Study and Analysis of Energy and Time Characteristics of Node in Wireless Sensor Network

Pragati Narayan Patil [a] , Dr. A. D. Raut[a*]

[a]Tulsiramji Gaikwad-Patil College of Engineering & Technology, Nagpur-441108, India

P.R. Pote College of Engineering and Management, 444602

ABSTRACT

Historically, information security in the form of secrecy, integrity, and authentication is applicable for any personal computer systems and information dissemination networks. Domains of the networking technologies and security requirements are complex these days. Wireless sensor network depicts a new computing class consisting of large numbers of resource-constrained nodes which are often embedded in their operating environments, distributed over wide geographic areas, or located in remote and largely inaccessible regions also faces the security problem.

Lots of security solutions has been made available for wired networks which can also be used for wireless networks, but because of low form factor properties of wireless nodes which are also mobile, it is infeasible to deploy the complex security solutions for wireless networks. In WSNs, challenges such as wireless nature, low battery power and mobility are prime reasons why we are not able to deploy complex security solutions. Hence it is important to study, design and analyse security solutions for this kind of networks.

Therefore, the concept of Cryptography Assistant is introduced, which is a highly powered device compared to sensor node. The crypto assistant node is capable of implementing high end cryptography algorithm. This paper mainly focused on energy and time trade-off of encryption algorithms and files communication. Based on the trade-off it can be decided whether encryption can be done by powerful assistant node or by mobile node itself. The algorithms used for implementation are Symmetric algorithm (AES), Asymmetric algorithm (RSA) & Message digest (SHA 512).

The results have proved that to make use of cryptography Assistant node for the encoding of information as it consumes less energy and time for encryption.

Keywords: *AES; Cryptography Assistant; RSA; SHA; WSN*

DOI Number: 10.14704/nq.2022.20.9.NQ44213 **Neuro Quantology 2022; 20(9):1840-1848**

1. Introduction

A wireless sensor network (WSN) comprises hundreds or thousands of networked sensor nodes. These sensor nodes are battery-constrained, and have limited computational capacity. They consist of many functions for monitoring a wide variety of surrounding conditions and collecting high-precision data, including light, humidity, temperature, magnet, acoustic, pressure and voice level information. Since sensor nodes are low-cost and tiny, a sensor network comprises hundreds to several thousand of small sensor nodes scattered throughout an area of interest [1]. Because WSN applications require long system lifetimes and fault tolerance, energy usage must be carefully monitored.

Reducing power consumption and achieving efficient power savings are essential in sensor networks. The data encryption is limited at the power supply therefore, WSN security issue is the main focused in this paper.

2. Literature Survey

[2] In this paper the main intention of the researcher is to reduce energy consumption. Mostly energy gets consumed during communication in the network whereas the sensor nodes have battery constraints. In this paper improved method is discussed for cluster head selection. [3] This paper has focused on

improving energy consumption of the network by clustering techniques and LEACH protocol. [4] Author has given comprehensive review of Data Mining techniques which can be used in WSN to reduce energy consumption of nodes. [5] Since the transmission as well as reception range of network is limited, the author has discussed routing protocols briefly. [6] The sensor nodes are resource constraints in nature therefore to increase life time of the wireless sensor network has always become a challenge. Many cryptographic methods are there to enhance the security of the network. In this paper, FlexCrypt scheme is presented which talks about mobility of sensor nodes. [7] Collection of Data from the network is also a big challenge in WSN. Since Sensor nodes are having limited battery support. In this paper cluster based data aggregation technique is discussed by the author. [8] Node scheduling and optimization of routing methods are the mostly used by many researchers to improve the energy consumption of sensor nodes. In this paper along with the aforementioned concept, uneven cluster in the network are formed.

3. Proposed Work

3.1 Motivation

There is a tremendous need of security for wireless communication, data sent by mobile phones. Mobile Phones have battery constraint, there by can't support high end cryptographic algorithm, therefore introducing concept of "**Cryptographic Assistant**", with assumption that vicinity area is safer than public area.

