ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 5, May 2015

A prototype for secret based data Encryption Scheme for Smart Grid Wireless Communication

Gadi Anvesh

B.Tech, Department of ECE, D.M.S S.V.H College of Engineering, Machilipatnam, India

Abstract: Integrating information network into power system is the key for realizing the vision of smart grid, but also introduces many security problems. Moreover, smart grid is an attractive target for various hackers with diversified motivations, e.g. unethical customers may want to modify their meter readings to evade the electric charge; malicious users are able to extract the behaviors of household by eavesdropping the communications of smart meters. Wireless communication offers the benefits of low cost, rapid deployment, shared communication medium and mobility at the same time, it causes many security and privacy challenges. In this paper, the concept of dynamic secret is applied to design an encryption scheme for smart grid wireless communication. Dynamic wireless encryption works in a different concept where the master key is changed during time. Master key, the key which is needed to communicate between sender and receiver. Even if a hacker captures the key, he will not be able to receive data continuously from sender since the master key will change with time. In our project, a smart grid platform is built, employing the ZigBee protocol for wireless communication. Thus a data encryption standard (DES) algorithm has been developed to transmit our data securely. The length of the key that is generated in data encryption standard (DES) is 64 bits out of which 8 bits are removed for parity so now the key is of length 56 bits .So there are 72 quadrillion number of keys that can be generated. A dynamic secret-based encryption demo system is designed based on this platform. The results show that it is impossible for the adversary to track the updating of the dynamic encryption key.

Index Terms: Dynamic secret-based encryption, retransmission, security, smart grid, wireless Communication, ZigBee.

I. INTRODUCTION

RAPID increase in electric power demand, renewable energy mandates, and a push towards electrification in the transportation sector is expected to increase power system stresses and disturbances. In the United States, 31 states have established the Energy Efficiency Resource Standards and Goals which target 30% energy savings by 2020; 30 states have launched the Renewable Portfolio Standards and Goals which require the renewable energy occupy 15% by 2020. The smart grid (SG) is considered as a desirable infrastructure for energy efficient consumption And transmission, where the built-in information networks support two-way energy and information flow, facilitate significant penetration of renewable energy sources into the grid, and empower consumer with tools for optimized energy consumption since the advent of the smart grid concept, security has always been a primary concern. Pricing information and control actions are transmitted via the information network. Various attacks such as eavesdropping, information tampering, and malicious control command injection that have almost ruined the Internet, would impose serious threat on secure and stable smart grids operation. Moreover, SG is an attractive target for various hackers with diversified motivations, e.g. unethical customers may want to modify their meter readings to evade the electric charge; malicious users are able to extract the behaviours of household by eavesdropping the communications of smart meters (called non-intrusive appliance load monitoring); vicious terrorists want to inject the false data or command to disrupt the grid. The U.S. National Institute of Standards and Technology lays out the guidelines for developers and policy makers, covering cyber security requirements of the smart grids that should be included from the beginning of the development process. . A DES (data encryption standard) demo system is developed on the SG platform. As shown in the experiments, it is inevitable for the adversary to miss few packets when he monitors the communication between the smart meter and control center.

These inevitable and unpredictable errors will prevent the hacker from tracking the secrets. We can implement applications and integrate with most wireless techniques. The DSE key is changes dynamically generated during the normal communication without additional traffic and control command.

The remainder of this paper is organized as follows. In Section II, many cryptography methods for SG are reviewed. In Section III, The experiments and analysis of DSE scheme are analyzed in Section IV. Section VII concludes this paper.

II. RELATED WORK

Cryptography plays a significant role in improving the integrity and confidentiality of the data in SG. Many existing standard encryption algorithms and authentication schemes are adopted in SG. Symmetric cryptographies, such as DES (Data Encryption Standard) are widely employed in SG to efficiently defend against possible threats. For example, ZigBee employs 64-bit DES encryption for security.

