Mody University International Journal of Computing and Engineering Research
Vol. 2 Issue 1, 2018, pp.31-36
ISSN:2456-9607 (Print) 2456-8333 (Online)

Analyzing Energy Consumption by Cryptographic Techniques for Secure Communication in Underwater Wireless Sensor Networks

Sheena Kohli[1], Partha Pratim Bhattacharya[2]

[1]Senior faculty- IT iNurture Education Solutions pvt. ltd. Bangalore
[2]Professor, Department of Electronics and Communication Engineering, Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan-332311

sheena7kohli@gmail.com, hereispartha@gmail.com

Received 1 Feb. 2018, Published 23 Feb. 2018

Abstract: Underwater Wireless Sensor Networks comprise of a spread of acoustic sensors or nodes deployed in a geographical area of interest under the sea or ocean. The nodes on capturing data from the particular region send it to a central processing point. Due to the characteristics of underwater channel, these types of senor networks are vulnerable to malicious attacks. Being battery powered, energy is an important and critical factor to be considered for underwater sensor networks, along with maintaining the security of data. This paper aims at analyzing the energy consumed by cryptographic algorithms, applied in routing data in a clustered manner, in this category of wireless sensor networks.

Keywords: Acoustic, asymmetric key cryptography, base station, cluster head, security, sensor node, symmetric key cryptography

1. INTRODUCTION

Underwater Wireless Sensor Networks (UWSNs) are composed of devices, called sensors or underwater vehicles that perform synergetic sensing and monitoring tasks in a marine territory and conditions [1]. They focus on connecting a number of tiny acoustic nodes, capable of sensing, detecting or measuring the different parameters of the various ambient activities from the water body. The sensors or nodes after capturing the environmental data, process it and communicate it to another sensor or any other desired point. Figure.1 illustrates the basic arrangement of an Underwater Wireless Senor Network [2].

UWSNs have a vast range of applications including oceanographic data retrieval and collection, pollution monitoring, offshore exploration, sea surveillance, disaster and natural calamity detection etc. [1].

2. SECURITY IN UNDERWATER WIRELESS SENSOR NETWORKS

There are many origins of underwater obstruction in communication between nodes like bounded bandwidth, multi-path propagation, end-to-end propagation delays, more data error rates, provisionary connection losses and limited battery power. An underwater channel can be slivered easily during data transmission and reception. Due to this reason, UWSNs are sensitive and accessible to various attacks [3].

Reliability and enervation of underwater communication link is greatly affected by the environment. Changes in pressure, salinity, ocean currents, wind speed, marine life etc. effects link reliability. An underwater sensor network may get deteriorate by either environment naturally or by the intended attacks. The protocols decide the behavior of networking. Causing damage to an underwater network protocol will break the network from operating. Authentication, confidentiality and integrity are the aims of introducing security measures in the Underwater Wireless Sensor Networks.

Because of the special and different characteristics of underwater channels and limitations, UWSNs are liable and weak to malicious attacks. Moreover, energy harvesting is almost unavailable in the ocean [4]; therefore, optimizing the amount of energy used for data transmission becomes an important issue underwater communication. More efficient routing protocols in underwater networks should be developed to ensure reliable data delivery while

optimizing energy consumption. On the same hand, it is also necessary to apply useful cryptographic techniques in the communication channel in Underwater Wireless Sensor Networks.

