Volume 4, No. 4, March-April 2013
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Encryption and Decryption Technique in Wireless Sensor Networks

S.Kannadhasan*
PG Scholar, Velammal College of Engineering and Technology, Madurai, Tamilnadu, India
kannadhasan.ece@gmail.com,

P.Suresh
PG Scholar, Velammal College of Engineering and Technology, Madurai, Tamilnadu, India
sureshkannan52@gmail.com

M.Rajesh Baba
PG Scholar, Kalasalingam University,
Krishnankovil, Tamilnadu, India
rajeshbabaece@gmail.com

Abstract:-The Networks are showing increasing into the number of Security threats in the wireless sensor networks. In this paper we have the energy efficient for different keys are generated as the purpose of security with encryption and decryption using the DES and RSA Algorithm is applied to the network. The channel quality is determined in wireless sensor networks. The different keys are generated to be secured data will send through the networks then the life time of the network is increased in the wireless sensor networks. Finally we analysis results using DES and RSA algorithm the given data are converted into encrypted and decrypted into the network to efficient the data secured. Our paper is done by using C++ simulation.

Keywords: DES, RSA, Network Structure, Block Cipher

I. INTRODUCTION

Wireless Sensor Networks is a composed of number of sensor nodes in a large number of application such as military, airspace, temperature, light , humidity and then communicate with each sensor in wireless networks[1]. In the Wireless sensor networks cannot replace or recharge the batteries compared to the ahoc networks. So energy conservations are an important factor in wireless sensor networks[2]. Therefore the designing the network structure in an efficient way to the increasing the life of the networks in wireless sensor networks. The challenges in the network system included as Limited Hardware, Limited support for networking and also the Limited support for software development [3].

II. SECURITY THREATS

Internet are growing a large of threat are affectation continue reliability in the Denial of Service (dos) attacks. Such attacks can occur at all levels in the protocol stack and threaten both routers and hosts. Data confidentiality is important issues related to the security [4]. The data transferred towards the passive attacks are very sensitive to the data confidentiality. It can maintain confidentiality using cryptography techniques in the complex way encryption and decryption process involved into public key based generation have a power consumes are at higher rate [5]. In the sensor network a maximum number of the attacks are involved in the network layer are given as follows like Active attacks, Passive attacks, Wormhole attacks, Sinkhole attacks, Sybil attacks etc..

III. NETWORK STRUCTURE

The Figure shows that of the given data are transferred to the network to be secured using the encryption and decryption are generated into the network in wireless sensor networks. The data are transferred through the nodes to be secured in the way of key generated to the base station using encryption and also the key generated in the destination for the purpose of decryption of the given data are secured way in the wireless sensor networks.

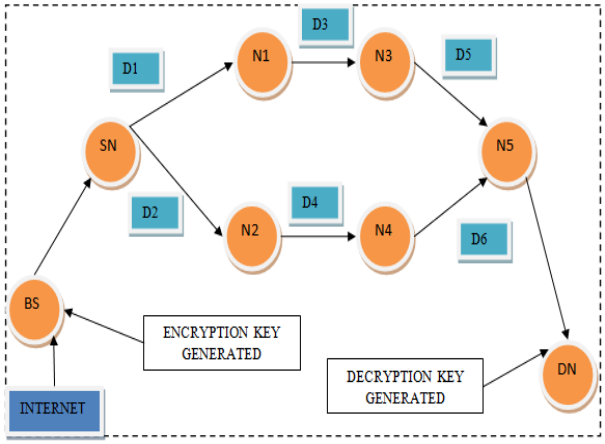

Figure: 1

IV. BLOCK CIPHER

The Energy Efficient provides the network security along with the small block size and key size using the block cipher [6]. We consider two block ciphers are the different energy performance in the wireless sensor networks. Characteristics of these ciphers are shown *in Table I*

