Research Article Impact Factor: 0.621 ISSN: 2319-507X
Charan Pote, IJPRET, 2014; Volume 2 (8): 235-249 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURE UPDATES USING OTAP AND PERFORMANCE OF SYMMETRIC ENCRYPTION ALGORITHMS ON POWER CONSUMPTION FOR WIRELESS SENSOR NETWORK

MR. CHARAN R. POTE[1], MR. PUNESH U. TEMBHARE[2], MR. MANOJ G. LADE[3]

1. Assi. Prof., Priyadarshini College of Engg., RTM Nagpur University, India.
2. Assi. Prof., Priyadarshini College of Engg., RTM Nagpur University, India.
3. Student ME(WCC), Priyadarshini College of Engg, RTM Nagpur University, India.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: Wireless Sensor Networks (WSNs) face many challenges including reliability, flexibility and security. When WSNs deployed in remote locations need to be reprogrammed, environmental conditions often make it impossible to physically retrieve them. Over the Air Programming (OAP) plays an important role in achieving this task. Over-the-air programming (OAP) is a fundamental service in sensor networks that relies upon reliable broadcast for efficient dissemination. SenSeOP Programming protocols provide a convenient way to update program images via wireless communication. In hostile environments where there may be malicious attacks against wireless sensor networks, the process of reprogramming faces threats from potentially compromised nodes. While existing solutions can provide authentication services, they are insufficient for a new generation of network coding-based reprogramming protocols in wireless sensor networks. The 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. 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.

Keywords: SenSeop, WSN, Security, Encryption Techniques, Power Consumption.

Corresponding Author: Mr. CHARAN R. POTE

Access Online On:

www.ijpret.com

How to Cite This Article:

Charan Pote. IJPRET. 2014: Volume 2 (8): 235-249

PAPER-QR CODE

INTRODUCTION

A Wireless Sensor Network (WSN) is composed of small and highly resource-constrained sensor nodes that monitor some measurable phenomenon in the environment, e.g., light, humidity, or temperature. WSNs are deployed in a steadily growing plethora of application areas.

These range from military (e.g., security perimeter surveillance) over civilian (e.g., disaster area monitoring) to industrial (e.g., industrial process control). Application scenarios of WSNs typically involve monitoring or surveillance of animals or humans, infrastructure, or territories. Their long-life and large-scale design, various deployment fields, and changing environments necessitate the feasibility of remote maintenance and in-situ reprogramming of sensor nodes using a so-called Over-The- Air Programming (OTAP) protocol. In particular, if sensor nodes are inaccessible after deployment, a reliable OTAP is crucial. We believe that in a plurality of WSNs, the network-wide dissemination of program code is not appropriate. Within a single WSN, the heterogeneity of sensor hardware, the deployment of manifold sensor technologies, the diversity of sensing and communication tasks, and possibly the event and location dependency of software require a flexible, group-wise selective OTAP approach in order to be able to efficiently reprogram a subset of nodes. Furthermore, securing the OTAP protocol is imperative in order to protect the OTAP from unauthorized reprogramming attempts, i.e., to prevent reprogram node attacks .

In this paper, present SenSeOP, a Selective and Secure Over The Air Protocol which is integrated in our intrusion detection system and offers both, selective and secure reprogramming in WSNs. For our approach, assume infrequent and non-regular software updates. On the one hand, these updates are supposed to be time- and energy- efficient.

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. 1. Introduction of OTAP and Encryption Technique 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.

Over-The-Air-Programming Protocol

In the over the air programming protocol (OTAP) for WSNs. This protocol is described in two phases: infrastructure and reprogramming. The infrastructure is responsible to aggregate into the WSN the small world features. The reprogramming specify the messages used to allow the code mobility. The problem assessed here is to reconfigure the program running on all sensor nodes of a WSN. Assuming the net- work is connected, all sensor nodes must receive the exact program image and be updated with the same version of code. Currently, only networks with stationary nodes are considered.

