Wireless Network Security Still Has no Clothes

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

Abstract: *As 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.*

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

Received November 25, 2009; Accepted September 19, 2010

1. 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 [6, 12, 23, 27] while AES uses various (128,192,256) bits keys [7, 20]. 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 [12, 23]. 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” [17, 19, 5].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.

2. 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.

2.1. Wireless LANs

Wireless LANs supply high performance within and around office buildings, factories, and homes[4]. Table 1 provides some key characteristics at a glance.

Table 1. 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 infigure 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.

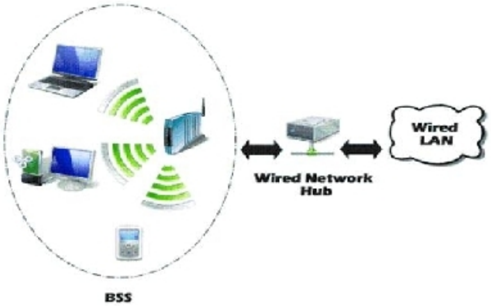

Figure 1. Wireless LANs (BBS structure).

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 figure2). Ad hoc networks are also commonly referred to as peer-to-peer networks [1].

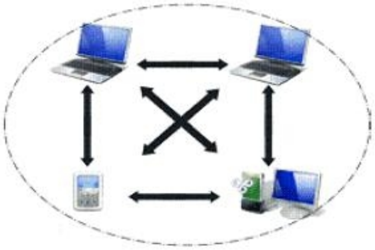

Figure. 2. Ad hoc Wireless LANs.

The two architectures of wireless LAN is applied in our experiment

2.1.1. 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 [18].

Open system authentication is mandatory (Figure 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 [15].

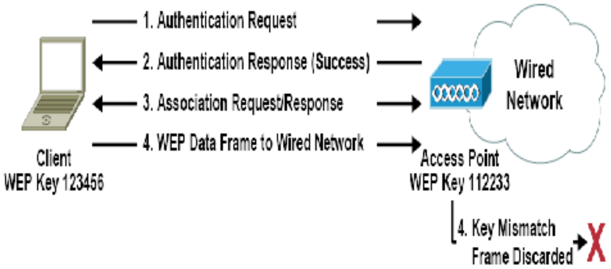
1. Authentication Request
2. Authentication Response (Success)
3. Association Request/Response
4. WEP Data Frame to Wired Network
Client
WEP Key 123456
Wired Network
Access Point
WEP Key 112233
4. Key Mismatch
Frame Discarded
X

Figure 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. Figure4 shows how Shared Key Authentication works.

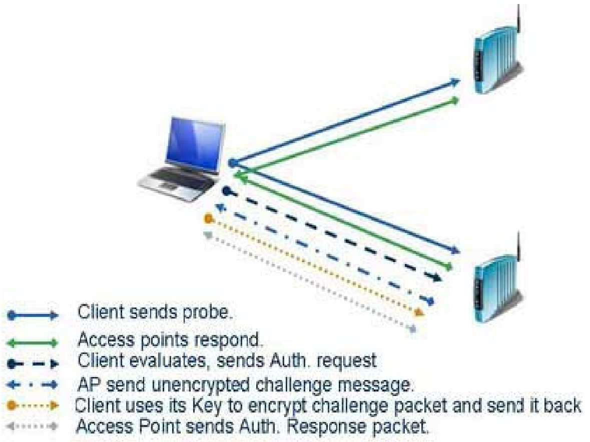
Client sends probe.
Access points respond.
Client evaluates, sends Auth. request
AP send unencrypted challenge message.
Client uses its Key to encrypt challenge packet and send it back
Access Point sends Auth. Response packet.

Figure 4. Shared Key Authentication.

2.1.2. Data Encryption and Authentication Protocol

The first data encryption and authentication protocol used in WLANs was called Wired Equivalent Privacy (WEP). WEP doesn't provide enough security for most enterprise wireless LAN applications. Because of static key usage, it's fairly easy to crack WEP with off-the-shelf tools [16, 24]. 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 [9]. A year later, another version of the WPA standard, WPA version 2 (WPA2) [10], 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) [25]. 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 [2]. 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.

