International Journal of Power Control Signal and Computation(IJPCSC)
Vol3. No1. Jan-Mar 2012 ISSN: 0976-268X
www.ijcns.com

Performance Analysis of Most Common Symmetrical Encryption Algorithms

G. RAMESH[1] Dr. R. UMARANI[2]
1Research Scholar, Research and Development Centre,Bharathiyar University, Coimbatore,INIDA
[2]Associate Professor in Computer Science, Sri Sarada college for women, Salem -16, INDIA
[1]mgrameshmca@yahoo.com, [2]umainweb@gmail.com

Abstract- The encryption and decryption process consume a significant amount of computing resources such as CPU time, throughput, and battery power. A wireless device, usually with very limited resources, especially battery power, is subject to the problem of energy consumption due to encryption algorithms. Designing energy efficient security protocols first requires an understanding of and data related to the energy consumption of common encryption schemes for wireless devices. This paper performs comparative analysis of five algorithm; DES, 3DES, AES, UMARAM and UR5 Algorithm, considering certain parameters such as throughput, encryption time and power consumption. A cryptographic tool is used for conducting experiments. The experimental results show the superiority of our UR5 encryption algorithm over other algorithms in terms of the power consumption, processing time, and throughput .

Keywords: ,Cryptography, Encryption techniques, AES, DES,3DES,UMARAM ,UR5,Computer security.

1. INTRODUCTION

The cryptography algorithms are divided into two groups: symmetric-encryption algorithms and asymmetric-encryption algorithms. There are a lot of symmetric-encryption algorithms used in WLAN, such as DES [2], TDES [3], AES [4], and RC6 [5],UMARAM[10], and UR5[12]. In all these algorithms, both sender and receiver have used the same key for encryption and decryption processes respectively. The outside attackers use the fixed plaintext (such as: the company-title which is sent in the first packets of the message) and encrypted text to obtain the key used in the WLAN. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [2]. 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". We need a way to make decisions about energy consumption and security to reduce the consumption of battery powered devices. This study evaluates five different encryption algorithms used or suggested for wireless local area network (WLANs) namely; AES, DES, 3DES,UMARAM and UR5 Algorithm.

This paper is organized as follows. The UR5 experimental design is described in section 2. Experimental results are shown in section 3. Finally the conclusions are in section 3.

2. EXPERIMENTAL DESIGN

For our experiment, we use two laptop IV 2.4 GHz CPU, in which performance data is collected. The two laptops (sender and receiver) had windows XP professional installed on it. The first laptop (sender) is connected to access point. In the experiments, the laptop encrypts a different file size ranges from 22 K byte to 96.06Mega Byte.

A. Measurement of Throughput:

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).

$$\text{Throughput of Encryption} = \frac{(\quad)}{(\quad)} \text{ ---------- (1)}$$

Where Tp – Total Plain Text (bytes), and 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.

B. Measurement of Energy Consumption

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 [7].

Energy consumption for encryption and decryption can be measured in many ways. These methods as follows: The First method used to measure energy consumption is to assume that an average amount of energy is consumed by normal operations and to test the extra energy

consumed by an encryption algorithms. This method simply monitors the level of the percentage of remaining battery that can computed by equations (2), (3)

The battery life consumed in percentage for one run = ——————————---------- (2)

———————————————

Average battery Consumed per iteration =----- (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 using the following equations.

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

Tenergy_cost(ampere-seconds)
= ——-————(————)——— ---------- (5)
(/)

Ecost(Joule) = Tenergy_cost (ampere-seconds) * V---(6)
Where Bcost-encryption: a basic cost of encryption(ampere-cycle): 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 : Clcok 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 IV 2.4 MHz processor or 180 mA on Intel Strong ARM . 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 × I × N × τ ----------(7)

Where N – The number of clock cycles and 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 Second and third methods were used in this work. A comparison is conducted between the results of selected different encryption algorithms using different setting such as different data types, different packet size, different key size.

