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

Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices

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

Abstract—s the popularity of wireless networks increases, so does the need to protect them. Encryption algorithms play a main role in information security systems. On the other side, those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. This paper illustrates the key concepts of security, wireless networks, and security over wireless networks. Wireless security is demonstrated by applying the common security standards like (802.11 WEP and 802.11i WPA,WPA2) and provides evaluation of six of the most common encryption algorithms on power consumption for wireless devices namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. 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, date transmission through wireless network and finally encryption/decryption speed. Experimental results are given to demonstrate the effectiveness of each algorithm.

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

I. INTRODUCTION

Data Security was found many years before the beginning of wireless communication. 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).

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. 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].

In Asymmetric keys encryption, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (E.g. RSA and ECC). Public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [1], [2]. 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

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" [9], [10].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. The performance measure of encryption schemes will be conducted in terms of energy for wireless devices, changing data types -such as text or document, and Video files on power consumption, changing packet size for the selected cryptographic algorithms on wireless devices.

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 experimental design is given in section 4. Experimental results are shown in section 5. Finally the conclusions are drawn section 6.

II. WIRELESS OVERVIEW

The primary difference between wireless and wired networks lies in the communications medium. Wired networks utilize cabling to transfer electrical current that represents information. With wireless networks, radio frequency (RF) and light signals have the job of carrying information invisibly through the air.

B. Wireless LANs

Wireless LANs supply high performance within and around office buildings, factories, and homes[11]. Table 1 provides some key characteristics at a glance.

TABLE I. TABLE I: KEY CHARACTERISTICS OF 802.11 WIRELESS LANS

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data Rates	1 Mbps, 2 Mbps, 5.5 Mbps (11b), 11 Mbps (11b), 54 Mbps (11a)
Data &Network Security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management. (AES is being considered for IEEE 802.11i.)
Operating Range	Up to 150 feet indoors and 1500 feet outdoors.9
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

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) shown in Fig. 1, in which the network consists of an access point and several wireless devices. When these devices try to communicate among themselves they propagate their data through the access point device.

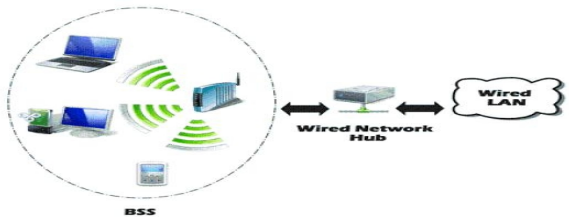

Fig. 1 Wireless LANs (BBS structure)

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" (shown in Fig.2). Ad hoc networks are also commonly referred to as peer-to-peer networks [12].

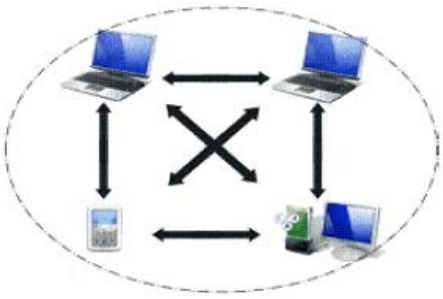

Fig. 2 ad hoc Wireless LANs

The two architectures of wireless LAN is applied in our experiment

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. The 802.11 IEEE standards were standardized in 1997. It consists of three layers: Physical layer, MAC (Medium Access Control) layer, and LLC (Logical Link Control) layer.

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].

Open system authentication is mandatory (Fig.3), and it's a two-step process. A radio NIC initiates the process by sending an authentication request frame to the access point. The access point replies with an authentication response frame containing approval or disapproval of authentication indicated in the status code field in the frame body [14].