3. 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 [23] 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 [13] 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 [14] 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 [11] 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.

4. 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.

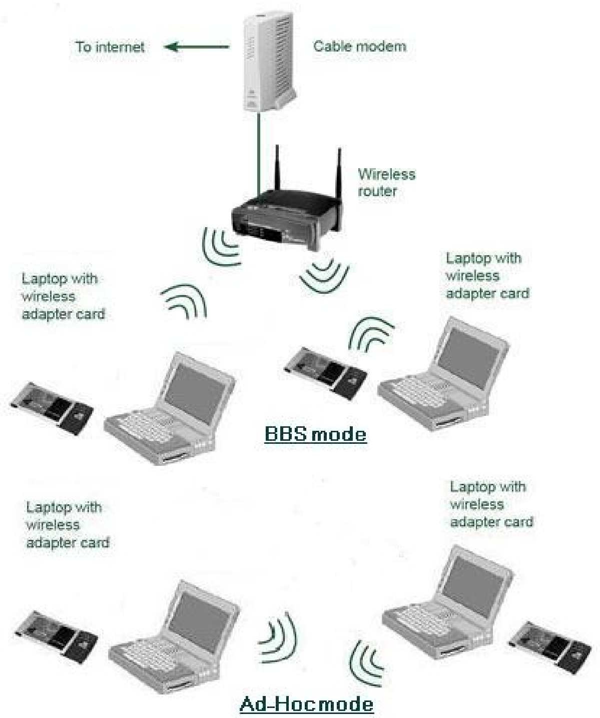
To internet
Cable modem
Wireless router
Laptop with wireless adapter card
Laptop with wireless adapter card
BBS mode
Laptop with wireless adapter card
Laptop with wireless adapter card
Ad-Hoc mode

Figure 5. 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).

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

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 road map for experiment steps are explained in sections 4.1., 4.2. and 4.3.

4.1. Results Comparison

A comparison is conducted between the results of selected different encryption algorithms using different setting such as different and 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 4.2.

4.2. 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

4.2.1. 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.

4.2.2. 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.

4.3. 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) and (3).

The battery life consumed in percentage for one run =

$$\frac{\text{Change in battery life}}{\text{the number of runs}} \tag{2}$$

Average battery Consumed per iteration=

$$\frac{\sum_{1}^{N} BatteryCon \quad sumedPer \quad Iteration}{N} \tag{3}$$

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.

$$\text{Bcost\_encryption (ampere-cycle)} = \tau * I \tag{4}$$

Tenergy_cost (ampere-seconds) =

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

$$\text{Ecost (Joule)} = \text{Tenergy\_cost (ampere-seconds)} \tag{6}$$

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

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

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

5. Experimental Results

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

5.1.1. 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 (figure 6, figure 7 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.
- 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.
- 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.

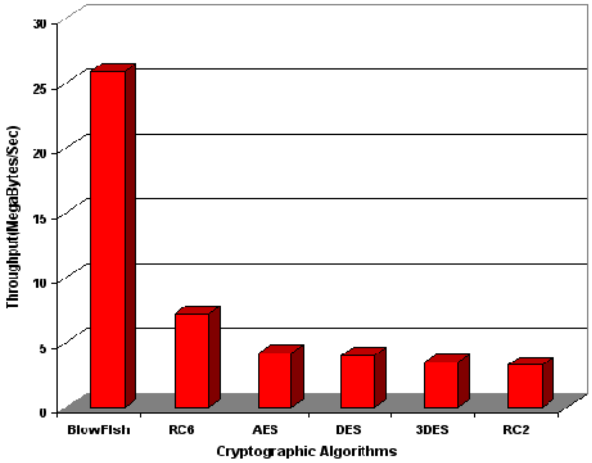

Figure 6. Throughput of each encryption algorithm to encrypt different text data (Megabytes/Sec) without data transmission.