Fig 1. Over The Air Programming

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 [11] 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 [12] 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 [13] 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 [14] 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.

1. EXPERIMTAL 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 K byte to 7.139Mega Byte139MegaBytes for text data, from 33 Kbytes to 8262 Kbytes for audio data, and from 4006 Kbytes to 5073 Kbytes for video files. Several performance metrics are collected:

1) Encryption time; 2) CPU process time; and 3) CPU clock cycles and battery power. 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 en- crypted divided by the encryption time [15]. The CPU process time is the time that a CPU is com- mitted 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. The CPU clock cycles are a metric, reflecting the en- ergy consumption of the CPU while operating on encryp- tion operations. Each cycle of CPU will consume a small amount of energy. The following tasks that will be performed are shown as follows:

• A comparison is conducted between the results of the selected different encryption and decryption schemes in terms of the encryption time at two different en- coding bases namely; hexadecimal base encoding and in base 64 encoding.

• A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm.

• A study is performed on the effect of changing data types - such as text or document, audio file, and video file - for each cryptography selected algorithm on power consumption.

• A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

4 EXPERIMTAL RESULTS

4.1 Differentiate Output Results of Encryption (Base 64, Hexadecimal)

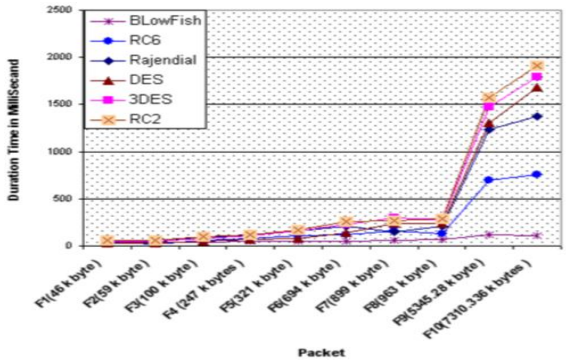
Experimental results are given in Figures 2 and 3 for the selected six encryption algorithms at different encoding method. Figure 2 shows the results at base 64 encoding while Figure 3 gives the results of hexadecimal base encoding. We can notice that there is no significant difference at both encoding method. The same files are encrypted by two methods; we can recognize that

the two curves almost give the same results. Time consumption of encryption algorithm (base 64 encoding)

4.2 Effect of Changing Packet Size for Cryptographic Algorithms on Power Consumption

4.2.1 Encryption of Different Packet Size

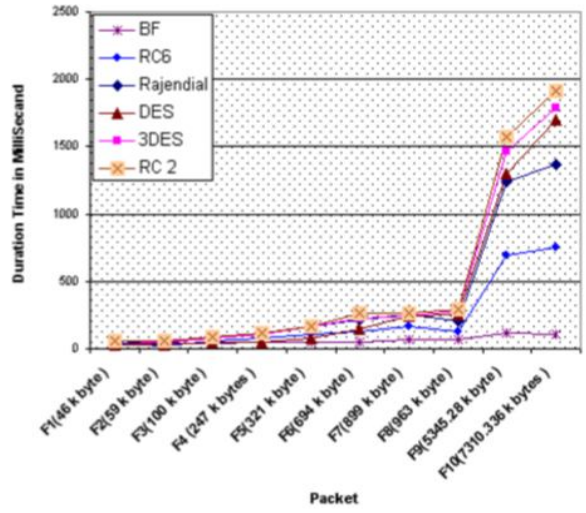
Encryption time is used to calculate the throughput of an encryption scheme. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption of this encryption technique is de- creased.