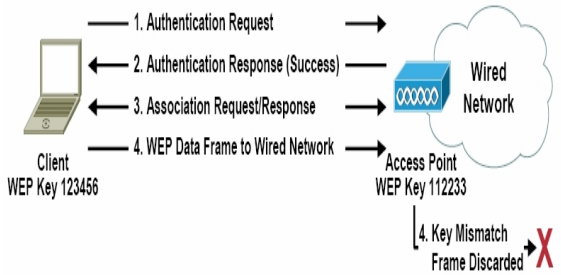

Fig.3 Open System authentication

Shared key authentication is an optional four-step process that bases authentication on whether the authenticating device has the correct WEP key. The radio NIC starts by sending an authentication request frame to the access point. The access point then places challenge text into the frame body of a response frame and sends it to the radio NIC. The radio NIC uses its WEP key to encrypt the challenge text and then sends it back to the access point in another authentication frame. The access point decrypts the challenge text and compares it to the initial text. If the text is equivalent, the access point assumes that the radio NIC has the correct key. The access point finishes the sequence by sending an authentication frame to the radio NIC with the approval or disapproval. Fig.4 shows how Shared Key Authentication works.

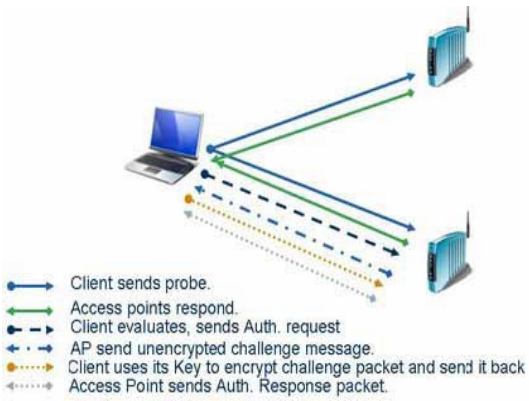

Fig. 4 Shared Key Authentication

b. Data Encryption &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) [18], was released to provide advanced security services. 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) [19]. 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.

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 [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 [21] 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.

III. 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, and from 4,006 Kilobytes to 5,073 Kilobytes for video files. using .NET environment. these implementations are thoroughly tested and are optimized to give the maximum performance for the algorithms. Then for transmission of data, we connect between the laptop with anther one wirelessly. We applied the experiment using BBS 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 .we study the effect of different signal to noise conditions and its effect on transmission of data (under Excellent signals and Poor signals)

Several performance metrics are collected in case of data transmission and without data transmission:

4- Encryption time.
5- Throughput.
6- Power consumption *(*micro joule*/*byte*).*
7- Power consumption *(*percent in 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 [25].

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 more CPU time is used in the

encryption process, the higher is the load of the CPU.

For computation of the energy cost of encryption (micro joule/byte), 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, on average, each cycle consumes approximately 270 mA on an Intel 486DX2 processor [26] or 180 mA on Intel Strong ARM [27]. Then, the amount of energy consumed by program P to achieve its goal (encryption or decryption) is given by: E=Vcc x I x T joules [26]. Since for a given hardware Vcc are fixed.

The second 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,

The following tasks that will be performed are shown as follows:

1) A comparison is conducted between the results of the selected different encryption and decryption schemes in terms of the encryption time, battery power and throughputs.
2) A study is performed on the effect of changing packet size on power consumption, throughput, and CPU work load for each selected cryptographic algorithms.
3) A study is performed on the effect of changing data types -such as text or document, and Video file for each selected cryptographic algorithms on power consumption.
4) A study is performed on the effect of changing key size for selected cryptographic algorithms on power consumption.
5) A study is performed on the effect of transmission of data wirelessly on power consumption using two different architecture (BBS or ad hoc) for all data type mention previously.
6) A study is performed on the effect of noise of signals on transmission data.
7) A study is performed on the effect transmitted data using IEEE 802.11 Standard (Open Key Authentication (no encryption), and Shared Key Authentication (WEP)).
8) A study is performed on the effect transmitted data using IEEE 802.11i (Open Key Authentication (no encryption), and WPA/TKIP)

IV. Experimental Results

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

a. Encryption of different packet size

Encryption time is used to calculate the throughput of an encryption scheme. In this section, we calculated CPU work load, Encryption throughput and power consumption for encryption text files without transmission to show which encryption is more powerful than others. The CPU work load (millisecond) , throughput (megabytes/second) , power consumption (micro joule/byte), and power consumption (percent of battery consumed) are shown in Fig 5, Fig 6 , Fig 7, and Fig 8 with respectively

