Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

A Novel Design of Effective Security for Data Communication by Designing Standard Algorithm for Encryption and Decryption

Baddam Mounika Reddy
Masters in Embedded Systems,
Department of Electronics and Communication Engineering,
Stanley College of Engineering and Technology for Women, Hyderabad,India.

V. Sudarshini Kataksham
Asst Professor,
Department of Electronics and Communication Engineering,
Stanley College of Engineering and Technology for Women, Hyderabad,India.

Abstract:

Data security is protecting data, from destructive forces, and from the unwanted actions of unauthorized users. Data Security is primary concern for every communication system. There are many ways to provide security to data that is being communicated. In this paper the proposed technique is data can be transmitted to and received from remote Zigbee communication device. However, what if the security is assured irrespective of the hackers or from the noise. This Paper describes a design of effective security for data communication by designing standard algorithm for encryption and decryption.

Keywords:

Encryption,Security,ARM,Wireless Communication, Zigbee.

I. INTRODUCTION:

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. 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 .Zigbee is a PAN technology based on the IEEE 802.15.4 standard. Unlike Bluetooth or wireless USB devices, Zigbee devices have the ability to form a mesh network between nodes.

Meshing is a type of daisy chaining from one device to another. This technique allows the short range of an individual node to be expanded and multiplied, covering a much larger area.The source information is generated by PS2 Keyboard and this will be encrypted and is sent to destination through Zigbee modules. The receiving system will check the data according to a specific algorithm and displays on the LCD.The proposed technique is built around the controller in the transmitter and receiver section. The controller provides all the functionality of the display and wireless control. It also takes care of creating different display effects for given text. Alphanumerical keyboard is interfaced to the transmitter to type the data and transmit. The message can be transmitted to multi point receivers.

After entering the text, the user can disconnect the keyboard. At any time the user can add or remove or alter the text according to his requirement. Whenever the message is transmitted to the receiver section the garbage or junk message will be displayed on the receiver section 16X2 LCD. In order to read the original message the user should press the encryption key which is connected in the receiver sectionHere we can also have the knowledge about the consuming units of the loads connected through the same wireless network.For example if 2 loads (fan, light) are connected and it has consumed 5 units that will be displayed in LCD at the receiver section. So that we cannot only have the data with security but also we can have the knowledge about the loads connected.

II. RELATED WORK:

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

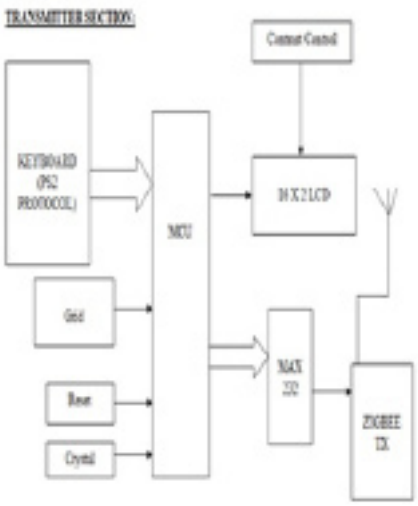

Fig 1: Transmitter Section

RECEIVER SECTION:

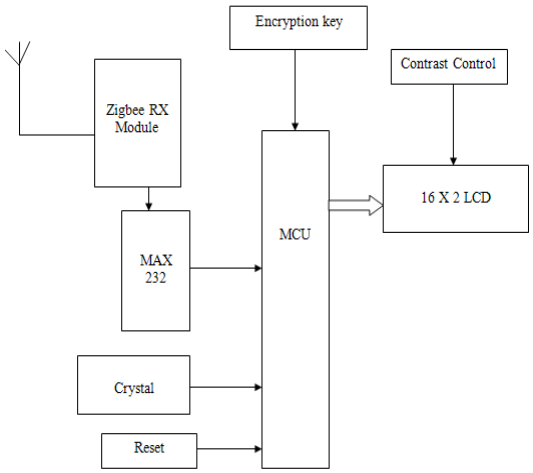

Fig 2: Receiver Section

The LPC2148 are based on a 16/32 bit ARM7TDMI-S™ CPU with real-time emulation and embedded trace support, together with 128/512 kilobytes of embedded high speed flash memory. A 128-bit wide memory interface and unique accelerator architecture enable 32-bit code execution at maximum clock rate. For critical code size applications, the alternative 16-bit Thumb Mode reduces code by more than 30% with minimal performance penalty. With their compact 64 pin package, low power consumption, various 32-bit timers, 4- channel 10-bit ADC, USB PORT,PWM channels and 46 GPIO lines with up to 9 external interrupt pins these microcontrollers are particularly suitable for industrial control, medical systems, access control and point-of-sale.

