Embedded Web Server with Data Security for Wireless Sensor Networks

Jayashri S Janiwarad

IBM India Pvt Ltd. Bangalore

Abstract- Sensor network has quick installation, dynamic configuration features. Security of the data in the wireless sensor network has become a critical issue. As the applications are increasing, privacy preservation is an important issue in wireless sensor network. Depending on the nature of the installment of the network and the data that is exchanged between two nodes, steps taken to secure the data have to be decided. Security mechanisms like authentication and encryption play a vital role. The existing encryption algorithms cannot be applied directly to WSN. Care has to be taken to modify these algorithms to fit into WSN, as these modifications may lead to additional computations which consume additional energy and additional communication. This paper aims at implementing one such encryption algorithm which is easy to develop using common programming language like C and easy to port across different processors varying in processing speed, computations and operating word size.

I. Introduction

A. Statement of the problem

Security of the data collected by a sensor node realized using an 8 bit microcontroller should be achieved by encrypting the data using a standard encryption algorithm. This encrypted data when received by 32 bit central node; it should decrypt the same and display the actual value on the webpage hosted by the embedded web server residing on the central node.

B. Objective of the project

- This project realizes an embedded web server, which enables data acquisition and status monitoring with the help of standard web browser.
- An efficient Encryption algorithm is implemented so that the data packets obtained from heat and temperature sensors are encrypted and sent to the base station. The base station will receive the data packets and decrypt them. The base station is also the center node with the functionality of the embedded web server.
- User can monitor remote temperature and heat information remotely through web browser.

C. Scope of the Project

- Implement a sensor node with PICF1877A as a processing unit, LM35 as a temperature sensor, CC2500 transceiver for data transmission and LCD interface for user interface.
- The data read from the sensor is encrypted by Tiny Encryption algorithm by the sensor node before transmitting it to the central node.
- Central node is realized on a Mini2440 Friendly Arm board. Transceiver CC2500 is used for data reception. Embedded web server is implemented on this board.
- The encrypted data received from sensor node through CC2500 is decrypted using the same Tiny encryption algorithm and the value is displayed on the webpage.

II. Implementation

The implementation of the project "Implementation of Embedded Web Server with Data Security for Wireless Sensor network" is divided into two modules. One module is the PIC module and the other is the ARM module. The two modules are connected through wireless media.

A. System Architecture

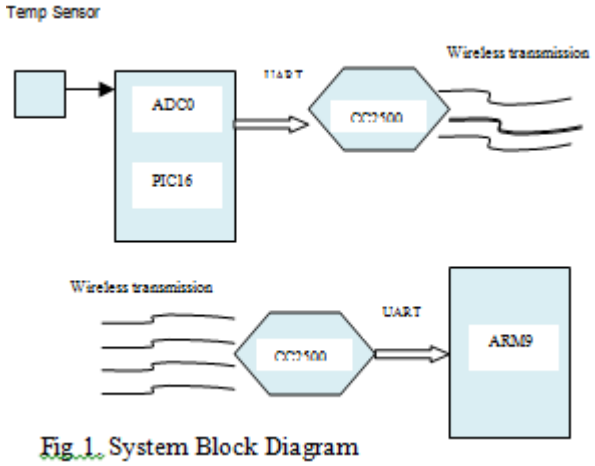


Fig.1. System Block Diagram

B. Diagram Software Design

PIC16F877A which realizes the sensor node with temperature sensor to sense the environmental temperature. The main task of the PIC module is to encrypt the data received from sensor through ADC module and send it to the CC2500 module to transmit it via wireless medium. When the power is ON, the first thing the controller has to do is to initialize the internal and the peripheral modules. So the ADC, UART and the LCD modules are initialized with proper settings, and the port numbers that are treated as either input or output by the respective peripheral. In a infinite loop the value of temperature is read into the registers of the ADC module. This value is multiplied by 0.48 to get the reading in the convention form. This value is written to the register which writes the data on the LCD, at the same time encoded calling encode_data method. The encoded data is written to UART register to send it through transceiver.

The ARM module is the one on which the central node is realized. This module collects the encrypted data sent by the sensor node. The encrypted data is read through transceiver connected to the arm board. The data is decrypted and displayed on the webpage. The embedded web server is also implemented here.

ARM is OS based system and software development process for OS based system includes the establishment of the cross-compiler, the transplant of the boot loader, transplant of the embedded Linux, development of the web server and decryption algorithm.

An embedded web server like any general purpose web server accomplishes tasks like receiving the request from client, processing that request and responding to those requests and finally returning the results to the client. This system works in B/S mode in which the client need not be programmed specifically for this application. The client PC is connected to the Internet through a browser can get access to the embedded Web server. The user can perform remote login view the web pages and perform required operation. Hence this mode is simple to use, convenient to maintain, and easy to extend as compared to traditional C/S mode. The static web pages are saved in the system file system and they get displayed on the browser of the client system.

