Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure and Efficient Data Collection in WSN

Gurpreet Kaur*, Navdeep Kumar
CSE& Kurukshetra University,
Haryana, India

Abstract— Wireless sensor networks (WSN) face security threats while sending and receiving data. The data transmission must be secured with reduced energy consumption. To enhance the security of sensor nodes, the data transmitted must be encrypted among sensor nodes In this paper we applied Data Encryption Standard scheme to add security to LEACH protocol. The objective of this paper is to add secret encryption scheme to the LEACH protocol. The network model is simulated in MATLAB to obtain the results. Performance of LEACH is evaluated based on various measures.

Keywords— WSN, LEACH, DES, BS, CH, SN, MATLAB

I. INTRODUCTION

Wireless Sensor Network (WSN) are the network of sensor nodes which communicate with each other and with the base station. WSNs are network of clustered nodes. These networks are often applied in numerous fields like military and health. Some of characteristics of the sensor nodes are reduced power, reduced bandwidth, memory size and lesser energy[6]. Wireless sensor networks are constrained due to reduced bandwidth, prone to attacks, collisions in channel. There must be some mechanism to make WSNs secure.

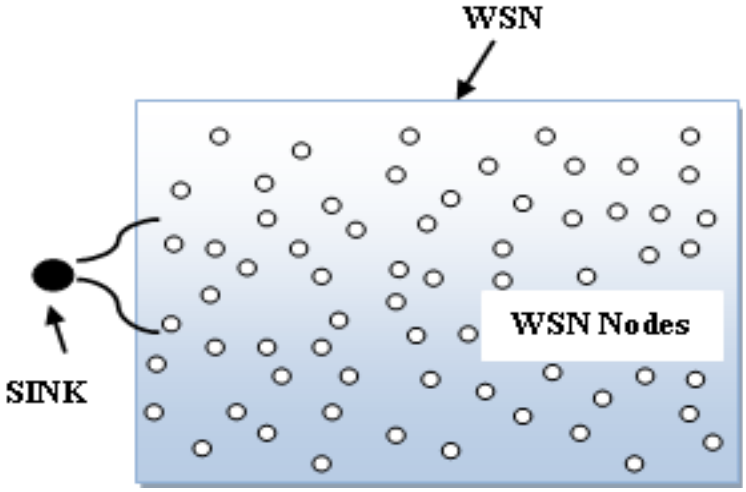

Fig 1.1 Wireless Sensor Network

Security In Wireless Sensor Networks:

Security of Wireless sensing element network has become a significant concern of industries. So it's necessary to enhance the protection of WSN since they're used at gaint scale. It is not known before that nodes are going to be in communication range of each other. To boost the protection of sensor nodes, it is necessary to apply encryption among detector nodes[6]. Key management will increase network security and build network resistant against attacks on it. The ancient network security technique isn't appropriate for sensing element networks attributable to its restricted computing power and cupboard space. All the protection needs cannot be satisfied by a single key technique as in Wireless sensor networks differing types of messages are changed having totally different needs for security. WSNs face security threats so there is a want of special key management schemes for WSNs beacuse most of the routing protocols for WSNs liable to reasonably security threats.

Key management is employed to form knowledge secure in sensor networks. Key technique in wireless sensing element network is tough. Wireless sensing element network consists of huge range of sensing element nodes with totally different hardware functions. Complex security algorithms can't be employed in sensing element networks since sensing element nodes have restricted memory resources and reduced energy. Hence, an energy economical key management theme is critical to mitigate the safety risks.

Energy Efficiency In Wireless Sensor Networks:

The nodes in an exceedingly wireless network are mobile and aren't connected to a relentless power offer in order that they derive energy from personal batteries. It can limit the nodes energy. These networks are used in places wherever individual nodes and batteries couldn't get replaced, thus it's necessary to extend the life of the network and is most popular that each one the nodes die along so the complete network may well be replaced by a replacement set of little nodes[2].

Since it's difficuilt to exchange or recharge the batteries of small device nodes once being deployed in order that they ar unnatural by energy consumption. Owing to this reason, researchers face challenges whereas planning a routing protocol enhancing energy potency and increasing the life of the network. Numerous cluster-based routing protocols are developed to extend WSN life uptil now. But there's a desire to develop routing protocol for WSN which might increase network life, tolerate node failure and might cut back information measure consumption.

