

Design of A network Data Security Circuit

¹ Nuha Abdelmageed Tawfig Khalil, ² Abdelrasoul Jabar Alzubaidi,

¹ Computer Department, Aljouf University, Sakaka – Saudi Arabia

² Electronics Engineering School, Sudan University of Science and technology, Khartoum – Sudan

Abstract

To safeguard information during electronic communication and data transmission processes across unsecured networks and provide security requirements, including authentication, confidentiality, integrity and non-repudiation. To achieve this goal, this paper proposed to design of a network data security circuit using two Basic Stamp2 Microcontroller, two wireless X-Bee modules, two computer and BASCOM language (TC++ program language) to generate non-standard algorithm (logic algorithm) for encrypted and decryption. The algorithm depends on ciphering the plaintext n times with n keys.

Keywords: Basic stamp2, ciphertext, Decrypted, Encryption, Network data security, plaintext, and X-Bee.

I. INTRODUCTION

Security of network communications is arguably the most important issue in the world today given the vast amount of valuable information that is passed around in various networks. Information pertaining to banks, credit cards, social security numbers, personal details, and government policies are transferred from place to place with the help of networking infrastructure. The high connectivity of the World Wide Web (WWW) has left the world 'open'. Such openness has resulted in various networks being subjected to multifarious attacks from vastly disparate sources, many of which are anonymous and yet to be discovered. This growth of the WWW coupled with progress in the fields of e-commerce and the like has made the security issue even more important.

A typical method for security that is used To safeguard information during electronic communication and data transmission processes across unsecured networks and provide security requirements is encryption [1].

Encryption is the process of encoding messages (or information) in such a way that cannot be read by eavesdroppers or hackers, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. An authorized party, however, is able to decode the ciphertext using a decryption algorithm, that usually requires a secret decryption key [2].

Implementing a demonstration project comprise of BASIC Stamp microcontroller, two wireless X-Bee modules, two computer and BASIC Stamp Editor v2.5 and Bascom language (TC++ program language) to protect information during electronic communication and data transmission across unsecured networks and most importantly to prevent data from falling into wrong hands.

II. METHODOLOGY

Design of a network data security circuit consists of two elements:

A. Hardware components:

The hardware components for this research paper consists of Parallax, Inc.'s BASIC Stamp2 modules, X-Bee wireless modules and computer. Upon using all this materials, a transmitter and a receiver circuit will be build.

Microcontrollers

Microcontrollers are frequently used device in embedded computing in which the application varies from computing, calculating, smart decision-making capabilities, and processes the data. Most of the electrical/electronic device, sensors and high-tech gadget can be easily interface and interact with microcontrollers to automate a system structure. For this research BASIC Stamp2 is used [3].

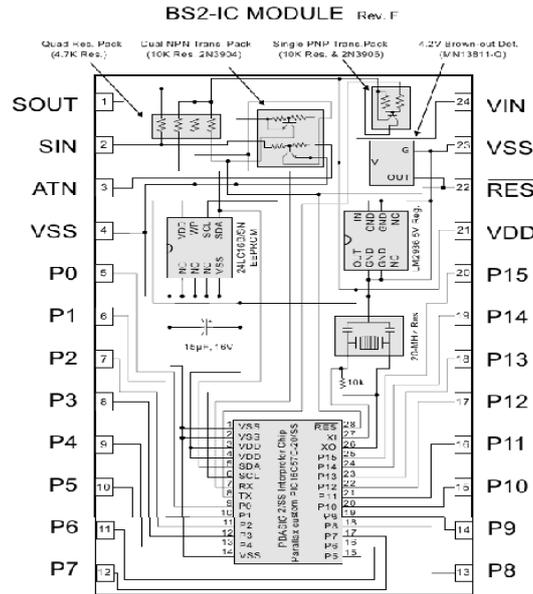


Figure 1: BASIC Stamp2

The BS2 microcontroller has a 24-pin Dual Inline Package (DIP) and 16 of them are used for I/O interface. The brain for the chip is Microchip Inc.'s PIC 16C57. Each pin can source (supply) a maximum current of 40mA and sink (draw) a maximum current of 50mA. A range of 5 to 15 direct current (VDC) power supply is sufficient to turn on BS2, because a voltage regulator embedded inside it, provides a steady 5VDC supply to the BS2 such that the high voltage will not damage the IC. BS2 has 2KByte (~500 PBASIC instructions) Electronically Erasable Programmable ROM (EEPROM), and RAM size 32 Bytes (6 I/O, 26 Variable) and is programmed using PBASIC language; the instruction set that is permanently stored on the BS2 ROM. The user-define program is downloaded into the EEPROM from a PC through a DB-9 serial cable connection between the PC and the microcontroller. The excess EEPROM can be used for long term data storage [4] [5].

