ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 4, April 2016

PERFORMANCE ANALYSIS OF SYMMETRIC ENCRYPTION ALGORITHMS FOR ENERGY EFFICIENT TWO TIER SCHEME

N.Deepika[1], Scholar
M.Tech, Wireless Communication,
Electronics and Communication
Engineering PeriyarManiammai University
Thanjavur, India

V.Violet Julie[2],
Assistant Professor,
Department of
Electronics and Communication Engineering
PeriyarManiammai University
Thanjavur, India

***Abstract*-Wireless sensor network have been broadly used in the fields of target detection and tracking, environmental monitoring, industrial process monitoring and tactical systems. Security and energy efficiency are the major concerns in the wireless sensor network (WSN) design. Cryptographic Algorithms are widely used to provide security. This paper, examine the performance of symmetric key cryptographic algorithms applied in wireless sensor networks (WSNs).In order to enhance the security of the existing energy efficient two-tier scheme and to find out the suitable symmetric algorithm, this paper compares the performance of Digital Encryption Standard (DES) and Advanced Encryption Standard (AES) based on some metrics.**

Key words: wireless sensor networks, Security, Cryptography, DES, AES.

1. Introduction

A Wireless Sensor Network is a network that is composed of numerous sensor nodes interconnected by means of wireless medium. The wireless sensors are used in health care, military application, environment application and they are essential in our daily day to day work. Security of the transmitted information plays a vital role in communication. Cryptography plays an important role in network security and it is an art of hiding the information using mathematics to encrypt and decrypt data [1]. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Cryptography Techniques can be broadly classified into two types Symmetric Key Cryptography and Asymmetric Key Cryptography which is shown in the figure 1.

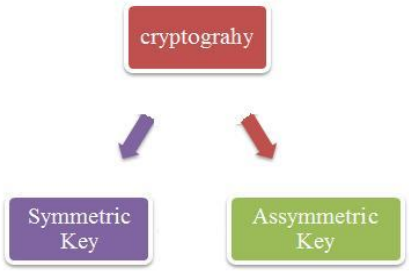

Fig1. Classification of Cryptography

1.1. Symmetric Key Cryptography:

This is also known as single Key, Which uses the same key called private key for the encryption of Plain text and for the decryption of cipher text [2] which is shown in the figure 2. Some of the examples are DES, TDES, Blowfish, IDEA, CAST5, TEA and AES.

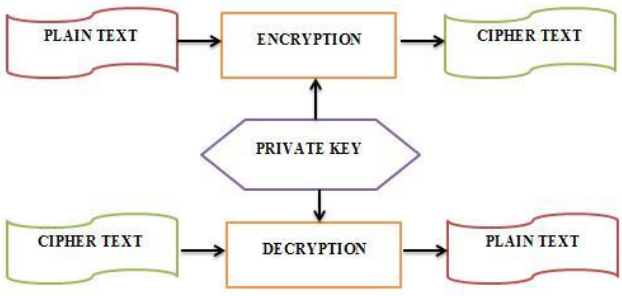

Fig.2. Symmetric Key Algorithm

1.2. Asymmetric Key Cryptography:

This employs two different keys called Public key and Private Key. Public key is meant for the encryption of Plain text and Private key is especially for decryption of the cipher text [2]. The process is shown in the figure 3 given below. Some of the examples are RSA, ELGAMAL, and ECC etc. There are various authors works on these Symmetric and Asymmetric algorithms and are discussed on the following chapter.

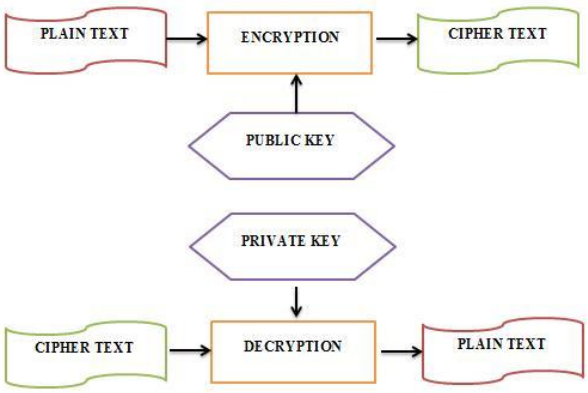

Fig.3. Asymmetric Key Algorithm

2. Related Works

To give more knowledge about the performance of the algorithms, this part discusses the outcome obtained from other authors. [2] Discuss the symmetric algorithms such as AES, DES and Blowfish to find out the best algorithm to use in future.