II. LEACH PROTOCOL

LEACH(Low Energy Adaptive Clustering Hierarchy) is a hierarchical routing protocol for wireless sensor networks. LEACH protocol was proposed for reducing the energy consumption among nodes. It works in rounds in which some of the detector nodes are selected randomly to become cluster-heads for each round. Each node has an equal chance of becoming cluster-head to balance the energy load. The cluster-heads compress and aggregate the information that is returning from the nodes that belong to their clusters, and transfer it to the base station to reduce the amount of information that must be transmitted to the base station. LEACH uses a TDMA/ CDMA (MAC) to reduce collisions within a cluster and within different clusters.

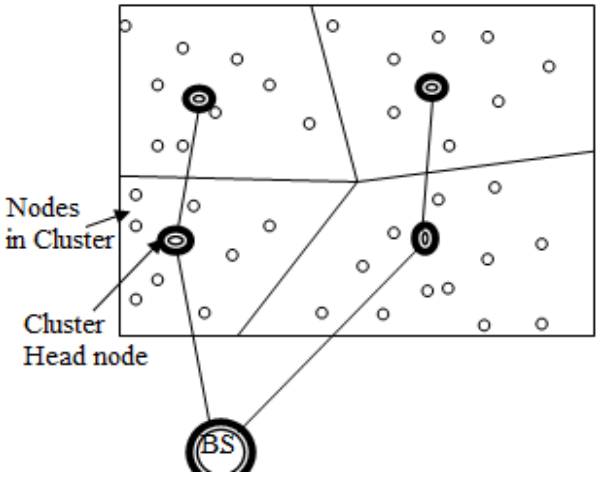

Fig 2.1 LEACH Protocol

The operating of LEACH protocol is split into 2 phases:

I. Set-up phase
II. Steady state phase

Setup Phase:

At the beginning of a round, each node can decide whether or not to become a cluster head for current round independent of other nodes. Then a random number is generated by each sensor node such that 0< random < 1 and is compared to a pre-defined threshold T (n). If random < T(n), the sensor node becomes cluster-head, else it is member of cluster[12]. When node has become CH it will broadcast an message. This message consists of the node ID and a header. A non-cluster-head node can choose the cluster to which it belong depending on the communication energy of cluster-head. Once the sensing node has chosen cluster it will notify CH. Then a message known as join-request message is transmitted by each node to the CHs. The cluster-heads are responsible for coordinating data transmissions in their clusters. A Time Division Multiple Access(TDMA) schedule is setup by the cluster-head and is transmitted to the nodes in the cluster[9].

Steady State Phase:

In the steady-state phase, depending on the TDMA schedule received at the setup phase the surroundings are sensed by cluster members and the sensed data is transmitted to their CH. The sensor nodes(SN) go into hibernate mode to save energy for other slots. The CH receives all the data sent by its member nodes, aggregate the data and send it to BS. After some time, the network will go back into the setup phase again and enter another round of choosing new CH. The process can be break down into frames in which nodes can send their data to cluster-head, onetime per frame. Since nodes are not evenly distributed so there is variation in the number of nodes in each cluster. The data transmitted by each node to its cluster-head depend on the number of nodes in cluster.

III. DATA ENCRYPTION STANDARD

Data Encryption Standard(DES) is also known as Feistel block cipher. Horst Fiestal, an IBM cryptography researcher developed a block cipher algorithm known as DES. The same algorithm and key are used for encryption and decryption in DES[14]. DES operates on 64 bit data block. The entire encryption process of DES depends on 56 bit secret key.