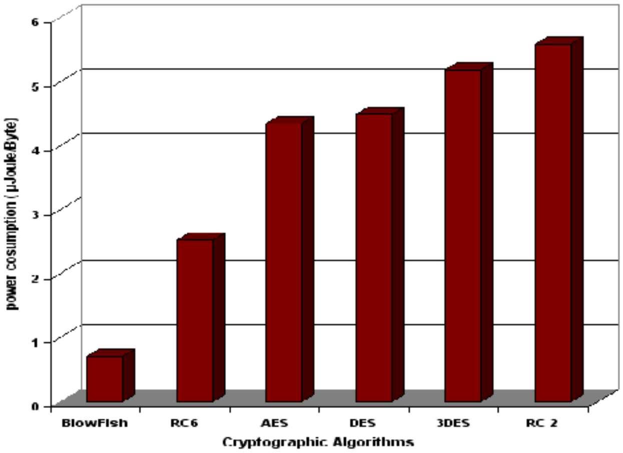

Figure 7. Power consumption (µJoule/Byte) for encrypting different Text document Files without data transmission.

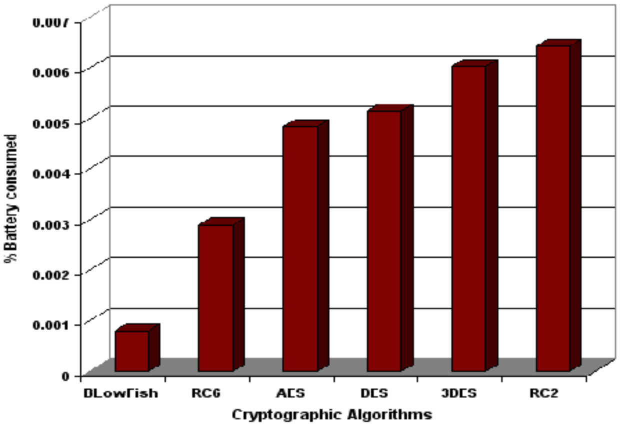

Figure. 8. Power consumption for encrypting different Text document Files without data transmission.

5.1.2. Decryption of Different Packet Size (.doc files)

- Decryption Throughput: The throughput of each encryption algorithm to decrypt different text data (Megabytes/Sec) without data transmission is calculated. Experimental results for this comparison point are shown in figure 9.

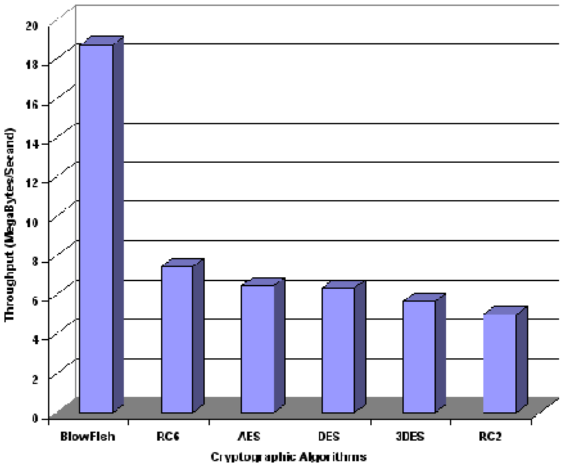

Figure 9. Throughput of each decryption algorithm (Megabyte/Sec) for text data without data transmission.

- Power Consumption (µJoule/Byte) .The Power consumption (µJoule/Byte) for decrypting different Text document Files without data transmission are calculated. Experimental results for this comparison point are shown figure 10.