[3] Presents survey of a number of the newest developments on cryptography algorithms in network security. It also presents survey of a number of the newest developments on cryptography algorithms in network security and additionally presents a number of the solutions for wireless sensor network alongside the results. [4] Author gives an overview of cryptographic frameworks designed so far and also an overview of comparison of existing schemes.

[5] Describes the secret key algorithms DES, 3DES, AES (Rijndael), Blowfish, and they were implemented in Java programming. Their performance was compared by encrypting input files of changeable data sources and sizes. Here the algorithms were implemented and were tested on two different hardware platforms, to present the comparison.

[6] Presented a comparison of AES, DES, 3 DES, RC2, Blowfish and RC6. In this each algorithm uses different settings such as information blocks of varying sizes, data types, battery power consumption, different key size and ultimately encryption and decryption speed. AES shows better performance than RC2, DES, and 3DES.

[7] Provides an analysis between AES along with RC4. This paper concentrates on performance comparison between block ciphers and stream cipher standard. Based on performance metrics such as Encryption time, Decryption time, Throughput, this paper concludes which algorithm is good to use in future.

3. Implementation

This paper compares the popular symmetric algorithms such as DES and AES in NS2 to find out the best algorithm to use for Energy-Efficient Two-Tier Scheme. The scheme is proposed to protect the sensor network by enhancing the security level. This scheme starts with secure topology creation stage followed by sender initiated scheme and finally data transmission. In data transmission session, the data is encrypted via DES and AES. The flow of the proposed scheme is shown in the figure 4.

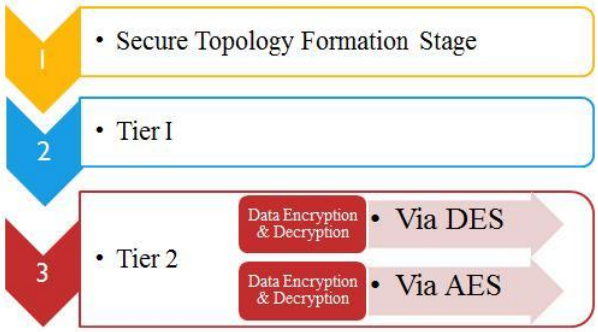

Fig.4. Flow of the Proposed Methodology

3.1. Secure Topology Creation Stage:

This stage involves four phases (1) Finding the attacker, (2) Grouping of clusters, (3) Distribution of key and (4) Renewal of key. In the preliminary stage we construct a clustering topology having a secrete key shared by cluster heads and their members. Based on this, an enhanced two tier scheme is designed to transmit the data quickly and securely.

Phase 1: Finding the attacker

In the phase 1, the sensor node detects the anti-node by broadcasting hello message encrypted by a pre distributed key, to every node in the network. Those nodes which cannot decrypt the message correctly, then the sender is said to be an attacker. This phase is to protect the WSN from the external attacks.

Phase 2: Grouping of clusters

Adaptive Distributed Topology Control Algorithm (ADTCA) algorithm [8] is used to partition the clusters and to form groups. In this phase cluster head selection and gateway selection is performed. After applying this algorithm, there are three different types of sensors (1) cluster heads (2) sensor nodes with assigned cluster ID (3) nodes without cluster ID. Gateway key is to interconnect the two adjacent clusters. One cluster member from each group becomes gateway. The distribution of cluster key and gateway key is shown in the figure 5.

Phase 3: Distribution of keys

A pre-distributed key encrypts the cluster key and gateway key and distributes them locally. Cluster key is mainly meant for the security of broadcast messages. The gateway key and the cluster key provides the security of inter –cluster communication and intra-cluster communication respectively.

Phase 4: Renewal of keys

When the same encryption key is used for long period it is easy for the adversary in getting the keys. Hence key renewal is necessary

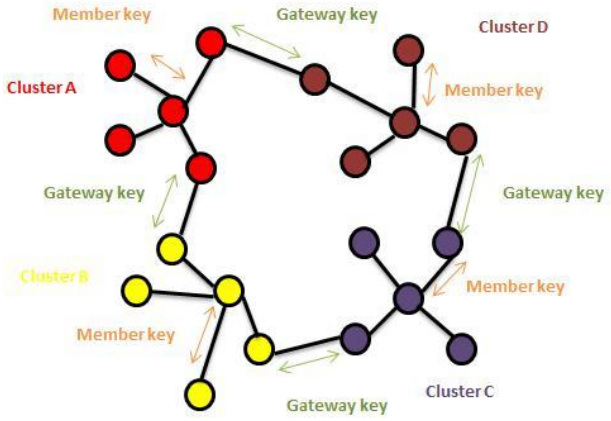

Fig.5. Distribution of keys

After this stage, the cluster head and its members share a common secrete key for the security of broadcast messages. Based on this secure topology, an enhanced secure two-tier scheme is proposed to transmit the information quickly and securely.