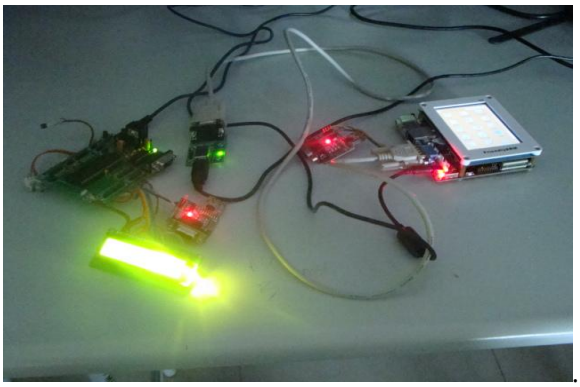
The programming on ARM includes creating a thread so that one thread takes care of serving the web requests, and the main process does the processing of the data read from transceiver. This process in a forever loop reads the data from serial port, once the data is read call the decryption method to decode and get the actual value.

The child process opens a socket, bind to the port and listen on that port. Whenever there is a request from the client, it identifies the page requested by client and the same is sent to the client through socket connection. Appropriate error pages and data pages are displayed.

III. RESULTS

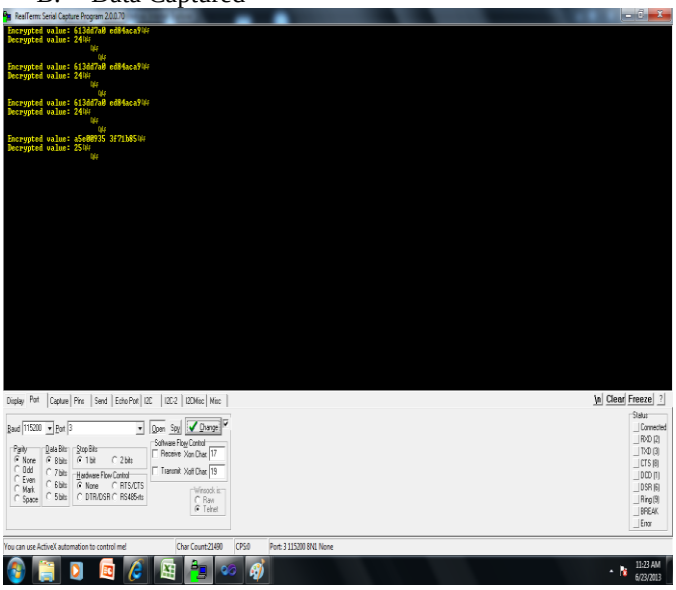
A. Hardware Connections

The overall connection of the modules together looks like



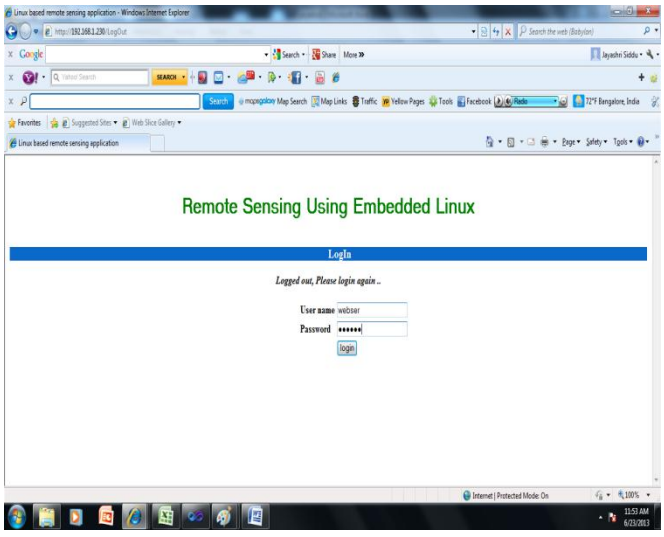
The data encrypted is sent by the wireless module of PIC. Since the data is sent through the serial interface, we can capture the data at the serial interface of the ARM 9 module. To view the encrypted data, I have used serial to USB converter from USB port of the laptop to the serial port of ARM. Real Term is the tool to capture the data on the serial link. It should be configured with proper port number (usually the OS does a auto detect) and baud rate. We can also specify the file name where the captured data can be saved.

B. Data Captured

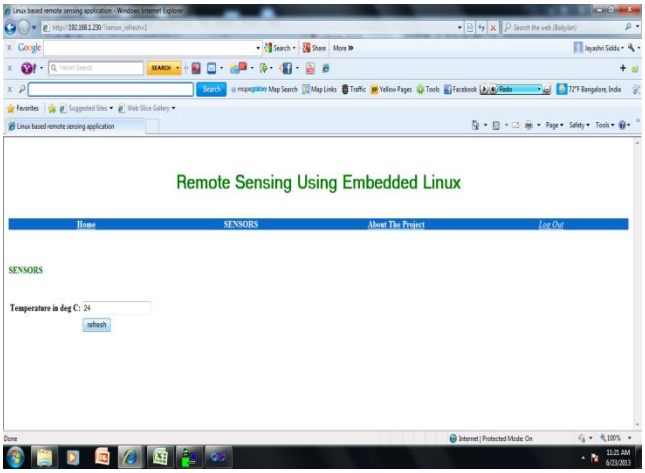


C. User Interface

The main login page which asks for username and password from the user looks like. The operator needs to authenticate himself by providing the username and password. If he is the right operator he will be allowed to view the sensor page.