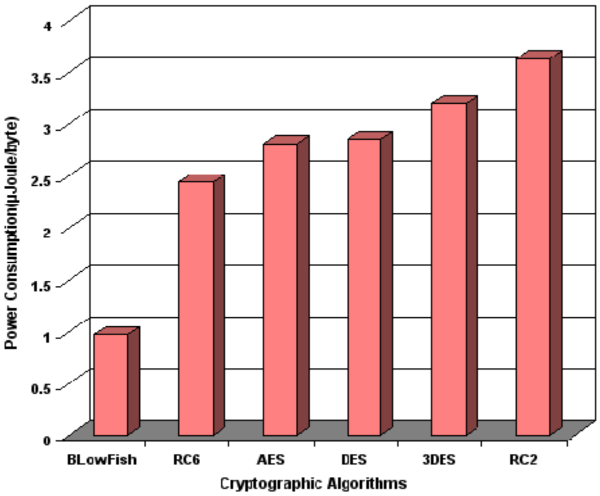

Figure. 10. Power consumption for Decrypting different Text document Files in µJoule/Byte without data transmission.

5.1.3. 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 11).

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

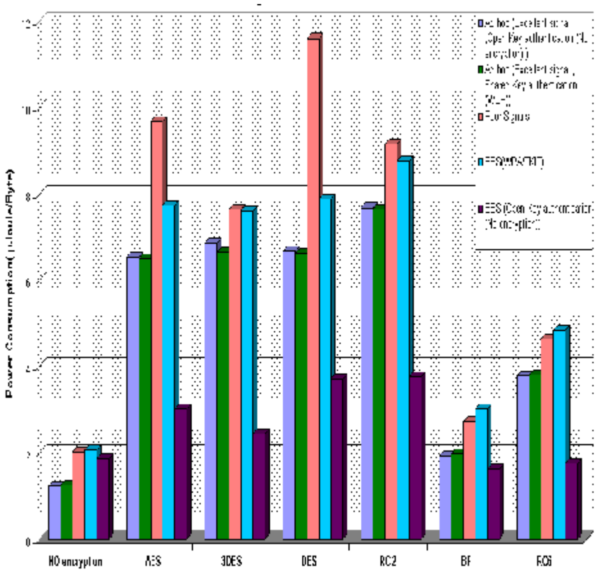

Figure 11. Power consumption for Encrypting different Text document Files in µJoule/Byte with data transmission.

5.1.4. 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.

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

- Encryption Throughput**.** Now a comparison between other types of data (Video files) will be made to check which one can perform better than other algorithms in this case. Experimental results for video data type are shown in figure 12 at encryption.
- Power Consumption (µJoule/Byte).The performance of cryptographic algorithms in terms of Power consumption for encryption process using a different video block size in µJoule/Byte are shown in figure 13.
- Power Consumption (Percentage of Battery Consumed). The performance of cryptographic algorithms in terms of Power consumption for encryption process by Battery consumed per iteration for different video block size are shown in figure 14.

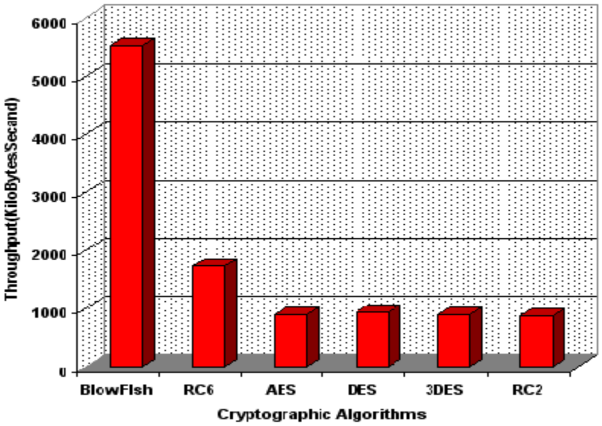

Figure 12. Throughput of each encryption algorithm (Kilobytes/Sec) without data transmission.