3. SIMULATION RESULTS

Simulation results for this compassion point are shown Figure. 1 and Table 1 at encryption stage. The results show the superiority of UR5 over other algorithms in terms of the processing time. It can also 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. Compare the UMARAM and AES, the AES better than the UMARAM algorithm.

A. Performance Analysis of Different Encryption Algorithm

All the five Encryption Algorithms have been tested with different text size files..

Table 1- Comparative Throughput(Mb/sec) of various algorithms with different packet size.

Text file Size in Kbytes	AES	3DES	DES	UMARAM	UR5
22	**41**	**35**	**20**	**17**	**15**
51	**58**	**59**	**30**	**23**	**18**
110	**43**	**47**	**35**	**29**	**23**
232	**98**	**86**	**51**	**55**	**54**
323	**125**	**115**	**47**	**48**	**36**
790	**165**	**173**	**85**	**82**	**56**
945	**223**	**238**	**145**	**168**	**115**
5653	**263**	**317**	**258**	**244**	**212**
7198	**211**	**286**	**269**	**251**	**232**
7185	**1489**	**1479**	**1286**	**1185**	**1074**
21385	**1589**	**1807**	**1727**	**1712**	**1459**
41586	**1537**	**2301**	**2107**	**2087**	**1994**
98367	**1956**	**2753**	**2603**	**2536**	**2358**
Average Time	**599.84**	**745.84**	**666.38**	**649**	**588.15**
Throughput (Mb/Sec)	**23.57**	**18.96**	**21.22**	**21.79**	**24.04**

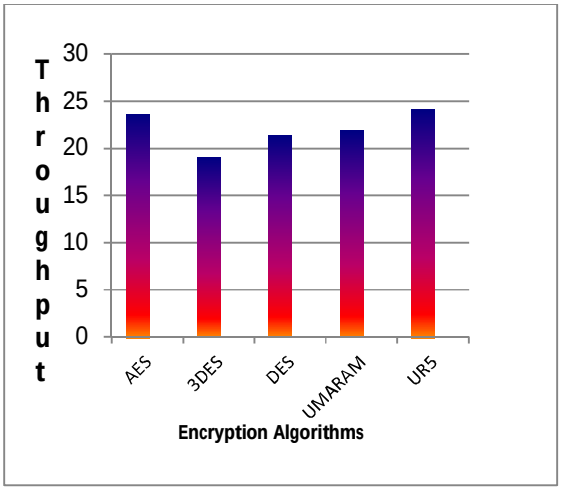

Figure 1; Comparative throughput of various algorithm with different packet size(Encryption)

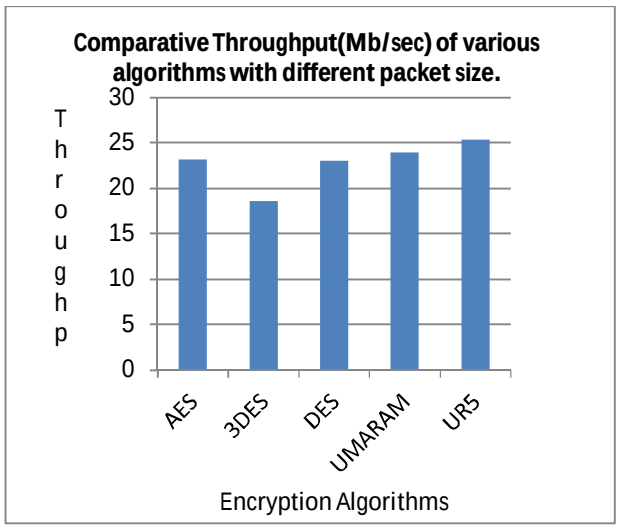

Figure.2; Comparative throughput of various algorithm with different packet size(Decryption)

B. 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. It indicates the speed of encryption. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased. The results show the superiority of UR5 over other algorithms in terms of the processing time. Another point can be noticed here; that AES requires less time than all algorithms except UR5. A third point can be noticed here; that UR5 has an advantage over other 3DES, DES and AES in terms of time consumption and throughput. A fourth 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. Finally, it is found that 3DES has low performance and low Simulation results for this compassion point are shown Figure. 2 and Table2 decryption stage. We can find in decryption that UR5 is the better than other algorithms in throughput and power consumption.

