IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 6, June 2016

A New RS Based Encryption Scheme for Wireless Communication

Priya Papechen[1], Shinto Sebastian[2]

PG Scholar, Dept of ECE, AJCE, Kottayam, India [1]

Assistant Professor, Dept of ECE, AJCE, Kottayam, India [2]

Abstract: This paper presents the design and simulation of a new encryption scheme for wireless communication which is simple in implementation as well as highly resistant against the attack. It utilizes the selective repeat ARQ to produce the retransmission sequence. The correct production of retransmission sequence relies on the fact that error detection should be very precise. For that purpose an error detection scheme is as also included. Then the retransmission key is hashed by using SHA-512 to produce an unpredictable key. Then the key is XOR-ed with the original message to produce the cipher text.

Keywords: Selective Repeat ARQ, SHA-512, Retransmission sequence, MATLAB GUI, CRC-32

I. INTRODUCTION

The advantage of use of wireless over wired network are flexibility, ease of use, lower cost, convenience, durability and mobility. Hence the wireless network is preferred over wired network. But the main concern related to the wireless network is the security of the data [1]. Hence a RS based encryption scheme is developed and simulated in MATLAB which can provide confidentiality to the data [2], [3]. First a retransmission sequence (RS) is generated. If the previous packet is retransmitted then it is coded as “1” otherwise as “0”. Same procedure is followed for all packets transmitted in a slot. So produced retransmission key nature is highly unpredictable due to the fact that any frame could be lost during transmission.

Corresponding to all retransmitted frame, RS is simultaneously coded at transmitter and receiver as one. Since selective repeat ARQ works based on ACK if the authorized sender doesn’t receive the ACK signalwithin the time out period then it implies that either the authorized receiver haven’t received the transmitted frame or the ACK signal sent by the authorized receiver is lost. In the former case the data is lost during transmission. Hence the receiver will code RS bit corresponding to the lost frame as one and transmitter will not get an ACK signal from the receiver for that frame. Hence it will also code RS as one. In latter case the receiver gets the frame but the ACK signal sent by the receiver is lost during transmission. Since the receiver get the frame in the first chance itself it will code the RS as zero. But the transmitter will code RS as one since it doesn’t receives any ACK signal and initiate the retransmission of the same frame. When the receiver again receives the same frame it will understand that the ACK signal for the previous frame was lost. Therefore it will change the corresponding bit in the RS as one. Thus both authorized receiver and sender generate the same RS. Then to use this RS as key, it is hashed by using secure hash algorithm. For this algorithm to work perfectly the error detection should be very precise. For that purpose CRC is performed.

II. DESIGN OF RS ENCRYPTION SCHEME

RS encryption scheme totally depend on retransmission sequence and secure hash algorithm. At first the retransmission sequence is simultaneously generated at both transmitter and receiver. RS generated at authorized transmitter will be in sync with that of the receiver. RS is generated by using selective repeat ARQ. Then to increase the strength of the RS, it is hashed by using secure hash algorithm (SHA 512).

Even a single bit change in the retransmission sequence will result in the generation of entirely different hashed key. That’s why hash function is selected for generating the key.

$$\text{Key }(k) = f_{HASH}\,(RS)\ldots\ldots\ldots\ldots (1)$$

Each time the key is updated by XOR-ing the previous key with the newly generated key.

$$\text{New key} = \text{key }(k) \oplus \text{key }(k\text{-}1)\ldots\ldots\ldots\ldots (2)$$

Once the key is generated, the cipher text is generated at the transmitter side by simply XOR-ing the message with the key.

$$\text{Cipher} = \text{Data} \oplus \text{new key}\ldots\ldots\ldots\ldots (3)$$

At the receiver side same way the key is generated. Then the receiver can decode the cipher text by performing XOR operation between the cipher text and the key. Thereby the original message can be retrieved.

$$\text{Data} = \text{Cipher} \oplus \text{new key}\ldots\ldots\ldots\ldots (4)$$

From this it can be seen that the algorithm is based on simple mathematical operation hence the complexity is reduced to a large extent. At the same time it is very difficult for an adversary to produce same retransmission sequence. Hence the adversary won’t be able to decrypt

DOI 10.17148/IJIREEICE.2016.4661

the cipher text. The schematic representation of this scheme is shown figure 2.