With a wide range of serial communications interfaces, they are also very well suited for communication gateways, protocol converters and embedded soft modems as well as many other general-purpose applications.

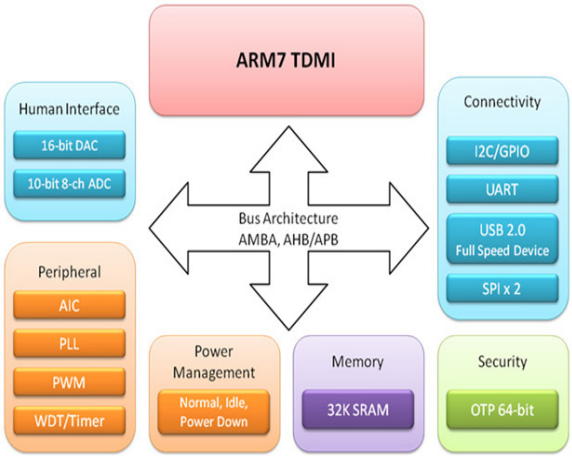

Fig 3 : ARM7 Architecture

ARM7TDMI Processor Core :

• Current low-end ARM core for applications like digital mobile phones

• TDMI

T: Thumb,16-bit compressed instruction set.

D: on-chip Debug support, enabling the processor to halt in response to a debug request

M: enhanced Multiplier, yield a full 64-bit result, high performance

I: Embedded ICE hardware

• Von Neumann architecture

Zigbee:

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

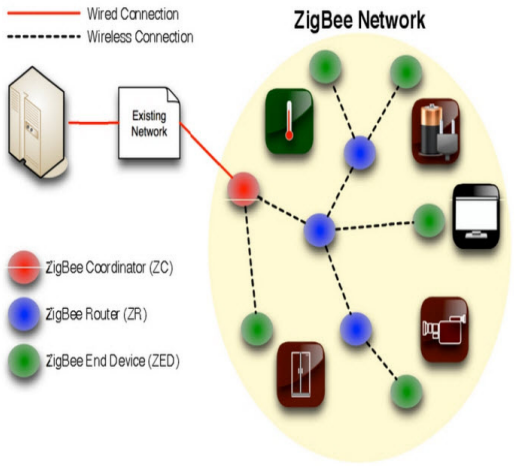

Fig 4 : Zigbee Technology

Zigbee is a PAN technology based on the IEEE 802.15.4 standard. Unlike Bluetooth or wireless USB devices, ZigBee devices have the ability to form a mesh network between nodes. Meshing is a type of daisy chaining from one device to another. This technique allows the short range of an individual node to be expanded and multiplied, covering a much larger area.

Zigbee is the wireless device for transmitting and receiving purpose or simply it called as Transceiver. The range of the Zigbee is covered as 100m. Its range is 10 times better than bluetooth device so it can be more preferable one in wireless device.

Technical Specifications of Zigbee

- Frequency band2.400 - 2.48 GHz
- Number of channels16
- Data rate250 kbps
- Supply voltage1.8 – 3.6 V
- Flash memory128 kB
- RAM8kB
- EEPROMkBOperating
- Temperature-40 — +85 °C

PS/2 (Play Station 2) :

The PS/2 connector is a round shape of 6-pin Mini-DIN connector used for connecting some keyboards and mice to a PC compatible compute r system.

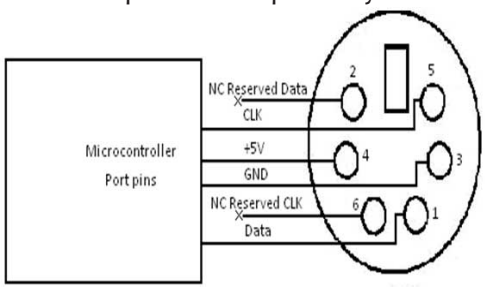

Fig5 :Interfacing PS2 with Micro Controller

Interfacing PS/2:

Fig. 5 shows how to interface PS/2 port to microcontroller.The PS/2 bus includes both clock and data. Both a mouse and keyboard drive the bus with identical signal timings and both use 11-bit words that include a start, stop and odd parity bit. However, the data packets are organized differently for a mouse and keyboard. Furthermore, the keyboard interface allows bidirectional data transfers so the host device can illuminate state LEDs on the Keyboard.

GRID :

The term grid usually refers to a network, and should not be taken to imply a particular physical layout or breadth. Grid may also be used to refer to an entire electrical network, a regional transmission network or may be used to describe a sub network such as a local utility's transmission grid or distribution grid. The proposed technique uses regulated 3.3V, 500mA power supply. Unregulated 12V DC is used for relay. 7805 three terminal voltage regulator is used for voltage regulation. Bridge type full wave rectifier is used to rectify the ac output of secondary of 230/12V step down transformer.

