International Journal of Engineering Research and General Science Volume 2, Issue 4, June-July, 2014
ISSN 2091-2730

Secured Communication for Missile Navigation

Kulkarni Laxmi G[1], Dawande Nitin A[1]

[1]P.G Scholar, Department of Electronics and Telecommunication, Dr.D.Y.Patil College of Engg, Ambi

E-mail- kulkarnilaxmi.g@gmail.com,

Abstract— In order to improve the security of the Military kinds of network this work is proposed. Here the position of missile navigates as per the user's requirement. The user sends the co-ordinates through pc based server on the base station. For security purpose encryption is done with RC4algorithm implementation. The system that uses Human Computer Interaction and Visualization technology provides several encryption algorithms and key generators.

Keywords— missile navigation, RC4 algorithm, VNC, PN sequence, USB, encryption

INTRODUCTION

In today's world enemy warfare is an important factor of any nation's security. The national security mainly depends on army (ground), navy (sea), air-force (air).The important and vital role is played by the army's artillery such as scud missile, Bo force guns etc.

As the name suggests we are making a secure Navigation of Missile using encryption based RC4 algorithm. This is done with the use of an encryption key. This encryption key specifies how the message is to be encoded. An authorized party is able to decode the cipher text using a decryption algorithm, which usually requires a secret decryption key that adversaries do not have access to.

There are various types of encryption as AES, DES, and RC4 Algorithm etc. Encryption has long been used by militaries and governments to facilitate secret communication. An encryption based on chaos and AES algorithm [1]where the design and realization of an encryption system is based on the algorithm on ARM(S3C6410), which can encrypt and decrypt the information in many kinds of memorizers, such as UDisk, SD card and mobile HDD. The system that uses Human-Computer Interaction and Visualization technology provides several encryption algorithms and key generators. In this paper, they designed and implemented an encryption system to encrypt the stored data based on ARM (S3C6410). The PN sequences with good properties are generated from chaotic map and the system provides two kinds of encryption algorithm, one is stream cipher with XOR operation, the other is a hybrid algorithm of AES and chaos. In order to improve the security of the private information in memorizer, an encryption algorithm, which inherits the advantages of chaotic encryption, stream cipher and AES algorithm, is proposed in this paper.

The chaotic selective encryption of compressed video (CS ECV) exploits the characteristics of the compressed video [2]. Encryption is needed to protect the multimedia data. Compared with text encryption; multimedia encryption has some unique characteristics, such as the large size, high throughput, and real-time processing. An efficient, secure, and lightweight encryption algorithm is desirable to protect the compressed video. A video clip is generally compressed in a transform Domain with some type of entropy coding. To protect a compressed video, encryption techniques can be applied to the original data, such as block swapping, or the data can be transformed using DCT or wavelet coefficients, entropy-coded bit streams, or format headers. The encryption has three separate layers that can be selected according to the security needs of the application and the processing capability of the client computer. The chaotic pseudo-random sequence generator used to generate the key-sequence to randomize the important fields in the compressed video stream has its parameters encrypted by an asymmetric cipher and placed into the stream. The resulting stream is still a valid video stream. CSECV has significant advantages over existing algorithms for security, decryption speed, implementation flexibility, and error preservation.

The paper presents the design and implementation of a software application for the provision of secure real time communication services between workstations, based on the AES prototype cryptographic algorithm and an advanced secret key management system [3]. The application has been designed based on the requirements of a military unit, so as to allow groups of authenticated users to

communicate and read the transmitted messages. This application can be used as the basis for the design of an integrated communication system for a military organization. The present design confines its operation within the limits of a local area network, but the possibilities are open for operation in extended networks or the internet.

Advanced Encryption Standard (AES) is the most secure symmetric encryption technique that has gained worldwide acceptance. "FPGA implementations of advanced Encryption standard: a survey" presents the AES based on the Rijndael Algorithm which is an efficient cryptographic technique that includes generation of ciphers for encryption and inverse ciphers for decryption[4]. Higher security and speed of encryption/decryption is ensured by operations like Sub Bytes (S-box)/Inv. (Inv.S-box), Mix Columns/Inv. Mix Columns and Key Scheduling. Extensive research has been conducted into development of S-box /Inv. S-Box and Mix Columns/Inv. Mix Columns on dedicated ASIC and FPGA to speed up the AES algorithm and to reduce circuit area. This is an attempt, to survey in detail, the work conducted in the aforesaid fields. The prime focus is on the FPGA implementations of optimized novel hardware architectures and algorithms.

