ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2014

Architecture and Implementation of a Security Algorithm CPBFC for WSN

Paramjit Shah Singh[1], Ajay Kumar Agarwal[2]

[1]Research Scholar, Singhania University, Rajasthan, India

[2]Associate Professor, UP Technical University, U.P., India

ABSTRACT - There are many countermeasure methods that have been extensively studied to provide WSN communication security. However, WSN is still exposed to some kinds of attacks. These defenses are ineffective against attacks from compromised servers due to the WSN level constantly increasing, and attacks are becoming more and more complicated. Moreover WSN has some restrictions when it comes to its applications, like limited power supplies, low bandwidth, small memory sizes and limited energy, which make it more vulnerable.To this end, we propose a security algorithm keeping in mind the constraints of WSN. We have modified the Feistel algorithm by using controlled permutation boxes. The modified Feistel scheme design can meet today's security challenges and generates high-quality results.

I. INTRODUCTION

Due to the increase in new trends of attack, previous security methods cannot combat or resist modern attacks. Analysis of work done in the field of encryption, shows that new and more stable security approaches need to be put in place to provide information safety taking into consideration the following attributes: availability, confidentiality, integrity authentication, and non-repudiation.On designing WSN protocol it is necessary to consider all specific features of WSN. For example, communication bandwidth is extremely limited in these networks: each bit transmitted consumes about as much power as executing 800~1000 operational instructions, and as a consequence, any message expansion caused by security mechanisms comes at a significant cost.Limitations in computational and battery power in sensor nodes are constraints on the diversity of security mechanisms. We must apply only suitable mechanisms to WSN which motivates development of efficient encryption scheme. Our work is an endeavor to develop such cipher to provide efficient security for sensor nodes. This accelerated-cipher design uses Feistel scheme with data-dependent permutations and more secure building blocks , and can be used for fast hardware, firmware, software and WSN encryption systems. The approach presented here is less likely to suffer, intrusion of differential cryptanalysis than currently used popular WSN ciphers like DES, Camellia and so on.

II. LITERATURE REVIEW

Block ciphers were developed in nineteen seventies and have been used to encrypt loads of valuable information while it is either stored or is in transit through network. Modern block ciphers have got a lot of strength through the work of Claude who introduced the idea of substitution-permutation (S-P) networks which form the basis of modern block ciphers. S-P networks are based on the two primitive cryptographic operations Substitution and Permutation. To provide more security to a cipher[1] it may make use of both substitution as well as permutation that to several times (combinations). The work of Kelleher, L.; Meijer showed that use of S-P network can protect against linear as well as differential attacks.[2][3].

Horst Feistel led to the invention of a suitable structure which adapted Shannon's S-P network in an easily inverted structure. Essentially the same h/w or s/w is used for both encryption and decryption, with just a slight change in how the keys are used. It involves use of several key dependent rounds, involving a round function which involves use of substitution and permutation. The idea is to partition the input block into two halves, L(i-1) and R(i-1), and use only R(i-1) in the ith round (part) of the cipher the function in each round, incorporates one stage of the S-P network, controlled by part of the key K(i)known as the ithsubkey [4].In 1999 NIST announced the five algorithms : MARS[12], RC6[13], Rijndael[14], Serpent[15], and Twofish[16]. MARS breaks the 128-bit input block into four 32-bit words. MARS uses a 32-round unbalanced Feistel network. RC6, a 20-round Feistel cipher out of RSA Security Inc., is much simpler. "Pre-whitening" and "Post whitening" steps have been used to increase the strength of algorithm. Twofish, is a 16- round Feistel network with two modifications. One is a one-bit rotation before and after the data enters the round function. The other alteration is dynamic S-boxes. In serpent ,there are 32 rounds—a high number—each of which consists of XORing the key and the intermediate data, a pass through Sboxes, and a linear function that combines fixed rotations and XOR. Bruce Scheneir[17] proposed a fast and unpatented block cipher available freely to people for public use. Blowfish[18] is a secret-key block cipher, is a Feistel network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits.