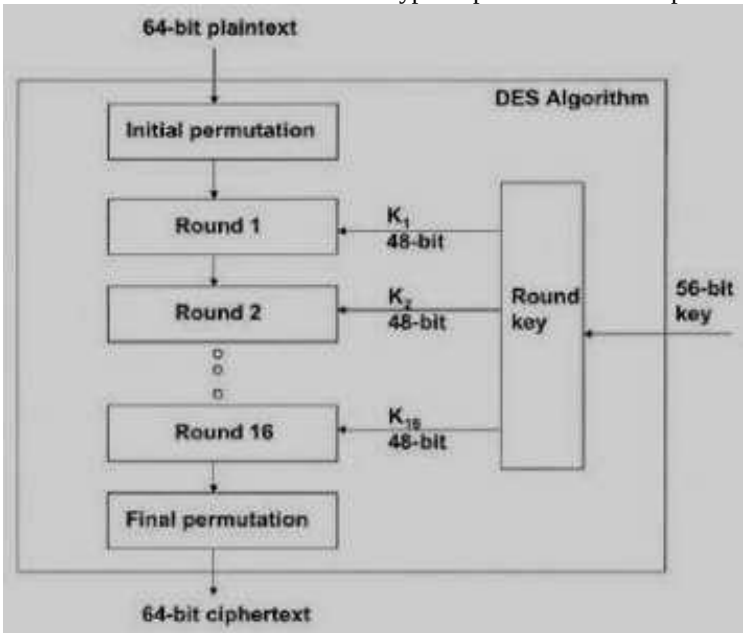

Fig 3.1 DES Algorithm

Steps of DES Algorithm:

1. Expansion (*E*): The thirty two bit input word is duplicated and reordered by half of bits and is then expanded to forty eight bits.
2. Key mixing: By choosing forty eight bits from fifty six bit secret key, we build a spherical key so the dilated word is XORed with the spherical key.
3. Substitution. The 48-bit result is obtained which is then split to eight words of six bit each. Eight S-boxes are filled with these words.
4. Permutation (P): Before sending to the output the remaining thirty two bits are reordered by applying a fixed permutation.

IV. RELATED WORK

Baiping Li and Xiaoqin Zhang in 2012 [2], presented a new improved version of LEACH known as LEACH-CC. This protocol is a chain based routing protocol based on low energy consumption. To reduce the number of nodes that can communicate with base station the author introduced a chain based routing. Sensor nodes send information to the base station about its current location and level of energy. Performance of LEACH-CC protocol is proved to be better than LEACH protocol in WSN by simulation. The lifetime of network and its energy efficiency was increased. The technique used in LEACH-CC protocol is centralized which can reduces the distance of transmission by non-cluster-head nodes and transfer of information to base station occurs by one cluster head in each round.

Alisha Gupta & Vivek Sharma in Sept 2013 [12], proposed a replacement secure protocol for LEACH referred to as LEACH_HE. During this protocol a confidentiality theme homomorphic cryptography is another to the LEACH protocol. For sending sensing information firmly and with efficiency to the receiver by minimizing energy consumption, it's necessary to style a confidentiality theme for WSN. Energy consumption is reduced during this protocol by aggregation of information. Some performance metrics were accustomed get the results of simulation. Performance of LEACH_HE is observed to be somewhat like LEACH.

Bi Jiana and E Xu in 2013 [7], planned a security node-based key management protocol for cluster-based sensing element networks. During this protocol generation of security nodes and differing types of keys is represented by the author. Performance analysis and simulation show that the by the planned key management protocol energy consumption is a smaller amount and key generation delay time is brief. At an equivalent time, additional cooperative authentication security for keys is provided by the protocol. It will strongly recover against node capture, and may support massive networks.

Sai Ji, Liping Huang and Jin Wang in Feb 2013 [10], proposed a novel key based for the dynamic WSNs. Within the network deploying phase, the protection authentication and random key distribution were initialized. Throughout the network stable phase, the scheme projected a dynamic updated key supported the AVL tree so as to make sure the period update security for the topology. Simulation results showed that this program will make sure the WSN's dynamic security furthermore as accomplish the energy potency goal.

V. PROPOSED WORK

The success of a key management scheme is determined by its ability to efficiently survive attacks on highly vulnerable and resource constrained networks. The new key management scheme is "Secure Key Pool Architecture" is proposed for wireless sensor networks. The main idea here is to break the whole problem into small problems and at the same time having the ability to apply different levels of security to the various sensor nodes. We divide the communication that appear in WSN, where there is node to node communication and node to B.S. communication. To have a secure network there is a need to secure these communications.

