International Journal of Instrumentation Electrical Electronics Engineering
p- ISSN: 2321 – 0621 e- ISSN: 2321- 063X

STUDIES AND IMPLEMENTATION OF VIRTUAL ENCRYPTION AND DECRYPTING IN WIRELESS SENSOR NETWORKS

Sai Sagar.N[1], E.V. Anirudh[2], Eswar Patnala[3]
Dept of IT, GIT, GITAM UNIVERSITY, Visakhapatnam
[1]sagarcse539@gmail.com, [2]anirudh_ev@yahoo.co.in, [3]eswar.patnala@gmail.com

Abstract-- Day by day internet plays a major role in sending and receiving the data, where internet plays the major communication medium. Where internet is the large collection of networks. As the data which has send through the internet i.e., it will passes through the different networks , so security issue of the data will be raised here, for this purpose we have to provide the encryption and the decryption process for the efficient data transfer through the internet . Now for the efficient data transfer we use the RC4 algorithm.

Keywords-- *virtual*, RC4 algorithm, Symmetric cryptosystem.

1. INTRODUCTION

Now days there are many communication mediums for the data transfer between the sender and the receiver. Each communication medium has their own advantages and disadvantages. While send the data we go through the so many issues like security, speed and time. One of the most important issue that we mostly look after is the security. Most of the users who wish to send the data mainly concern about the security. Sometimes they mostly not give importance to the speed and time, this type of situation will arise in some situation only where the data accuracy is more important than speed and time.

For providing security to the data which passes different networks, a numerous security algorithms are provided. All algorithms are come under the symmetric crypto system and the asymmetric cryptosystem. In symmetric key crypto system a single key is used to encrypt and decrypt the message , in asymmetric cryptosystem the message will be encrypted by using the public key and the intended receiver decrypt using the his own private key.

2. SYMMETRIC CRYPTOSYSTEM

It is one of the conventional techniques for efficient data transfer it was introduced in the year 1976. And it was only technique which was in use before developing public key cryptography [2].

This symmetric cryptosystem technique includes five phases.

2.1 Plain text

It is the original message which will be readable format.

2.2 Encryption algorithm

In this phase whatever the algorithm we have chosen for encryption performs various permutation and substitution on the original message.

2.3 Secret key

It is one of the inputs along with the original message; encryption algorithm performs substitutions and permutations based on the key which we select.

2.4 Cipher text

It is the text produced after combining both plain text and secret key, and this message will be in the unreadable format.

2.5 Decryption algorithm

The reverse of the encryption algorithm is decryption algorithm. In this in order to get the plain text we use both the cipher text and the secret key [2].

There are two requirements for a symmetric cryptosystem:

1. While we are using the techniques that belong to the symmetric crypto system. Mainly we should concentrate on the secret key rather than the algorithm that we have used. If algorithm is known nothing will happen unless we tell the secret key
2. Now most important thing that we have remaind is sender and receiver should know keep secret key in advance in order to decrypt the message. And they should exchange the secret key in a secure fashion.

International Journal of Instrumentation Electrical Electronics Engineering
p- ISSN: 2321 – 0621 e- ISSN: 2321- 063X

3. RC4 ALGORITHM

It is the stream based symmetric cryptosystem algorithm. RC4 is the stream cipher designed by the Ronald rivest in 1994. RC4 is the byte oriented stream cipher, in which byte of plain text is exclusively ORed with byte of key to produce a byte of cipher text.

RC4 is used in many data communication and networking protocol like SSL/TLS [1].

3.1 RC4 key generation

RC4 is based on the concept of state and the each time the state of 256 bytes is active from which one of the byte is randomly selected as a key for encryption[7][8]. The state is initialized to the values 0 to 255. The key array k[0],k[1],……k[255] is created. If the secret key has exactly 256 bytes the bytes are copied k-array otherwise bytes are repeated until the k- array is filled [1] [3][4][5][6].

for i=0 to 255

{

S[i] ← i

K[i] ← key[i mod key length]

}

Initialized goes to the permutation based on the values of bytes ink [i]. After this step the state bytes are completely shuffled.

f=0

for (i=0 to 255)

{

f ← (f + s[i] + k[i]) mod 256

Swap(s[i],s[f])

}

Keys in the key stream are generated one by one. 1st state is permutated based on the value of the state element and the value of the state element i & f are used to define intense key element that serves as k.

The following code is repeated for each byte of element to create new key element in the key stream.

The variables i & f are initialized to zero before 1st iteration

i ← (i+1) mod 256

f ← (f +s[i]) mod 256

swap (s[i], s[f])

k ← s[(s[i] + s[f]) mod 256]

3.2 RC4 Encryption

The following is the encryption formula for the plain text [6][7][8]. C = ‘p’ is exclusive ORed with ‘k’ where p is the plain text and k is the secret key [1][3][4][5] .