1. CPU work load

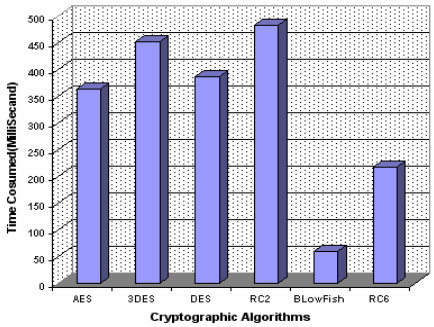

Fig. 5 Time consumption for encrypt different Text and Document with out data transmission(millisecond)

2. Encryption throughput

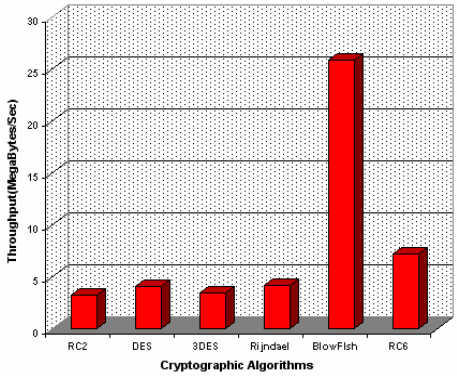

Fig. 6 Throughput of each encryption algorithm to encrypt different text data (Megabytes/Second)

3. Power consumption (Micro joule/byte)

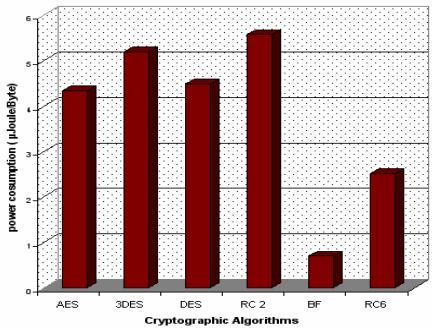

Fig.7 Power consumption for encrypt different Text document Files (micro Joule/Byte)

4. Power consumption (percent of power consumed)

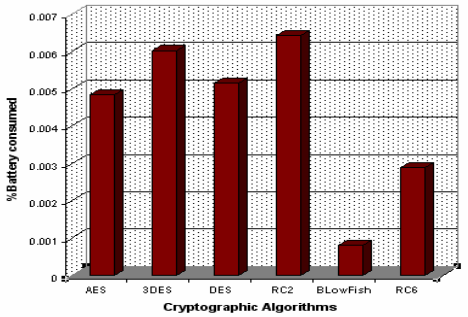

Fig. 8 Power consumption for encrypt different Text document Files

b. Decryption of different packet size

1. Decryption throughput

We calculated the Throughput (Megabytes/Second), CPU work load, and Power consumption (micro joule/byte) using each encryption algorithm to decrypt different text data with out data transmission. Experiment results for this compassion point are shown Fig 9, Fig 10, and Fig 11.

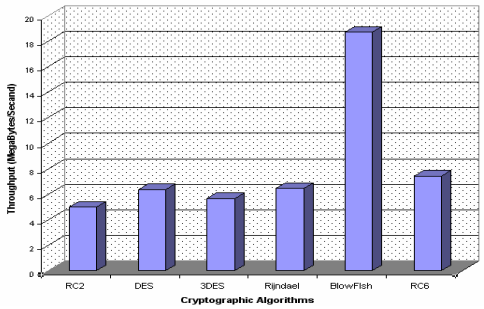

Fig .9 Throughput of each decryption algorithm (Megabyte/Second) for text data with out data transmission