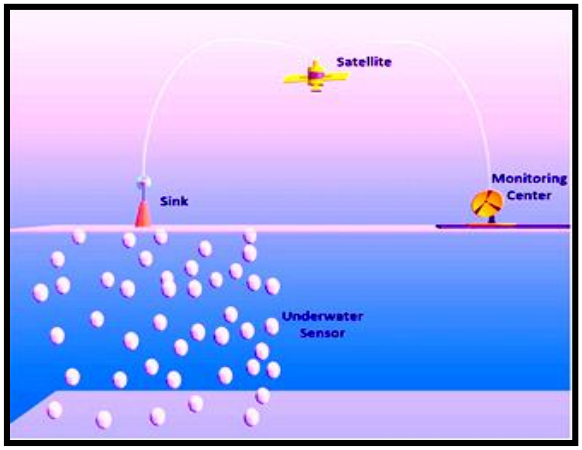

Fig. 1: Basic Arrangement of an Underwater Wireless Sensor Network

3. ROUTING IN UNDERWATER WIRELESS SENSOR NETWORKS

Routing is a way of determining a path between source and destination upon request of data transmission. Ordering sensor nodes into clusters has been widely and wisely selected by researchers to assure the scalability and acquire high energy efficiency to prolong network lifetime in UWSN environments. The hierarchical cluster-based organization of the sensor nodes allows data fusion and aggregation, which saves a lot of energy. Clustering involves hierarchically organizing the network topology. Sensor nodes in cluster architecture are organized into clusters in which a cluster head is elected and a bunch of source sensor nodes are directly connected to it. The cluster head commonly performs the special tasks like (fusion and aggregation) and many general sensor nodes are its members [5]. Figure 2 shows the cluster arrangement in UWSN. When clusters have been formed, the nodes start to transmit the captured data. Cluster heads receive data sent from the other nodes and forward it to the sink after being fused.

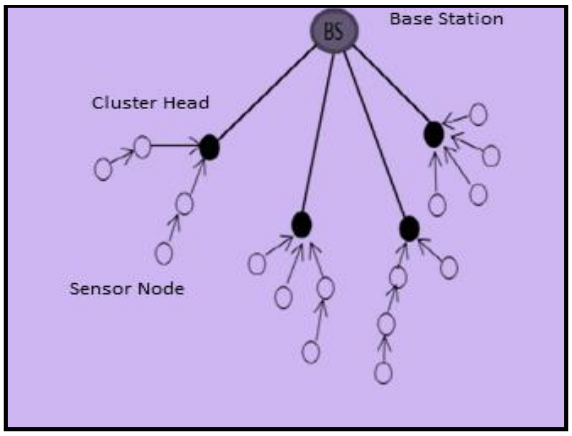

Fig. 2: Clustering in Sensor Networks

4. CRYPTOGRAPHIC TECHNIQUES

Data confidentiality may be served by one of two categories of encryption algorithm, specifically symmetric cryptography and asymmetric cryptography. Symmetric, secret or conventional, cryptography requires that the sender and receiver share a key, which is a component of secret information used to encrypt and decrypt data. Figure 3 shows how symmetric cryptography works.

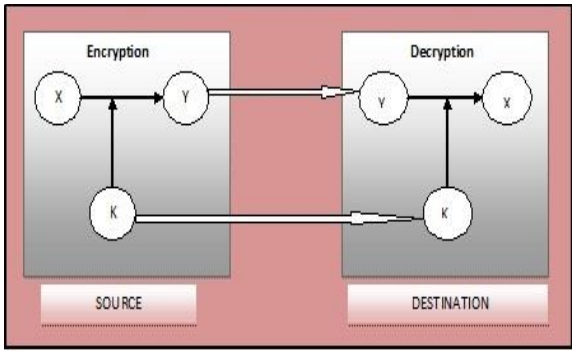

Fig. 3: Symmetric Key Cryptography

Asymmetric, or Public Key, cryptography uses two keys, either of which may be used to encrypt a message. The encrypted data may then only be decrypted by means of the other key [6]. Figure 4 shows how the asymmetric key cryptography works.

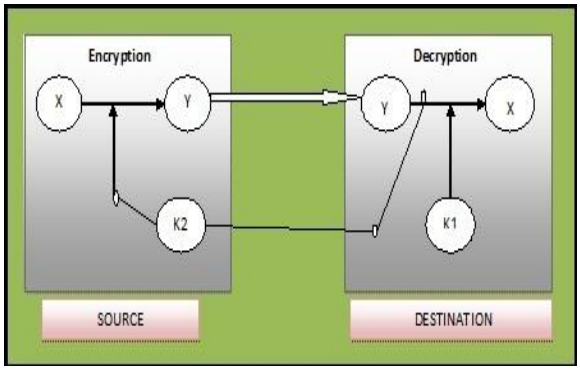

Fig. 4: Asymmetric Key Cryptography

On account of symmetric key cryptography, we have taken Blowfish and Data Encryption Standard (DES), while for asymmetric key cryptography, Rivest - Shamir - Adleman Algorithm (RSA) algorithm has been observed.