3.2. Tier 1: Agreement of Session key

This section describes cross layer design integrating the MAC protocol.

Using the cluster key C_k, a hash chain is created to provide symmetric encryption key and for mutual authentication. C_k is a shared secrete key between cluster head and its members. The agreement of session key for the sender initiated scheme is shown in the figure 6. The explained implementation of this stage is given below,

Sender-Initiated Scheme:

The initiator of the scheme depends on the design and here the sender starts the process.

Step1: The sender computes the secure token from the random number S_r.

Step2: Then sender sends the secure token, random number S_r, its ID (ID_s) and receiver ID (ID_r) as the preamble.

Step3: Receiver receives and validates the secure token. If the received token is not valid it goes back to sleep. If it is valid, the receiver computes the session key $S_k = h(C_k|S_r|R_r)$ from the randomly selected number R_r. It also computes $h(S_k)$ and $h(h(S_k))$.

Step4: The receiver sends $h(h(S_k))$ and R_r as the acknowledgement.

Step5: The sender computes the hash chain $h(S_k)$, $h(h(S_k))$ and the session key $S_k = h(C_k|S_r|R_r)$. If not valid the data will not be sending to the receiver.

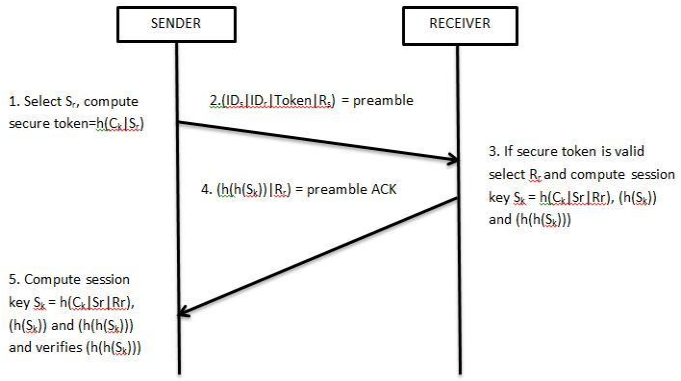

Fig.6. Sender-Initiated Scheme

Therefore the mutual authentication is obtained from the hash chain ($h(S_k)$) and ($h(h(S_k))$). The dynamic session key agreement is reached by the sender and receiver. In this tier, a session key is created and exchanges of data packets are performed in the following section.

After the preamble ACK is received in the step 5, the sender and receiver are considered as time synchronized.

3.3 Tier 2: Transmission of Data

The sender encrypts the data with the newly created session key S_k by symmetric encryption algorithms AES and DES. The data transmission is implemented and is shown in the figure 7.

Step 1: The sender sends the $E_{Sk}(DATA|MAC_{Sk}(DATA))$ and $h(S_k)$ to the receiver where $E_{Sk}(y)$ denotes encryption of y by using symmetric key S_k, DATA is the input message and $MAC_{Sk}(DATA)$ is the message authentication function.

Step 2: The receiver verifies $h(S_k)$ and if $h(S_k)$ is not valid, it enters into sleep mode. If $h(S_k)$ is valid , it decrypts the data from sender and verifies the MAC of the data.

Step 3: Finally the receiver sends ACK to the sender.

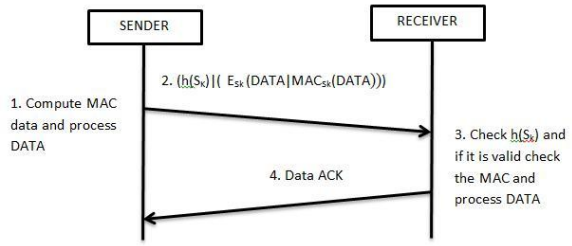

Fig.7. Transmission of Data

The hash chain $h(S_k)$ and $h(h(S_k))$ provide the mutual authentication between sender and receiver. The results obtained for the proposed scheme is given in the following section.