2. CPU work load(Millisecond)

Experimental results for this compassion point are shown Fig. 18

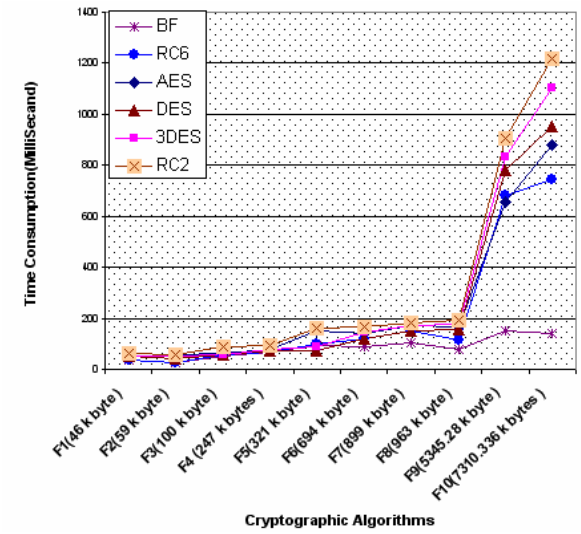

Fig. 10 Time consumption for Decrypt different text Files (millisecond)

3. Power consumption (Micro Joule/Byte)

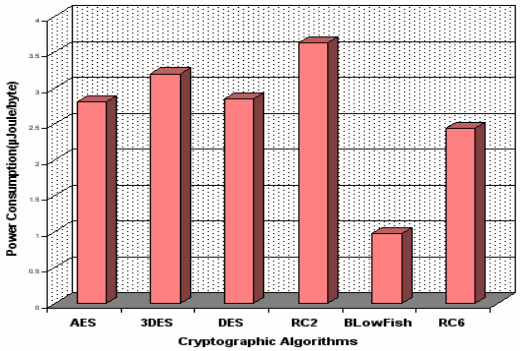

Fig. 11 Power consumption for Decrypt different Text document Files (Micro Joule/Byte)

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.12

TABLE II. TABLE II: 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

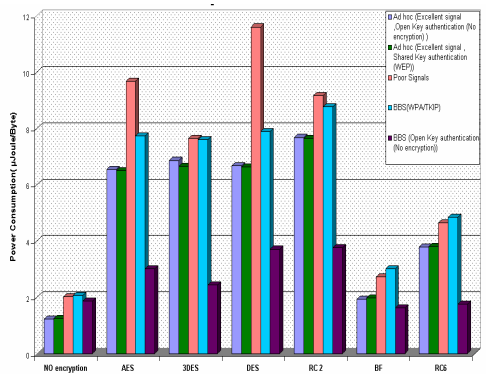

Fig. 12 Power consumption for Encrypt different Text document Files (Micro Joule/Byte) with data transmission

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 . 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

B. The effect of changing data type (Video files) on power consumption.

a. Encryption of different Video files (different sizes)

1. Encryption throughput

Now we will make a comparison between other types of data (Video files) to check which one can perform better in this case(Fig.13).

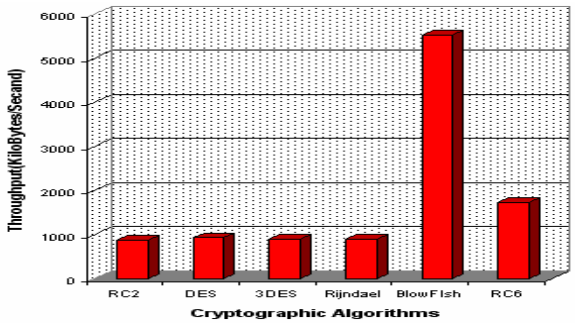

Fig. 13 Throughput of each encryption algorithm (Kilobytes/Sec)

2. CPU work load(Millisecond)

In Figure 14, we show the performance of cryptographic algorithms in terms of sharing the CPU load. With a different video block size