MAX 232:

Max232 IC is a specialized circuit which makes standard voltages as required by RS232 standards. This IC provides best noise rejection and very reliable against discharges and short circuits.MAX232 IC chips are commonly referred to as line drivers.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

III . METHODOLOGY:

The data can be sent to other place with full security. Data need to be given using keyboard and sent using zigbee to other place.The used power (number of units) will also be sent to the receiver. Garbage value is received at other place first.If the encryption key is given then it will be known that the person is authorized. So that the entered data at the other end will be given displayed here .

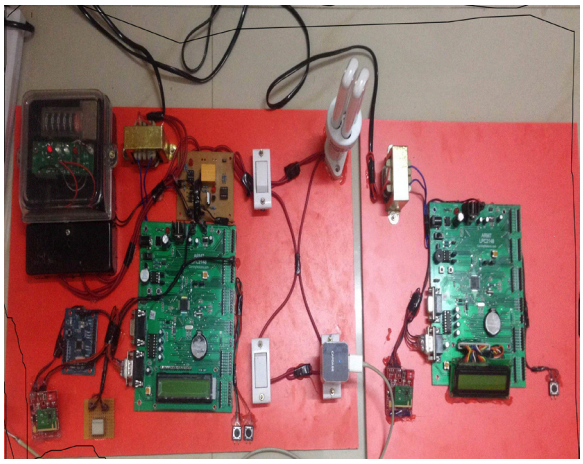

Fig 6 : Demo System

DSE:

In present work, the dynamic secret is employed to design the DSE scheme for grids wireless communication. In this session, we firstly introduce the basic algorithms of dynamic secret; and then present the DSE scheme. The sender and receiver monitor the error retransmission in link layer to synchronously select a group of frames. These frames are hashed into dynamic secret to encrypt the data.

1)Dynamic secret Generation: On the link layer's communication, error retransmission happens unavoidable and randomly at both side of the sender and the receiver. According to Stop-and-Wait (SW) protocol, the sender transmits a frame and waits for the corresponding acknowledgement before sending a new frame. If a frame is only transmitted once and its acknowledgement frame is received in time, this frame is named as one time frame (OTF). After transmitting, the packet 1 is confirmed as an OTF on the sender until the acknowledgement of packet 1 is received; it is confirmed on the receiver until the second packet is received.

It will be added into OTF set . Both the transmitted frame (packet 2) and acknowledgement (packet 3) are retransmitted, thus they are not added into OTF set. Once the number of OTF set reaches the threshold, the sender and receiver agree on a uniformly random choice of universal-2 hash functions to com-press into the dynamic secret . Then, the is reset to empty.

2)Encryption/Decryption: When a new dynamic secret is generated, it will be applied to update the encryption key at both sides of communication. This symmetric encryption key is used to encrypt the data at sender and decrypt the cipher at receiver. To reduce the computation consumption, the XOR function is used for encryption and decryption.

DSEScheme for Wireless Communication

Dynamic secret-based encryption (DSE) scheme is designed to secure the wireless communication between the smart devices and control center. The framework of DSE scheme consists of retransmission sequence generation (RSG), DS generation (DSG), and encrypt/decrypt.

1) RSG: This module is applied to monitor the link layer error retransmission.The communication packets which have been retransmitted are marked as "1" and the non-retransmitted packets are marked as "0."The pervious packets are coded as 0/1 sequence , named as retransmission sequence (RS).In DSE, RS is applied to replace the OTF set for dynamic secret generation due to the limitation of computation capability and storage resources.

2) DSG: Once reaches the threshold (length of RS), it would be compressed to a DS in DSG module. Considering the limitation on computation power, the hash functions are recommended in DSG module.are recommended in DSG module.

$$DS(k) = f_{HASH}(\text{RS})$$

3) Encrypt/Decrypt: The new dynamic secret is applied to update the dynamic encryption key (DEK) by

$$DEK(k) = DS(k) \oplus DEK(k-1)$$

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

D is generated at both sides of communication synchro-nously. The sender applies it to encrypt the , and the re-ceiver applies it to decrypt the . XOR function, as one of the most light- weight and easy-implementation algorithm, is applied to update the DEK and encrypt/ decrypt the data on both sides. If DEK is shorter than the data, is replicated and padded circularly to generatewhose length is equal to the raw data or the raw data or cipher text.

$$Data \bullet DEK^{*}(k) = Cipher$$
$$Cipher \bullet DEK^{*}(k) = Data$$

IV.CONCULSION:

