International Journal of Research Studies in Science, Engineering and Technology
Volume 2, Issue 7, July 2015, PP 185-189
ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

Implementation of Crypto System Based Single Ended Wireless Communication Link for Defense Sensor Network Applications

M. Reddamma

Arjun College of Technology and Sciences
keerthana.mr@gmail.com

J. Lingaiah

HOD (ECE Dept) & Associate Professor
Arjun College of Technology and Sciences
hodeceacts@gmail.com

Y. Kiran

Application Engineer
Unistring Tech Solutions Pvt Ltd.
ykiran.uts@gmail.com

Abstract: *The communication system which requires sensitive data transfer uses secured cryptographic algorithms to convert the data into an unrecognizable format. These algorithms are classified into symmetric and asymmetric, which employs private and public keys respectively. The symmetric cipher is further classified into stream and block ciphers. This proposed paper focuses on the block cipher which allows feasibility for the key generation and these generated keys are used for cryptographic applications with reduced hardware complexity. Wireless sensor networks are one of the highly emerging areas and found really useful in environmental studies and military applications. In sensor networks a set of nodes randomly deployed communicate through wireless links and provide the information as on when required.*

Keywords: *Key, Wireless.*

1. INTRODUCTION

The communication system which requires sensitive data transfer uses secured cryptographic algorithms to convert the data into an unrecognizable format. These algorithms are classified into symmetric and asymmetric, which employs private and public keys respectively. The symmetric cipher is further classified into stream and block ciphers. This proposed paper focuses on the block cipher which allows feasibility for the key generation and these generated keys are used for cryptographic applications with reduced hardware complexity.

In the existing system, the hardware implementation of block ciphers has limited feasibility in scheduling the key which is the primary resource for high secured data transfer. Since the existing system uses predefined key for the encrypting process, the system can offer narrowed security level though they use complex security algorithms. The major drawback in the existing system is that there is no key generation unit to increase the efficient change of key parameter for a secured data transfer.

2. PROPOSED SYSTEM

In order to increase the speed and to reduce the hardware complexity, this proposed system focuses on the light weight security algorithm Tiny Encryption Algorithm TEA which can be implemented in microcontroller to adapt with many real time constraints such as memory, The embedded based applications need sensitive data transfer between different nodes. Data loss and low cost. The additive feature of this proposed system is that it uses Key Generation Unit (KGU) to produce the random key to make it optimal for sensitive data transfer in many real-time applications. This above work uses microcontroller and the performances of this cryptosystem is analyzed by implementing the cryptographic algorithm TEA with key generation unit. The work extends with implementing the two different modes of communication serial (UART) and wireless transmission ZigBee to transfer the data from encryption unit to decryption unit. It also includes EEPROM chip to save different keys which can be accessed by using I2C protocol. To overcome the above disadvantages we go for wireless network protocol ZigBee which can be used in different applications such as oceanography, weather monitoring, and defense, scientific, commercial, agricultural and industrial applications.

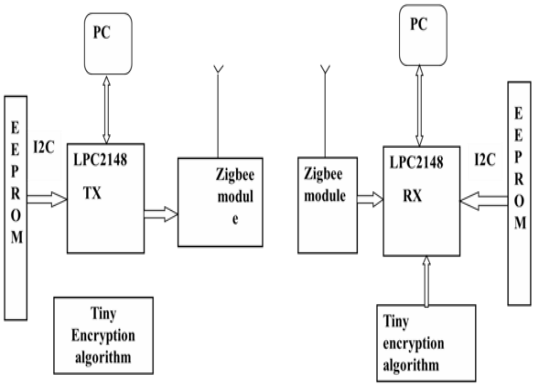

Fig1. *Block Diagram*

3. HARDWARE IMPLEMENTATION

3.1. LPC2148 Microcontroller

LPC2148 microcontrollers are based on a 32 bit ARM7TDMI-S CPU with real-time emulation and embedded trace support that combines the microcontroller with embedded high speed flash memory of 512kb. A 128-bit wide memory interface and unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces the code by more than 30% with minimal performance penalty.