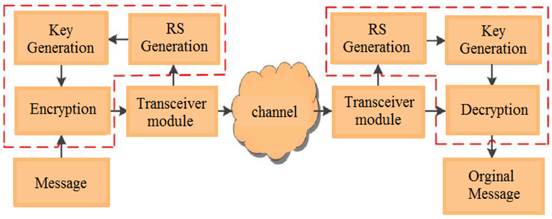


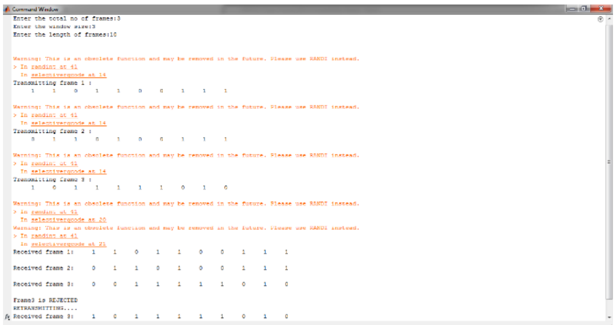
Fig. 2: Block diagram of RS encryption scheme

III.RETRANSMISSION SEQUENCE GENERATION

Retransmission sequence is the basis of the key generation. So far introduced encryption schemes it involves complicated mathematics and larger number of rounds to produce an unpredictable key. Here the key is the hashed retransmission sequence. The nature of retransmission sequence is such that each time it is completely different [3]. It is impossible to derive relation between so produced retransmission sequences because the generation of RS fully rely on the ACK and NACK signals. ACK signal is transmitted by the authorized receiver in response to the successful reception of message, whereas NACK signal is transmitted by the authorized receiver in response to the unsuccessful reception of the message. For each unsuccessful transmission of the message RS is coded as “1” at both transmitter and receiver. Otherwise it is coded as “0”. It is vital that RS generated at both transmitter and receiver should be same. It is well possible by implementing selective repeat ARQ.

A. Selective Repeat ARQ

Automatic Repeat Request (ARQ) is a technique used to ensure that data stream is delivered accurately to the user despite errors that occur during transmission [4]. ARQ form the basis for peer to peer protocols that provide for the reliable transfer of information. The most efficient ARQ protocol is the selective repeat ARQ.



```
Enter the total no of frames:3
Enter the window size:3
Enter the length of frames:10


Warning: This is an obsolete function and may be removed in the future. Please use RANDI instead.
> In randint at 41
  In selectivercode at 14
Transmitting frame 1 :
     1     1     0     1     1     0     0     1     1     1

Warning: This is an obsolete function and may be removed in the future. Please use RANDI instead.
> In randint at 41
  In selectivercode at 14
Transmitting frame 2 :
     0     1     1     0     1     0     0     1     1     1

Warning: This is an obsolete function and may be removed in the future. Please use RANDI instead.
> In randint at 41
  In selectivercode at 14
Transmitting frame 3 :
     1     0     1     1     1     1     1     0     1     0

Warning: This is an obsolete function and may be removed in the future. Please use RANDI instead.
> In randint at 41
  In selectivercode at 20
Warning: This is an obsolete function and may be removed in the future. Please use RANDI instead.
> In randint at 41
  In selectivercode at 21
Received frame 1:     1     1     0     1     1     0     0     1     1     1

Received frame 2:     0     1     1     0     1     0     0     1     1     1

Received frame 3:     0     0     1     1     1     1     1     0     1     0

Frame3 is REJECTED
RETRANSMITTING....
Received frame 3:     1     0     1     1     1     1     1     0     1     0
```

Fig. 3.1: MATLAB simulation of selective repeat ARQ

First, the receiver window is made larger than one frame so that the receiver can accept multiple frames. Second the retransmission mechanism is modified so that only individual lost frame is selectively retransmitted. I.e. in a slot if 10 frames are transmitted and if 5th frame is lost during transmission then only the 5th frame is retransmitted again. It increases the efficiency of the scheme and transmission speed. Figure 3.2 explains the selective repeat ARQ scheme.