Table 2: Comparative Throughput(Mb/sec) of variousalgorithms with different packet size.

Text file Size in Kbytes	AES	3DES	DES	UMARAM	UR5
22	45	40	34	33	31
51	63	53	50	55	52
110	57	50	47	47	48
232	61	78	72	70	65
323	77	88	75	76	72
790	150	151	122	123	121
945	144	173	160	155	145
5653	172	180	168	161	166
7198	997	1108	988	977	889
7185	1025	1507	1052	1023	989
21385	1245	1708	1207	1191	1028
41586	1759	2033	1802	1752	1653
98367	2152	2738	2207	2018	1997
Average Time	611.31	762.07	614.15	590.84	558.15
Throughput(Mb/Sec)	23.13	18.55	23.02	23.93	25.34

The second point should be notice here that AES requires less time than all algorithms except UR5. A third point that can be noticed that AES has an advantage over other 3DES,DES.The fourth point that can be considered is that 3DES still has low performance of these algorithm. Finally, Triple DES (3DES) still requires more time than DES.

C. The effect of changing file type for cryptography algorithm on power consumption.

In the previous section, the comparison between encryption algorithms has been conducted at text and document data files. We found that UR5 has a performance greater than other the other four types. Now we will make a comparison between other types of data (Images) to check which one can perform better in this case. Simulation results for image data type (JPEG images) are shown Figure. 3 and Fig 4 at encryption and decryption respectively.

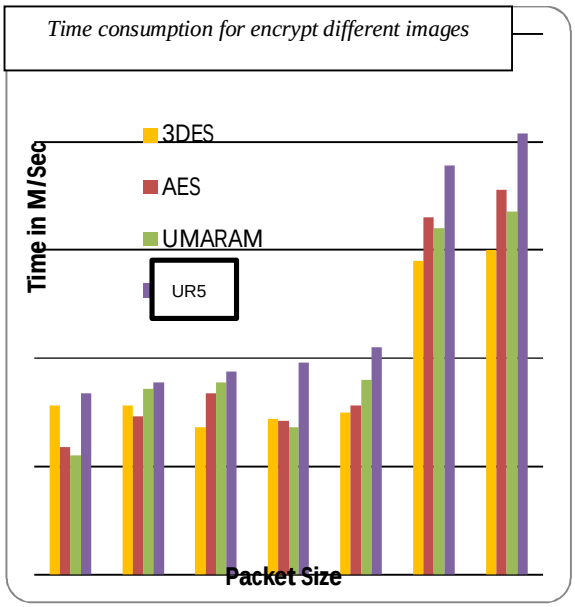

Figure. 3 Time consumption for encrypt different images

D. The effect of changing key size of AES on power consumption.

The last performance comparison point is the changing different key sizes for AES and UR5. 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 Figure. 5 and Figure.6. 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 9% and to 256 bit key causes an

increase of 17% [9].Also in case of UR5, We consider the three different key sizes possible i.e., 128 bit, 192 bits and 256 bit keys.