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 5, May 2015

III. METHODOLOGY BLOCK DIAGRAM

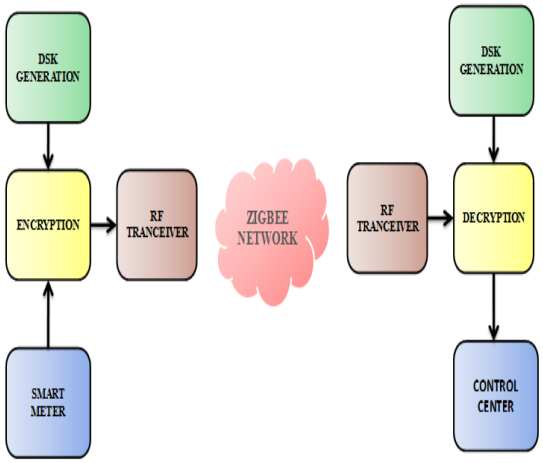

Fig 1: overall block diagram.

Since the advent of the smart grid concept, security has always been a primary concern. Pricing information and control actions are transmitted via the information network. The working principle of the proposed system is shown in fig. In this proposed system the data from the smart meter is first encrypted before transmitting it via wireless channel. Here, we are using a zigbee network to transmit the encrypted data. At the receiver, the cipher text is received if the zigbee port is matched and the cipher text is decrypted using the same key and data will be send to control center The main objective of our project is to transmit the data securely using wireless communication. A zigbee protocol has been utilized for the transmission of the data wirelessly .Thus a data encryption standard (DES) algorithm has been developed to transmit our data securely. DES is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Most symmetric encryption schemes today are based on this structure (known as a feistel network).

OVERALL STRUCTURE OF DES:

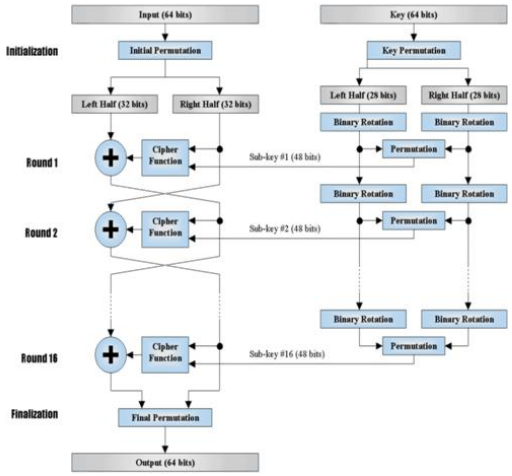

Fig 2: block diagram for DES

So in total the processing of the plaintext proceeds in three phases as can be seen from the left hand side of figure:

1) Initial permutation (**IP)** rearranging the bits to form the "permuted input".
2) Followed by 16 iterations of the same function (substitution and permutation).The output of the last iteration consists of 64 bits which is a function of the plaintext and key. The left and right halves are swapped to produce the pre output.
3) Finally, the pre output is passed through a permutation which is simply the inverse of the initial permutation (**IP**). The output of inverse permutation is the 64-bit cipher text. The initial and final permutation can be clearly seen in Fig 2.

SINGLE ROUND OF DES:

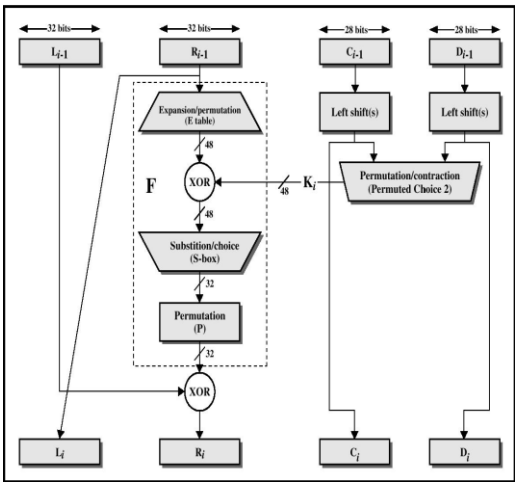

Fig 3: one round of DES

Details of an individual round can be seen in fig: 3.The main operations on the data are encompassed into what is referred to as the cipher function and is labeled F. This function accepts two different length inputs of 32 bits and 48 bits and outputs a single 32 bit number. Both the data and key are operated on in parallel; however the operations are quite different. The 56 bit key is split into two 28 bit halves Ci and Di(C and D being chosen so as not to be confused with L and R). The value of the key used in any round is simply a left cyclic shift and a permuted contraction of that used in the previous round.

