International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 3, June 2012 www.ijcsn.org ISSN 2277-5420

PC-RC4 Algorithm: An Enhancement Over Standard RC4 Algorithm

[1]Pardeep, [2]Pushpendra Kumar Pateriya

[1]M.Tech Student (Computer Science), Lovely Professional University, Phagwara, India
[2]Assistant Professor (Computer Science), Lovely Professional University, Phagwara, India

Abstract

RC4 is most widely used stream cipher. In many standard security protocols is used the RC4 like in Wi-Fi Protocol Access (WPA) and Wired Equivalence Privacy (WEP). Here we propose a new enhanced RC4 algorithm named as PC-RC4. It is an extension of standard RC4 Algorithm. The basic purpose of this enhancement is to making strong RC4 algorithm. RC4 stream cipher is basically two stages process named: KSA & PRGA. The weakness and attacks are found in both the stages of RC4. In this context, this paper is trying to making strong to both the stages of RC4 Stream Cipher. The backbone of the RC4 algorithm is shuffling operation in both the stages KSA & PRGA. In the PC-RC4 Stream cipher is improved randomness in KSA as well as in PRGA to make it strong. In this paper we studied and analyzed some potential vulnerabilities of RC4 algorithm and proposed some appropriate changes on standard RC4 algorithm to overcome. A pragmatic approach used to analyze PC-RC4 in different scenarios.

Keywords**:** Stream Cipher, Symmetric Cipher, Wireless Sensor Network, WPA (Wi-Fi Protected Access) and WEP (Wired Equivalent Privacy), RC4 (Rivest Cipher 4), PC-RC4 (PardeepCipher-RC4).

I. Introduction

Wireless Sensor Networks and Wireless Networks are most popular and widely used types of network of this era. Because of the openness these types of networks are not very much secure.

WN is commonly configured network in this era. The most attractive features of WN are the cost effectiveness, availability and mobility. WN gives cost efficiency, low maintaining cost, and lower installation cost [1].

WSN is also most popular type of network today. But the WSN network is resource constrained network. Wireless sensor nodes are limited in processing speed, storage capacity, and communication bandwidth and battery power supply [2].

To provide the security over the WSN and WN used algorithm must be fast enough which can encrypt and decrypt data comparatively in less amount of time and must require less resource also. In this concern WPA (Wi-Fi Protected Access) and WEP (Wired Equivalent Privacy) protocols are used as standard. These standards have adopted the RC4 stream cipher algorithm to secure the data over the wireless networks. These standard adopted RC4 algorithms because RC4 algorithm gives speedy encryption and decryption of data, utilize less hardware resources during processing, and easy to implement [3].

In context to WSN, requires the algorithm for data security, which used less hardware resources. So in this concern, RC4 algorithm is the best option available. Basically RC4 algorithm is a Stream Cipher under the Symmetric Ciphers algorithms [4].

Presently RC4 algorithm is not secure in many aspects. Lots of weaknesses and attacks have been detected by the cryptanalysis. RC4 algorithm is basically a two stage process. The two stages of RC4 stream cipher are KSA and PRGA. The weaknesses and attacks are detected in both the sub processes inside the RC4 algorithm [5].

RC4 algorithm is best suitable approach for WN and WSN for data security but on the other hand the RC4 is not secure enough. In this paper a more secure enhanced algorithm has been introduced named as "PC-RC4". It enhances the security of RC4 algorithm and takes less number of resources. It also speeds up the encryption and decryption process. The main concern of PC-RC4 is to improve the security of RC4 algorithm.

The paper organizes in the seven sections. In the first section, this paper describe the introduction, in the second section describes the RC4 algorithm, in the third section describes the weaknesses over the RC4, in the fourth section describes the self design algorithm, in the fifth section describes the simulation result, in the sixth section describes the conclusion of this paper work and in the end giving the reference section.

2. RC4 Stream Cipher Algorithm

2.1 Introduction [12]

The backbone of RC4 algorithm is the shuffling operations performed over the state matrix.