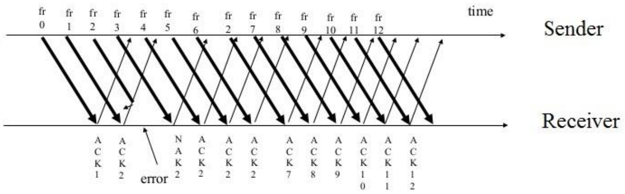


Fig. 3.2: Selective Repeat ARQ scheme

B. Cyclic Redundancy Check

In this whole process the most vital condition that has to be satisfied is that error detection must be very precise. For that purpose CRC is introduced [5].

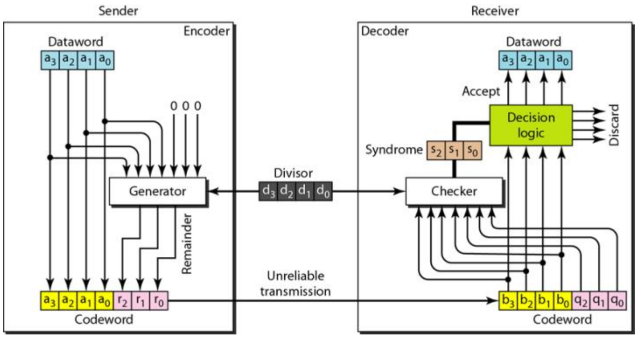


Fig. 3.3: CRC Encoder and Decoder

A cyclic redundancy check is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents. On retrieval, the calculation is repeated and, in the event the check values do not match, corrective action can be taken against data corruption. In this case CRC 32 is used where the generator polynomial will be $x^{32}+ x^{26} +x^{23} + x^{22} +x^{16} +x^{12} +x^{11} +x^{10} +x^{8} +x^{7} +x^{5} +x^{4} +x^{2} +x +1$.

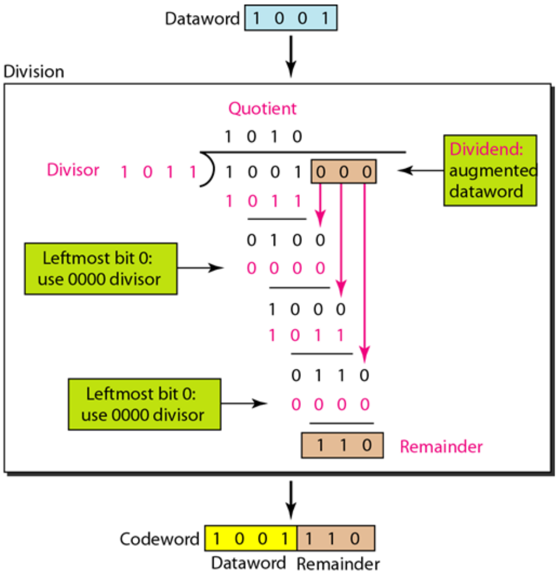


Fig. 3.4: Division in the CRC Encoder

DOI 10.17148/IJIREEICE.2016.4661

At the transmitter side CRC is performed as shown in figure 3.3 and the resultant code word obtained is 1001110. Now at the receiver the received code word is again divided by the same generator polynomial. If the remainder obtained in that case is all zeros then there is no error in the received code word otherwise, there is error in the received code word.

C. Generation of RS at transmitter and receiver

It is vital that RS generated at authorized transmitter should be the exact replica of the RS generated at the authorized receiver. Now two cases can be considered. In the first case, five frames are transmitted by the authorized sender where the 2nd frame is lost during the transmission. In this scenario only 4 frames will be received by the authorized receiver. Since each frame have a sequence number the receiver learns that 2nd has been lost. Hence it will send back an acknowledgment signal for all the frames excluding the second frame. Since the sender won't get an ACK signal for 2nd frame it learns it have been lost at some point of transmission. Hence it will selectively retransmit the second frame. Then both the authorized sender and receiver will code the 2nd bit of RS as "1" and rest of the bits as "0".

