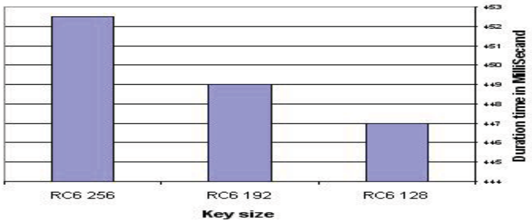

Fig 15. Time consumption for different key size for RC6

In case of RC6 it can be seen that higher key size leads to clear change in the battery and time consumption.

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 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 video 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. 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] K.Fischer, "Embedded wi-fi market undergoing major shift," Web article, 23 Aug 2004.

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

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

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

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

[6] J.Endey,W.A.Arbaugh, "Real 802.11 Security: Wi-Fi protected access and 802.11i ," Addison Wesley ,July 15,2003

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

[8] 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.

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

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

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

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

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

[14]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.

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

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

[17] M.A.Saleh,"Weakness of Authentication and Encryption Methods Used in IEEE802.11b/g Wireless Networks, "IEEE Alexandria student Branch, 2006

[18] J.KEMPF,"Wireless Internet Security: Architecture and Protocols," CAMBRIDGE University Press, 2008

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

[20] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol forwireless microsensor networks," in Proceedings of the 33rd Hawaii International Conference on System Sciences, Maui, Hawaii, 4-6 Jan 2000.

[21] L. Li and J. Halpern, "Minimum energy mobile wireless networks revisited," in Proceedings of IEEE International Conference on Communications (ICC), Vol.1,PP.278-283, 11-14 June, USA , 2001.

[22] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, and A. Chandrakasan, "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 , July 2001.

[23]"802.11: the security differences between b and i," "Potentials, IEEE Volume 22, Issue 4, Oct-Nov 2003, pp 23-27 At: portal.acm.org/citation.cfm?id=383768

[24] 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.

[25] Diaa Salama Abdu.Ellminaam, Hatem Mohamed Abdul kader, Mohie Mohammed ,Performance Evaluation of Symmetric Encryption Algorithms, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12 pp: 280- 286, December 2008.

[26] D. S. Abdul_Elminaam, H. M. Abdul_ kader, M. M. Hadhoud ,Evaluating The Effects of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices, IJICIS International Journal of Intelligent Computing and Information Sciences, Vol.9 No.2 ,pp:143-159, July 2009.

[27] Diaa Salama Abdul.Elminaam, Hatem Mohamed Abdul kader, Mohie Mohamed Hadhoud, Performance Evaluation of Encryption Algorithms on power consumption for wireless devices, International Journal of Computer Theory and Engineering (IJCTE), VOL.1 No.3, pp: 308- 316, August 2009.

[28] Diaa Salama A.Elminaam, Hatem Mohamed Abdul kader, Mohie Mohamed Hadhoud, Measuring and Reducing Energy Consumption of Cryptographic Schemes for Different Data Types, International Journal of Computer Theory and Engineering (IJCTE), VOL.1 No.3, pp: 334- 341, August 2009.

[29] Diaa Salama Abdul.Elminaam, Hatem Mohamed Abdul kader, Mohie Mohamed Hadhoud, Tradeoffs between Energy Consumption and Security of Symmetric Encryption Algorithms, International Journal of Computer Theory and Engineering (IJCTE) ,VOL.1 No.3, pp: 342- 350, August 2009.

[30] Diaa Salama Abdul.Elminaam, Hatem Mohamed Abdul kader, Mohiy Mohamed Hadhoud." Evaluating the Performance of Symmetric Encryption Algorithms ".International Journal of Network Security (IJNS), VOL.10 No.3, pp: 216- 222, May 2010.

[31] Diaa Salama Abdul.Elminaam, Hatem Mohamed Abdul kader, Mohiy Mohamed Hadhoud." " Evaluating the Effects of Cryptography Algorithms on Power Consumption for Different Data Types ".International Journal of Network Security (IJNS),VOL.11 No.2, pp: 91- 100, Sep 2010.