International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Improved Reed-Solomon for Network security at Physical Layer

Priyanka[1] , Bhavika Jagga[2]
[1]M.Tech Student Department of Computer Science JCDMCOE Sirsa, Haryana, India
[2]Assistant Professor Department of Computer Science JCDMCOE Sirsa, Haryana, India

ABSTRACT

A secure and efficient data transmit method is required by Wireless sensor Network. The communicating parties share similar channel information at physical layer that the others cannot grasp. The capacity of a binary channel is increased by adding extra bits to this data. This improves the quality of digital data. The process of adding redundant bits is known as channel encoding. In many situations, errors are not distributed at random but occur in bursts. For example, scratches, dust or fingerprints on a compact disc (CD) introduce errors on neighboring data bits. Cross-interleaved Reed-Solomon codes (CIRC) are particularly well-suited for detection and correction of burst errors and erasures. It can implemented as Wireless security which provides speed and security. This way can achieve both high security and efficiency.

Keywords :- Wireless Senor Network, Reed-Solomon Encoding/Decoding, Glorious Field, Polynomial, Cauchy cell matrix, Cross-interleaved Reed-Solomon codes (CIRC)

I. INTRODUCTION

Security protocols are the most important elements involved in enabling the growth of the wide variety of wireless data networks and applications. The broadcast nature of wireless communications, however, makes them particularly vulnerable to eavesdropping. With the creation of more complex modern infrastructure systems, there is an increasing need for secure communication solutions. Cryptography is a established filed that provides computationally secure protocols at the application layer. The goal of cryptography has recently been diversify from providing the important confidentiality service, to other issues including authentication, key exchange and management, digital signature, and more. Unlike the cryptographic approaches, the lately reintroduced physical-layer security aims to develop effective secure communication schemes exploit the properties of the physical layer. This new example cans strength the security of existing systems by introducing a level of information theoretic security which has provable security, as compared with computational security.

II. OBJECTIVE STUDY

Needs of Communication Systems

The transmitter can have several roles together. To compress data, to secure data, to make it more reliable and lastly to transmit it as signals suited for the physical channel. Compressing data is also called source coding; it consists of mapping sequences of symbols in the original data stream to shorter ones. This is done based on the statistical distribution of the original data: the most frequent sequences are mapped to shorter ones while rare sequences are mapped to longer ones. By doing this, the resulting sequences are on average shorter, i.e. sequences with fewer symbols. On the opposite, in order to make the

sequence of symbols robust to errors, redundancy is added to it. This is called channel encoding and consists of mapping shorter sequences to longer ones so that if a few symbols are corrupted the original data can nevertheless be found back. This seems contradictory since one reduces the number of sent symbols while the other increases it. However, it is not really. The source coding reduces the redundancy of unstructured data which would not provide protection if symbols were corrupted. For example, despite knowing that a message contains on average 99% of zeros, you cannot know which bits were corrupted when sending the message as it is. On the opposite, channel coding adds structured data to improve protection against such errors during the transmission. By taking the compressed message and repeating three times each bit, you can decode correctly up to one error per three bits introduced. One could wonder if a technique performing both in a single step could be more efficient than doing it sequentially. This is known as the source-channel coding separation theorem and is one of the results of Shannon's ground breaking work. For finite sequence length, such joint encoding techniques are still a subject of research. However, the physical channel does not, technically speaking, transmit symbols but signals (waves, voltage, etc...). We however assume a one-to- one mapping between symbols and signals which is done by a modulator to map a symbol to the corresponding signal and a demodulator mapping back a received signal to a received symbol, or information about the likelihood of each potential symbol. Notice that by separating the source and channel coding, an encryption module can also be conveniently inserted between both.

III. PROPOSED METHODOLOGY

Reed-Solomon codes

RS codes, which are BCH codes, are used in applications such as spacecraft communications, compact disc players, disk drives, and two-dimensional bar codes .Reed Solomon codes are a subset of BCH codes and are linear block codes.

Let GF(q) be a finite field with q elements and it generate a rather specific BCH code C over GF(q) of length n , called a Reed-Solomon code. Let α be a primitive nth root of unity of GF(q) and let code C have a length of $n=q-1$. Now take d so that $1 \le d \le n$ and the generator polynomial g(x).Therefore, a Reed-Solomon code is a cyclic (n, n+1–d, d) code with codewords corresponding to polynomials, where each f (x) is a polynomial with coefficients in GF(q) that cannot be factored into lower degree polynomials while assuming that the highest non-zero coefficient is 1:

$g(x)f(x)$ with $\deg(f) \le n-d$.

It follows that there are q choices for each n–d+1 coefficients of f (x), and thus there are qn–d+1 codewords in code C . Therefore, an RS code is a MDS code since it makes the Singleton bound an equality.

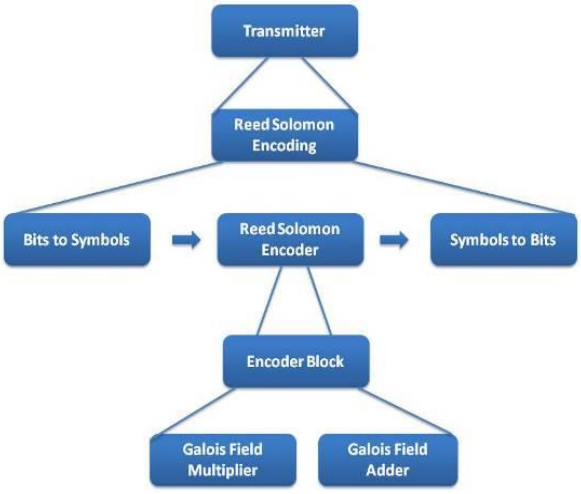

Figure 1. Reed Solomon Algorithm

REED-SOLOMON ENCODING AND DECODING

The capacity of a binary channel is increased by adding extra bits to this data. This improves the quality of digital data. The process of adding redundant bits is known as channel encoding. In many situations, errors are not distributed at random but occur in bursts. For example, scratches, dust or fingerprints on a compact disc (CD) introduce errors on neighboring data bits. Cross-interleaved Reed-

Solomon codes (CIRC) are particularly well-suited for detection and correction of burst errors and erasures. Interleaving redistributes the data over many blocks of code. The double encoding has the first code declaring erasures. The second code corrects them.