3.2 Scope of Research

This paper concentrates on evaluating the performance of encryption schemes in terms of the time and energy consumed when implemented at the application layer through standard encryption libraries on wireless devices.

The research work has been divided into following tasks to achieve this goal.

1. Gain knowledge and understanding of security of information systems.

2. Study the performance and energy consumption of popular symmetric key schemes such as AES, Asymmetric Schemes as RSA and Hashing Algorithm as SHA.

3. Study the effect of changing key size for AES and RSA.

4. Study the effect of file transmission and reception.

3.3 Need of Cryptography Assistant

Generally higher security is achieved by using larger key sizes and stronger encryption algorithms. The higher security algorithms come at the cost of increased computational time and energy consumption. But the battery power available on wireless device is limited so, introduced the concept of Cryptography Assistant which is assumed to be highly powered device. This Cryptography Assistant able to implement heavy cryptography algorithms and provide a secure wireless communication.

3.4 Features

a. Secure Cryptosystem:

Cryptography Assistant uses high end cryptography algorithm, there by provide more security.

b. Fast Cryptosystem:

Compared to sensor node, cryptography assistant provides fastest service in term of time and energy consumption.

c. Confidentiality & Authentication:

The designed system maintains confidentiality and data authentication using symmetric and asymmetric cryptography.

d. Integrity:

The designed system also supports message integrity by implementing SHA algorithm.

4. Research Methodology

The programming logic is discussed for AES, RSA, & SHA.

4.1. AES

The class used is AESFastEngine which extends java.lang.Object and implements BlockCipher.

Following are the methods used for AES

–getAlgorithmName() : Return the name of the algorithm the cipher implements

–getBlockSize() : Return the block size for this cipher (in bytes).

–init
(boolean forEncryption, CipherParameters para ms) : initialise an AES cipher.

–processBlock(byte[] in,int inOff,byte[] out,int o utOff) : Process one block of input from the array in and write it to the out array.

–reset(): Reset the cipher.

4.2. RSA

RSA algorithm extends java.lang.Object and implements AsymmetricBlockCipher, this does basic RSA algorithm. Following are the methods used for the implementation of RSA
–getInputBlockSize(): Return the maximum size for an input block to this engine. For RSA this is always one byte less than the key size on encryption, and the same length as the key size on decryption.

-getOutputBlockSize(): Return the maximum size for an output block to this engine. For RSA this is always one byte less than the key size on decryption, and the same length as the key size on encryption.

-init(boolean forEncryption, CipherParameters param) : initialise the RSA engine.

-Parameters: forEncryption - true if we are encrypting, false otherwise.

-param - the necessary RSA key parameters.

-processBlock(byte[] in,int inOff,int inLen) : Process a single block using the basic RSA algorithm. Parameters: in - the input array. inOff - the offset into the input buffer where the data starts. inLen - the length of the data to be processed.

-Returns: the result of the RSA process. Throws:DataLengthException - the input block is too large.

4.3 SHA 512

Below are the constructors used in program.

1. -public SHA512Digest() : Standard constructor

2. -public SHA512Digest(SHA512Digest t) : Copy constructor. This will copy the state of the provided message digest.

Following are the methods used in SHA.

-getAlgorithmName: return the algorithm name

-getDigestSize: Returns the size, in bytes, of the digest produced by this message digest.

-doFinal: producing the final digest value. The doFinal call leaves the digest reset. Parameters: out - the array the digest is to be copied into.outOff - the offset into the out array the digest is to start at.

-reset: reset the chaining variables.