Mathematically, this can be written as
Ci = Lcsi (Ci−1),
Di = Lcsi (Di−1)
Ki = PC2 (Ci, Di)

Where Lcsi is the left cyclic shift for round i, of shifts is one and for every other round it is two. Ci and Di are the outputs after the shifts, PC2 (.) is a function which permutes and compresses a 56 bit number into a 48 bit number and Ki is the actual key used in round is changed. The common formulas used to describe the relationships between the input to one round and its output (or the input to the next round) is:

Li = Ri−1
Ri = Li−1 _ **F**(Ri−1,Ki)

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 5, May 2015

Where L and R have their usual meaning and **F**(.) is the cipher function.

IV. EXPERIMENTS AND ANALYSIS

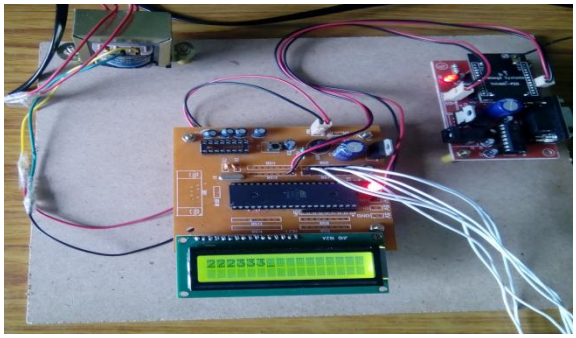

Fig 4: data entry in encryption side

Data can be entered in the LCD display through a numerical keypad instead of smart meter.

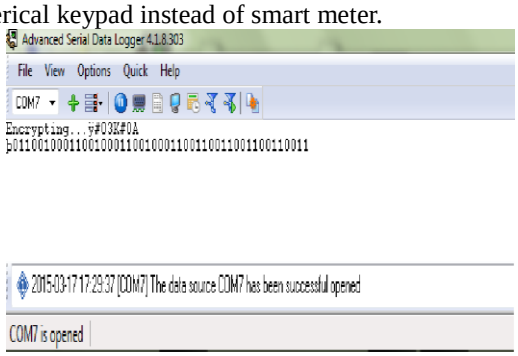

Fig 5: encrypted data

The data what we entered will encrypt here and a 64-bit chiphertext will dispalyed in adavanced serial data logger.

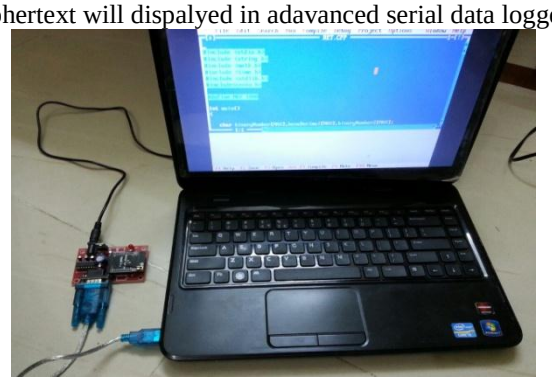

Fig 6: receiving side with zigbee module

The 64- bit encrypted data or chipher text will be decrypted here in the software design.

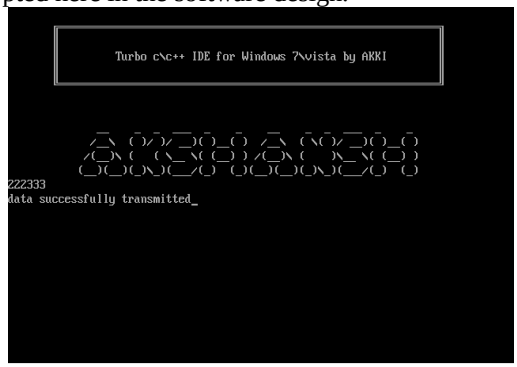

Fig 6 : output data

The data what we entered in the program is decrypted and displayed.