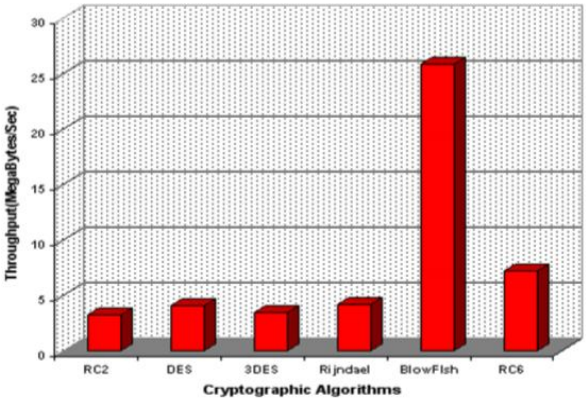


Experimental results for this compassion point are shown Figure 4 at encryption stage. The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Another point can be noticed here; that RC6 requires less time than all algorithms except Blowfish. A third point can be noticed here; that AES has an advantage over other 3DES, DES and RC2 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 always requires more time than DES because of its triple phase encryption character- istics. 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.

4.2.2 Decryption of Different Packet Size

Experimental results for this compassion point are shown Figure 5 decryption stage. We can find in decryption that Blowfish is the better than other algorithms in throughput and power consumption. The second point should be no- ticed here that RC6 requires less time than all algorithms except Blowfish. A third point that can be noticed that AES has an advantage over other 3DES, DES, RC2.The fourth point that can be considered is that RC2 still has low performance of these algorithm. Finally, Triple DES (3DES) still requires more time than DES.





4.3 The Effect of Changing File Type (Audio Files) for Cryptography Algorithm on Power Consumption

4.3.1 Encryption of Different Audio Files (Different Sizes)

Encryption Throughput In the previous section, the comparison between en- cryption algorithms has been conducted at text and document data files. Now we will make a compari- son between other types of data (Audio file) to check which one can perform better in this case. Experi- mental results for audio data type are shown Figure 6 at encryption.

CPU Work Load In Figure 7, we show the performance of crypto- graphic algorithms in terms of sharing the CPU load. With a different audio block size Results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time (CPU work load) and throughput. Another point can

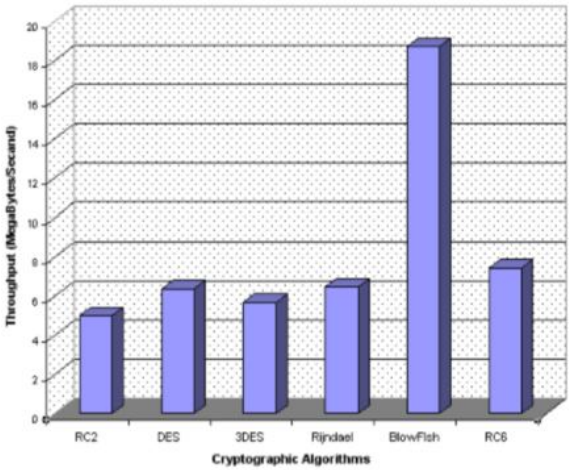


Figure 5: Throughput of each decryption algorithm (Megabyte/Sec)

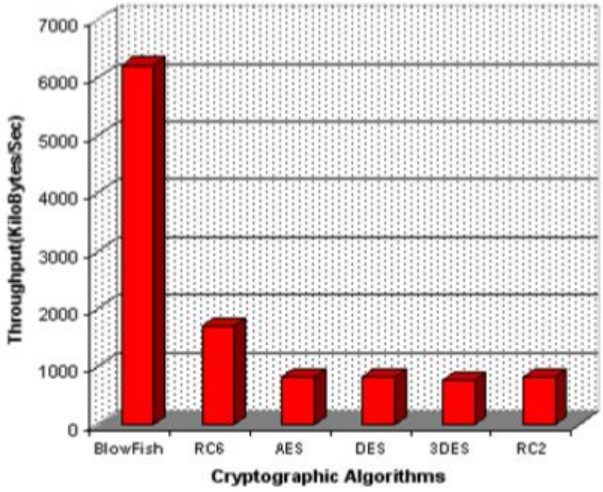


Figure 6: Throughput of each encryption algorithm (Kilo- bytes/Second)

be noticed here; that RC6 requires less time than all algorithms except Blowfish. A third point can be noticed here; that AES has an advantage over other 3DES, DES and RC2 in terms of time con- sumption and throughput especially in small size file. A fourth point can be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It always re- quires more time than DES. 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.