III. PROPOSED ALGORITHM

The Encryption Process

First of all, given plaintext message is divided into blocks of 128 bits (or 16 characters).If the length of plaintext message is l and no. of plaintext blocks in this length are 'n' and if l < n*16, then original plaintext message is augmented with padding of blank spaces so that last block should also be of 16 characters (128 bits).

Each of the blocks of plaintext message is encrypted to produce final block of ciphertext.

Detailed Architecture of Encryption Process

Encryption algorithm:

1. Plaintext of 128 bits is XORED with first intermediate key K1 of 128 bits.
2. The output of 128 bits is considered as consisting of two independent 64 bits left half (L0) & 64 bits right half (R0).
3. L0-R0 is passed through main function (F).
4. The output of main function is

   $LO' = R0 \oplus F(L0, K2)$

   $RO' = L0$
5. LO'-RO' is then passed through sub function which acts like a wrapper layer to strengthen the other half (RO') using 128 bits key K3.
6. 128 bits output of sub function is then passed through main function (F).
7. Repeat steps 2-5 using intermediate keys K4 & K5 in main functions & sub main function.
8. 128 bits output of sub function is then passed through main function (F).
9. Repeat step 4 using intermediate keys K6.
10. 128 bits output is XORED with 128 bits intermediate key K7 to generate 128 bits output.

The detailed architecture of encryption process is shown below :

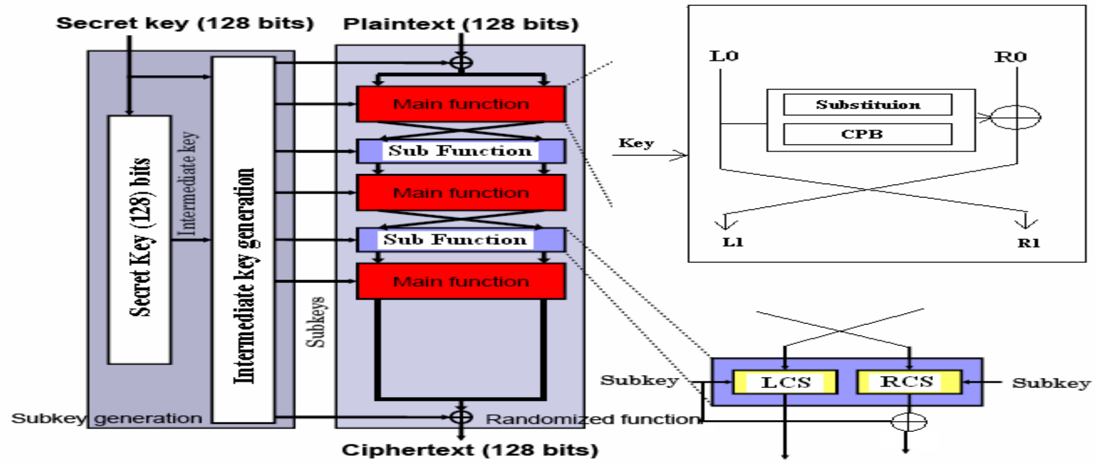


Fig. 1 Detailed Architecture of Encryption Process

The encryption process consist of following segments :

1. Generation of intermediate keys
2. Application of Main function
3. Application of Sub function

Alongwith this key whitening is used to ensure resistance against key search attack.