Blowfish Algorithm

Blowfish is a symmetric encryption algorithm with flexible length key of up to 448 bits. It encrypts block length of 64 bits at a time [7]. It is a feistel network that does same process for 16 rounds. Encryption is done in two parts - key expansion, where the key is converted into a group of sub keys and data encryption, in which the data is encrypted with the use of sub keys in 16 round network. Each round has a key dependent variation, a key and data dependent exchange. All operations are XORs and additions on 32-bit words. Blowfish uses a large number of sub keys. These keys should be precollated before any data encryption or decryption.

Data Encryption Standard (DES) Algorithm

DES algorithm is designed to encrypt a block of 64 bits data using a key whose length is 64 bit. It is a symmetric algorithm so it uses the same key for decryption [8]. The algorithm goes through 16 iterations that mix blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used for decryption. There are many attacks and methods observed till now that can exploit the weaknesses of DES, but still it is widely used by financial services and other industries worldwide to protect sensitive on-line applications [9].

Rivest-Shamir-Adleman (RSA) Algorithm

In the introductory paper about RSA, the authors [10] suggested a method to implement cryptosystem based on public key whose security is dependent upon the difficulty to factor large prime numbers. This technique makes it possible to encrypt data and to create digital signatures. The encryption scheme uses RSA and signature of the fact that:

$$m^{ed} \equiv m(\text{mod } n) \text{ for m integer}$$

The decryption works because $cd \equiv (m^e)^d \equiv m(\text{mod } n)$. The defense lies in the difficulty of computing a clear text m from a cipher text c and the public parameters n(e).

5. ENERGY CONSUMPTION FOR COMMUNICATION USING CRYPTOGRAPHIC TECHNIQUES

The energy required for communication using the two types of cryptographic techniques in Underwater Wireless Sensor Networks is computed in this paper. The underwater channel takes into various acoustic characteristics in account for communication. The simulations have been performed on MATLAB [11]. The energy calculated is as follows:

In Symmetric or Private Key Cryptography:

At sensor node- Energy is consumed in the following:

- Data Transmission to cluster head
- Transmission of private key to BS

Total Energy = ETransmission + EKeyTransmission
= [l(EElectronic + d1m . Eamplification)
+ Pt .(l/B.h)] + [k(EElectronic
+ d3m . Eamplification) + Pt .(k/B.h)] (1)

At cluster head- Energy is consumed in the following:

- Data Reception from all sensor nodes
- Data transmission to BS

Total Energy = EReception + ETransmission
= [l(EElectronic)+ Pr.(l/B.h)]
+ [l(EElectronic + d1m . Eamplification)
+ Pt .(l/B.h)] (2)

At base station- Energy is consumed in the following:

- Data Reception from cluster head
- Data Decryption
- Reception of Private Key

Total Energy = EReception + EKeyReception
= [l(EElectronic) + Pr.(l/B.h)]
+ [k(EElectronic) + Pr.(k/B.h)] (3)

In Asymmetric or Public Key Cryptography

At sensor node– Energy is consumed in the following:

- Data Transmission to cluster head
- Key Reception at Sensor

Total Energy = ETransmission + EKeyReception
= [l(EElectronic + d1m . Eamplifyication)
+ Pt .(l/B.h)] + [k(EElectronic) + Pr.(k/B.h)] (4)

At cluster head- Energy is consumed in the following:

- Data Reception from all sensor nodes
- Data Transmission to base station

Total Energy = EReception + ETransmission

$$= [l(EElectronic) + Pr.(l/B.h)] + [l(EElectronic + d2m \,.\, Eamplification) + Pt\,.(l/B.h) \quad (5)$$

At base station- Energy is consumed in the following:

- Data Reception from cluster head
- Transmission of public key to sensors

$$\text{Total Energy} = EReception + EKeyTransmission = [l(EElectronic) + Pr.(l/B.h)] + [k(EElectronic + d3m \,.\, Eamplification) + Pt\,.(k/B.h)] \quad (6)$$

The parameters and their values are mentioned in Table1 in the next section. Besides, the communication energy, the other parameters or types of energies which must be considered are: Encryption Energy, Decryption Energy, Data Fusion or Aggregation Energy, Data De-fusion Energy. Encryption and Decryption Energies depend upon the number of clock cycles per bytes (CC/B) used in the process in any cryptographic algorithm. Data Fusion or Aggregation Energy and Data De-fusion Energy is the energy required for compressing and decompressing the data received from different sensors at the cluster head and from cluster head to base station respectively.