Table 1: Characteristics of Block Ciphers

Block cipher	Block size	Key size
DES	64 bits	64 bits
AES	128 bits	128 bits

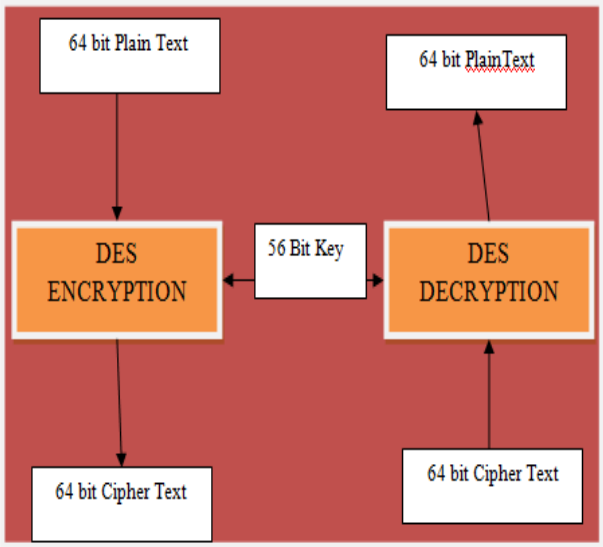

Figure 2: DES Block Diagram

V. DATA ENCRYPTION STANDARD

DES is a symmetric key block cipher published by NIST. It takes 64 bit plain text and 64 bit cipher text both the encryption and decryption site [7]. The 56 bit cipher key is used for both encryption and decryption of the given data [8]. The encryption process is consists of two permutations (P-Boxes) are also called as initial and final permutations and also sixteen feistal rounds. Each Round with two elements consists of mixer and swapper. It is also called as invertible [9]. The decryption algorithm should be identical to the encryption algorithm in a reverse order. But in case of DES cipher, the encryption algorithm is so well designed, that the decryption algorithm is identical to the encryption algorithm only with the sub keys applied in the reverse order [10]. Feistel structure makes encryption and decryption processes.

VI. RSA ALGORITHM

Diffie and Hellman introduced a new approach to cryptography to design a general-purpose encryption algorithm that satisfies the public-key encryption requirements. One of the first responses to the challenge was developed in 1977 by Ron Rivest, Adi Shamir, Len Adleman at MIT. Since then, the Rivest-Shamir-Adleman (RSA) scheme has become the most widely accepted and implemented general-purpose approach to public-key encryption [11].

VII. RESULTS AND DISCUSSION

This paper presents on Encryption and Decryption using DES algorithm and RSA algorithm is done by C ++Simulator. Results are shown in below. Figure 2: Shows the Node Results of the given Network. Figure 3: Shows that DES Encryption and Decryption and also Figure 4: Shows that RSA Encryption and Decryption. Figure 5: Shows that AES Encryption and Decryption. Figure 6: shows the energy consumption of the given network.

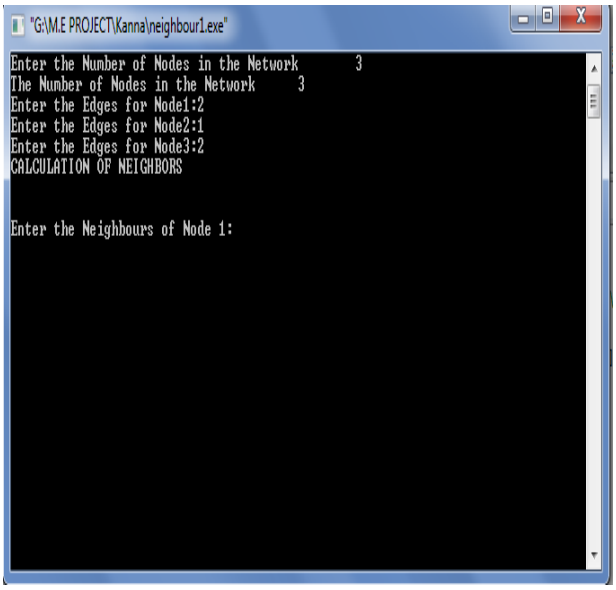

Figure 3: Node Results of the given Network

Figure 4: DES Encryption and Decryption.