Fault attacks are powerful and efficient cryptanalysis techniques to find the secret key of the Advanced Encryption Standard (AES) algorithm [5]. The paper shows that these attacks are based on injecting faults into the structure of the AES to obtain the confidential information. To protect the AES implementation against these attacks, a number of counter measures have been proposed. In this paper, a fault detection scheme for the Advanced Encryption Standard is proposed. They present its details implementation in each transformation of the AES. The simulation results show that the fault coverage achieves 99.999% for the proposed scheme. Moreover, the proposed fault detection scheme has been implemented on Xilinx Virtex-5 FPGA. Its area overhead and frequency degradation have been compared and it is shown that the proposed scheme achieves a good performance in terms of area and frequency.

2. PRAPOSED WORK

2.1 Block Diagram

In this project, I am trying to make secure Navigation of Missile using encryption based RC4 algorithm. The main application of the project is to navigate the Missile position to the user's requirement.

The user sends the co-ordinates through PC based server on the base station. The co-ordinates consist of two parts: first the circular co-ordinates and then the linear co-ordinates. At base station PC send these co-ordinates through pen drive to the field station.

After receiving the co-ordinates the field, then compares the coordinates to the on board DC motor. It drives the DC motors of the tires of buggy until the received co-ordinates and the received co-ordinates match. After which the buggy indicate the linear co-ordinates sent by user. In this way the missile can be navigated to destination.

After the connection has been made the user first has to enter the Password. Then the user can enter the co-ordinate of Missile Navigation. After enter the X and Y co-ordinates the user can send the codes to the Missile unit.

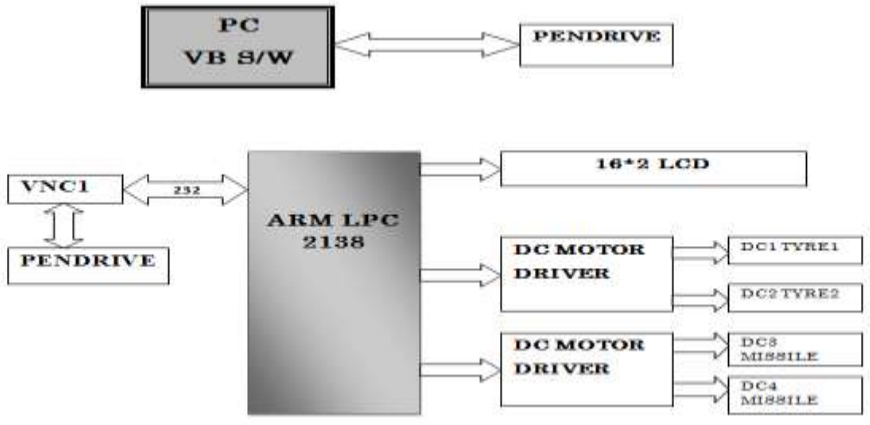

Figure 2.1 Block diagram of Secured Communication for Missile Communication

Liquid Crystal Display:

LCD is used in a project to visualize the output of the application. 16x2 LCD is used which indicates 16 columns and 2 rows. So, we can write 16 characters in each line. So, total 32 characters we can display on 16x2 LCD.

LCD can also use in a project to check the output of different modules interfaced with the . Thus LCD plays a vital role in a project to see the output and to debug the system module wise in case of system failure in order to rectify the problem.

Pen drive Interfaced:

The pen drive is the most commonly used device now days. This device is used to store the data via USB interfaced devices like computers, laptops or other USB hub devices.

VNC1 is a device which is used for mapping the files on the pen drive. give the basic DOS commands and access all the files functions like copy, paste, store , delete, cut, etc.

With the help of VNC1, we can do all the basic file functions like copy, paste, store , delete, cut, etc without using the computer. We can control all these file functions using VNC.

2.2 Encryption method used

Encryption is the process of encoding messages (or information) in such a way that third parties cannot read it, but only authorized parties can. Encryption doesn't prevent hacking but it prevents the hacker from reading the data that is encrypted. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message.

2.2.1 RC4 Algorithm

In the algorithm the key stream is completely independent of the plaintext used. An 8 * 8 S-Box (S0 S255), where each of the entries is a permutation of the numbers 0 to 255, and the permutation is a function of the variable length key. There are two counters i, and j, both initialized to 0 used in the algorithm.

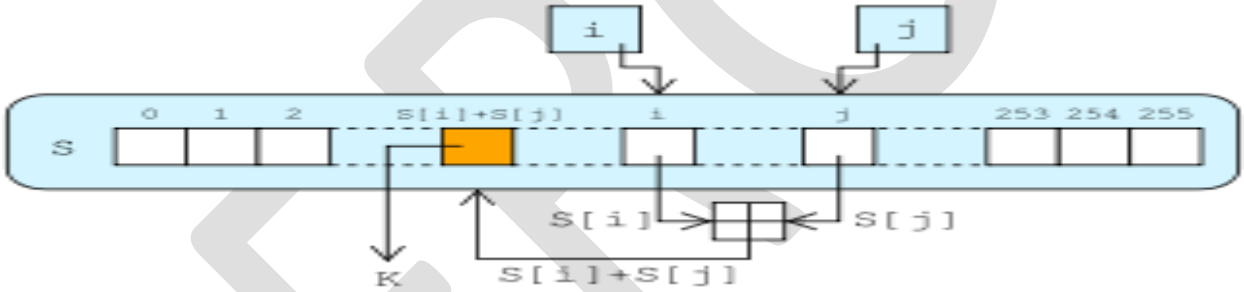

Fig2.2.1 RC4 Algorithm

Algorithm Features:

- Uses a variable length key from 1 to 256 bytes to initialize a 256-byte state table. The state table is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text. Each element in the state table is swapped at least once.
- The key is often limited to 40 bits, because of export restrictions but it is sometimes used as a 128 bit key. It has the capability of using keys between 1 and 2048 bits. RC4 is used in many commercial software packages such as Lotus Notes and Oracle Secure SQL.
- The algorithm works in two phases, key setup and ciphering. Key setup is the first and most difficult phase of this encryption algorithm. During a N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations. These mixing operations consist of swapping bytes, modulo operations, and other formulas. A modulo operation is the process of yielding a remainder from division. For example, 11/4 is 2 remainder 3; therefore eleven mod four would be equal to three.
- The algorithm works in two phases, key setup and ciphering. Key setup is the first and most difficult phase of this encryption algorithm. During a N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations. These mixing operations consist of swapping bytes, modulo operations, and other formulas. A modulo operation is the process of yielding a remainder from division. For example, 11/4 is 2 remainder 3; therefore eleven mod four would be equal to three.

3. EXPERIMENTAL RESULTS

First pen –drive is detected by the system after detection of drive; angle and position are to be entered with the help of user interface as shown below.

Fig.6.1 Directions entered onto pen-drive using the User Interface

When we connect pen- drive to the controller, the missile navigates as per data entered in the pen drive, and display is shown by LCD.

Fig.6.2 Display on the LCD

5. CONCLUSIONS

The goal of this paper is to form secured communication for missile navigation. In military application security of data is the most important factor. Here I have tried to illustrate a secured communication with the help of encryption method and VNC which is useful for interfacing of pen drive with which missile can be navigated as per the instructed directions. It is done by entering the position, an angle of missile and giving directions in forward/ reverse, left/ right directions of missile onto user interface.

The algorithm used for the encryption is simple and easy. There are various types of encryption algorithms, which can are useful in many applications. Out of this RC algorithm is the easiest algorithm to implement but also is easy algorithm to crack comparatively.

ACKNOWLEDGEMENTS

I would like to thank all the staff members of E&TC Department, Dr. D.Y.College of engineering, Ambi. for their support .

REFERENCES:

[1] Chunlei Wang, Guangyi Wang, Yue Sun and Wei Chen "ARM Realization of Storage Device Encryption Based on Chaos and AES Algorithm" 2011 Fourth International Workshop on Chaos-Fractals Theories and Applications

[2] Chun Yuan, Yuzhou Zhong, and Yuwen He, "Chaos Based Encryption Algorithm for Compressed Video," Chinese Journal of Computers, Vol.27 No.2, Feb 2004, pp.257- 263.

[3] Nikolaos G. Bardis, Konstantinos Ntaikos, "Design of a secure chat application Based on AES cryptographic algorithm and key management"

[4] Shylashree.N; Nagarjun Bhat; V. Shridhar, "FPGA implementations of advanced Encryption

standadrd: a survey" Directory of Open Access Journals (Sweden), Jan 2012

[5] Hassen Mestiri; Noura Benhadjyoussef; Mohsen Machhout; Rached Tourki, "A Robust Fault Detection Scheme for the Advanced Encryption Standard," Directory of Directory of Open Access Journals (Sweden), Jan 2013

[6] Rui Zhao, Qingsheng Wang, and Huiping Wen, "Design of AES algorithm Based On Two Dimensional Logistic and Chebyshev Chaotic Mapping," Microcomputer

[7] Yi Li, and Xingjiang Pan, "AES Based on Neural Network of Chaotic Encryption algorithm," Science Technology and Engineering, Vol.10 No.29, Oct 2010, pp.7310- 7313.

[8] Ruxue Bai, Hongyan Liu, and Xinhe Zhang, "AES and its software implementation based on ARM920T," Journal of Computer Applications, Vol.31 No.5, May 2011, pp.1295-1301.

[9] Shaonan Han, and Xiaojiang Li, "Compatible AES-128、AES-192,AES-256 Serial AES Encryyption and Decryption Circuit Design," Microelectronics & Computer, Vol.27 No.11, Nov 2010, pp.40-50.

[10] http://we pp.7310-nku.baidu.com/view/5ebbd326ccbff121dd36831a.html