3.2. 4K I2C Serial EEPROM

The Microchip Technology Inc. 24AA04/24LC04B (24XX04*) is a 4 Kbit Electrically Erasable PROM. The device is organized as two blocks of 256 x 8-bit memory with a 2-wire serial interface. Low-voltage design permits operation down to 1.7V, with standby and active currents of only 1 μA and 1 mA, respectively. The 24XX04 also has a page write capability for up to 16 bytes of data. The 24XX04 is available in the standard 8-pin PDIP, surface mount SOIC, TSSOP, 2x3 DFN, 2x3 TDFN, and MSOP packages and is also available in the 5-lead SOT-23, or 4-lead Chip Scale package.

3.3. ZigBee

ZigBee is the product of the ZigBee Alliance, an organization of manufacturers dedicated to developing a new networking technology for small, ISM-band radios that could welcome even the simplest industrial and home end devices into wireless connectivity ZigBee uses a basic master-slave configuration suited to static star networks of many infrequently used devices that talk via small data packets. It allows up to 254 nodes. Bluetooth's protocol is more complex since it is geared towards handling voice, images and file transfers in adhoc networks. Bluetooth devices can support scatter nets of multiple smaller non-synchronized networks. It only allows up to 8 slave nodes in a basic master-slave.

4. FLOW CHART

Transmitter Side

- Message is entered by the user.
- Set the baud rate as 9600.
- The converted data is sent to LPC2148 through UART0, which is initialized to receive and transmit data.
- A 128 bit random key is generated already stored in EEPROM which is entered and the plain text is displayed on the terminal and is sent to LPC2148 through UART0.
- The data and the key are stored in a FIFO buffer.
- In the microcontroller, the data is encrypted using TEA to obtain cipher text also consisting of the key no which is received using UART1.
- The encrypted data is also displayed on the LCD and the terminal.

- UART1 which is initialized to transmit data sends the cipher text to the receiver using ZigBee module.

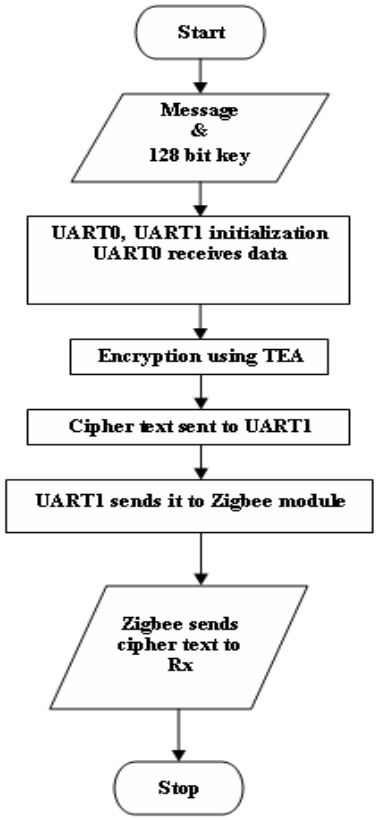

Fig2. *Implementation at Transmitter*

Receiver Side

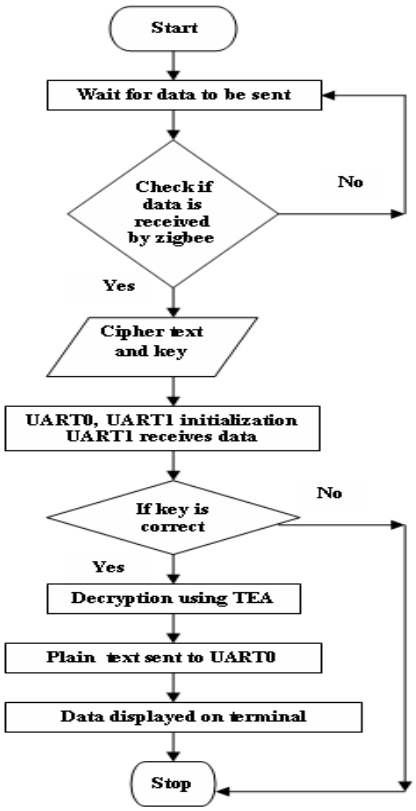

Fig3. *Implementation at Receiver*

- Set the baud rate as 9600.
- Wait for the cipher text to be sent by the transmitter.
- The ZigBee module receives the data and sends it to UART1, which is initialized to receive and transmit data.
- After the reception of cipher text by UART1, the key no is decoded.
- The key and the data are stored in a FIFO buffer.
- The cipher text and the key are displayed on the terminal.
- With the help of key number the 128 bit key is read from EEPROM which is used to decrypt the cipher text using corresponding decryption algorithm as in transmitter at LPC2148.
- After decryption, the data is sent to UART0 which is initialized as a receiver.