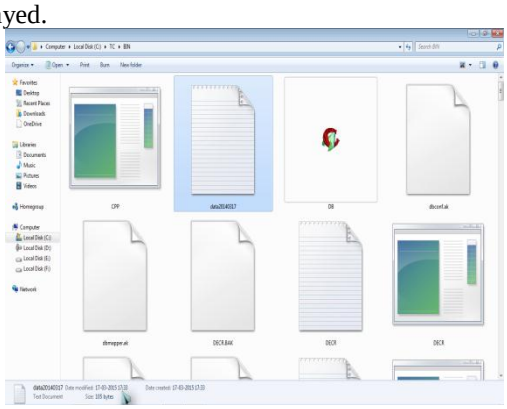

Fig 7: date manipulation

If the reveciver want to manipulate date or to change the amount of power can be shown in fig 7

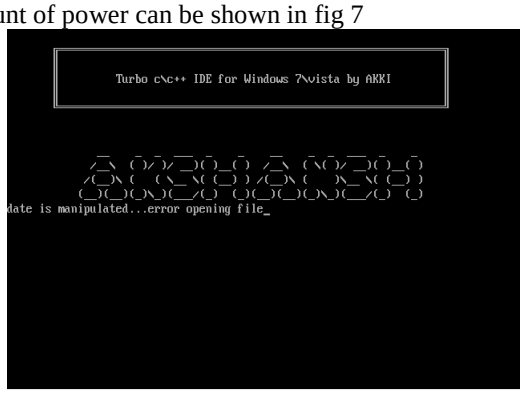

Fig 8: output display for the control center after manipulation

The output will be displayed in the form of an error opening file.

V. ADVANTAGES

- high security
- Less expensive
- Testing procedure is simple

VI. LIMITATIONS

- key is too short i.e. just 56 bit key length.

VII. CONCLUSIONS

In order to avoid the security problems in the smart grid, we employed an effective encryption algorithm for smart grid communication, where the master key is changed during time. Data Encryption Standard algorithm is a type of symmetric-key encryption. Symmetric-key encryption is a type of cryptosystem in which encryption and decryption are performed using a single (secret) key. As we can see, secret key play a very important role in DES security, so that a good key generation unit required. Using Dynamic key generator, the generated key has characteristics of unpredictability and unrepeatability. Using this approach the dynamic key generator can achieve the high speed and can be reduce logic complexity. Using proposed design, a general purpose IC can be designed for DES algorithm with high secrecy of the key in real time data communication. This design has a

broad application area in field of data communication, and secure data transmission.

ACKNOWLEDGEMENT

We pay our most gratitude to the almighty for showing his gracious blessings during the completion of this project. We also express a deep sense of gratitude to thank **Dr.K.V.S.V.R.Prasad**, Head of the Department, ECE for and **Dr.K.Surya Prakasa Rao**, Principal, Daita Madhusudhana Sastry Sri Venkateswara Hindu college of Engineering, Machilipatnam for providing well organized infrastructure being helpful in completion of our project.

REFERENCES

[1]. "The smart grid: An introduction," in DOE's Office of Electricity Delivery and Energy Reliability 2008.
[2]. Office of the National Coordination for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability standards,"2010 [Online].
[3]. William Stallings, "Cryptography and Network Security-Principles Practice", Fifth Edition, Prentice Hall, 2006.
[4]. A dynamic secret based encryption scheme for smart grid wireless communication by Ting Liu, Member, IEEE, YangLiu, YashanMao, Yao Sun, Xiaohong Guan, Fellow, IEEE, Weibo Gong, Fellow, IEEE, and Sheng Xiao.

BIOGRAPHY

Gadi Anvesh is pursuing B.Tech in the faculty of electronics and communication from D.M.S.S.V.H College of engineering. Machilipatnam, Andhra Pradesh. His area of research in cryptography and wireless communication