5. Experimental Setup

5.1 Architecture and Design of Cryptography Assistant

Below diagram represents actual experimental design for mobile and cryptography assistant node. The mobile phone is considered to be a sensor node having less computational power, minimum storage etc. Laptop is assumed to be a Cryptography Assistant node, a high-powered device. Sensor node is having 396 MHz processor speed, whereas cryptography assistant works on 1.83 GHz. Sensor node provide the storage capacity is of 128MB and cryptography assistant having 2GB of memory. For the implementation, JAVA programming language is used as sensor node is java enabled device. The sensor node sends data or file to cryptography assistant node using Bluetooth technology. Once data received by cryptography assistant node, then encryption will take place using the algorithm specification sent by sensor node. After successful encryption cryptography assistant send encrypted data to sensor node.

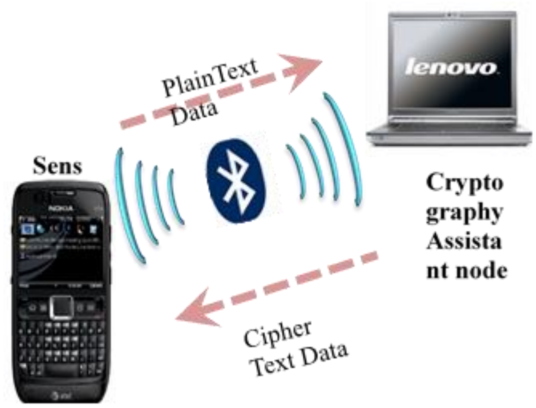

Figure 1. Experimental design of Cryptography Assistant

6. Implementation

At the time of implementation, we used NOKIA E71 as sensor node with S60 3rd Edition, Feature Pack 1, Symbian OS v9.2, speed of the processor is 369MHz with CPU ARM11 is used.

The battery type is Li-Po and memory storage are 120MB. It is JAVA MIDP 2.0 and Bluetooth v2.0 with A2DP supportable. For the energy calculation, we made use of Nokia Energy Profiler. As cryptography assistant we used LENOVO model name: 7757 9QQ, Memory (RAM) Size 2GB and the processor is Intel(R) Core 2 Duo with 1.83 GHz speed. The software used are Net beans 6.8, JAVA jdk 1.6.0.

6.1 System Architecture Diagram for Mobile side Encryption

In this module, three algorithms are implemented:

1. AES Key Size 256, 512 bit
2. RSA Key Size 1024, 2048 bit
3. SHA 512 bit

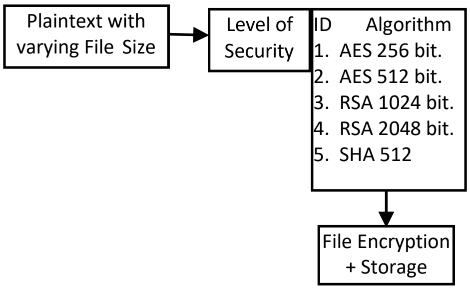

Figure 2. System Architecture Diagram for Mobile side Encryption

Mobile can browse any random size file from the its storage and also select the level of security. The algorithm name and its key size details come under level of security. With the help of provided information, mobile do encryption and forward that file to another node.

6.2 System Architecture Diagram for File Transmission from Mobile Node to Cryptography Assistant

Before file transmission, authentication of device has to be done. Mobile Node and Cryptography Assistant connected with each other using Bluetooth technology. So, first step is to open Bluetooth connection on both sides, after that the device authentication has been performed. Once it is authenticated then they go to connection establishment phase.

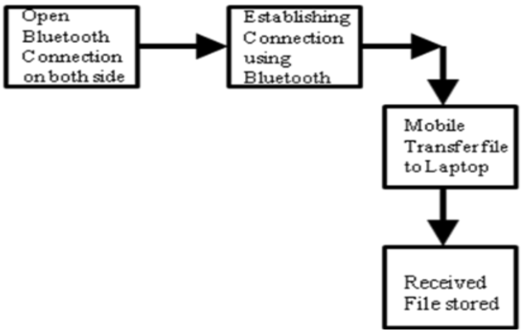

Figure 3. System Architecture Diagram for File Transmission from Mobile Node to Cryptography Assistant

Now, mobile node will send file of varying size to cryptography Assistant, once the file received, it will get stored on cryptography assistant disk. The purpose of this module is to find out, what time and energy mobile node consumed at the time of file transmission. For the experimental purposes following file size has been used: 50KB, 100KB, 500KB, 1MB, 3MB, 5MB, 10MB, 30MB.