4. Simulation Results

These proposed symmetric algorithms are simulated using NS_2 and their performance is compared in terms of Energy consumption, Encryption time and Decryption time. The parameters required for this simulation is shown in the Table 1.

Table.1. Simulation parameters

parameter	value
Simulation area size	500m x 500m
Number of nodes	37
channel	Wireless
Antenna	Omni-directional
Propagation	Two Ray ground
Simulation time	100s
Traffic source type	TCP

The comparison performance of the DES with that of the AES obtained from the simulation is shown in the graphs given below. Fig 8 shows the graph of encryption time of DES algorithm against 10-80 milliseconds of simulation time where x-axis shows the simulation time (sec) and y-axis shows the encryption time (ms).

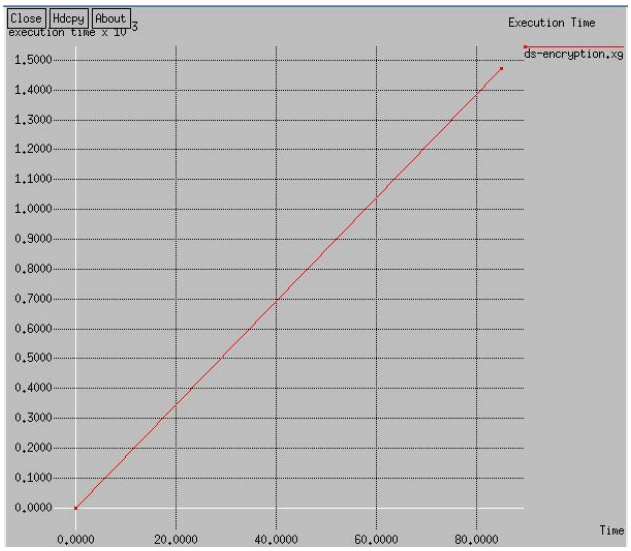

Fig.8. Encryption Time of DES algorithm

Fig 9 shows the graph of encryption time of AES algorithm against 10-80 milliseconds of simulation time where x-axis shows the simulation time (sec) and y-axis shows the encryption time (ms).

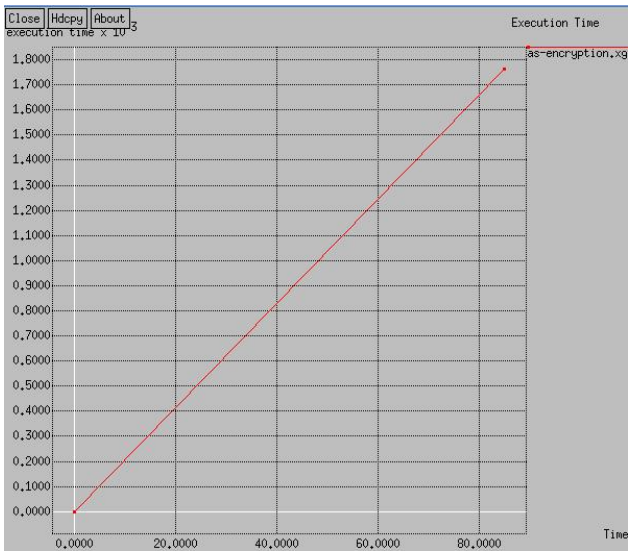

Fig.9. Encryption Time of AES algorithm

On comparing the encryption time of these two graphs, DES takes lesser time than AES to encrypt the same text file of 512bytes.

Fig 10 shows the graph of Decryption time of DES algorithm against 10-80 milliseconds of simulation time where x-axis shows the simulation time (sec) and y-axis shows the encryption time (ms).