Two phase of RC4 algorithm, KSA and PRGA, are as Follows:

2.2 RC4 Algorithm: [13]

N=256
KSA:

```
1. Input Key (Key Length)(Basic Key)// len from 1
   to 256 bytes
2. Initialize the Key[length]
   For i=0 to length
   Key[i]=random value;// Secret //key
   End for
3. Initialize the Temporary Matrix
   For i=0 to N
   Temp[i]=value of key[keylenth]
   End for
4. Initialize the State Matrix
   For i=0 to N
   S[i]=I;
   End for
5. Permutation on State Matrix
   j=0
   For i=0 to N
   j=j+s[i]+ temp[i] % N;
   swap(s[i], s[j])
   End for
```

PRGA:

```
    1. Generate the random values used for
       encryption
       i=j=0
       While (True)
       i=i+1 % N
       j=j+s[i] % N
       swap(s[i],s[j])
       index=(s[i]+s[j]) % N
       output= s[index]
       CT= PT XOR output
             Wend( End While)
```

2.3 Description

RC4 algorithm basically depends on the shuffling operations on the state matrix. The first stage of the RC4 stream cipher is KSA. In the KSA, first the basic keylen will be taken (As basic Key) from 1 to 256 bytes and then on the bases of keylen, a key matrix (Secret Key) will be generated, which contains the random values.
In the end of the step, generates the state matrix of size 256, where we insert the 256 bytes from 0 to 255 in ascending order. Then, on the bases of key [keylen] matrix, generates the Temp [256] with the values of the key [keylen] matrix, which further used to perform the swapping on the state[256] matrix.
In KSA, inside the loop in 5th steps, the swapping is performed on the state matrix for each index location from 0 to 255 for randomizing the state matrix. This process is performed on the bases of j random index location indicator (j=j+s[i]+temp[i]%N). KSA process completion gives a randomized state matrix as output. This state matrix will be passed as input for stage PRGA and other temp[256] discarded.
At the end for stage of RC4 algorithm is PRGA now start after KSA. In this stage, a Key stream generated as equal to the length of the plain text and then character by character XOR operation will be performed with the generated key stream. After, the successful completion of both the phases cipher text generates.

3. Weaknesses AND Attacks over RC4

Pardeep & Pushpendra [13], after 1994, RC4 Stream cipher is disclosed publicly. Cryptanalysis started to analyze the RC4 stream cipher algorithm. Two aspects are to analyze the RC4 algorithm, one from KSA and Second from PRGA. In KSA, cryptanalyst tried to capture the randomness of the State matrix. In PRGA, cryptanalyst tried to capturing the internal state of the state matrix and index on the bases output generated[6].
Follows are given some weaknesses and attacks point, detected by the cryptanalysts during cryptanalysis:
1. Mantin and Shamir[7], detected weakness inside the RC4 algorithm that the most generated means the probability of generated Zero output byte at the PRGA stages, which applied over the plain text to encrypt and decrypt the data.
2. Fluhrer et al. [8], has discovered the weakness, if any one known the some portions of the secret key matrix generated from the keylen (Basic Key), then RC4 possible to attack completely.

3. Paul and Maitra [9] [11], introduced the concept that possible to captured the secret key from the initial state matrix by using the biases.
4. Klein [10], first time introduced the statistical relation in between the output byte generated and the value of s[j] at the time, when output generated.

4. PC-RC4 Self Designed Stream Cipher

4.1 Introduction

In the earlier section discussed RC4 algorithm is just based on the Shuffling Principal. This paper has explained that there are lots of attacks and weaknesses inside the RC4 stream cipher in both the stages, KSA and PRGA. RC4 algorithm is having weak shuffling inside.

An algorithm is proposed here to provide the strong shuffling inside the RC4 algorithm. The proposed algorithm is named as, “PC-RC4” to improve the security of the RC4 stream cipher and to overcome various weaknesses and attacks. In this algorithm a new way is proposed for the KSA and PRGA.