6.3 System Architecture Diagram for File Reception from Laptop to Mobile

Before file reception, authentication of device has to be done. Mobile Node and Cryptography Assistant connected with each other using Bluetooth technology. So, first step is to open Bluetooth connection on both sides, after that the device authentication has been performed. Once it is authenticated then they go to connection establishment phase.

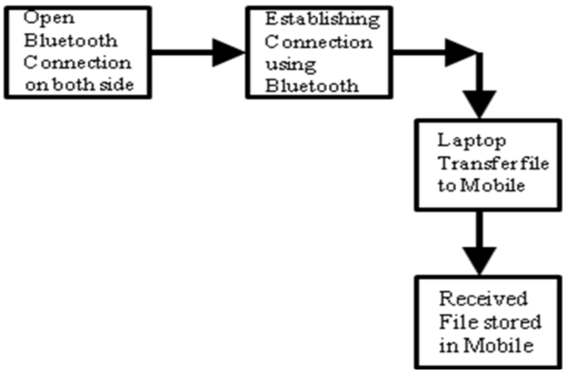

Figure 4. System Architecture Diagram for File Reception from Laptop to Mobile

Now, Cryptography Assistant will send file of varying size to mobile node, once the file received, it will get stored on mobile node disk.

The purpose of this module is to find out, what time and energy mobile node consumed at the time of file reception. For the experimental purposes following file size has been used: 50KB, 100KB, 500KB, 1MB, 3MB, 5MB, 10MB, 30MB.

6.4 System Architecture Diagram for Cryptography Assistant

Input to cryptography assistant is file with varying sizes. Based on the information given by mobile node, crypto assistant will go for encryption of a file.

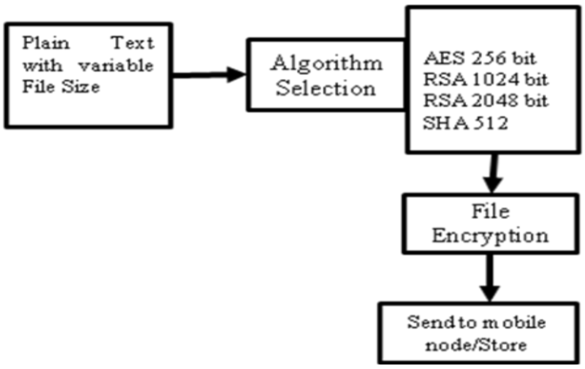

Figure 5. System Architecture Diagram for Encryption on Cryptography Assistant

After file encryption that ciphered file send back to mobile node and same copy is also stored on assistant node.

7. Experimental Results

7.1 Time Analysis of AES 256,512 bit

The below graph is used for the analysis of AES, RSA, and SHA algorithms in term of Time and Energy consumed by mobile node at the time of encryption. The results have been taken with the variation of file size from 50 KB to 30 MB.

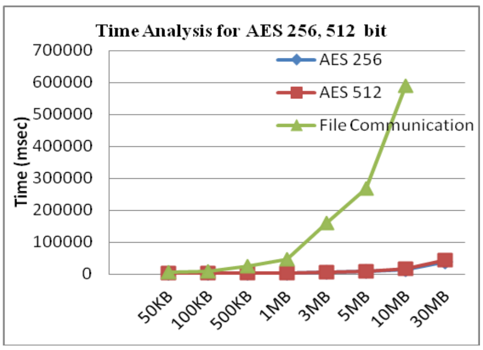

Figure 6. Time Analysis of AES 256,512 bit

The graph depicts that the time taken by AES 256 bit to produce cipher text is less than AES512 bit. File communication is a combination of time required to send and received a file. So, from the above analysis it's clear that the mobile node is enough capable to do encryption on itself. Therefore, in this case mobile node will not take help of cryptography assistant in case of AES.