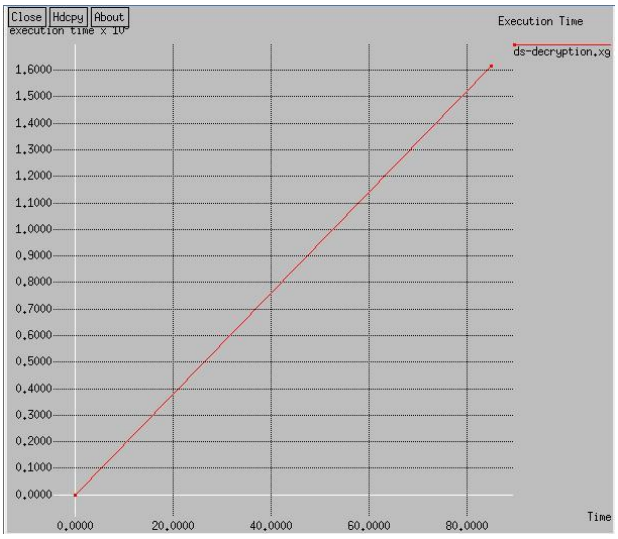

Fig.10. Decryption Time of DES algorithm

Fig 11 shows the graph of Decryption time of DES algorithm against 10-80 milliseconds of simulation time where x-axis shows the simulation time (sec) and y-axis shows the encryption time (ms).

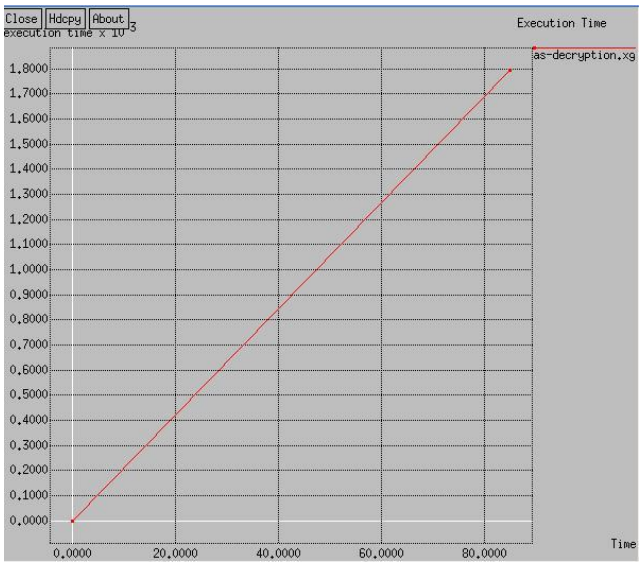

Fig.11. Decryption Time of AES algorithm

Same as that of previous case, the time taken for decrypting the same file of 512bytes DES consumes lesser time than AES.

5. Conclusion

In order to give protection to the intended data from hacking, cryptography is performed. In this paper we briefly discussed about cryptography and various symmetric algorithms. This algorithm performs encryption and decryption on vital data in wireless sensor networks. This paper compares the performance of the symmetric algorithms DES and AES in terms of Encryption and Decryption. And the results show that the DES is better for encryption and decryption of two tier energy efficient scheme than AES. This paper can be used to enhance the security features of the existing energy efficient two tier scheme. In future, we will work on employing the same comparisons for other duty cycling and low power listening schemes.

6. References

[1] Atulkahate, “Cryptography and network security” second edition.

[2] Sunil Kumar Sahu, and Ajay Kushwaha, “ Performance Analysis of Symmetric Encryption Algorithms for Mobile Ad hoc Networks”, International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 6, June 2014.

[3] Yogesh Kumar, Lecturer in CSE Deptt, BPR College of Engg Gohana (Sonipat), Rajiv Munjal, lecturer in CSE Deptt., CBS Group of institution (Jhajjar), Harsh Sharma, Lecturer in CSE Deptt, BPR College of Engg Gohana (Sonipat), 2011, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", IJCSMS International Journal of Computer Science and Management Studies.

[4] Manish Singh, Shailender Gupta and Bharat Bhushan, YMCA University of Science and Technology, Faridabad, 2012, "Comparison of symmetric and asymmetric key cryptography: A study", Proceeding of the National Conference "Science in Media 2012" Organized by YMCA University of Science and Technology, Faridabad, Haryana (India)

[5] Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

[6] Elminaam, D S Abd; Kader H M Abdual and Hadhoud, M Mohamed. ―Evaluating the Performance of Symmetric Encryption Algorithms‖, International Journal of Network Security, Vol. 10, No. 3, pp. 216-222, May 2010.

[7] Singhal, Nidhi and Raina, J P S. ―Comparative Analysis of AES and RC4 Algorithms for Better Utilization‖, International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011, pp. 177-181.

[8] K.-T. Chu, C,-T. Wen, Y-C.Ouyang, and W.A. Sethares, "Adaptive distributed topology control for wireless ad-hoc sensor networks," in Proc. Int. Conf. Sensor Technol. Appl. (SensorComm), Valencia, Spain, 2007, pp. 378-386.