4.2 PC-RC4 Algorithm

```
N=256
KSA:
    1. input Key (Key Length) (basic key)
    2. initialize the Key[length]
       For i=0 to length
       Key[i] =random value;
       End for
    3. Initialize the Temporary Matrix
       For i=0 to N
       Temp[i]= value
       End for
    4. initialize the State Matrix
       For i=0 to N
       S[i]=i;
       End for
    5. Permutation on State Matrix
       j=0
       For i=0 to N
       j=(j+s[i]+s[j]+temp[i]+temp[j]) % N;
       swap(s[i],s[j])
       End for
PRGA:
    1. Generate the random values used for encryption
           i=j=0
           while(True)
           i=i+1 % N
           j=j+s[i]+s[j] % N
           swap(s[i],s[j])
           index=(s[i]+s[j]) % N
           output= s[index]
           CT= PT XOR output
           Wend( End While)
```

4.3 Description

Basic description of this algorithm is same as the standard RC4 algorithm.

Now, about the changes:
Basic idea behind this approach is to provide the more randomness inside the KSA and PRGA to generate the random index location pointer j in for loop of both the stages.

In KSA, during generating the value of j index pointer on the bases does the shuffling over the state matrix; add up some other strong statement to improve the randomness of this j index location pointer. In KSA, this approach uses the index pointer j to provide the randomness at the index which not provided in the RC4 algorithm. This approach also uses the temp[j] and s[j], in side the statement **j=(j+s[i]+s[j]+temp[i]+temp[j]) % N** to add up some strength in generation of j index location pointer. These changes also use the state matrix to provide the randomness on the j index location pointer on the bases, select the random index during the swapping over the state matrix. This use of random index location also provides the way to use the state matrix in the random manner, this done as using this statement s[j] (j is random generated value used as index location pointer in the end for statement of the algorithm).

In PRGA, also increases the randomness on generating the j value that uses as index location pointer for another statement inside the algorithm. This does by using the statement s[j] in **j=j+s[i]+s[j] % N** this statement. In this statement, this approach adding the s[j], j a random index location indicator after the first loop of execution because t the starting point j initializes by 1. In this manner, more randomness provided upon the index level in this step also, which not provided by the standard RC4 algorithm.

So we can say “PC-RC4” algorithm is more robust than RC4 against the number of attacks. This approach increases the level of randomness inside the RC4 algorithm, which is the basic principle where RC4 stands. Also this new approach provides the randomness at the index level in the both KSA and PRGA.

In this algorithm, run time complexity and time taken for encryption and decryption not increases and resource requirement is also not higher than RC4 algorithm

4.4 Encryption/Decryption Process

In this algorithm, the encryption and decryption is done in the same manner as standard RC4 Algorithm.
Let's see with the help of a diagram.

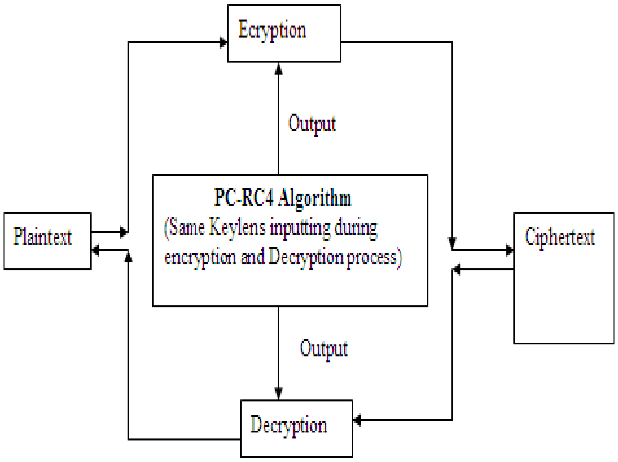

Figure1: PC-RC4, Encryption and Decryption Process

Figure1:PC-RC4 Encryption/Decryption Process

Figure1 describes the encryption and decryption process of the PC-RC4 algorithm. This shows, PC-RC4 algorithm generates the output bytes and these bytes XORed with the plaintext in character by character manner.