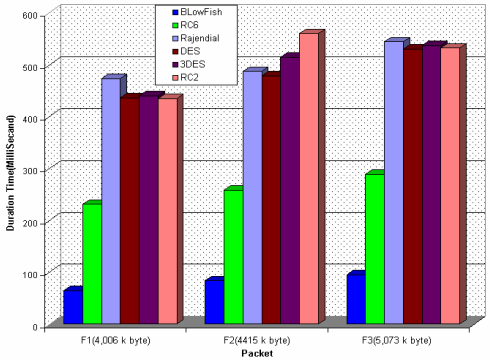

Fig. 14 Time consumption for encrypt different video Files

3. Power consumption (Micro joule/byte)

Experimental results for this compassion point are shown Fig. 15

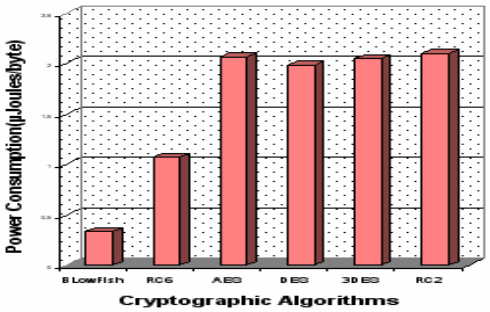

Fig. 16 Power consumption for encrypt different Video Files

4. Power consumption (percent of power consumed)

In Figure16, we show the performance of cryptographic algorithms in terms of Power consumption for encryption process with a different video block size

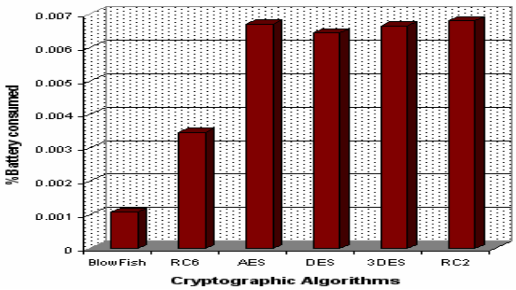

Fig. 16 Power consumption for encrypt different Video Files

The result is the same as in text.The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time , power consumption, and throughput (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). Another point that can be noticed here is that RC6 requires less power consumption and less time than all algorithms except Blowfish (when we encrypt the same data by using RC6 and AES, we found that RC6 requires approximately 51% of the power which is consumed for AES). 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. Finally, it is found that RC2 has low performance and low throughput when compared to the other five algorithms

b. Decryption of different Video files (different sizes)

1. Decryption throughput

Experimental results for this compassion point are shown Fig. 17

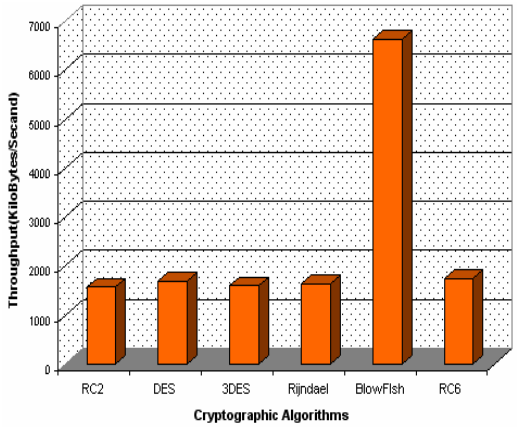

Fig. 17 Throughput of each Decryption algorithm (Kilobytes/Second)

2. work load(Millisecond)

Experimental results for this compassion point are shown Fig. 18

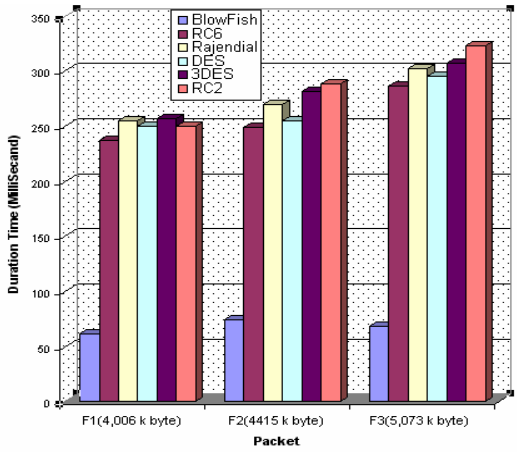

Fig. 18 Time consumption for Decrypt different video Files (millisecond)