3.3 RC4 Decryption

The following is the decryption formula for the plain text [6][7][8]. P = ‘c’ is exclusive ORed with ‘k’ where c is the cipher text and k is the secret key [1][3][4][5].

4. EXPERIMENTAL RESULTS

Fig1: Save encryption data sending the encrypted data

Figure 2: Sending File

International Journal of Instrumentation Electrical Electronics Engineering
p- ISSN: 2321 – 0621 e- ISSN: 2321- 063X

In the figure 2 while sending the data using RC4 algorithm, it takes the attributes like file path, content of

the file and after entering the data we click on the encrypt button, now we can see the encrypted data which was in unreadable format. And we enter the encryption key, here we can see the encryption key as '1' and now click we on the save button. Then the following screen shot appears.

4.1 Receiving the file

After receiving the file by the intended receiver, he will opens the content using the same encryption key which was used by the sender, The figure 3shows attributes like select folder , browse and save button and the worksapce of encryption and the decryption. The encryption work space consists the unreadable data and whereas the decryption workspace consists of the readable data, the data is only readable unless and untill we enter only the encryption key.

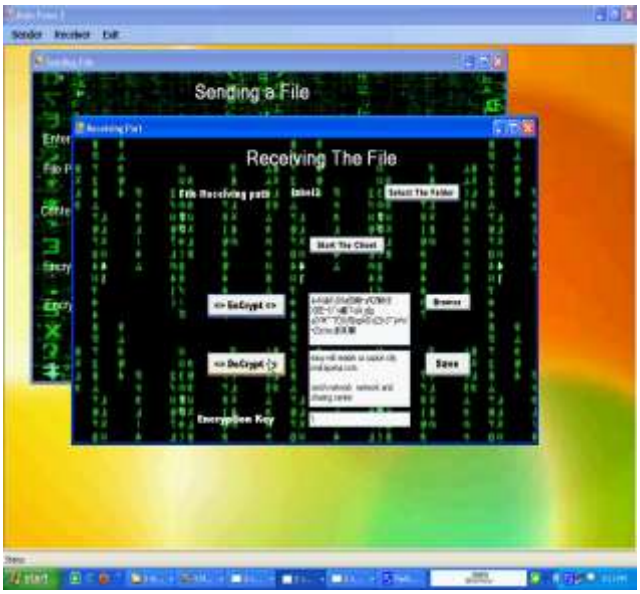

Figure 3: Receiving the encryption file and decrypt with key

5. CONCLUSION

In the above sections we describe about how to send the data more securely for this we discuss the about the symmetric cryptosystem and the ingriedents in it and then we came across the RC4 algorithm in this we discuss about the key generation and the encryption and the decryption mechanism.and we also mentioned the algorithm that how to perform key generation and the we also provided with the equation for encryption and decryption. And we take an example and develop an application using RC4 algorithm and we provide screen shots in above section.

REFERENCES

1. http://en.wikipedia.org/wiki/RC4#RC4-based_cryptosystems
2. Kartik Krishnan,"SFWR 4Co3 computer Networks and computer security", mar 8-11-04,lectures 22-24
3. Alaa M. Riad et al," evolution of the RC4 algorithm as a solution of converged networks", journal of electrical engineering,vol 60, no.3,2009,155-160
4. Fatehgarh Sahib et al "comparative analysis of AES and RC4 algorithms for better utilization" IJCTT, jul to Aug issue 2011,177-181.
5. Pardeep et al "PC1-RC4 and PC2-RC4 Algorithms: PragmaticEnrichment Algorithms to Enhance RC4 Stream CipherAlgorithm"IJCSN,vol 1,issue 3, june 2012,
6. www.uow.edu.au/~ymu/journal.html
7. cseweb.ucsd.edu/~mihir/journals.html
8. airccse.org/journal/ijcis/

TEXTBOOKS

1. Cryptography and Network Security Behrouz A. Forouzan, TMH
2. Cryptography and Network Security Third Edition, William Stallings, Pearson Education

BIOGRAPHIES

Eswar Patnala has obtained B.Tech in Information technology from Kaushik college of Engineering, Vishakhapatnam and currently pursuing my M.Tech in Information technology from Gitam Institute of technology, Gitam University, Vishakhapatnam, A.P, India

Sai Sagar.N has obtained B.Tech in Computer Science and Engineering from Moula Ali college of Engineering & Technology, Ananthapur and currently pursuing M.Tech in Information technology from Gitam Institute of technology, Gitam University, Vishakhapatnam, A.P, India

International Journal of Instrumentation Electrical Electronics Engineering
p- ISSN: 2321 – 0621 e- ISSN: 2321- 063X

E.V. Anirudh have obtained B.Tech in Computer Science and Engineering from MRITS, Hyderabad and currently pursuing M.Tech in Information technology from Gitam Institute of technology, Gitam University, Vishakhapatnam, A.P, India