5. Simulation Result

Now in this section, this paper describes the simulation result of both RC4 stream cipher and Self Enhanced PC-RC4 Stream Cipher Algorithm. The simulation the algorithms are done on the bases of execution time (Encryption Time) and memory utilization at the run time.

Figure2: is describing the execution time (Encryption Time) for the RC4 Stream Cipher and Figure3: is describing the execution time (Encryption Time) for the PC-RC4 Algorithm.

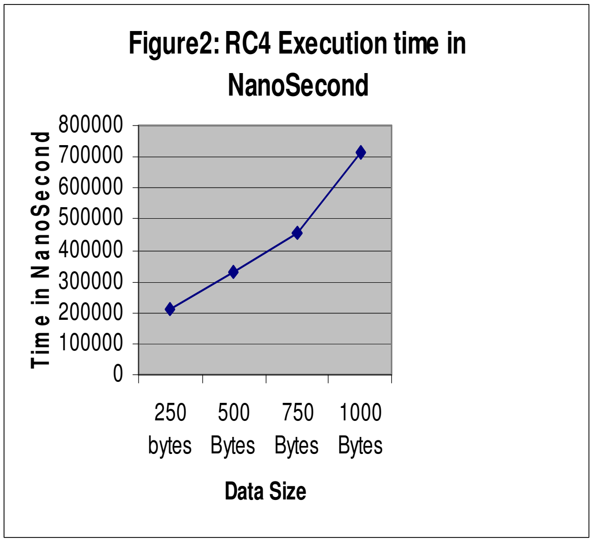

Figure 2: RC4 Execution time

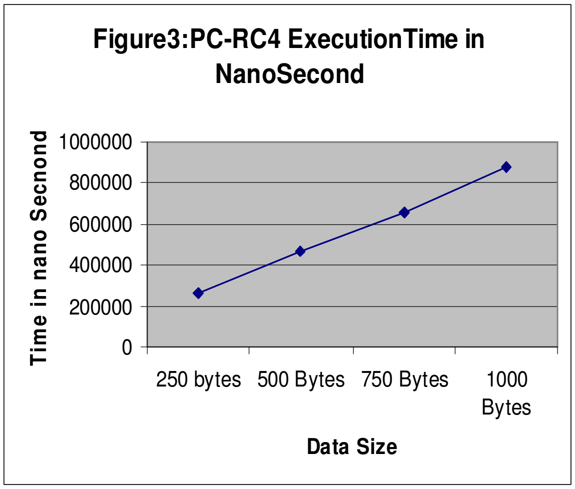

Figure 3: PC-RC4 Execution Time

Figure4: is describing the total memory utilize by the RC4 Stream Cipher at run time in bytes and Figure5: is describing the total memory utilize by the PC-RC4 Stream Cipher at run time in bytes.