The Network Model

The basic idea for communication between cluster head and base station is, Cluster heads (CHs) pass messages between groups of nodes (group for each CH) and the base station (BS). This proposed scheme is safe, when the CHs are rotating from node to node in the network making it harder for intruders to know the routing elements and attack. In this scheme a pool of keys is generated at base station that has specific number of keys generated randomly using a random number generator function. The base station randomly generates key ID for uniquely identifying each key. Then, each sensor is provided with group of keys with equal sizes for each node, the keys has to be picked randomly without removing any key from the key pool. Thus the sensor nodes have some sharing keys between each other which make node to node communication possible. The base station provides each sensor with at least one unique key (named Master Key) which is to be used to communicate between each node and the base station.

Assumptions made for communication in wireless sensor network are as following:

- The network is shaped by N sensors nodes deployed in square field and has cluster hierarchical topology.
- Some sensor nodes are mobile.
- The base station is outside the sensing field
- Nodes are deployed randomly.

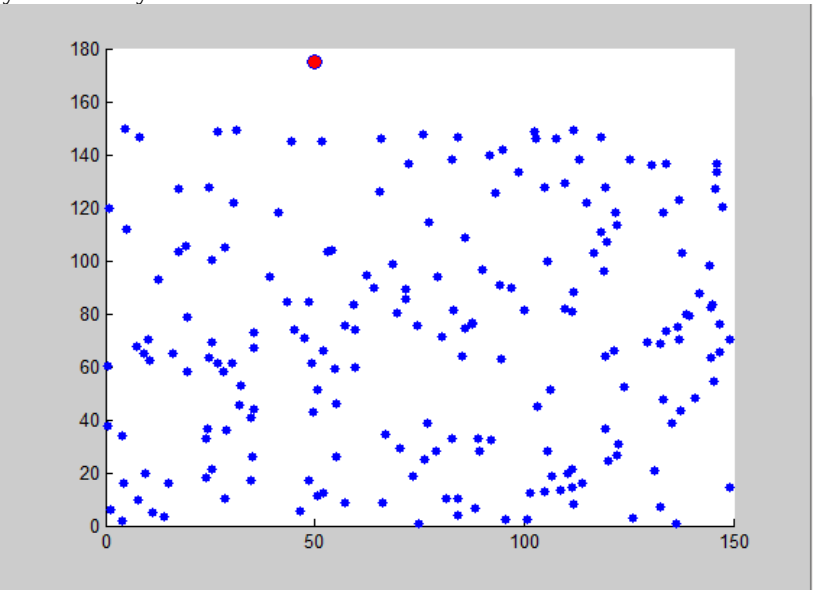

Fig 5.1 Network Model

VI. SIMULATION RESULTS

We examine the performance of proposed LEACH with existing LEACH. MATLAB platform is used to obtain results A network of 200 nodes is deployed in an area of 150m*150m with BS at (50,175). We run the network model for 1000 rounds. Following are some parameters of the simulation experiments as described in Table 1.

Table 1: Parameters Values

S.No	Parameter Name	Value
1	No of Nodes	200
2	BS location	(50,175)
3	Simulation Area	150m*150m
4	Optimal Election Probability	0.2
5	Maximum No of Rounds	1000
6	Initial Node Energy	0.5 J

We use 3 performance measures for the comparison for comparing the performance of proposed LEACH with existing LEACH : numbers of dead nodes, remaining energy of the network & the packets transmitted by the two different protocols. Following figures 6.1-6.3 shows simulation results.