4.3.2 Decryption of Different Audio files (Different Sizes)

Decryption Throughput Experimental results for this compassion point are shown Figure 8.

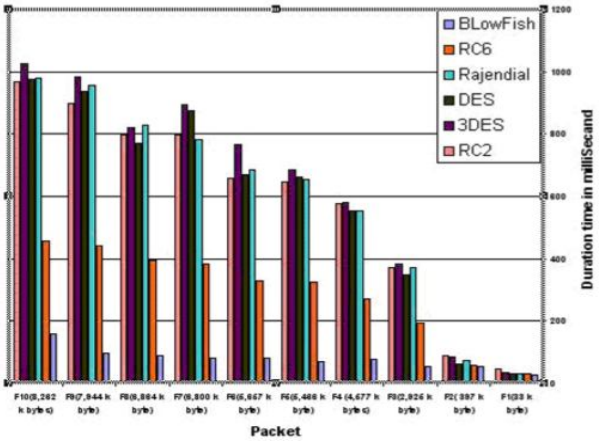


Figure 7: Time consumption for encrypt different audio files

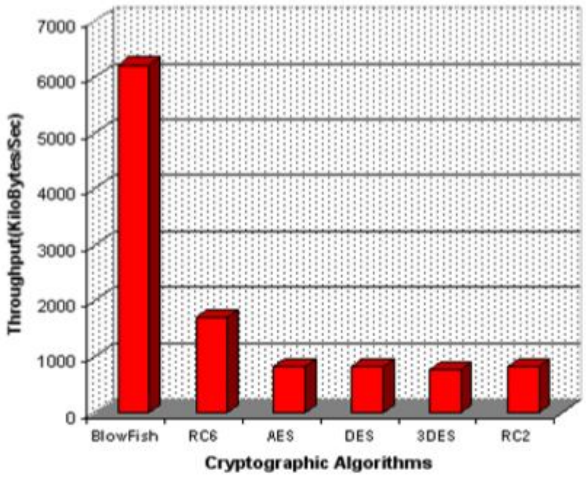


Figure 8: Throughput of each Decryption algorithm (Kilobytes/Second)

CPU Work Load

Experimental results for this compassion point are shown Figure 9.

From the results we found the result as the same as in encryption process for audio files.

4.4 The Effect of Changing File Type (Video Files) for Cryptography Algo- rithm on Power Consumption

4.4.1 Encryption of different video files (different sizes)

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. Experimental results for video data type are shown Figure 10 at encryption.

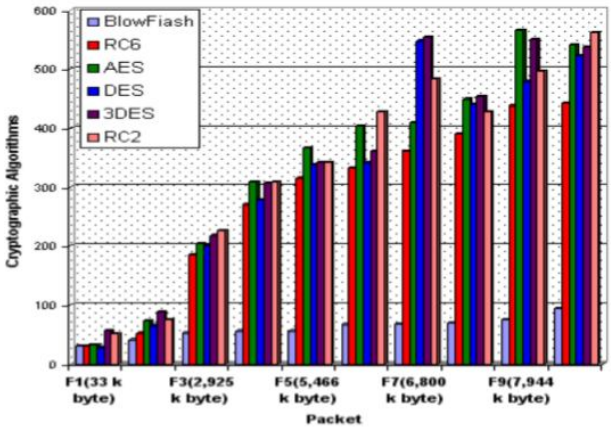


Figure 9: Time consumption for decrypt different audio files

CPU Work Load In Figure 11, we show the performance of cryptog- raphy algorithms in terms of sharing the CPU load. With a different audio block size.