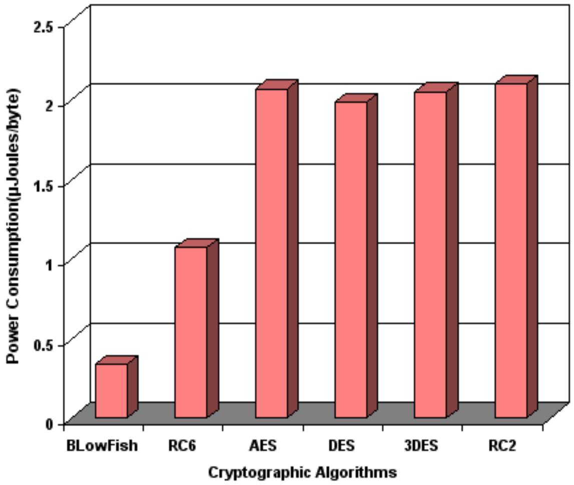

Figure. 13 Power consumption for encrypting different Video Files in µJoule/Byte without data transmission.

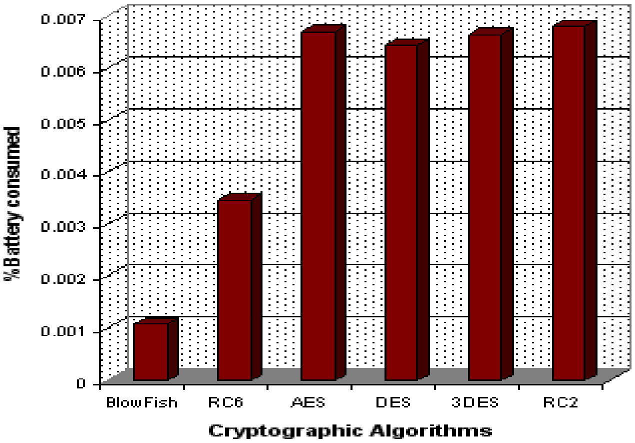

Figure. 14: Power consumption for encrypting different Video Files in µJoule/Byte without data transmission.

5.2.2. Decryption of Different Video Files (.wav files-Different Sizes)

- Decryption Throughput .The throughputs of each encryption algorithm to decrypt different video data (Kilobytes/Sec) without data transmission are calculated. Experimental results for this comparison point are shown figure 15.

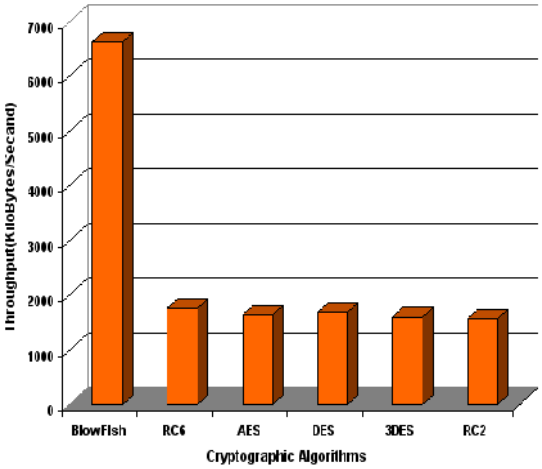

Figure. 15 Throughput of each Decryption algorithm (Kilobytes/Sec) without data transmission.

- Power Consumption (µJoule/Byte).The Power consumption (µJoule/Byte) for decrypting different audio Files without data transmission are calculated. Experimental results for this comparison point are shown figure 16.

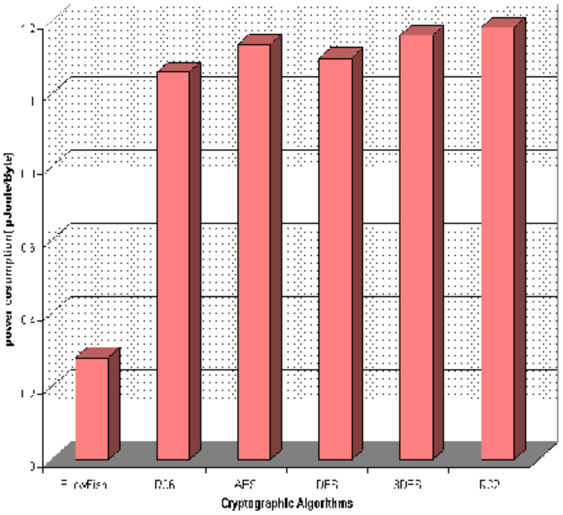

Figure. 16: Power consumption for Decrypting different Video Files in µJoule/Byte without data transmission.