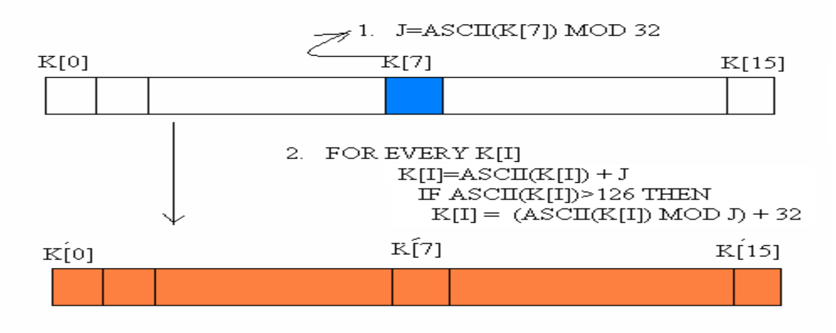
In intermediate key generation, from main key of 128 bits main keys and sub keys are derived.

The top and bottom rounds of the cipher play a different role than the middle rounds in protecting against cryptanalytical attacks.

Therefore, in the design of this cipher the middle rounds are viewed as the “cryptographic core” and are designed differently than the top and bottom rounds, which are viewed as “wrapper layers”.

A. Intermediate Key Generation

New intermediate key is produced from existing key using followingalgorithms**:**



B. Main Function

The main function is the cryptographic core, which plays very important role in ensuring the security of the data. It performs substitution on left half of the input i.e. leftmost 64 bits, it produces pre-purmuted output which is passed through CPB, which dynamically generated the permutation box which helps in rearranging the pre-purmuted output to produce the permuted output. The block diagram of Main Function is shown below :

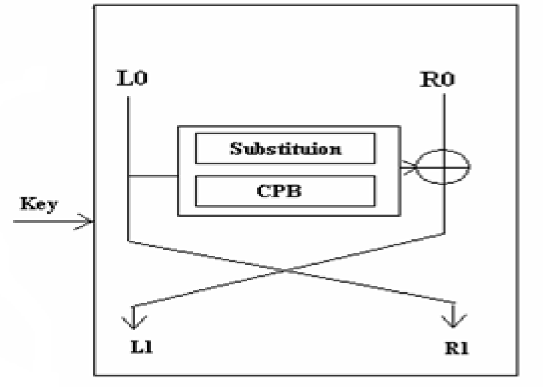


Fig. 2 Block Diagram of Main Function

C. Sub-Main Function

This plays very important role, as it tightens the security further. This heterogeneous structure of Feistel cipher is far more secure than standard Feistel cipher where each step is just similar to previous one, hence is less resilient to attacks being predictive in nature. Output of main function is passed through the sub main function where shifting operation is performed using sub keys, ensuring better diffusion.

The block diagram of Sub Main Function is shown below:

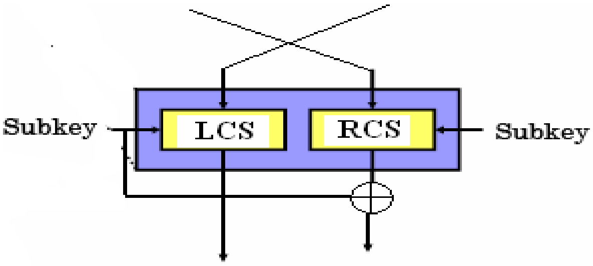


Fig. 3 the block diagram of Sub-Main Function

D. Substitution

- In principle, a carefully chosen substitution can provide good resistance against linear and differential attacks, as well as good avalanche of data and key bits.
- A drawback of using S-box lookups is that it is relatively slow for software implementations and in order to use all the bits of a data word, one needs to do several S-box lookups, which slows the cipher even further.
- Therefore, direct substitution is performed rather than large number of S-box lookups. This approach prevents memory wastage and exhaustive computations.