In the second case all the five frames are received by the authorized receiver. Then the receiver will sent back ACK signals for all the five frames. Also code RS as all zeros. But the ACK signal for the 3rd frame is lost during transmission. Therefore the sender will get only ACK signal for 1st, 2nd, 4th, and 5th. Then the transmitter will misinterpret the 3rd frame have not received by the receiver. Then it retransmit the 3rd frame and code the 3rd bit of RS as "1" and the rest as "0". When the authorized receiver again receives the 3rd frames it will change the 3rd bit of RS as one since it is a retransmitted frame. Likewise retransmission sequence is generated. This is a simple scenario where only one frame is lost. But in practical cases its number could be more than one and also the number of frames to be transmitted during a slot could be in the range of 1000's. So RS thus generated could be very large.

Now the case of attacker is considered. The attacker hides somewhere between transmitter and receiver. If the authorized receiver doesn't receive the third frame it doesn't mean that attacker will also won't get the third frame. That's because the transmission path between the transmitter and receiver is different from the path towards the attacker.

Assume the authorized receiver gets the first 4 frames and the authorized receiver and transmitter code RS as [0 0 0 0 1] and attacker catch all the frames and code RS [0 0 0 0 0]. Sender have encrypted the message using the key produced from his RS. Now both the receiver and attacker will generate the key using their RS. Then try to decrypt those frames. Since the attacker have a different RS, its key will be entirely different from that of the sender. Hence the attacker won't be able to decrypt the message even the adversary knows the details of RS scheme. Thus through the RS based encryption scheme security to the data is provided.

IV. KEY GENERATION

The key is generated by hashing the retransmission sequence as represented in equation (1). For that purpose a secure hash algorithm is introduced.

A. Secure Hash Algorithm

A hash function is a mathematical function that converts a numerical value into another compressed numerical value [6]. The input to the hash function is of arbitrary length but the output is of fixed length. Computationally hash functions are much faster than a symmetric operation. The efficiency of hash function are:

- Pre-image resistance

It is computationally hard to reverse a hash function. Given an input and hash function it is hard to find a different input with the same hash.

- Collision resistance

It is hard to find two different inputs of any length that result in same hash.

B. SHA 512 Algorithm

The algorithm takes as input a message with maximum length less than 2^{128} bits and produces as output a 512-bit message digest [7]. The input is processed in 1024-bit blocks. Figure 4.1 depicts the overall processing of a message to produce a digest.

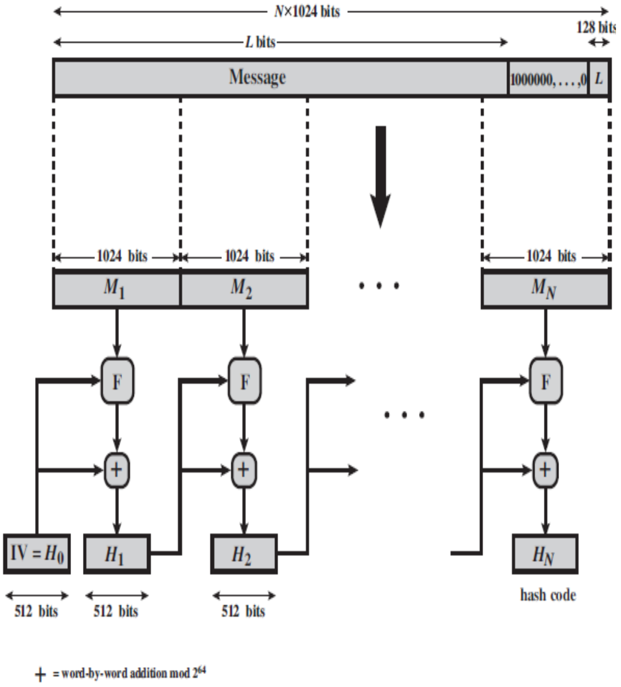


Fig. 4.1: Message Digest Generation Using SHA_512

The processing consists of the following steps:

1. Append padding bits

The message is padded so that its length is congruent to 896 modulo 1024 [length= 896(mod 1024)]. Padding is always added, even if the message is already of the desired length. Thus, the number of padding bits is in the range of 1 to 1024. The padding consists of a single 1 bit followed by the necessary number of 0 bits.

