Review Paper on Zigbee based Secured Wireless Communication by using DES Encryption

Renuka Londhe, Shalmali Kumawat, Pooja Gaware, C. K. Bhange
Department of Electronics and Telecommunication, Savitribai Phule Pune University, India
Academic Year 2016-2017

Abstract:- IEEE 802.15.4(Zigbee)[1] standard is low data rate,low power consumption and low cost wireless personal area network.In order to transmit large amount of information that require high data such as video, image and audio and its encryption and decryption is considered.Zigbee in general uses a single channel for data transmission.In this paper we proposeddata transmission (pdf,image) over zigbee networks with DES encryption,which aims to improve total throughput of networks and secure transmission of data.

Keywords: *Zigbee, DES encryption.*

*****

I. Introduction:

While exploding growth on wireless communication in recent years,security issues in wireless networks also become a growing concern.Security requirements for wireless networks are similar to those for wired networks [2].However networks are inherently less secure compared their wired counter parts due to the lack of physical infrastructure.Therefore,special attention should be paid to the security of wireless networks.Thesecurity objective forwireless and wired networks are the same, ac are the major high level categories of threats that they face.However,while these objectives are well understand and addressed in the relatively mature wired network environment this has not always been the case in the new and rapidly evolving wireless environment.

In this system,it is desired to transmit the data with more security.The data can be apdf or string of message or an image.The data is encrypted in computer and send it to the microcontroller using MAX232.Microcontroller will receive this data and send to another computer by wireless module zigbee.The encrypted data is divided into small packets and these packets are transmitted through zigbee transmitter and received at zigbee receiver[3].At receiver,the data is decrypted.

II. Need of system:

Data security plays a crucial and critical role in modern times for businesses and inmilitary wars [4]. Transmission of sensitive information 0over the wireless medium,ensuring security is critical issue. So there should be firm system which will transmit the sensitive data safely. This system can be used in militaryareas ,in corporate world,also in school,colleges for securing their important and confidential data.

III. DES Algorithm:

The Data Encryption Standard (DES) is symmetric key block cipherpublished by the National Institute of Standard and Technology (NIST)[5].DES implementation uses key of length 64 bits i.e. the block size 64 bit. Out of 64 bit it uses key length of 56 bits effectively. Since 8 of 64 bits of the key are not used by encryption algorithm. It consist of number of rounds where each round contain bit shuffling, nonlinear substitutions and exclusive OR operation.

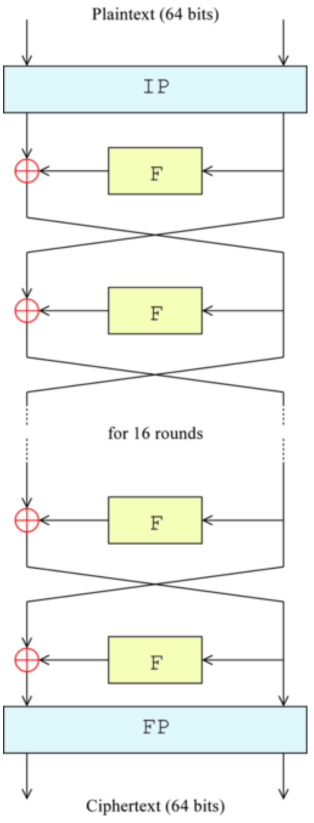

Fig. 1

DES algorithm takes two inputs the plaintext that is to be encrypted and secret key. DES uses same key for both encryption and decryption and operates on 64 bits block of data at time, therefore DES is symmetric. The least significant bit of each byte is used for parity(odd for DES). All blocks are numbered from left to right, that makes eight bit of each byte parity bit. Once plain text message is received which is to be encrypted is arrange into 64 blocks required for input.DES algorithm uses two techniques as substitution and permutation. Substitution is mapping of one value to another and permutation is reordering of bit positions for each of inputs.

IV. Working of DES Algorithm:

Figure shows sequence of events during encryption operation. DES performs initial permutation on 64 bit plaintext. Then this plaintext is split into two 32 bit sub blocks called left plain text (LPT)and right plain text(RPT)[6]. Each of LPT and RPT passes through 16 rounds of encryption operation, each with its own key. Different 48 bit key is generated from 56 bit key using key transformation. By using expansion transformation, RPT is extended from 32 bit to 48 bit. Then 48 bit key is XORed with 48 bit RPT, corresponding output is given to next step. S box substitutions produces 32 bit from 48 bit which are permuted using P box permutations. 32 bit output of P Box is XORed withLPT 32 bits. XORed 32 bit output becomes RPT and old RPT become LPT which is called as swapping. After completion of 16 rounds final permutation is done.

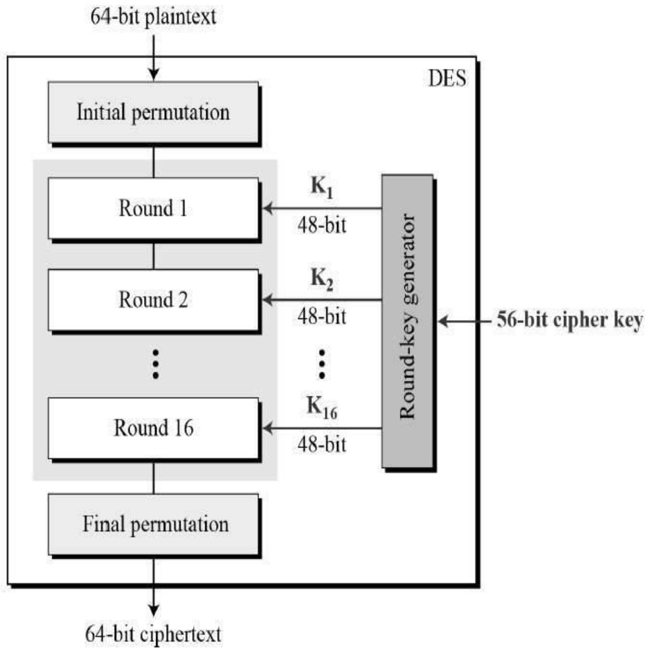

Fig. 2

V. Conclusion:

This research paper discusses the DES algorithm, which is the science of data encryption, a technology that provides for a safe, secure, and privateinformation exchange. Using this systemwecan transfer pdf, image securely and safely.

REFERENCES:

[1] Dr. S.S. Riaz ahemed proposed *"The Role Zigbee Technology In Future Data Communication System"***,** Journal of Theoretical and Applied Information Technology.

[2] Wongsavan chantharat and Chaiyed Pirak proposed *"Image Transmission overZigbee Network with Transmit Diversity".*

[3] CRS Bhardwaj proposed *"Modification of DES Algorithm",*International Journal of Innovation Research and Development.

[4] SombirSingh,Sunil k. Makaar, Dr.Sudesh Kumar proposed "*Enhancing the security of DES Algorithm Using Transpositions Cryptographytechniques***",** International Journal of Advanced Research in Computer Science And Software Engineering, Volume 3, Issue 6,June 2013