The block diagram of Substitution is shown below:

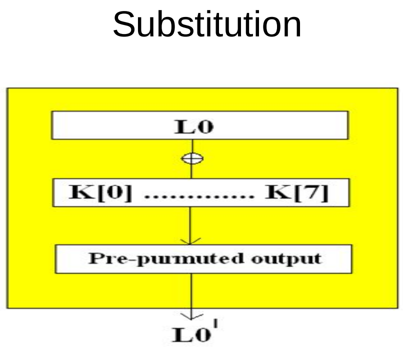


Fig.4 The block diagram of Substitution

Steps of Substitution Algorithm

1. 64 left most bits (L0) is XORED with 64 bits of intermediate key i.e.

$$oi = LOi \oplus ki$$

LOi = ith binary digit of plaintext
ki = ith binary digit of key
oi = ith binary digit of output
⊕ = (XOR) operation

E. CPB-Controllable Permutation Box

- Key-dependent, pseudo-randomly generated controllable permutation boxes (CPB) are used.
- Traditional systems, however, uses the cryptosystem itself to generate the P-boxes, which Produces weak P-Boxes – here this approach is avoided.
- Key dependent pseudo randomly generated CPB is used which is created at runtime only using the secret key, which is more secure than static P-Box.
- Permutation operation rearranges the contents and adds to diffusion in the given contents but if static permutation tables are used, they get easily attacked than when CPB based key dependent permutations are used.
- CPB are fast even if implemented in cheap hardware or limited resource devices.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 8, August 2014

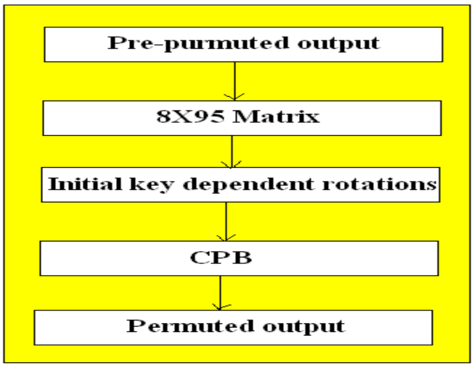


Fig.5CPB-Controllable Permutation Box

Permutation Algorithm

```
1.        Initialize 8X95 matrix.
                    For i = 0 to 7
                              For j = 0 to 94
                                        M[i][j] = j+32
                    EndFor
2.        Perform initial key dependent rotation using 64 bits of sub key i.e. K[8]…K[15].
                    rotateith row of matrix K[i+1] times.
                    rotateith row of matrix K[i] times.
3.        For i = 0 to 7
                    pi = M[i][0]
```

CPB-Controllable Permutation Box-Generation

1. The ith row of the matrix is rotated k[i+1] times

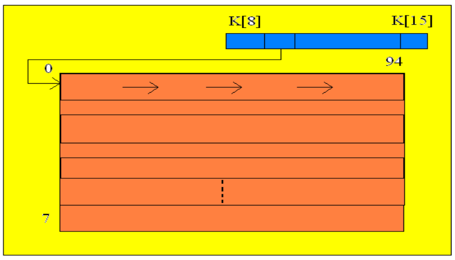


Fig. 6 CPB-Controllable Permutation Box-Generation

2. The ith row of the matrix is rotated k[i] times
3.

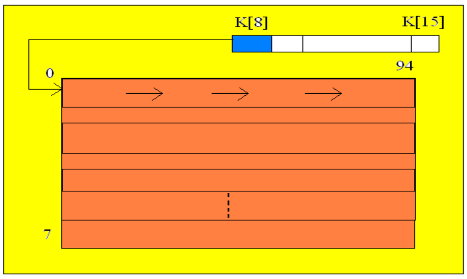


Fig. 7 CPB-Controllable Permutation Box-Generation

IV. PERFORMANCE COMPARISON OF PROPOSED ALGORITHM

By considering different sizes of data blocks the algorithms are evaluated in terms of the time required to encrypt and decrypt the data block. The time between two test points in the algorithm during execution is calculated using system clock. The number of bytes encrypted in one second is ascertained.
The comparison between proposed algorithm (CPB-FEISTEL CIPHER) with standard algorithms given below reveals the fact that proposed algorithm, performs better than other algorithms.