6. RESULT AND DISCUSSION

Parameters and Values

All the equations stated in the above section have the following parameters with the following values as shown in Table1.

TABLE I. PARAMETERS AND VALUES

Parameter	Value
d1 (distance between sensor and cluster head) in meters	40m
d2 (distance between cluster head and base station) in meters	60m
d3 (distance between base station and sensor)	100m
l (message) in bits	4000 bits
m (coefficient for multipath fading)	4
ETransmission (data transmission energy) in microJoules	Calculated from equations
EReception (data reception energy) in microJoules	Calculated from equations
EKeyTransmission (energy required for key transmission) in microJoules	Calculated from equations
EKeyReception (energy required for key reception) in microJoules	Calculated from equations
EElectronic (electronic energy of the transmitter/receiver) in microJoules	5microJoules
Eamplification (energy required for amplification) in microJoules	2microJoules
Pt (transmission power) in microWatt	6 x105microW
Pr (reception power) in microWatt	4 x 105microW
B (bandwidth)	4x109microHz
SNR (Signal to Noise Ratio)	20
k (key size) in bits	As per Algorithm

The following are the key sizes of the three algorithms as shown in Table2.

TABLE II. KEY SIZES

Type of Algorithm	Algorithm	Key Size
Symmetric	Blowfish	32 to 448 bits
	DES	64 bits
Asymmetric	RSA	512,768,1024,2048,3072 bits

As of 2003 RSA Security claims that 1024-bit RSA keys are equivalent in strength to 80-bit symmetric keys, 2048-bit RSA keys to 112-bit symmetric keys and 3072-bit RSA keys to 128-bit symmetric keys [12].

Analysis

The paper has given analysis for energy consumption at sensor node, cluster head and base station by using both symmetric and asymmetric cryptography techniques on the basis of equations formed in section 5.

Energy Consumption for Secure Communication using Symmetric Key Cryptography

Energy consumed at sensor node

As shown in equation (1), the energy required for secure communication at the sensor node depends upon data transmission energy and the key transmission energy. On comparing Blowfish and DES algorithm, we observe that the former one consumes less energy at a sensor node. The results are shown in Figure 5.

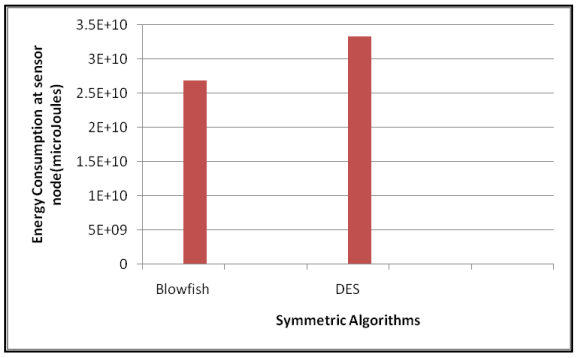

Fig. 5: Energy Consumption at Sensor Node in Symmetric Algorithms

Energy consumed at cluster head

As shown in equation (2), the energy required for secure communication at the cluster head depends upon data reception and transmission energy. Hence, both the symmetric cryptography algorithms consume same amount of energy as depicted in Figure 6.

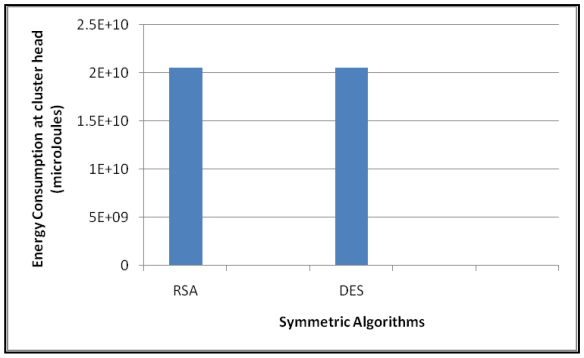

Fig. 6: Energy Consumption at Cluster Head in Symmetric Algorithms

Energy consumed at base station

As shown in equation (3), the energy required for secure communication at the base station depends upon data reception and key reception energy. On comparing Blowfish and DES algorithm, we observe that the former one consumes less energy at base station. The results are shown in Figure 7.