7.2 Energy Analysis of AES 256,512 bit

The energy readings are recorded with the help of Nokia Energy Profiler Tool. The energy readings are noted down for AES 256 bit, AES 512 bit and for File Communication. The graph comparison shows that, AES 256bit consumed least energy as compared to AES 512 bit and file communication respectively.

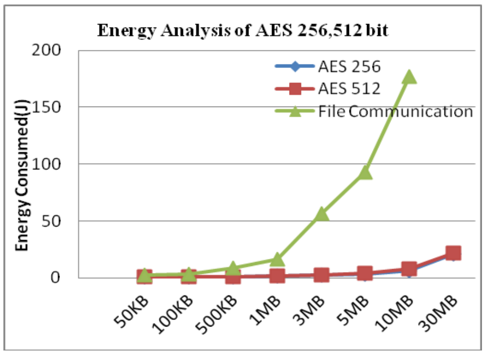

Figure 7. Energy Analysis of AES 256,512 bit

As energy consumption of File Communication is much more than AES 256, 512bit, so it will be better if mobile node will do encryption at his own level.

7.3 Time Analysis of RSA 1024, 2048 bit

The figure depicts analysis for RSA algorithm with key size 1024 and 2048bit. The time consumed by mobile node for RSA 1024 is less as compared to RSA 2048 bit and file communication. From 100KB onwards the time consumption of RSA 2048 bit is much more as compared to File Communication time.

Therefore, in that case mobile node will send data to cryptography assistant and get it encrypted. After encryption, cryptography assistant will send that encrypted data to mobile node. Above analysis shows that, in case for RSA 2048 bit, it's better to take help of cryptography assistant.

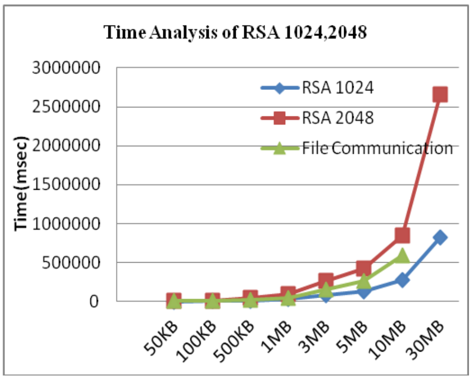

Figure 8. Time Analysis of RSA 1024, 2048 bit

7.4 Energy Analysis of RSA 1024, 2048 bit

The graph shows energy analysis for RSA 1024 and 2048 bit. The energy consumption for file communication with varying file sizes of 50 KB to 30 MB is less as compared to RSA 2048 bit. The RSA 1024 bit, consumed takes less time and energy for doing encryption with the file variation compared to RSA 2048 bit.

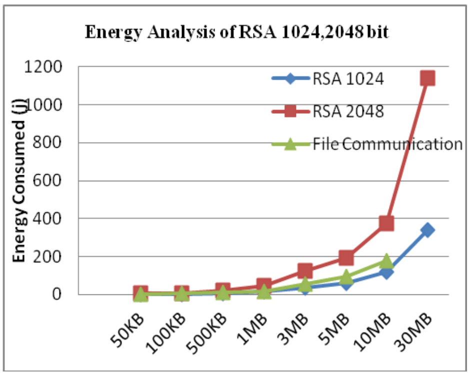

Figure 9. Energy Analysis of RSA 1024, 2048 bit

Therefore, it's clear from above analysis that files RSA 2048bit algorithm can take help of cryptography assistant for doing encryption.