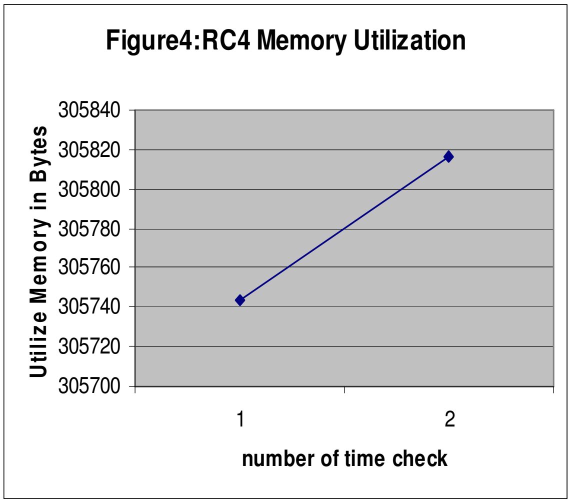

Figure 4: RC4 Memory Utilization

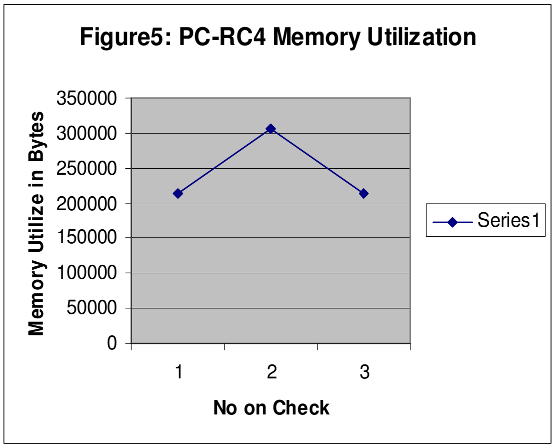

Figure 5: PC-RC4 Memory Utilization

This simulation result of the both algorithms show that the execution time of the PC-RC4 algorithm is increase at miner level as compare to the RC4. And Memory utilization of the PC-RC4 algorithm is less as compare to the memory utilize by the RC4 Algorithm.

6. Conclusion

This research paper provides the pragmatic study over the RC4 Stream cipher and various weaknesses over the RC4. Later discuss the self design Algorithm "PC-RC4", which design to making strong RC4 stream cipher against the attacks. This paper is proposed to use this new self design algorithm over the WN & WSN because this algorithm increases the randomness of the algorithm in technical manner.

References

[1]A.A. Noman, Dr. Roslina b. Mohd. Sidek, Dr. A.R.b. Ramli, Dr. L. Ali, "RC4 Stream Cipher for WLAN Security: A Hardware Approach", 5th International Conference on Electrical and Computer Engineering, ICECE 2008.

[2] Chuan-Chin Pu, Wan- Young Chung, "Group Key Update Method for Improving RC4 Stream Cipher in Wireless Sensor Network", International Conference on Convergence Information Technology.

[3] Suhaila Omer Sharif, S.P. Mansoor, "Performance analysis of Stream Cipher algorithms", 3rd international conference on Advanced Computer Theory and Engineering (ICATE), 2010.

[4] C.S Lamba, "Design and Alnalysis of Stream Cipher for Network Security ", Second International Conference on Communication Software and Networks, 2010.

[5]Fahime Javdan Kherad, Mohammad V. Malakooti, Hamid R. Naji, Payman Haghinghat, "A New Symmetric Crtptographic Algorithm to Secure E-Commerce Tracsactions", International Conference on Financial Theory and Engineering, 2010.

[6]Jian Xie, Xiaozhong Pan, "An Improved RC4 Stream Cipher ", International Conference on Computer Application and System Modeling (ICCASM), 2010.

[7] I. Mantin, A. Shamir "A practical Attack on Broadcast RC4", FastSoftware Encryption 2001 (M.Matsui,ed.), pp. 152-164, Springer-Verlag, 2001.

[8] S.Fluthrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", SAC2001 (S. Vaudenay, A. Youssef,eds.), col. 2259 of LNCS, pp. 1-24, springer-Verlag, 2001.

[9]G. Paul, S.Maitra, "RC4 state in formation at Any Stage Reveals the Secret Key ", presented in the 14th Annual Workshop on Selected Areas in Cryptography, SAC 2007, August 16-17, Ottawa, Canada, LNCS (Springer) vol. 4876, pages 360-377.

[10]A. Klein, Attacks on the RC4 Stream Cipher, cage.ugent.be/~**klein/RC4/RC4**-en.ps

[11] S. Paul, and B. Preneel, "A New Weakness in the RC4 Keystream Generator", Fast Software Encryotion, FSE 2004, LNCS 3017, 245-259, Springer- Verlag, 2004.

[12] Atul Kahate ,"Cryptography and Network Security" , pp-123-125, 2008.

[13] Pardeep and Pushpendra, "A Pragmatic Study over the Different Stream Cipher and on Different flavor of RC4 Stream Cipher", 2012.