The sensor page displays the decoded value on the box specified. This page gets refreshed every two seconds, and any variation in the temperature will be captured automatically when the page gets refreshed. There is also option for refreshing the page manually whenever the operator feels like.



IV. Conclusions

This project has demonstrated how to get fully functional embedded product developed from scratch. This included working on two different controllers, cross compilation and deployment of essential libraries, the configuration of embedded Linux and the development of embedded web server.

It was a great learning in implementing this project. I started this project keeping in mind lot of features to implement on the web server side and the security algorithm was a bit unclear. I could not implement the full set of requirements that were set out before the commencement of this project. However I have implemented at least the minimum. The original requirement list was not possible to accomplish so a re-scope was necessary.

Finally I would like to say that this paper explains a end to end deployable embedded product.

V. Future Work

- To achieve higher security the cipher key used for encryption and decryption can be generated in the PIC module using rand() function. The generated key can be used for encryption in PIC module and the same needs to be transmitted to arm module before transmitting the encoded data. The arm module can use this key to decrypt the data.
- The current project is tested with a single client node, the same can be enhanced with multiple client nodes, and then the client should send a identifier to the server so that it can display the correct data on web page for each client node.
- The embedded web server is currently supporting single user login, it can be enhanced to multiple user login with different user privileges.
- The SNMP support on ARM can be enabled to send email alerts to configured user email ids which correspond to client nodes.

References

[1] Fundamentals of Wireless Sensor Networks by Wiley Series on Wireless Communications and Mobile Computing.

[2] First Step Toward Internet Based Embedded Control System Eka Suwartadi, Candra Gunawan, Ary Setijadi P, Carmadi Machbub Laboratory for Control and Computer Systems Department Of Electrical Engineering Bandung Institute Of Technology, Indonesia

[3] Design and development of embedded web server based on Arm9 and Linux Deepa.Chekka1*and Ravi Kanth2 World Journal of Science and Technology 2012, 2(10):94-97 ISSN: 2231 – 2587

[4] Design and Implementation of Embedded Web Server Based on ARM and Linux Yakun Liu Xiaodong Cheng College of Electronic Information Engineering Inner Mongolia University Hohhot, P.R. China

[5] Design and Development of ARM Processor Based Web Server V.Billy Rakesh Roy1, Sanket Dessai1, and S. G.Shiva Prasad Yadav 1 1 M S Ramaiah School of Advanced Studies in Collaboration with Coventry University (UK)/Embedded Design Centre,

[6] Embedded Web Server Based on DAC System Using ARM S.A.N.Sandeep, P.Malyadri / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 4, July-August 2012, pp.

[7] Security in cognitive wireless sensor networks. Challenges and open problems Araujo et al. EURASIP Journal on Wireless Communications and Networking 2012, 2012:48

[8] SECURITY IN WIRELESS SENSOR NETWORKS By ADRIAN PERRIG, JOHN STANKOVIC, and DAVID WAGNER

[9] A review on security issues in wireless sensor network

Rajeshwar Singh1, Singh D.K.2 and Lalan Kumar3 Journal of Information Systems and Communication, ISSN: 0976-8742 & E-ISSN: 0976-8750, Vol. 1, Issue 1, 2010, PP-01-07

[10] Coverage and Connectivity Issues in Wireless Sensor Networks AMITABHA GHOSH and SAJAL K. DAS Department of Computer Science and Engineering, University of Texas at Arlington

[11] Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey Network Protocols and Algorithms ISSN 1943-3581 2011, Vol. 3, No. 1

[12] Performance evaluation of scalable encryption algorithm for wireless sensor networks Murat Çakıro_lu*, Cüneyt Bayilmi_, Ahmet Turan Özcerit and Özdemir Çetin

[13] Energy Efficient Encryption Algorithm for Wireless Sensor Network A. Babu Karuppiah1, Dr. S. Rajaram2 International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 3, May - 2012 ISSN: 2278-0181 www.ijert.

[14] Analyzing and Modeling Encryption Overhead for Sensor Network Nodes Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu Center for Embedded Systems Research Departments of Electrical and Computer Engineering / Computer Science North Carolina State University, Raleigh, NC 27695

[15] SPINS: Security Protocols for Sensor Networks 2009 International Conference on Machine Learning and Computing IPCSIT vol.3 (2011) © (2011) IACSIT Press, Singapore

[16] Sensor Data Encryption Protocol for Wireless Network Security By Bharat Singh, Parvinder Singh & Dr. V.S. Dhaka Global Journal of Computer Science and Technology Volume 12 Issue 9 Version 1.0 April 2012 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[17] WIRELESS SENSOR NETWORK SECURITY ANALYSIS Hemanta Kumar Kalita1 and Avijit Kar

Authors

First Author – Jayashri S Janiwarad, e-mail :jaishri.sj@gmail.com, IBM India Pvt Ltd. Bangalore.