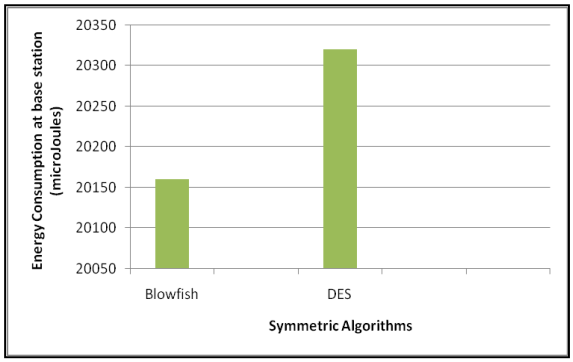

Fig. 7: Energy Consumption at Base Station in Symmetric Algorithms

Energy Consumption for Secure Communication using Asymmetric Key Cryptography

Energy consumed at sensor node

As depicted in equation (4), the computations are same as that of equation (1) for both symmetric and asymmetric cryptographic algorithms. It can be observed in Figure 8 that the RSA algorithm has been taken in two variations with key size as 512 and 1024.

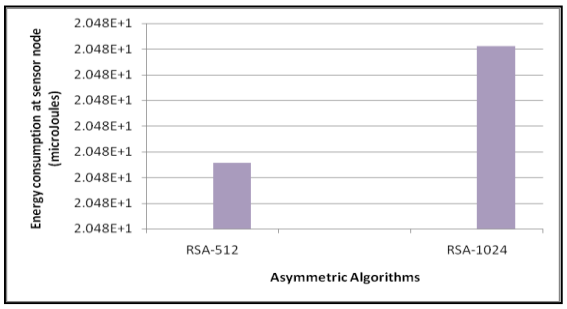

Fig. 8: Energy Consumption at Sensor Node in Asymmetric Algorithms

Energy consumed at cluster head

As shown in equation (5), the energy required for secure communication at the cluster head depends upon data reception and transmission energy. Hence, both the asymmetric cryptography algorithms consume same amount of energy as depicted in Figure 9.

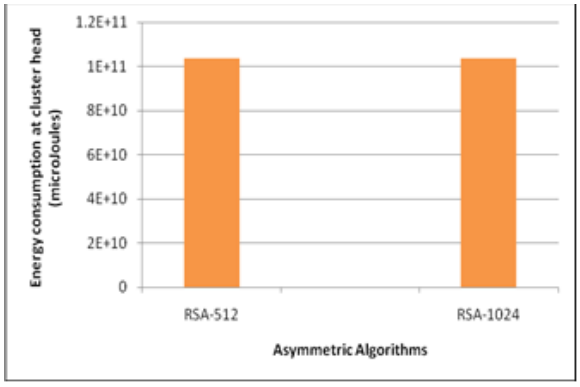

Fig. 9: Energy Consumption at Cluster Head in Asymmetric Algorithms

Energy consumed at base station

As per equation (6), the two variants of RSA algorithm shows difference in energy consumption at the base station due to difference in key size. The results are depicted in Figure 10.

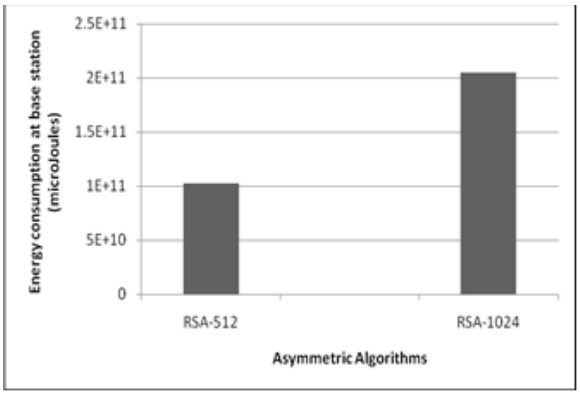

Fig. 10: Energy Consumption at Base Station in Asymmetric Algorithms

Total energy consumption in secure communication in Symmetric and Asymmetric Cryptography Algorithms

The result of total energy consumption made by the Symmetric and Asymmetric Cryptography Algorithms for secure communication in Underwater Sensor Networks depicts that the symmetric algorithms consume less energy as compared to the asymmetric ones. The same has been shown with the help of bar graph in Figure 11.