5.2.3. Wireless Environment

The effects of change when data transmission is taken in consideration under different scenario are considered. The results are shown in table 3and figure 17.

Table 3. Comparative execution times for transmission of text 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

5.2.4. Results Analysis for Video 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 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

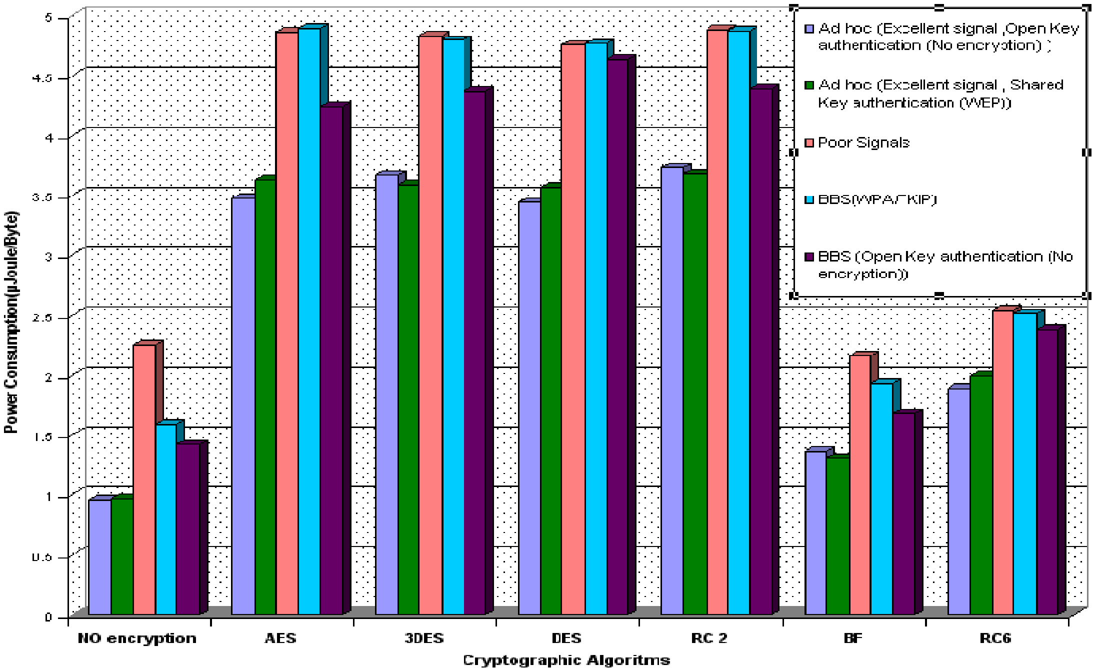

Figure 17. Power consumption for Encrypt different Video Files (micro Joule/Byte).

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.

6. Conclusions

This study 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.

Firstly: In the case of changing packet size (text data .DOC file) with / without data transmission using different architectures and different WLANs protocols, It is found that Blowfish has better performance than other encryption algorithms, followed by RC6 in case of encryption time, throughput, and power consumption for encryption and decryption.

Rijndael, an AES (Advanced Encryption standard), is faster than 3DES, DES, and RC2.These results are compatible with the scientific background. DES encrypts and decrypts data faster than 3DES and RC2. 3DES is faster than RC2.RC2 turns out to be the slowest method when the data being encrypted is small. It has an expensive computation up front to build a key-dependent table, which apparently is high compared to the cost of encrypting small data. RC2 is a variable key-length symmetric block cipher, which is designed to be alternatives to DES. These results are the same in encryption and decryption process with different packet size with and with out data transmission. 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 changing data type such video files (.WAV file).It is found that the result as the same as in text and document. it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6 in case of encryption and decryption with and with out data transmission. 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.

Finally: In the case of data transmission under poor signal we found transmission time increased by 70% over open shared authentication in ad hoc mod.

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 18+ 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.

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 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.