The results show the superiority of Blowfish algo- rithm over other algorithms in terms of the process- ing time and throughput as the same as in Audio files. Another point can be noticed here; that RC6 still requires less time has throughput greater than all algorithms except Blowfish. 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. Finally, it is found that RC2 has low per- formance and low throughput when compared with other five algorithms.

4.4.2 Decryption of Different Video Files (Dif- ferent Sizes)

Decryption Throughput Experimental results for this compassion point are shown Figure 12.

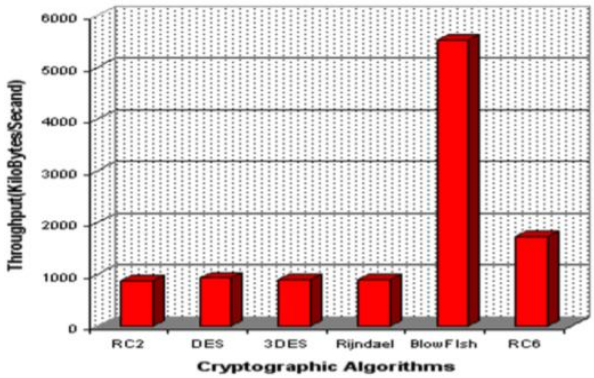


Figure 10: Throughput of each encryption algorithm (Kilobytes/Second)

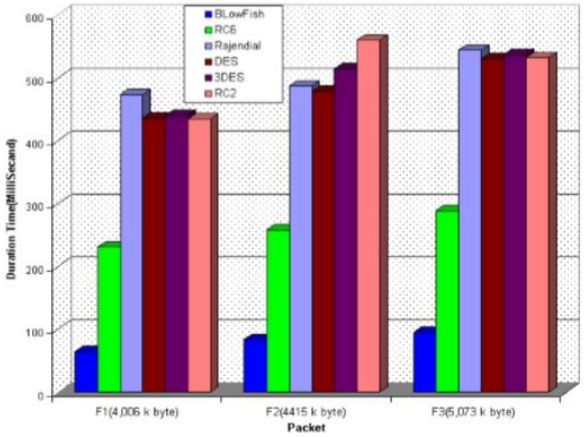


Figure 11: Time consumption for encrypt different video files

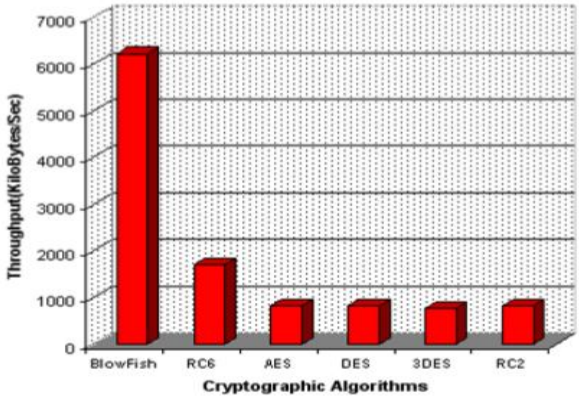


Figure 12: Throughput of each decryption algorithm (Kilobytes/Second)

CPU Work Load Experimental results for this compassion point are shown Figure 13.

From the results we found the result as the same as in encryption process for video and audio files.

4.5 The Effect of Changing Key Size of AES, And RC6 on Power Consumption

The last performance comparison point is changing different key sizes for AES and RC6 algorithm. In case of AES, we consider the three different key sizes possible i.e., 128- bit, 192-bit and 256-bit keys. The Experimental results are shown in Figures 14 and 15. 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-bit key to 192-bit causes increase in power and time consumption about 8% and to 256-bit key causes an increase of 16% [8]. Also in case of RC6, we consider the three different key