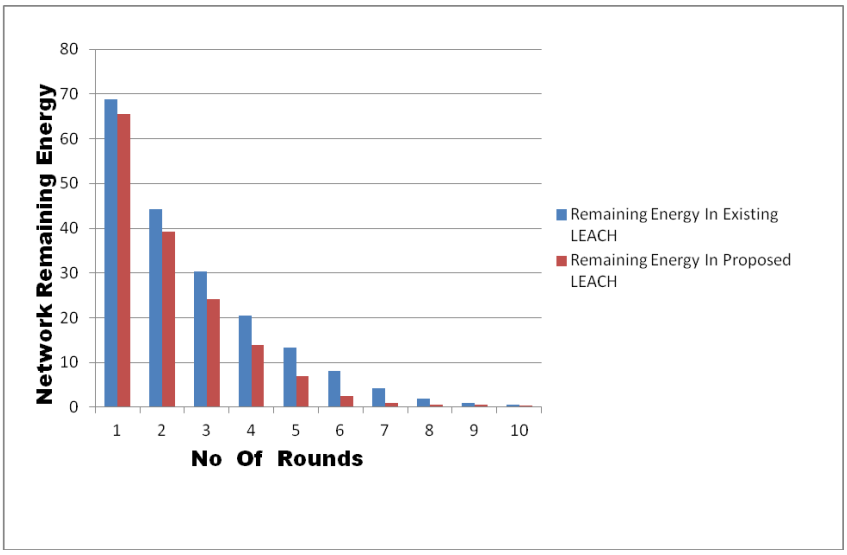

Fig 6.1 Network Remaining Energy v/s Rounds

After 1000 rounds the remaining energy in proposed LEACH is equal as that of remaining energy in existing LEACH.

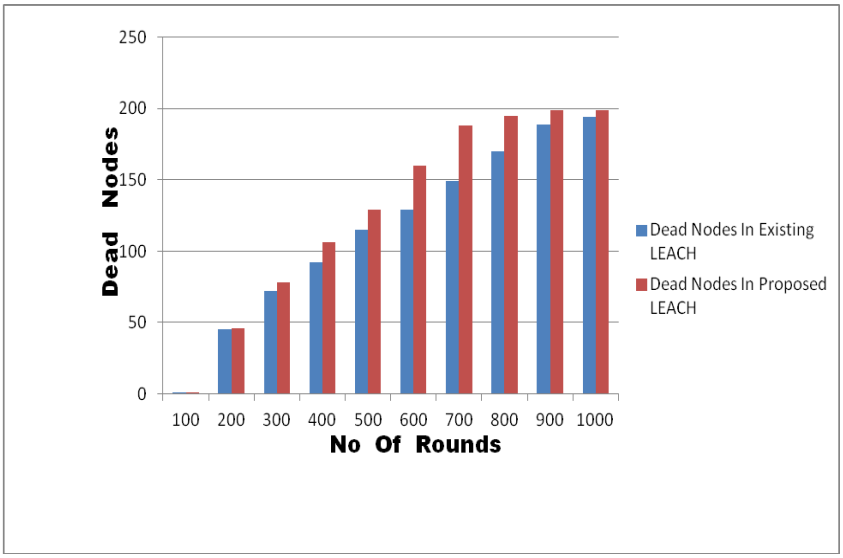

Fig 6.2 Dead Nodes v/s Rounds

After 1000 rounds the network is still alive in proposed LEACH with 1 alive node left.

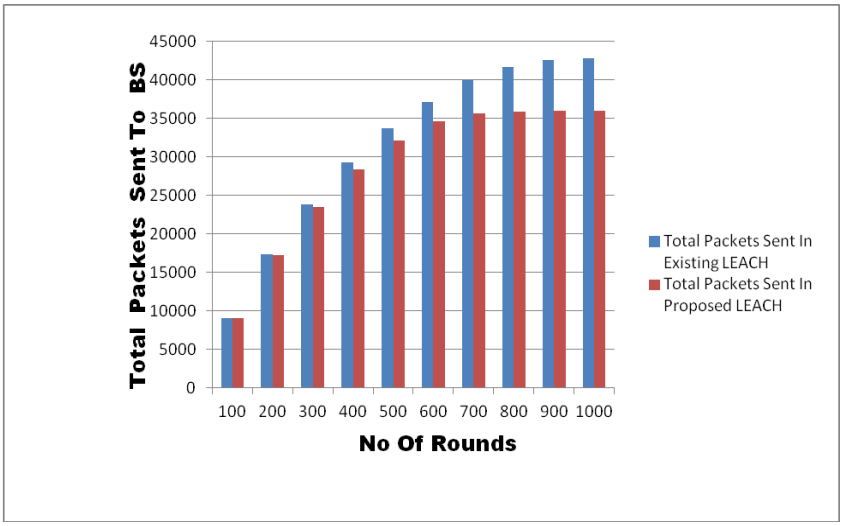

Fig 6.3 Total Packets Sent to BS v/s Rounds

After 1000 rounds the data transmitted in proposed LEACH is at par with data transmitted in existing LEACH.