7.5 Time Analysis of SHA 512

The following fig. depicts the usage of time for SHA 512 and File Communication resp. The analysis has been shown for 50KB to 30MB files sizes and their comparison is evaluated.

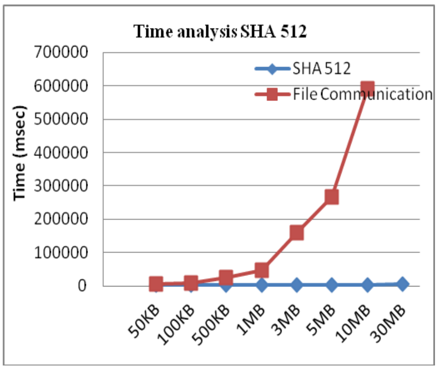

Figure 10. Time Analysis of SHA 512

SHA 512 consumed less time for file encryption.

7.6 Energy Analysis of SHA 512

The energy consumption for SHA 512 is very less as compared to file communication.

Therefore, the mobile node itself is capable to do message digesting because it consumed minimum energy.

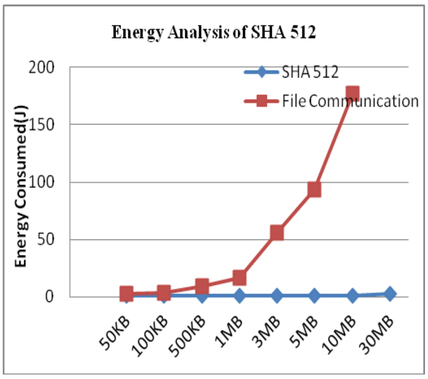

Figure 11. Energy Analysis of SHA 512

7.7 Time Analysis for File transmission and reception

Following graph represents time required to transmit and receive a file. The analysis shows that time taken from transmission is greater than reception of a file.

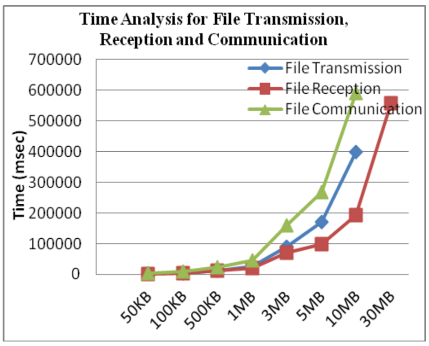

Figure 12. Time Analysis for File transmission and reception

7.8 Energy Analysis for File transmission and reception

The time and energy cost to transmit a file is more as compared to receiving a file. The same analysis has been done for file communication which represents overall communication cost in term of time and energy.

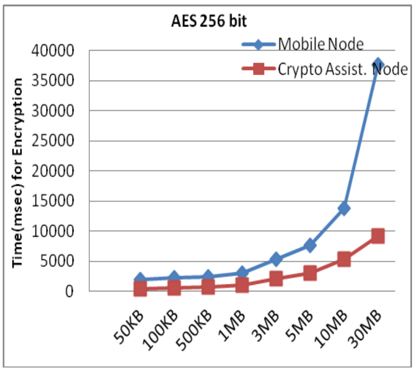

Figure 13. Energy Analysis for File transmission and reception

7.9 Time Comparison between Mobile and Crypto Assistant Node using AES algorithm

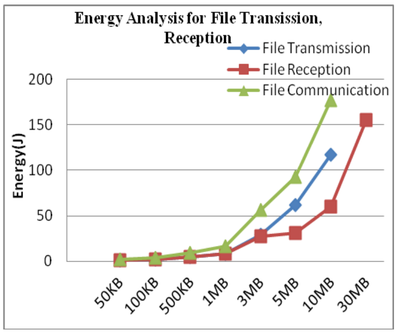

Figure 14. Time analysis for mobile and Crypto Assist node

The above graph depicts time taken by mobile node and crypto assist node. With the variation of file size and using AES 256bit algorithm, it shows that time required for crypto assistant node is comparatively much less than mobile node.