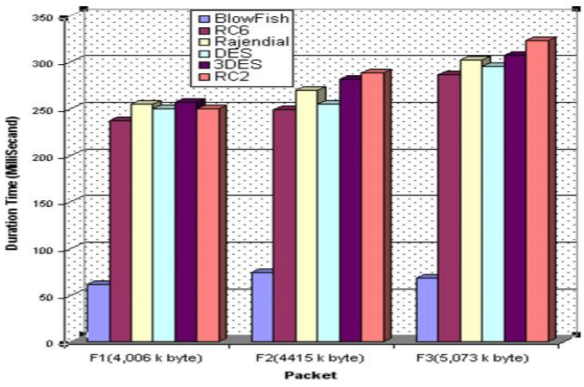


Figure 13: Time consumption for decrypt different video files

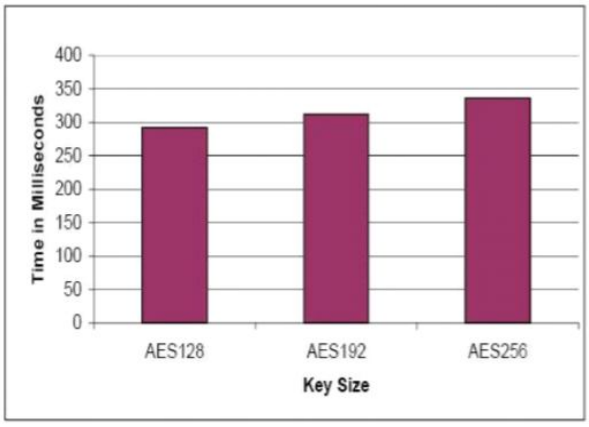


Figure 14: Time consumption for different key size for AES

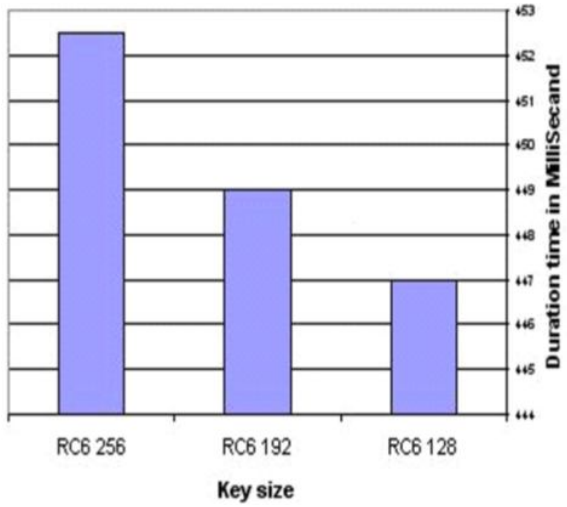


Figure 15: Time consumption for different key size for RC6

sizes possible i.e., 128-bit, 192-bit and 256-bit keys. The result is close to the one shown in the following figure: In case of RC6 it can be seen that higher key size leads to clear change in the battery and time consumption.

5. CONCLUSION

This paper presents a performance evaluation of selected symmetric encryption algorithms. The selected algo- rithms are AES, DES, 3DES, RC6, Blowfish and RC2. Several points can be concluded from the Experimental results. Firstly; there is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding. Secondly; in the case of changing packet size, it was concluded that Blowfish has better per- formance than other common encryption algorithms used, followed by RC6. Thirdly; we find that 3DES still has low performance compared to algorithm DES. Fourthly; we find RC2, has disadvantage over all other algorithms in terms of time consumption. Fifthly; we find AES has bet- ter performance than RC2, DES, and 3DES. In the case of audio and video files we found the result as the same as in text and document. 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.

REFERENCE:

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. 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

12. "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP. 84- 89.

13. 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.

14. W. S. Elkilani, H. m. Abdul-Kader, "Performance of Encryption Techniques for Real Time Video Streaming, IBIMA Conference, Jan 2009, PP 1846-1850

15. "Shared vs. Open authentication method", Retrieved October25,2008,http://www.startawisp.com/index2.php?option=com_content&do_pdf =1&id=147.