Reed Solomon codes for enhancing the security in IOT based Home Automation

Rekha K B
rekhakb_24@gmil.com

Naveen Chandra Gowda
ncgowdru@gmail.com

Abstract

Internet of Thing is the emerging technology in the networking field. The term Internet of Things general refers to everyday items not only a computer it can also be sensors, computing devices which generates or exchange or consume data with lesser human intervention. It visualizes the interaction and cooperation among smart objects such as mobile devices, medical devices and overwhelming the technologies such as smart grids for digital communication technology or for smart homes or for smart cities etc. The human interaction for smart homes may leads to errors in bit pattern due to noise or other issues in data communication channel leading to catastrophic. This paper proposes a framework for implementing reed Solomon codes before any operation given by user is executed for preventing any such catastrophic in home automations. Raspberry Pi computer system is designed for implementing this proposed scheme.

Keywords: Internet of Things (loT); Reed Solomon Code; Galois Field.

I INTRODUCTION

The **Internet of things** (**IoT**) is the inter-networking of physical devices, smart devices, buildings, and for embedded systems in electronic devices, software, sensors, actuators, and by using network connection these devices will b able to send the data or collect the data or exchange the data. The aim behind using the IOT is to make human life faster and comfort.

The IOT uses the objects for sensing or for controlling the things in existing networks to incorporate the physical world into more computer based systems so that efficiency is improved and provides more accuracy and also provide more economical benefits with lesser human intervention. When IoT make use of sensors and actuators, then it can include the technologies which may be used for developing smart cities, smart home, smart vehicles or smart devices with greater benefits to human life etc.

II APPLICATiONS OF IOT

Internet of Things (IoT) is network transfer data without human to human and human to machine communication. loT offers a wide range of applications some of the important applications are listed below.

A. Home Automation

IOT can be implemented to our home by using Smart Home Automation technique with Raspberry Pi and it is done by integrating cameras and motion sensors into a web application to control various home appliances such as for smarter lighting, for smarter door locks etc for security enhancement with minimum power and energy consumptions.

B. Healthcare

loT can be used for medical appliances for monitoring patients health and earlier detection of any diseases by IOT techniques. It can also be used for implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up.

C. Environment Monitoring

Environmental monitoring applications of the IOT uses sensors to protect the environment by monitoring the quality of air and water, to monitor the movements of wildlife's and also for earlier waning system applications like earthquake or tsunami.

D. Building and home automation

IOT devices can be used to monitor as well as to control the electrical or electronics devices, used in various public or private institutes, industries, homes.

III. SMART HOMES

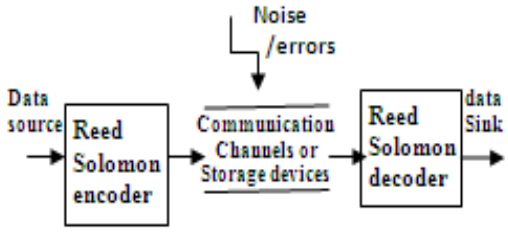
The center of attention of this paper is on smart home systems. Smart home is the one which incorporates various computing devices along with sensors using network connection to maintain our daily appliances in smarter as well as faster way. So, in our Home system, there are many such devices that can be accessed and controlled using loT. Such devices can be included for lighting systems, heating systems, for a media and also for entertainment systems and for several others things for home appliances.

IV. PROBLEM STATEMENT

From the security and safety aspects of smart home system, any operation invoked by the user may prove catastrophic if either the operation and!or the corresponding script to be executed on the server get corrupted due to noise, dust or any other external interference. This can prove really critical in case of a home system wherein there are appliances that involve a high degree of risk factor. So the aim of our paper is to address this security! Safety issue.