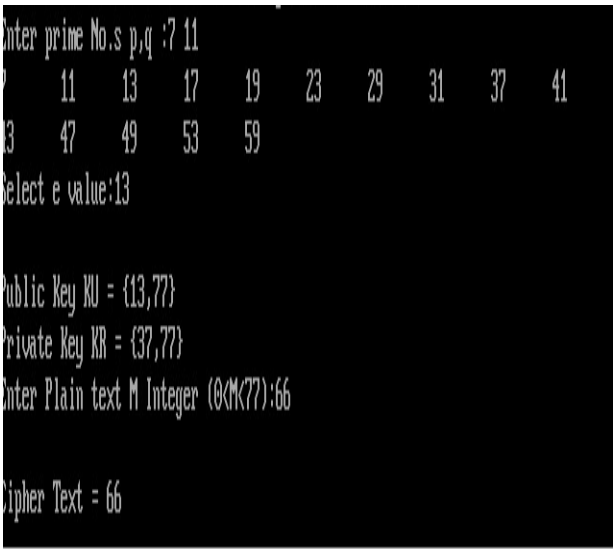

Figure 5: RSA Encryption and Decryption

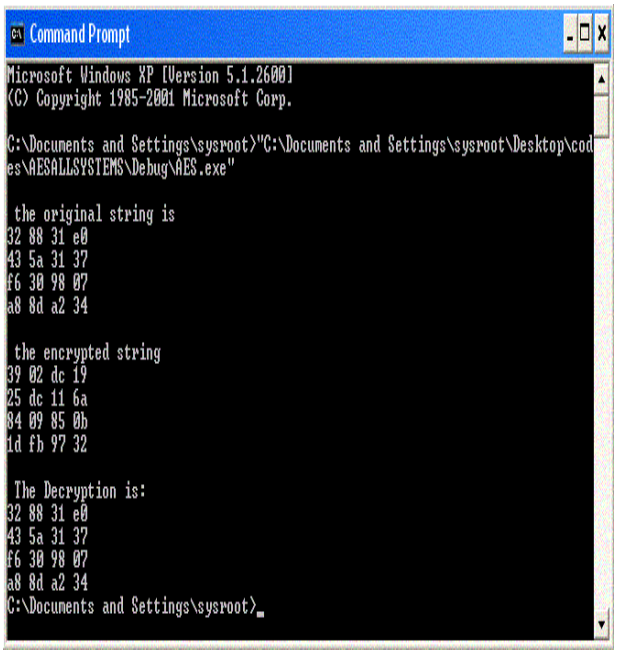

Figure 6: AES Encryption and Decryption

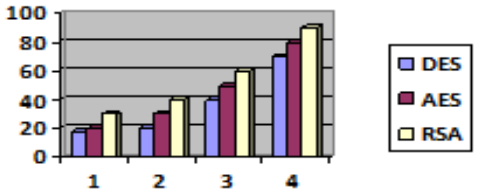

Figure 7: Energy Consumption

VIII. CONCLUSION

In this paper, we examine the energy efficiency of symmetric key cryptographic encryption algorithms applied in wireless sensor networks (WSNs) and in our study we consider block ciphers. Evaluating a number of symmetric key ciphers, we compare the energy performance of block ciphers applied to a WSN. Finally we conclude the data are transferred through the network are secured using the encryption and decryption in the way of energy efficiency to increases the life time of network in wireless sensor networks

IX. REFERENCES

[1]. Lingling Si,Zhigang Ji,Zhihui Wang," The Application of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks," Lingling Si et al. /Physics Procedia (2012)552 – 559

[2]. Topology Control code, February 2010. Available from: <http:// code.google.com/p/protocon/>.

[3]. OLSR-MC-NI, OLSR-TV code, and TopoView configuration, February 2010. Available from: <http://code.google.com/p/olsr/>.

[4]. L. Dong, H. Liu, Y. Zhang, S. Paul, D.Raychaudhuri, On the Cache-and- Forward network architecture, in: Proceedings of the IEEE International Conference on Communications (ICC), 2009, pp. 1–5.

[5]. H. Liu, Y. Zhang, D. Raychaudhuri, Performance evaluation of the Cache-and-Forward (CNF) network for mobile content delivery services, in: Proceedings of the IEEE International Conference on Communications (ICC), 2009, pp. 1–5.

[6]. S. Paul, R. Yates, D. Raychaudhuri, Jim Kurose, The Cache-And- Forward network architecture for efficient mobile content delivery services in the future Internet, in: Proceedings of the First ITU-T Kaleidoscope Academic Conference on Innovations in NGN: Future Network and Services, 2008.

[7]. W. K. Koo, H. Lee, Y. H. Kim and D. H. Lee, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks," in Proc of 2008 Information Security and Assurance (ISA 2008), pp.73-76, Korea, April 2008.

[8]. M. Henricksen, "Tiny Dragon - An Encryption Algorithm for Wireless Sensor Networks," in Proc of 10th High Performance Computing and Communications, (HPCC '08), p.p. 795-800, 25-27 Sept. 2008.

[9]. L. Bokor, L. Lois, C.A. Szabo, S. Szabo, Testbed of a novel media streaming architecture for heterogeneous wireless environment, in: Third International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities (TridentCom), May 2007.

[10]. F. Jan, B. Mathieu, D. Meddour, Video streaming experiment on deployed ad hoc network, in: Third International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities TridentCom), May 2007.

[11]. Y. Lin, A. Hamed Mohsenian Rad, V.W.S. Wong, J-H Song, Experimental comparisons between SAODV and AODV routing protocols, in: First ACM Workshop on Wireless Multimedia Networking and Performance Modeling, October 2005, pp. 113–122.

[12]. E. Borgia, Experimental evaluation of ad hoc routing protocols, in: Third IEEE International Conference on Pervasive Computing and Communications Workshops, March 2005, pp. 232–236.

[13]. A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy Analysis of Public-key Cryptography for Wireless Sensor Networks," in Proc of 2005 Pervasive Computing and Communications (PerCom 2005), pp. 324-328, Germany, March 2000