7.10 Time Comparison between Mobile and Crypto Assistant Node using RSA Algorithm

RSA 1024 and 2048 bit implementation on mobile and crypto assistant node is shown in the graph. The time required for different files encryption is very less compared to mobile node. And therefore, it better to use crypto assistant node when the key size is 2048 bit and above, in an order to provide strong security to information.

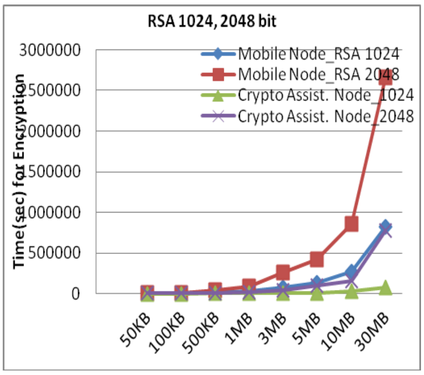

Figure 15. Time analysis for mobile and Crypto Assist node using RSA

7.11 Time Comparison between Mobile and Crypto Assistant Node using SHA Algorithm

The comparative graph of mobile and crypto assist node shows that, time analysis for different file sizes using SHA 512 algorithm. The time taken for encryption of file on mobile node side is much more than crypto assistant node.

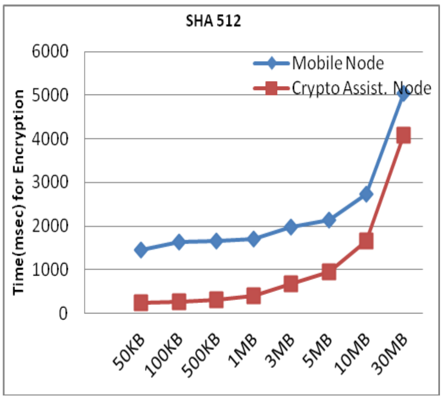

Figure 16. Time analysis for mobile and Crypto Assist node using SHA

8. Conclusion

The innovative concept of "Cryptography Assistant" is introduced in this paper. The analysis shows that SHA consumed least time and energy as compared to symmetric and asymmetric algorithms. The energy and time cost of asymmetric algorithms is much more because its dependent on the key size, while that of symmetric algorithms is not significantly affected by the key size. The energy and time consumption of a symmetric algorithm depends not only on the bulk data encryption/decryption cost but also on the key set-up cost.

From the graphs it's clear that the time and energy consumed by RSA 2048 is more than file communication costs. Therefore, when mobile node wishes to use RSA 2048bit algorithm to provide strong security then, it can take help of Cryptography Assistant. For SHA 512 and AES 256, 512bit, the sensor node is enough capable for doing encryption at their level itself.

The result of Crypto Assistant shows that, the time required for encryption on Crypto Assistant node is very less as compared to mobile node.

The other cryptographic algorithm can also be used to measure their performance on sensor node & cryptography assistant. Using same concept, RSA 4096 bit and AES 1024 bit can also be performed which predictably need a help of cryptography assistant.