V. REED SOLOMON CODES FOR ERROR DETECTION! CORRECTION

RS codes are widely used in data transmission and data storage in electronic devices through wireless communication channels.
A Reed-Solomon encoder takes computerized information pieces and includes additional repetitive bits. The Reed-Solomon decoder forms each square and endeavors to right blunders and recoup the first information where the number and sort of mistakes to be amended depends on the Reed-Solomon code trademark. These codes accomplish the biggest code least separation for direct codes with the same encoder information sources and yield piece lengths. The separation between two code words for no twofold codes is characterized as the quantity of images in which arrangements vary.
Reed-Solomon codes are used to correct errors for storage devices like disk, DVD, barcodes etc. These are also used for mobile communications, even for high speed modems like ADSL etc.
A typical system is shown here:



RS encoder is one of the forward mistake redress strategies utilized as a part of remote correspondence frameworks. RS codes are efficient direct square code.

Give us a chance to comprehend RS Encoder with (N=255, K=239,T=8)specifications:
image length : m bits per image (8 bits)
Piece length: N=2^m - 1 images (255 bytes)
Information length: K images (239 bytes)
size of check code: N-K = 2*t images (16 images)
Least separation: 2*t + 1 images

As appeared in the figure the RS encoder grows a piece of K images to N images by including N-K excess images. For the most part, m is energy of 2 and famous incentive for m is 8.

The Reed-Solomon decoder processes each block and attempts to correct errors and recover the original data by using error correction algorithm. The number and type of errors that can be corrected depends on the characteristics of the Reed-Solomon code.

Properties of Reed-Solomon codes

Reed Solomon codes are block codes and are represented as RS(n,k). where n is the size of output code and k is number of data symbols. n-k = 2t is the number of parity symbols.
The RS encoder takes k data symbols of s bits each along with this parity symbols are added to get n-symbol data called codeword. Hence n-k parity symbols are use for each of s-bits.
A reed-solomon decoder does error correction upto t symbols which are having errors in a codeword where
2t = n - k

The following figure illustrates a typical Reed-Solomon codeword:

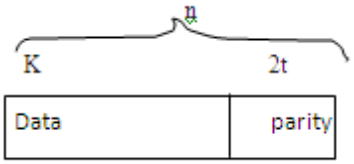


Figure: structure of RS codeword

Data block length: n
Number of message symbols: k
Number of parity symbols: n-k=2t
Each symbol at input is composed of m bits given by relation:
n = 2m – 1 (1)
The massage is divided into k symbols each of m bits long and 2t parity symbols are added to the m-bit k symbols to give n symbols of RS code. The information symbols are represented as a polynomial in powers of x from k-1 to 0 with most significance symbols having higher power. Reed Solomon codes are constructed using generator polynomial which is given by equation

$$g(x) = (x+\alpha)\,(x+\alpha^2)\,(x+\alpha^3)\,\ldots\,(x+\alpha^{2t})$$

The code created will be totally separable by generator polynomial. The data images are first duplicated with Xn-k which will add n-k zeros to images and then isolated by generator polynomial. The rest of be held and added to data images. Hence RS code is given

$$g(x) = (x+\alpha)\,(x+\alpha^2)\,(x+\alpha^3)\,\ldots\,(x+\alpha^{2t})$$

All the arithmetic calculation are done over Galois fields.

Implementation of rs encoder and rs decoder can be done either in software or hardware.

The measure of handling "power" required to encode and interpret Reed-Solomon codes is identified with the quantity of equality images per codeword. A substantial estimation of t implies that

an expansive number of mistakes can be rectified however requires more computational power than a little estimation of t.

A . Architectures for Reed-solomon encoder and decoder

Reed-solomon encoder and Reed-solomon decoder can be carried out in software or in hardware. It is based mainly on following two principles:

1) Finite/ Galois Field Arithmetic

Reed-Solomon codes are based on area of mathematics called as Galois fields or finite fields.the property of his field is that any arithematic operations like +,-,/,* performed on field elements will always leads to result in the field.The RS encoder or decoder needs software or hardware functions to be implemented to perform any of these arithmetic operations.