X-Bee

X-Bee module is a device use to communicate via wireless network, it utilizes the IEEE 802.15.4 protocol which implements the entire features list below as to ensure data delivery and integrity:

- Media Access: A special feature to make certain two network nodes do not transmit at the same time causing data collisions and errors in communication.
- Addressing: A technique to ensure only the intended node uses the receive data, allowing data to be sent from one point to another point, or point to multi-point by sending a broadcast meant for all nodes on the network.
- Error Detection: A way to validate data received at the node correctly.
- Acknowledgements & Retries: A way to notify the transmitting node that the data was delivered successfully. Lacking this, several retries may be performed in an effort to deliver the data [3] [6].

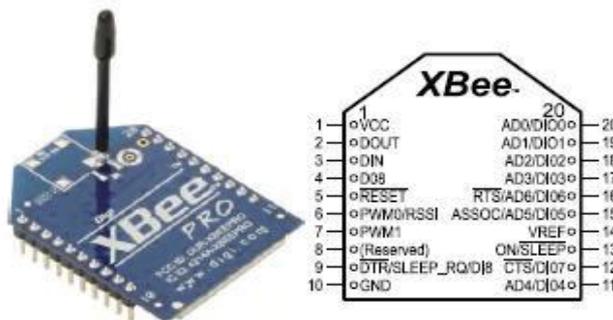


Figure 2: X-Bee Pro modules and Pin outs

Computer

To program the Basic Stamp2 with the windows interface, an IBM PC or compatible computer system the following components is needed [7] :

- IBM PC or compatible computer running windows 95, windows 98, or windows NT4.0 (S.P.3 recommended).
- 80468 (or greater) processor.
- 16 MB RAM (24 recommended).
- 1 MB free hard drive space.
- 256-color VGA video card (24 bit SVGA recommended).

D25 connection

The D25 connection used to connect Basic Stamp2 to computer parallel port for programming.

B. Software:

For this research there are two main softwares being used BASIC Stamp Editor v2.5 and Bascom language (TC++ program language).

- BASIC Stamp Editor v2.5, used to program the Basic Stamp2 microcontroller.
- Bascom language (TC++ program language) , used to write non-standard algorithm (logic algorithm) for encrypted and decryption.

The circuit design for this research is divided into two parts namely the transmitter and the receiver circuit. The interconnection for the transmitter and the receiver circuit are shown in Figure 3.

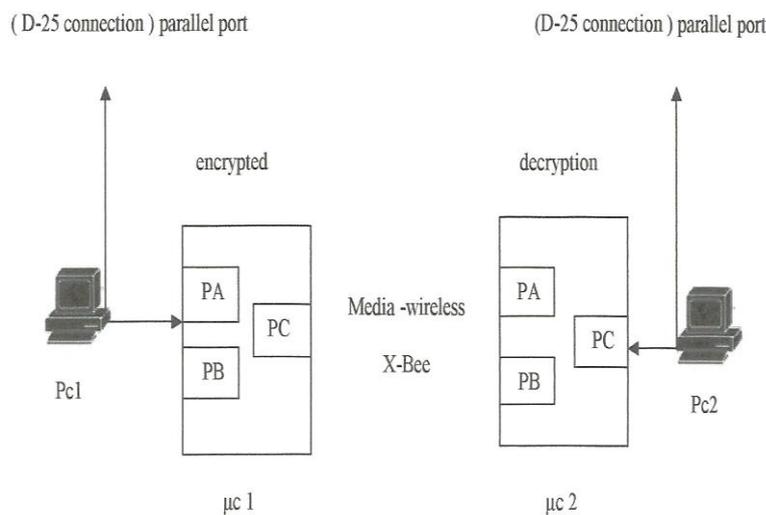


Figure 3 : block diagram for the circuit

In the transmitter circuit the message will be encrypted m times depending on the length of the key. The key will be converted to equivalent ASCII code. In this algorithm key will be inserted into the encrypted message after any encryption stage to form the new message for the next encryption stage. This process will be repeated m times. The number of the encryption stages will be given depending on the length of the key.