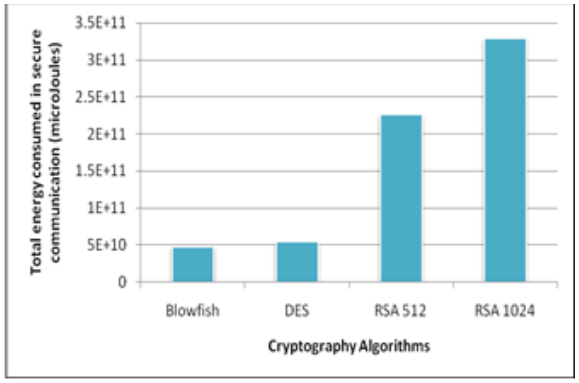

Fig. 11: Total Energy Consumption in Secure Communication in Symmetric and Asymmetric Cryptography Algorithms

7. CONCLUSION

The paper aimed at analyzing the energy consumption by cryptographic algorithms applied in routing data in a clustered manner in underwater wireless sensor networks. The not so convenient environment offers a large number of characteristics, difficulties and needs to be taken care of. One of the needs is that of securing the data while communicating it from one end to another in the wireless network. Another important consideration is that of energy saving routing. We have applied both symmetric and asymmetric cryptographic techniques to the UWSNs and calculated the energy the consume depending upon the key and data transmission and reception at sensors, cluster heads and base stations in the network. The results show that the symmetric key cryptography consumes less energy if Blowfish algorithm is taken in comparison to DES algorithm but RSA algorithm takes more energy in communication, being asymmetric key cryptography algorithm.

REFERENCES

[1] Das Anjana P., Sabu M. Thampi. "Secure communication in mobile underwater wireless sensor networks" International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015, IEEE.

[2] Akyildiz Ian F., Dario Pompili, Tommaso Melodia. "Underwater acoustic sensor networks: research challenges" Ad hoc networks, vol. 3(3), 2005, pp. 257-279.

[3] Kim J. E., Yun N. Y., Muminov S., Park S. H., Yi O. Y. "Security in underwater acoustic sensor network: focus on suitable encryption mechanisms" AsiaSim 2012, pp. 160-168.

[4] Sozer Ethem M., Milica Stojanovic, John G. Proakis. "Underwater acoustic networks" IEEE Journal of Oceanic Engineering, vol. 25(1), 2000, pp. 72-83.

[5] Mamalis Basilis, et al. "Clustering in wireless sensor networks" RFID and Sensor Networks: Architectures, Protocols, Security and Integrations, Y. Zhang, LT Yang, J. Chen, eds, 2009, pp. 324-353.

[6] https://community.jisc.ac.uk/library/advisoryservices/introduction-cryptographic-techniques

[7] G. Guimaraes, E. Souto, D. Sadok and J. Kelner, "Evaluation of security mechanisms in wireless sensor networks" Proceedings Systems Communications, vol. 1(1), 2005, IEEE, pp. 428-433.

[8] G. Padmavathi, D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks" International Journal of Computer Science and Information Security, vol. 4(1-2), 2009, pp.315-321.

[9] M. Marine, C. Raphael, W. Phan. "Energy-efficient cryptographic engineering paradigm" Open Problems in Network Security, vol. 1(1), 2012, Springer, pp.78-88.

[10] R. L. Rivest, A. Shamir, L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems" Communications of the ACM, vol. 21(2), 1978, pp. 120–126.

[11] Desmond J. Higham, Nicholas J. Higham. "MATLAB guide" Siam, 2005.

[12] "RSA Laboratories - TWIRL and RSA Key Size" emc.com. Retrieved September 2016.