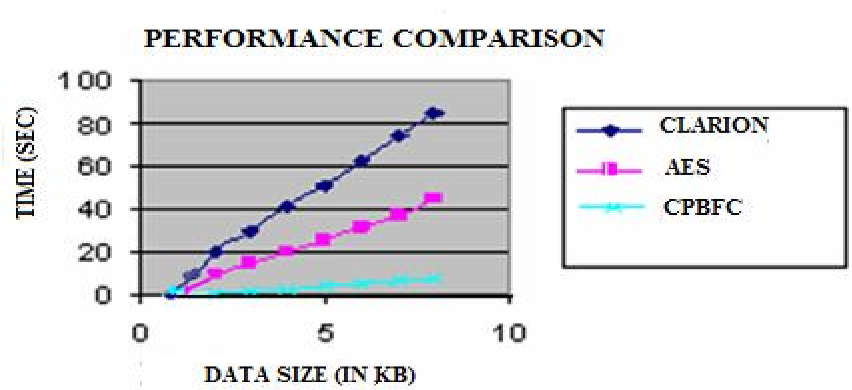


Fig 8. Performance Comparison

REFERENCES

[1]. Bilstrup, U., Sjoberg, K., Svensson, B., Wiberg, P.A., 2003. Capacity Limitations in Wireless Sensor Networks. Proc. 9th IEEE Int. Conf. on Emerging Technologies and Factory Automation, Lisbon, Portugal, p.529-536.
[2]. Bodrov, A.V., Moldovyan, A.A., Moldovyan, P.A., 2005. DDP-based ciphers: differential analysis of Spectr-H64.
[3]. *Comput. Sci. J. Mold.*, **13**(3):268-291. Feistel, H., 1973. Cryptography and computer privacy. *Sci.Am*., 228(5):15-23.
[4]. Goots, N.D., Moldovyan, A.A., Moldovyan, N.A., 2001. Fast encryption algorithm a need *LNCS*, 2052:275- 286. [doi:10.1007/3-540-45116-1_27]
[5]. Elena C. Laskari, Gerasimos C. Meletiou and Michael N. Vrahatis, "Utilizing Evolutionary Computation Methods for the Design of S-Boxes", Federal InformationProcessing Standards Publication 197 November 26, 2001.
[6]. Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standard Publication197,November 26, 2001.
[7]. Juan Soto and Lawrence Bassham, "Randomness Testing of the Advanced EncryptionStandard Finalist Candidates", Computer Security Division, National Institute of Standards and Technology, March 28, 2000
[8]. Susan landau "communications security for the twenty-first century:the advanced encryption standard" the notices of the AMS,volume 47,no.4,apr 2000.
[9]. SchneierB.,"Fast Software Encryption" , Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204,1993
[10]. AameerNadeem , Dr. M. YounusJaved " A performance analysis of of data encrption standard ", 0-7803-9421-6/2005 IEEE.
[11]. Susan Landau "Standing the Test ofTime: The DataEncryption Standard", Notices of the AMS march ,Vol47,No.3 ,MARCH2000.
[12]. Carolynn Burwick, Don Coppersmith, Edward D.Avignon, "The MARS Encryption Algorithm",CiteSeer,1997.
[13]. Ronald L. Rivest1, M.J.B. Robshaw2, R. Sidney2, and Y.L. Yin2, "The RC6 Block Cipher" M.I.T. Laboratory for Computer Science report, pp 20-30, 1998.
[14]. Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, NielsFerguson**"**TwofishA 128-Bit Block Cipher",CiteSeer,1998.
[15]. Ross Anderson1,EliBiham, Lars Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard"2000.
[16]. Christophe De Canniere , Alex Biryukov and Bart Preneel " An introduction to block crypt Analysis " proceedings of the IEEE,vol 94,no.2,2006.
[17]. PriyaDhawan, "Performance Comparison: Security Design Choices",Microsoft Developer Network,October 2002.
[18]. Schneier B., "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)"Fast Software Encryption, Cambridge Security Workshop Proceeding**,,**Springer-Verlag, pp. 191-204**,** 1994.