In the receive circuit the message will be decrypted by used the inverse method for encryption.

III. RESULTS

The flowchart of the program of the design of a network data security circuit is shown in Figure 4.

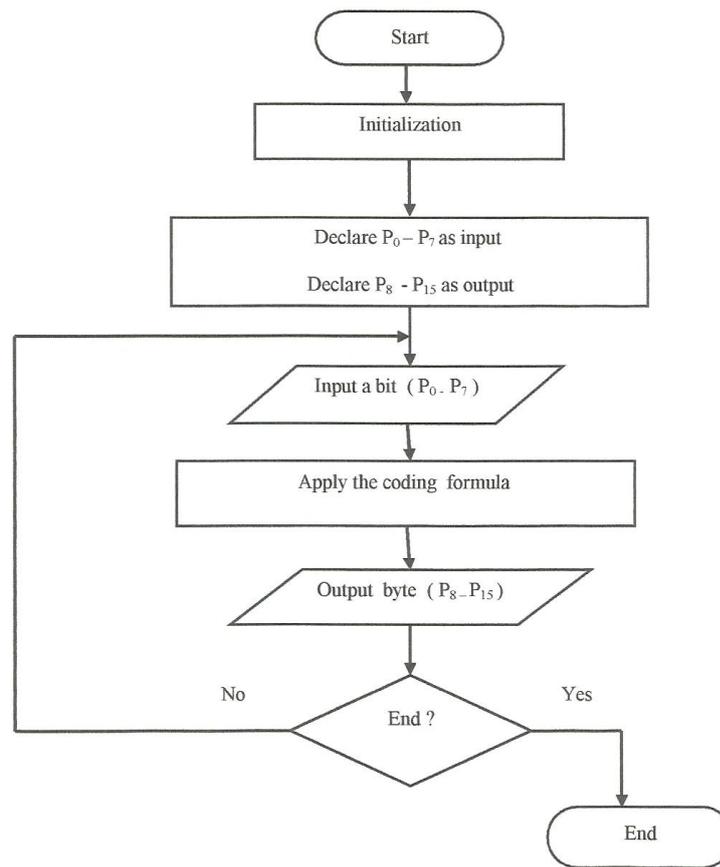


Figure 4: flowchart of the program of the design of a network data security circuit

IV. CONCLUSION

Design of a network data security circuit is the most important system to enhance security in transmission of data in network, to prevent data from falling into wrong hands and to provide the data security requirements, including integrity, authentication, non-repudiation and confidentiality. Design of a network data security circuit includes the following advantages:

- 1- Encrypted the message by using non-standard algorithm.
- 2- Very complicated because it encrypted and decrypted the message m times.

REFERENCES

- [1.] A Novel Scheme for Secured Data Transfer Over Computer Networks, Rangarajan Athi Vasudevan (University of Michigan, Ann Arbor, USA ranga@umich.edu). <http://arxiv.org/ftp/arxiv/papers/1002/1002.4530.pdf>.
- [2.] <http://en.wikipedia.org/wiki/Encryption>.
- [3.] International Symposium on Robotics and Intelligent Sensors 2012 (IRIS 2012), Wireless Traffic Light Controller for Emergency Vehicle through XBee and Basic Stamp Microcontroller, R.Hussin*, R.C.Ismail, E.Murralli, A.Kamarudin, School of Microelectronic Engineering, University Malaysia Perlis (UniMAP), <http://www.sciencedirect.com/science/article/pii/S187705812026239?np=y>
- [4.] Basic Stamp 2 microcontrollers comparisons. Retrieved April 28, 2012 from http://www.parallax.com/detail.asp?product_id=BS2-IC website of Parallax. Inc. developer and distributor of Basic Stamp 2 microcontroller.
- [5.] <http://www.parallax.com/BASICStampComparison/tabid/436/efault.aspx>.
- [6.] Basic Stamp 2 microcontrollers. Retrieved April 13, 2012 from <http://www.parallax.com/go/XBee> website of Parallax. Inc. developer and distributor of Basic Stamp 2 microcontroller.
- [7.] <http://books.google.com.sa/books?id=sQ9AigIIOKgC&pg=PA41&dq=connect+basic+stamp+2+with+computer+by+parallel+port&hl=ar&sa=X&ei=2llpUqv0Aeno4gTZ34CICQ&ved=0CC4Q>.