VII. CONCLUSION

In this paper, we added security to LEACH protocol by applying Data Encryption Standard scheme for encryption and decryption. We performed simulation in MATLAB to obtain results for three performance metrics: Network Remaining Energy v/s Rounds, Dead Nodes v/s Rounds, Total packets sent to BS v/s Rounds. We performed simulation of network model for 1000 rounds and compared the performance of existing LEACH with proposed LEACH. Graphs of fig shows that the proposed LEACH remaining energy is 0.4 whereas remaining energy of existing LEACH is 0.6. Dead nodes in proposed LEACH is 199 whereas in existing LEACH it is 194. Total number of packets sent in proposed LEACH is 35976 whereas it is 42819 in existing LEACH. This shows that after applying encryption in LEACH the results are not much altered. Thus after applying DES scheme the performance of LEACH protocol is not deteriorated. The proposed LEACH is safer and secure than existing LEACH.

REFERENCES

[1] Leonardo B. Oliveira, Hao C. Wong and M. Bern, "SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks", Supported by FAPESP under grant 2005/00557-9.

[2] Baiping Li**,** Xiaoqin Zhang, "Research and Improvement of LEACH Protocol for Wireless Sensor Network", International Conference on Information Engineering, 2012.

[3] Yi Liu, Shan Zhong, Licai You, Bu Lv, Lin Du, "A Low Energy Uneven Cluster Protocol Design for Wireless Sensor Network", Int. J. Communications, Network and System Sciences, 2012, 5, 86-89, February 2012.

[4] Pengcheng Zhao, Yong Xu, Min Nan, "A Hybrid Key Management Scheme Based on Clustered Wireless Sensor Networks", Wireless Sensor Network, 2012, 4, 197-201, August 2012.

[5] Nguyen Duy Tan, Longzhe Han, Nguyen Dinh Viet, and Minho Jo, "An Improved LEACH Routing Protocol for Energy-Efficiency of Wireless Sensor Networks", Smart Computing Review, vol. 2, no. 5, October 2012.

[6] Abdoulaye Diop, Yue Qi, Qin Wang, and Shariq Hussain, "An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks", International Journal of Computer and Communication Engineering, Vol. 1, No. 4, November 2012.

[7] Bi Jiana, E Xu, "An Energy-efficient Security Node-based Key Management Protocol for WSN", Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation, 2013.

[8] Chunyao Fu, Zhifang Jiang, Wei Wei and Ang Wei, "An Energy Balanced Algorithm of LEACH Protocol in WSN", IJCSI International Journal Of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.

[9] Meena Malik, Dr. Yudhvir Singh , Anshu Arora, "Analysis of LEACH Protocol in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.

[10] Sai Ji, Liping Huang and Jin Wang, "A Novel Key Management Scheme Supporting Network Dynamic Update in Wireless Sensor Network", International Journal of Grid and Distributed Computing Vol. 6, No. 1, February, 2013.

[11] Parul Bakaraniya, Sheetal Mehta, "K-LEACH: An improved LEACH Protocol for Lifetime Improvement in WSN", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 5- May 2013.

[12] Alisha Gupta and Vivek Sharma, "Implementation Of LEACH protocol using Homomorphic Encrytion", International Journal of Electrical and Electronics Engineering (IJEEE), Vol. 2, Issue 4, Sep 2013, 63-74

[13] Honggui Deng, Chen Yang and Yi Sun, "A Novel Algorithm for Optimized Cluster Head Selection", Science Journal of Electrical & Electronic Engineering, 2013.

[14] Amritpal Singh, Mohit Marwaha, Baljinder Singh and Sandeep Singh, "Comparative Study of DES, 3DES, AES and RSA", International Journal Of Computers & Technology, Vol 9, No 3, July 2013.

[15] Prashanti.G, Deepthi.S and Sandhya Rani.K, "A Novel Approach for Data Encryption Standard Algorithm", International Journal of Engineering and Advanced Technology (IJEAT), Volume-2, Issue-5, June 2013.

[16] Shah Kruti R., Bhavika Gambhava, "New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-1, March 2012.