Reference

1. Kui Ren, Member, IEEE, Shucheng Yu, Student Member, IEEE, Wenjing Lou, Senior Member, IEEE, and Yanchao Zhang, Member, IEEE, "Multi-User Broadcast Authentication in Wireless Sensor Networks" , in IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 8, OCTOBER 2009, pp. 4554-4564.
2. Mohamed Elshrkawey, Samiha M. Elsherif ⇑ , M. Elsayed Wahed, "An Enhancement Approach for Reducing the Energy Consumption in Wireless Sensor Networks", Journal of King Saud University – Computer and Information Sciences, Available online 7 April 2017
3. K. Praghash , R. Ravi, "Energy Consumption Architecture for Wireless Sensor Networks With Different Clusters", 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)
4. Pragati Patil Bedekar, Atul Raut, and Abhimanyu Dutonde, "Energy Conserving Techniques of Data Mining for Wireless Sensor Networks—A Review", Lecture Notes in Networks and Systems 244 Springer IoT and Analytics for Sensor Networks Proceedings of ICWSNUCA 2021
5. Prof. B.N. Jagdale1 , Prof. Pragati Patil2 , Prof. P. Lahane3 , Prof. D. Javale4, "Analysis and Comparison of Distance Vector, DSDV and AODV Protocol of MANET", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2, March 2012
6. Osama A. Khashan a,* , Rami Ahmad b , Nour M. Khafajah c, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks", Ad Hoc Networks 115 (2021) 102448
7. Bhagyashri Julme(&) and Pragati Patil, "A Review on Clustering Algorithms in Wireless Sensor Networks for Optimal Energy Utilisation", Lecture Notes on Data Engineering and Communications Technologies 33, Springer Intelligent Communication Technologies and Virtual Mobile Networks S. Balaji Álvaro Rocha Yi-Nan Chung Editors ICICV 2019.
8. Yun Xu, Wanguo Jiao * and Mengqiu Tian, "Energy-Efficient Connected-Coverage Scheme in Wireless Sensor Networks", Sensors 2020, 20, 6127; doi:10.3390/s20216127
9. Alexandros Karagiannis1 and Demosthenes Vouyioukas, "A Framework for the Estimation and Validation of Energy Consumption in Wireless Sensor Networks", Hindawi Publishing Corporation Journal of Sensors Volume 2015, Article ID 124987, 13 pages http://dx.doi.org/10.1155/2015/124987
10. Kyung-Ah Shim ; Div. of Math. Modeling, Nat. Inst. for Math. Sci., Daejeon, South Korea ; Cheol-Min Park , "A Secure Data Aggregation Scheme Based On Appropriate Cryptographic Primitives In Heterogeneous Wireless Sensor Networks", in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, 2014, pp. 2128-2139.
11. Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan,and Niraj K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols", in IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 2, FEBRUARY 2006, pp. 128-143.
12. Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz," Security Issues in

Wireless Sensor Networks" INTERNATIONAL JOURNAL OF COMMUNICATIONS Issue 1, Volume 2, 2008, pp.106-115.

13. Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud," Measuring and Reducing Energy Consumption of Cryptographic Schemes for Different Data Types", International Journal of Computer Theory and Engineering, Vol. 1, No. 3, August, 2009 1793-8201, pp. 318-324.
14. Guangyu Chen, Byung-Tae Kang, Mahmut Kandemir, Narayanan Vijaykrishnan, Mary Jane Irwin, and Rajarathnam Chandramouli," Studying Energy Trade Offs in Offloading Computation/Compilation in Java-Enabled Mobile Devices", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 15, NO. 9, SEPTEMBER 2004, pp. 795-809.
15. R.Satheesh Kumar, E.Pradeep, K. Naveen and R. Gunasekaran," A Novel Approach for Enciphering Data of Smaller Bytes", International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010 1793-8201, pp. 654-659.
16. William Stallings, 'Cryptography and Network Security', Prentice Hall Publication,1999
17. Md. Anisur Rahman and Mitu Kumar Debnath," An Energy-Efficient Data Security System for Wireless Sensor Network", in Proceedings of 11th International Conference on Computer and Information Technology (ICCIT 2008), pp.381-386.
18. Shi-Chun Tsai, Wen-Guey Tzeng, and Kun-Yi Zhou," Key Establishment Schemes against Storage-Bounded Adversaries in Wireless Sensor Networks", in IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 3, MARCH 2009, pp. 1218-1222.
19. AES Proposal: Rijndael, Joan Daemaen and Vincent Rijmen, March 9, 1999. The New RSA Factoring Challenge, http://www.rsasecurity.com/rsalabs/challenges/factoring/index.html.