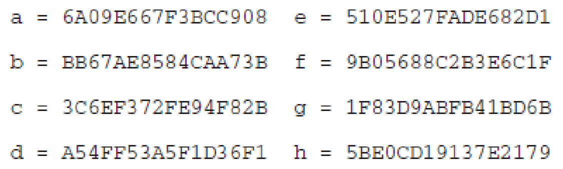
DOI 10.17148/IJIREEICE.2016.4661

2. Append length

A block of 128 bits is appended to the message. This block is treated as an unsigned 128-bit integer (most significant byte first) and contains the length of the original message (before the padding). The outcome of the first two steps yields a message that is an integer multiple of 1024 bits in length. In Figure 4.1, the expanded message is represented as the sequence of 1024-bit blocks M_1, $M_{2,}$ ……….,M_N, so that the total length of the expanded message is N x 1024bits.

3. Initialize hash buffer

A 512-bit eight buffers are used. It is used to hold intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers (a, b, c, d, e, f, g, h).These registers are initialized to the following 64-bit integers (hexadecimal values):



```
a = 6A09E667F3BCC908   e = 510E527FADE682D1

b = BB67AE8584CAA73B   f = 9B05688C2B3E6C1F

c = 3C6EF372FE94F82B   g = 1F83D9ABFB41BD6B

d = A54FF53A5F1D36F1   h = 5BE0CD19137E2179
```

Fig. 4.2: Initial Values Stored in the Buffer Registers

These values are stored in big-endian format, which is the most significant byte of a word in the low-address (leftmost) byte position. These words were obtained by taking the first sixty-four bits of the fractional parts of the square roots of the first eight prime numbers.

4. Process message

The heart of the algorithm is a module that consists of 80 rounds; this module is labelled F in Figure 4.1. The logic is illustrated in Figure 4.3. Each round takes as input the 512-bit buffer value, [abcdefgh], and updates the contents of the buffer. At input to the first round, the buffer has the value of the intermediate hash value, H_{i-1}. Each round t makes use of a 64-bit value W_t, derived from the current 1024-bit block being processed (M_i). Each round makes use of an additive constant K_t, where $0 \leq t \leq 79$ indicates one of the 80 rounds. These words represent the first 64 bits of the fractional parts of the cube roots of the first 80 prime numbers. The constants provide a "randomized" set of 64-bit patterns, which should eliminate any regularities in the input data. The output of the eightieth round is added to the input to the first round (Hi-1) to produce Hi. The addition is done independently for each of the eight words in the buffer with each of the corresponding words in H_{i-1}, using addition modulo 2^{64}.

5. Output

After all N 1024-bit blocks have been processed, the output from the N_{th} stage is the 512-bit message digest. The summary of the behaviour of SHA-512 as follows:

$$H_0 = IV \text{ ………………………….. } (5)$$

$$H_i = SUM_{64}\,(H_{i-1}, \text{abcdefgh}_i)\text{…………… } (6)$$

$$MD=H_N\text{………………………… } (7)$$

Where IV is the initial value of the buffers (a b c d e f g h) shown in figure 4.2, $[abcdefgh]_I$ is the output of the last round of processing of the i_{th} message block, N is the number of blocks in the message (including padding and length fields), SUM_{64} is the addition modulo performed separately on each word of the pair of inputs and MD is the final message digest value.

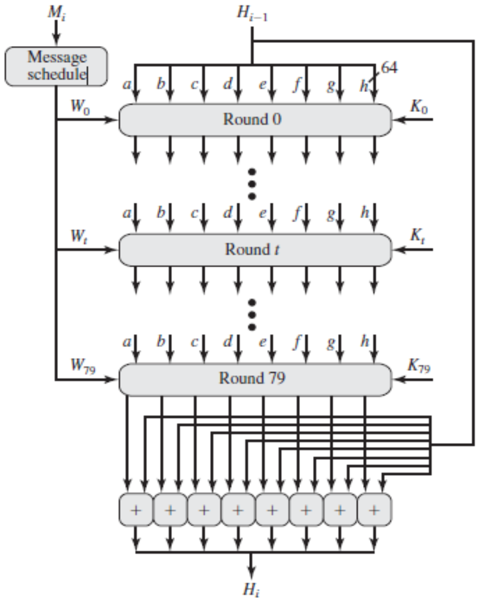


Fig. 4.3: SHA_512 Processing of a Single 1024-Bit Block

V. SIMULATION AND RESULT

The algorithm is executed in MATLAB. MATLAB(matrix laboratory) is a multi-paradigm numerical computing environment and fourth-generation programming language [8]. It is a proprietary programming language developed by Math Works. MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, JAVA, FORTRAN and Python.GUIDE (graphical user interface design environment) provides tools for designing user interfaces for custom apps.