5. HARDWARE & RESULTS

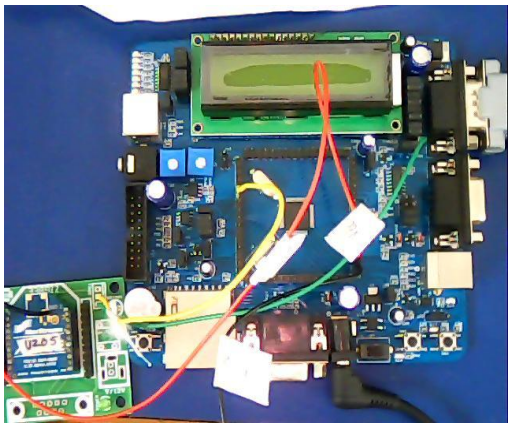

Fig4. *Hardware*

```
Enter any key  to Transmit

Enter Message You want to Transmit

Data is : akbarkha

Data before enc  :  akbarkha

EEPROM Location is (random) == 3Key
is-->3333333333333333
```

Fig5. *Transmitter Data*

```
Data Received a3Yáła]äŘ1


EEPROM Location is (random) == 3Key
is-->3333333333333333

data before dec  :  Yáła]äŘ1

Data after Decryptionakbarkha3

 Enter any key to Transmit
```

Fig6. *Receiver Data*

REFERENCES

[1] Soren Rinne, Thomas Eisenbarth, and Christ of Paar, "Performance Analysis of Contemporary Light-Weight Block Ciphers on 8-bit Microcontrollers", Horst Gortz Institute for IT Security Ruhr University Bochum 44780 Bochum, Germany.

[2] Edi Permadi, "The Implementation of Tiny Encryption Algorithm (TEA) on PIC18F4550 Microcontroller", Electrical Engineering 2005, President University.

[3] Devesh C. Jinwala, Dhiren R. Patel, Department of Computer Engineering S. V. National Institute of Technology, INDIA; Kankar S.Dasgupta Space Applications Centre, Indian Space Research Organization, INDIA, "Investigating and Analyzing the Light-weight ciphers for Wireless Sensor Networks", March 10, 2009.

[4] Thomas Eisenbarth, Ruhr University Bochum; Sandeep Kumar, Philips Research Europe; International Journal of Advanced Electrical and Electronics Engineering, (IJAEEE) ISSN (Print): 2278-8948, Volume-2, Issue-3, 2013 72 Christ of Paar and Axel Poschmann, Ruhr University; Bochum Leif Uhsadel, Catholic University of Leuven, "A Survey of Lightweight-Cryptography Implementations", IEEE Design & Test of Computers dtco-24-06-pos.3d 4/10/07.

[5] P.Israsena, Thailand IC Design Incubator (TIDI) National Electronics &Computer Technology Center (NECTEC), "Design and implementation of low power hardware encryption for low cost secure RFID using TEA", 2005 IEEE ICICS.

[6] Issam Damaj, Samer Hamade and Hassan Diab "Efficient tiny hardware cipher under verilog", in High Performance Computing & Simulation Conference, 2008.

[7] Laszlo Hars, Cortlandt Manor, NY (US), "Switching electronic circuit for Random Number Generation", US Patent August 3, 2004.

[8] Laszlo Hars, Cortlandt Manor, NY (US),"Latching electronic circuit for random number generation", US Patent October 17, 2006.

AUTHORS' BIOGRAPHY

M. Reddemma is presently pursuing final semester M. Tech in Embedded Systems at Arjun College of Technology and Sciences, Secunderabad, Telangana, India.

Jada Lingaiah is presently working as Head Of Department (ECE), Associate Professor in the department of Electronics and Communication Engineering in Arjun College of Technology and Sciences, Secunderabad, Telangana, India.

Y. Kiran is presently working as Application Engineer in Unistring Tech Solutions Pvt Ltd, Hyderabad, Telangana, India.