2) Generator Polynomial

A Primitive Polynomial Is Used to Define the Finite Field .primitive polynomial is uses a functions which defines the finite fields that are needed to define R-S codes

The generating polynomial fo an RS Code takes the following form:

$g(X)=g_0 + g_1X + g_2X^2 +\ldots.+ g_{2T-1}X^{2t-1} + X^{2t}$

The degree of the generator polynomial is equal to the number of parity symbols

The roots of a generator polynomial, g(X), must also be the roots of the codeword generated by g(X). And the resulting codeword is constructed using the following form,

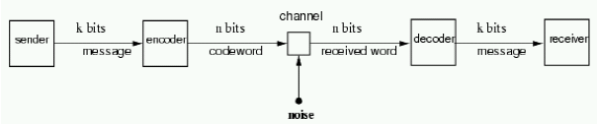
$$c(x) = g(x). i(x)$$

Where g(x) denotes the generator polynomial, i(x) refers as the information block, c(x) is the generated codeword which is the primitive element of the field.

Therefore, an arbitrary codeword, when evaluated at any root of g(X), must yield zero.

3) Encoder Architecture

The encoder combines the message with some redundancy, in order to create a codeword. This makes it possible to detector correct errors introduced by the channel. At the receiver's end, the codeword , which may be corrupted by errors is decoded to recover the message.



The RS encoder internal structure is 2t shift register with each width of m bits.

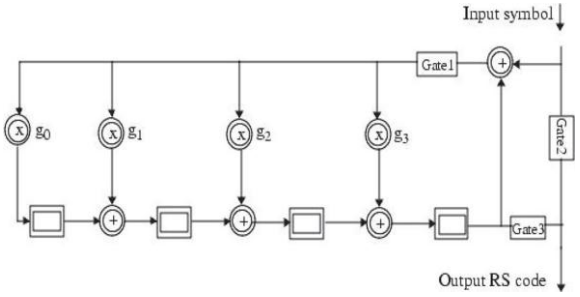
Encoding process is used to find the remainder or parity symbols for the message ,where g(x) is polynomial.

g(x)

codeword is obtained by concatenating these parity symbols to the end of data symbols.

On the other side, when the decoder receives the message block it divides the message by RS generator polynomial.If the remainder is zero then it indicated as no errors in the data else it indicated as errors in the data.

The RS encoder is shown in the figure below:



B. RS Decoder Architecture:

In RS decoder syndromes for each codewords received is calculated to determine the number of errors in received codewords.if there are errors then the decoder finds out the location of the error by Berlekamp-massey Algorithm using error locator polynomial.

The Chien search algorithm is used to find out the roots of this polynomial

Given below is the architecture of RS decoder:

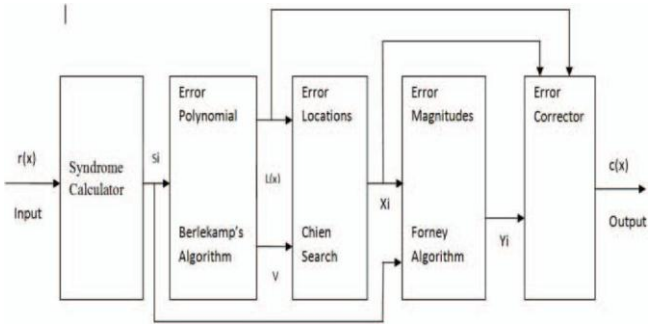


Fig.2 RS Decoder

r(x) is the input Codeword given to the syndrome calculator, Si are the Syndromes generated by syndrome calculator, L(x) is the Error locator polynomial which is obtained by using berlekamp's algorithm, Xi are the locations in which error are found by using chien search algorithm, Yi refers to the magnitude of errors, c(x) is received codeword and v is number of errors that are generated.

r(x) is the original codeword that was transmitted over the channel in an encoded format which may contain errors e(x). Thus the received codeword is the original codeword with addition of errors.

$$r(x) = c(x) + e(x)$$

A Reed-Solomon decoder performs error detection up to t errors or 2t errors and also performs the error correction.