Using the GUIDE Layout Editor, it is possible to graphically design the UI. GUIDE then automatically generates the MATLAB code for constructing the UI, which can be modified to program the behaviour of the app.

For more control over design and development, it is possible to create MATLAB code that defines all component properties and behaviours.

A. SETUP

First a user interface window is created through MATLAB GUI. The window contains four inputs. Frame number, window size, frame length and input. Frame number is the total number of frames to be transmitted. Window Size is the number of frames to be transmitted in one slot. Frame Length is the length of each frame. The input is the input the message to be encrypted. Figure 5.1 shows the user interface window designed in MATLAB GUIDE for implementing the RS encryption scheme.

DOI 10.17148/IJIREEICE.2016.4661

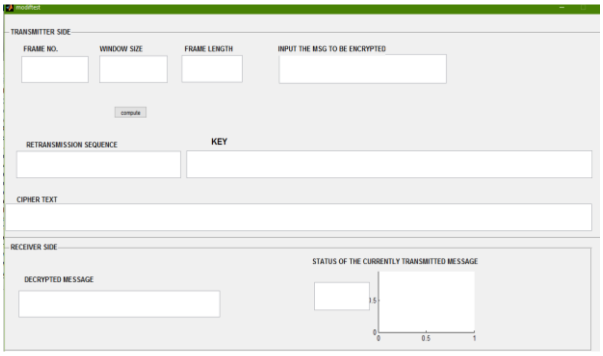
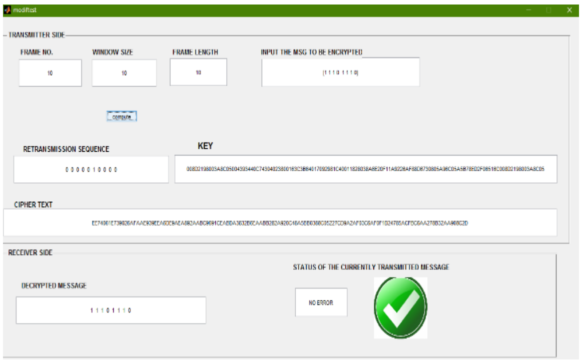


Fig 5.1: User interface window

At the transmitter side it will produce a retransmission sequence as per selective repeat ARQ. Then this RS is hashed to produce a dynamic secret key of length 512bits. Both of this result are given out via RS block and KEY block respectively. Then the message to be encrypted is zero padded to produce a sequence of length 512bits. Then the resultant input is XOR-ed with the DS to produce the CIPHER text. At the receiver side, same RS is produced (property of selective repeat ARQ) and it is hashed to produce same dynamic secret key. Then the receiver will XOR the received cipher text with the DS to retrieve the original message. For error detection CRC is implemented. Based on the result of CRC status (error / no error) will be displayed.

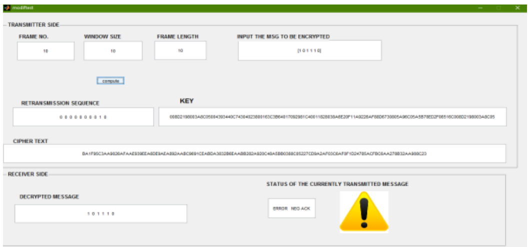
B. RESULT

To analyse the result, two cases can be considered. In the former case no error occurred during transmission. First the cyclic redundancy check is performed at the receiver. In this case the obtained syndrome will be all zeros. It implies that no error has been occurred. Then the receiver will display the no error status and proceed to decrypt the received sequence. For that purpose it will XOR the received sequence with the key to produce the original message sequence. The output obtained in this case is shown in figure 5.2. In the latter case, error have been occurred during transmission. The cyclic redundancy check is performed at the receiver. In this case the syndrome will not be all zeros. Then the receiver will display the error status. It implies that transmitter will not get an ACK for that frame before the time out period. Such sequence will be selectively retransmitted using selective repeat ARQ. The output obtained in this case in shown in figure 5.3.