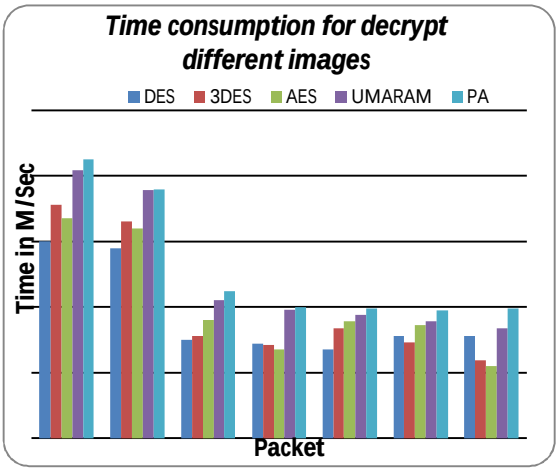

Figure. 4 Time consumption for decrypt different images

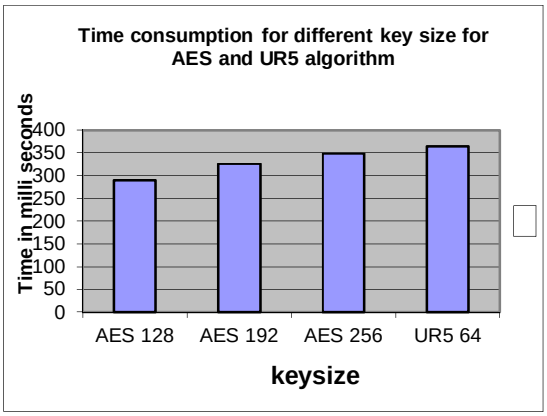

Figure. 5 Time consumption for different key size for AES

In case of RC6 it can be seen that higher key size leads to clear change in the battery and time consumption. Encryption time is used to calculate the throughput of an encryption scheme. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is decreased. The results show the advantage of UR5 over other algorithms in terms of the processing time. A second point can be noticed here; that PA has an advantage over other 3DES, DES,UMARAM and AES in terms of time consumption and throughput. A third point can be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It always requires more time than DES because of its triple phase encryption characteristics. Finally, it is found that 3DES has low performance and low throughput when compared with other four algorithms in spite of the small key size used.

4. CONCLUSION

Encryption algorithm play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern. The selected encryption AES, DES,3DES,UMARAM and UR5 algorithms are used for performance evaluation. 3DES showed poor performance results compared to other algorithms, since it requires more processing power. This paper presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. The selected algorithms are AES, DES,3DES,UMARAM and UR5. Several points can be concluded from the simulation results.

REFERENCES

[1] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader, Mohly Mohamed Hadhoud, “Evalution the Performance of Symmetric Encryption Algorithms”, international journal of network security vol.10,No.3,pp,216-222,May 2010.

[2] Diaasalama, Abdul kader, MohiyHadhoud, “Studying the Effect of Most Common Encryption Algorithms”, International Arab Journal of e-technology, vol 2,no.1,January 2011.

[3] Erik Olson, Woojin Yu, “Encryption for Mobile Computing”

[4] Anoop MS, “Public key Cryptography (Applications Algorithm and Mathematical Explanations)”

[5] P.Ruangchaijatupon, P.Krishnamurthy, “Encryption and power consumption in wireless LANs-n,” The Third IEEE workshop on wireless LANS, pp. 148-152, Newton,Massachusetts, sep. 27-28, 2001.

[6] Marshall D.Abrams, Harold J.podell on Cryptography.

[7] S. Hirani, Energy Consumption of Encryption schemes in wireless device Thesis, university of Pittsburgh, Apr. 9, 2003, Retrieved Oct.1, 2008.

[8] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn

[9] Andrea Pellegrini, Valeria Bertacco, Todd Austin on topic Fault-Based attack of RSA Authentication

[10] G. Ramesh and R. Umarani ‘UMARAM: A novel fast encryption algorithm for data security in local area network’ pp758 – 768 http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5654672

[11] G. Ramesh and R. Umarani “Data Security in Local Area Network Based on Fast Encryption Algorithm” Communications in Computer and Information Science, 2010, Volume 89, Part 1, 11-26 http://www.springerlink.com/content/m3301508219h7g66/

[12] G. Ramesh and R. Umarani ‘A Novel Symmetrical Encryption Algorithm with High Security Based on Key Updating’ pp.57-69. http://www.ijcns.com/pdf/207.pdf