To sum up the decoding process,
1.The error syndrome is calculated and to generate an error polynomial we use Barlekamp algorithms.

2.Calculate roots of the polynomial using Chein search algorithm.
3.Determine the type of error by using Forney's algorithm

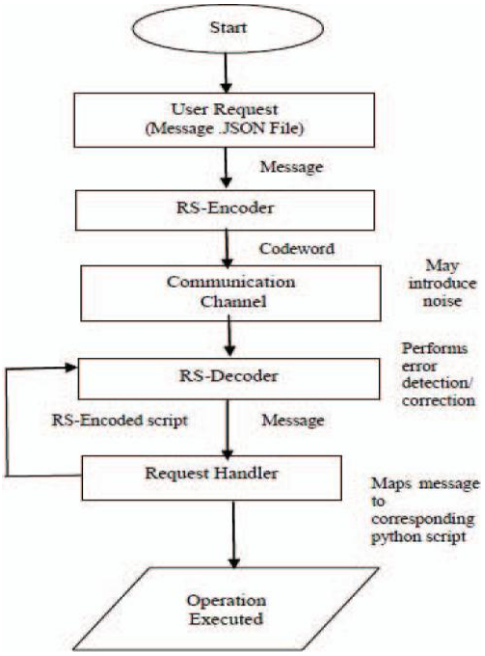
4.Error correction of symbols by comparing the mask and data word and then sequentially inverting all erroneous bits

VI. PROPOSED METHODOLOGY

In our proposed IOT based home automation we use Reed Solomon codes to provide better safety and security.
The proposed Home automation system based on IOT uses Reed Solomon codes to lessen the risks and also it provides error correction scheme both during data storing process as well as at the communication channel to enhance the security.
We have used Raspberry Pi computer to implement our proposed system.
We have designed the front end using PHP scripts to accept the user's requests or messages. These requests will be in JSON file format which is then given to the encoder to encode the message to generate codeword. This codeword is then transferred to the receiver side through the communication channel.
At the receiver side the RS decoder accepts the encoded codeword sent by user and decodes it to check the errors due to noise or some other factors which might have generated during transmission of the data through communication channel. The RS-decoder detects and corrects any error if found in the codeword.
The decoder then sends the codeword to the request handler to process the user request.
The request handler takes the request sent by decoder and tries to map this request to corresponding script which is stored in the encoded format on the server. This script is later verified by RS decoder on the server side to check the errors caused due to noise or dust or any scratches or any other factors through communication channel.

Finally, If it is error free then the script will be executed to perform the user requested operation and the acknowledgment is sent to the user.

The flowchart below demonstrates the entire procedure:



CONCLUSION

In this paper we have implemented IOT based robust home automation in our proposed system. We have implemented this by providing a 2-tier security, firstly at user level and secondly at server level so that operation performed will not lead to malfunction and by this way it enhances more security and provides safety to the home appliances.

References:

1.Vamsikrishna Patchava, Hari Babu Kandala, P Ravi Babu. "A Smart Home Automation technique with Raspberry Pi using IoT", 2015International Conference on Smart Sensors andSystems (IC-SSS), 2015
2. Moon. "BCH and Reed-Solomon Codes: Designer Cyclic Codes", Error CorrectionCoding, 05/13/2005
3. R. Logeshwaran. "Performance study on the suitability of Reed Solomon Codes in WiMAX", 2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC), 01/2010
4. "Study of Reed Solomon "Encoder International Journal of Innovative Research in Computer and Communication Engineering *Vol. 1, Issue 2, April 2013*
5. Xiaojun Wu, Xianghui Shen, Zhibin Zeng, "An improved RS encoding algorithm", IEEE CECNet International conference, pp. 1648-1652, April 2012. (Conference)
6. Bernard Sklar is the author of *Digital Communications: Fundamentals and Applications, Second Edition* (Prentice-Hall, 2001, ISBN 0-13-084788-7).