Reed Solomon Encoding

Reed Solomon encoding can be done in many ways. Some of them being

- ✓ Encoding by polynomial division
- ✓ Encoding in the frequency domain
- ✓ Encoding using Cauchy cell matrix method

However, the basic encoding principle is going to be the same.

1. First of all, the information symbols are being transferred to the output using generator polynomial or Cauchy cell matrix.
2. Then the parity bits are added to these information symbols.

Reed Solomon Decoding

RS decoding is done in three levels. First one being, syndrome calculation that tells us whether an error has occurred during the transmission of data. The second step includes error location which tells us where the error is present, and the third one is the error evaluation which corrects the error. However, the decoder has the capability of correcting t errors where n=k+2t.

When a code word is decoded, there are three possible outcomes:

• If 2s + r < 2t (s errors, r erasures) then the original transmitted code word will always be recovered.

• The decoder will detect that it cannot recover the original code word and indicate this fact.

• The decoder can incorrectly decode and recover an incorrect code word without any indication.

IV. RESULT AND DISCUSSION

Experiment

Following command need to run for Encoding.

Experiment 1

ENCODE

Run “EncodeTest.m

```
INPUT DATA

msg = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

     2     7     3
     4     0     6
     5     1     1
```

We have taken three codewords composed of 3-bit symbols.

```
ENCODED DATA

encode = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

     2     7     3     3     6     7     6
     4     0     6     4     2     2     0
     5     1     1     4     5     4     0

Elapsed time is 0.119943 seconds.
```

The codes are systematic so the first three symbols of each row match the original rows of msg.

DECODE

Run “DecodeTest.m

```
DECODED DATA

rxcode = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

     2     7     3
     4     0     6
     5     1     1

Elapsed time is 0.160465 seconds.
```

Experiment 2

ENCODE

```
INPUT DATA

msg = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

     1     6     3
     4     7     6
     2     1     1

ENCODED DATA

encode = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

     1     6     3     6     4     3     1
     4     7     6     5     5     4     6
     2     1     1     0     2     0     3

Elapsed time is 0.256311 seconds.
```

DECODE

```
DECODED DATA

rxcode = GF(2^3) array. Primitive polynomial = D^3+D+1 (11 decimal)

Array elements =

     1     6     3
     4     7     6
     2     1     1

Elapsed time is 0.029863 seconds.
```

Time Graph and Table

Table 1

EXPERIMENT	ENCIODE TIME (S)	DECODE TIME (S)
1	0.119943	0.060465
2	0.256311	0.029863

We can see from result, Encoded takes less than 0.3 seconds while decoding is more fast and takes less time then encoding

Following is performance graph of Time

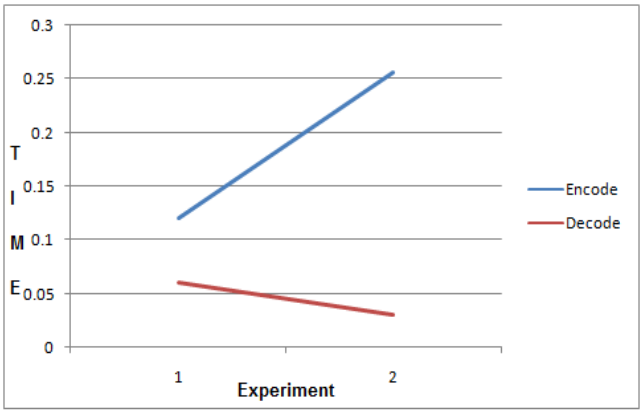

Figure 2. Time Graph

V. CONCLUSION

In the paper, we proposed Reed-Solomon Encoding/Decoding. We also examine the time consumption by Reed-Solomon. The simulation results demonstrate that our proposed method have high efficiency and accuracy. Reed Solomon Encoding and decoding was simulated in MATLAB. It was found that Time taken in encoding and decoding is very less and output is also accurate.

VI. REFERENCES

[1]. Zhouzhou Li and Honggang Wang, "A Key Agreement Method for Wireless Body Area Networks", 2016, IEEE

[2]. Mustafa Duruturk," Study of Physical Layer Security in Wireless Communications", Spring 3-5-2010.

[3]. Maja Malenko,"Implementation Of Reed Solomon RS(255,239) Codes", March 2014

[4]. Hazem Al-Bermanei,"Reed-Solomon Encoding And Decoding", Spring 2011.

[5]. Hao Li, "Physical-Layer Security Enhancement in Wireless Communication Systems", "September 2013"

[6]. Vishali.R, "Security in Wireless Local Area Networks", International Journal of Computer Science and Information Technology Research, 2014

[7]. Abu Taha Zamani, Javed Ahmad, "Wireless LAN Security : IEEE 802.11g & VPN", International Journal of Advanced Research in Computer Science and Software Engineering, 2014