In this paper, a dynamic secret based encryption scheme is designed to secure the wireless communication of SG. To reduce its complexity, the retransmission sequence is proposed to up-date dynamic encryption key, replacing the OTF set;A demo system is developed to investigate the performance of DSE scheme. The numerous experiments reveal that:

1) the DSE scheme can protect the users against eavesdropping by updating the dynamic encryption key with retransmission sequence in communication, even the attackers know the details of DSE scheme and obtain the encryption key at some time; 2) it is a light-weight encryption method with only simple operations, such as MD2 and XOR; 3) it has good compati-bility, which could be integrated with many wireless techniques and applications, such as ZigBee and Modbus.

REFERENCES:

[1]Ting Liu, Member, IEEE, Yang Liu, Yashan Mao, Yao Sun, Xiaohong Guan, Fellow, IEEE,Weibo Gong, Fellow, IEEE, and Sheng Xiao,"A Dyanamic Secret Based Encryption using Smartgrid Wireless Communication", 1949 -3053 © 2013 IEEE.

[2]R. Moghe, F. C. Lambert, and D. Divan, "Smart "Stick-on" sensors for the smart grid," IEEE Trans. Smart Grid, vol. 3, pp. 241–252, 2012.

[3]Federal Energy Regulatory Commission, "Renewables & energy effi-ciency—Generation & efficiency standards" 2011 [Online]. Available: http://www.ferc.gov/market-oversight/othr-mkts/renew.asp

[4]K. Ren, Z. Li, and R. C. Qiu, "Guest editorial cyber, physical, and system security for smart grid," IEEE Trans. Smart Grid, vol. 2, pp. 643–644, 2011.

[5]"The smart grid: An introduction," in DOE's Office of Electricity De-livery and Energy Reliability 2008.

[6]P. Jokar, N. Arianpoo, and V. C. M. Leung, "A survey on security issues in smart grids," Security Commun. Netw., 2012 [Online]. Avail-able: http://http://onlinelibrary.wiley.com/doi/10.1002/sec.559/ab-stract

[7]T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, "A novel method to de-tect bad data injection attack in smart grid," in Proc. IEEE INFOCOM Workshop Commun. Control Smart Energy Syst..

[8]P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security Privacy, vol. 7, pp. 75–77, 2009.

[9]Office of the National Cordination for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability stan-dards," 2010 [Online]. Available: http://www.nist.gov/smartgrid/

[10]Cisco,, "Security for the smart grid," 2009, White Paper [On-line]. Available: http://www.cisco.com/web/strategy/docs/en-ergy/white_paper _c11_539161.pdf

[11]W. Xudong and Y. Ping, "Security framework for wireless communi-cations in smart distribution grid," IEEE Trans. Smart Grid, vol. 2, pp. 809–818, 2011.

[12]P. Jokar, H. Nicanfar, and V. C. M. Leung, "Specification-based intru-sion detection for home area networks in smart grids," in Proc. 2011 IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), pp. 208–213.

[13]Z. Yichi, W. Lingfeng, S. Weiqing, R. C. Green, and M. Alam, "Arti-ficial immune system based intrusion detection in a distributed hierar-chical network architecture of smart grid," in Proc. 2011 IEEE Power Energy Soc. Gen. Meet., pp. 1–8.

[14]M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "A lightweight message authentication scheme for smart grid commu-nications," IEEE Trans. Smart Grid, vol. 2, pp. 675–685, 2011.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

[15]S. Nguyen and C. Rong, "ZigBee security using identity-based cryp-tography autonomic and trusted computing," in Proc. 4th Int. Conf. Autonomic Trusted Comput. (ATC'07), 2007, vol. 4610, Lecture Notes in Computer Science, pp. 3–12.

BIOGRAPHIES:

B.Mounika Reddy

received her B.E degree in Electronic and Communication Engineering from Stanley College of Engineering and Technology for Women, Hyderabad. She is pursuing Masters in Embedded Systems from Stanley College of Engineering and Technology for Woman, Hyderabad, India.

V.Sudarshani Kataksham

received her Bachelor of Engineering degree in Electronics and communication Engineering from Jawaharlal Nehru Technological University, Hyderabad in 2009 and pursued her M.TECH in VLSI SYSTEM DESIGN from CVSR college of Engineering and Technology JNTU, Hyderabad. She is currently working as a Asst Professor in Electronics and communication Engineering Department at Stanley College of Engineering And Technology For Women ,Abids, Hyd. And she has three years of teaching experience and attended various seminars. Her areas of interest include High performance VLSI Design andVHDL based system design.