FRAME NO.: 10
WINDOW SIZE: 10
FRAME LENGTH: 10
INPUT THE MSG TO BE ENCRYPTED: [1 1 1 0 1 1 1 0]
RETRANSMISSION SEQUENCE: 0 0 0 0 0 1 0 0 0 0
KEY: 008D2198003A8C05004393440C743040238001 83C3B84017092981C40011828038A8E20F11A9228AF88D8730805A08C05A5B78ED2F08518C008D2198003A8C05
CIPHER TEXT: EE74061E738026AFAAE909EEA6DE8AEA882AABC9691CEABDA3032B6EAAB8282A920C40A5BB0368C05227CD8A2AF03C6AF0F1D24785ACFBC6AA278B32AA908C2D
DECRYPTED MESSAGE: 1 1 1 0 1 1 1 0
NO ERROR

Fig. 5.2: Output when there is No Error in Received Sequence



FRAME NO.: 10
WINDOW SIZE: 10
FRAME LENGTH: 10
INPUT THE MSG TO BE ENCRYPTED: [1 0 1 1 1 0]
RETRANSMISSION SEQUENCE: 0 0 0 0 0 0 0 0 1 0
KEY: 008D2198003A8C05004393440C74304023800183C3B84017092981C40011828038A8E20F11A9228AF88D8730805A06C05A5B78ED2F08516C008D2198003A8C05
CIPHER TEXT: BA1F95C3AA9926AFAAE939EEA6DE9AEA892AABC9691CEABDA3032B6EAAB8282A920C40A5BB0368C05227CD9A2AF03C6AF0F1D24785ACFBC6AA278B32AA998C23
DECRYPTED MESSAGE: 1 0 1 1 1 0
ERROR NEG ACK

Fig. 5.3: Output when there is error in the Received Sequence

The experiments reveal that:

1) The RS scheme can protect the users against eavesdropping by updating the encryption key derived from the RS. Even the attackers know the details of RS scheme, they will not be able to predict the key.
2) It is a light-weight encryption method with only simple operations, such as SHA 512 and XOR; therefore mathematical complexity is less.
3) It is self-contained. i.e. retransmission sequence is generated on the spot during the normal communication without additional traffic and control command;
4) Hardware implementation is very simple and it has good compatibility

VI. CONCLUSION

In this paper, a new encryption scheme is simulated in MATLAB to secure the wireless communication. To reduce its complexity, the retransmission sequence scheme is proposed to generate the encryption key. The key is generated by hashing the RS using SHA 512 algorithm. The proposed scheme seems to be simple but also possess high resistance against eavesdropping.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to **Mr. Shinto Sebastian**, Asst. Professor, Dept. of ECE, Amal Jyothi College of Engineering, for his valuable guidance and encouragement throughout the project work. I would also like to acknowledge the Department of Electronics and Communication Engineering, Amal Jyothi College of Engineering, Kottayam, Kerala, India.

REFERENCES

[1] X. Sheng, G.Weibo, and D. Towsley, “Secure wireless communication with dynamic secrets,” in Proc. 2010 IEEE INFOCOM, pp. 1–9.

[2] S. Xiao and W. Gong, “Wireless network security using randomness,” U.S. Patent 8 204 224 B2, Jun. 19, 2012

[3] Ting Liu, YangLiu, YashanMao, Yao Sun, XiaohongGuan, , Weibo Gong, , and Sheng Xiao, “A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication”, IEEE transactions on smart grid, vol, no.3, may 2014

[4] Article on selective repeat ARQ at https:// en.wikipedia. org/wiki/ Selective Repeat ARQ

[5] Behrouz A. Forouzan “Data Communication and Networking”, 4th edition, 2007

[6] Article on hash function at https:// en.wikipedia. org/wiki/ cryptographic hash function

[7] Willam Stalling “cryptography and network security” 2006

[8] An article on “MATLAB GUIDE”, at http://in.mathworks.com/discovery/-gui.html

DOI 10.17148/IJIREEICE.2016.4661