3. Power consumption for Decryption

Experimental results for this compassion point are shown (Fig.19)

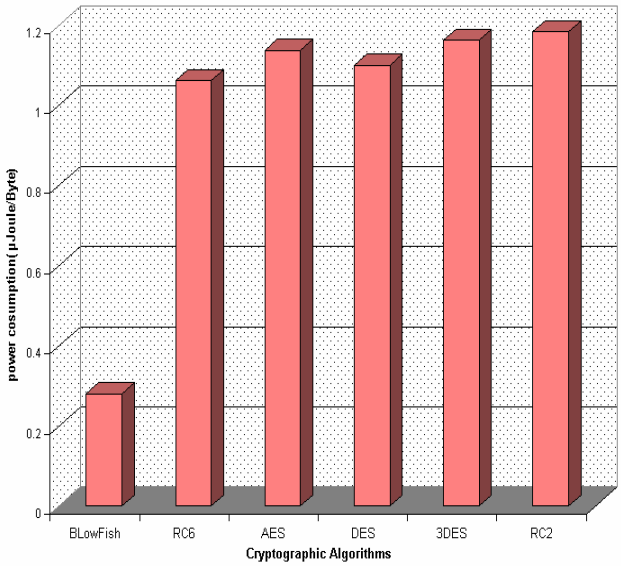

Fig. 19 Power consumption for Decrypt different Video Files in (micro joule/Byte)

From the results we found that the result is the same as in the encryption process for Video, audio files, and text data. When we decrypt the same data by using Blowfish and AES, we found that Blowfish requires approximately 24% of the power which is consumed for AES. When we decrypt the same data by using RC6 and AES, we found that RC6 requires approximately 93% of the power which is consumed for AES.

c.Wireless Environment

We consider the effect of change when transmitted of data is taken in consideration under different scenario the results as shown in table 3, Fig .20

TABLE III. 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	14.24	16.89	26.84	27.1	21.47
DES	16	16.66	26.72	26.4	22.7
RC2	15.18	16.3	26.5	26.6	25.5
3DES	16.4	16.85	26.77	26.7	22.5
BF	8.78	9.3	16.17	14.2	12
RC6	8.49	9.36	14.13	13.9	12.68

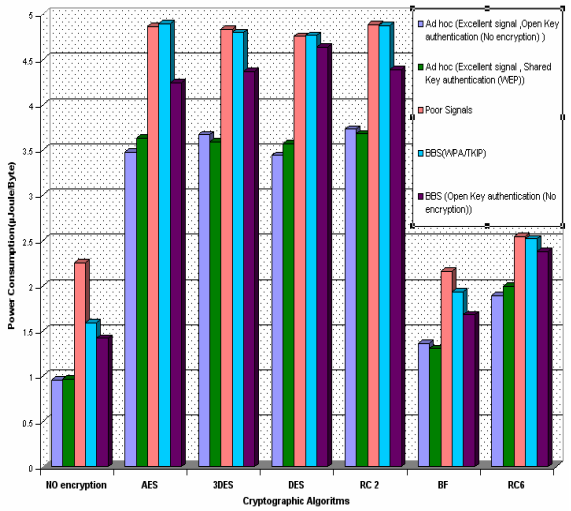

Fig. 19 Power consumption for Encrypt different Video Files (micro Joule/Byte)

In case of data transmission, we found, there is there is insignificant difference in performance of different symmetric key schemes .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 57% 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 51% of the time consumption which is consumed for AES. In case of ad hoc mode (poor signal) , we found transmission time increased approximately by 71% over open shared authentication in ad hoc mod using excellent signals.

V. 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 case of changing data type such as video files we found the result as the same as in text and document. Third point; when the transmission of data is considered there was insignificant difference in performance of different symmetric key schemes. 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 Fromhttp://www.cs.wustl.edu/~jain/cse56706/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 University, 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. (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, 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. 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.