Australian Journal of Basic and Applied Sciences, 9(27) August 2015, Pages: 506-510

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Design of MELP Transmission with Elliptic Curve Cryptography Algorithm

[1]Sandeep Allada and [2]Srinivasan Nagaraj

[1] GMR Institute of Technology, Computer Science Engineering, Rajam, Srikakulam, Andhra Pradesh, India.
[2] Assistant Professor, GMR Institute of Technology, Computer Science Engineering, Rajam, Srikakulam, Andhra Pradesh, India.

ARTICLE INFO

Article history:
Received 23 June 2015
Accepted 25 August 2015
Available online 2 September 2015

Keywords:
Elliptic Curve Cryptography, MELP, FEC and Filter method.

ABSTRACT

Main aim of cryptographic research is in device protocols that provide confidentiality, integrity, non repudiation and authenticated transmission of messages take over an insecure channel. In battlefield, messages must be encrypted to provide protection from enemy interception. The recently, selected U.S federal was standardization for 2400 bps speech or voice compression technique i.e., MELP. In this, we have been advised a new approach that provides security for MELP – compressed speech transmission in noisy channels in conjunction with a forward error control scheme is including RS, BCH and Turbo Codes. In this method by using ECC algorithm is encrypting, decrypting the data and over the unsecured channel.

To Cite This Article: Sandeep Allada and Srinivsan Nagaraj., Design of MELP Transmission with Elliptic Curve Cryptography Algorithm. ***Aust. J. Basic & Appl. Sci.,*** *9(27): 506-510, 2015*

INTRODUCTION

This paper presents secure speech transmission using ECC. In this, speech was transmitted through MELP (Mixed Excitation Linear Prediction) and then for any error checking using Turbo codes and then for security purpose here using ECC (Elliptic Curve Cryptography). Here the Speech can be taken as 2400 bps for the speed processing.

MELP:

Introduction:

The MELP speech coder was developed by the US military. The MELP vocoder supports 3 different vocoders i.e., 2400bps, 1200bps and 600bps (Victor Demjanenko, David Satterlee, 2014).

Table 1: MELP Compression Technique.

Bit rate	Compression ratio	Payload size	Payload interval
2.4 kbps	26.7 X	54 bits	22.5 ms
1.2 kbps	53.3 X	81 bits	67.5 ms
0.6 kbps	106.7 X	54 bits	90 ms

The MELP encoder compression algorithm can operate with a limited low bandwidth signal; there is some degradation in performance (Weiran Lin, *et al.,*).

MELP Processing:

The first step in this encoding process is filtering out the low frequency noise by using the shaping filters.

The next step is to process The basic 2400 bps rate vocoder uses a 22.5 ms frame of speech consisting of 180 8000 Hz, 16-bit speech samples. The payload sizes for each of the rates are 54bits, 81bits, and 54 bits respectively, for the 2400bps, 1200bps, and 600 bps frames (Lynn, M., *et al*.,).

Forward Error Correction:

In telecommunication, the coding and information theory, channel coding or forward error correction is the technique to control the errors in information transmission over unreliable the noise communication channels (https://en.wikipedia.org/wiki/).

The redundancy tolerates the receiver to detect a limited number of errors that may occur anywhere in the message, and often to correct these errors without retransmission. FEC data are usually added to devices of mass storage to enable recovery of corrupted data, and is widely used in modems.

Corresponding Author: Sandeep Allada, GMR Institute of Technology, Computer Science Engineering, Rajam, Srikakulam District, Andhra Pradesh State, India-532001.
E-mail: allada.sandeep@gmail.com

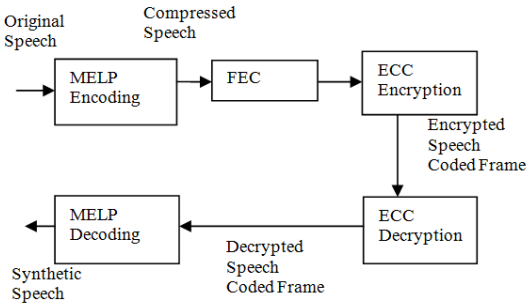

Fig. 1: Basic Architecture of Total performance.

FEC is achieved by adding redundancy to the transmitted information using an algorithm. A redundant bit may be a complex function of many original information bits. The original data may or may not appear literally in the encoded output; codes that include the unmodified input in the output are systematic, while those that do not are non-systematic.

Main articles: Convolutional code and Block code.

The main categories of FEC codes are convolutional codes and block codes.

- Block codes should work on fixed-size blocks (packets) of bits or symbols of predetermined size. Practical block codes can generally be hard-decoded in polynomial time to their block length.
- Convolutional codes work on a bit or symbol streams of arbitrary length. They are most often soft decoded with the Viterbi algorithm, though other algorithms are sometimes used. Viterbi decoding allows asymptotically optimal decoding efficiency with increasing constraint length of the convolutional code, but at the expense of exponentially increasing complexity.

Noise Reduction:

For Noise Reduction here we use Z-transform. Z-transforms are to difference equations what Laplace transforms are to differential equations.

Definition of Z-transform as below:

- Given a finite length signal, the z-transform is defined as

$$X(z) = \sum_{k=0}^{N} x[k]z^{-k} = \sum_{k=0}^{N} x[k](z^{-1})^{k} \quad (1)$$

Where the sequence support interval is [0, N], and z is any complex number.

- This transformation produces a new representation of x[n] denoted X(z).
- Returning to the original sequence (inverse z-transform) x [n] requires finding the coefficient associated with the nth power of z-1.

Mainly in Z-transform gain the data as

gain=gain+aCoeff(index,nframe)*exp(-i*2*pi*cft).^index (2)

Turbo code Introduction:

Turbo codes were first introduced in 1993 by Berrou, Thitimajshima and Glavieux. They were reported in, where a scheme is described that achieves a bit-error probability of 10-5 using a rate 1/2 code over an additive white Gaussian noise (AWGN) channel and BPSK modulation at an Eb/N0 of 0.7 dB (Nabeel Arshad, Abdul Basit,).

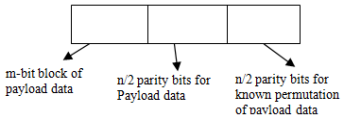

Fig. 2: Sub-blocks of Turbo code encoding.

Turbo codes are the class of high performance. The turbo code is the first practical codes to closely approach the channel capacity. This turbo code is mostly used at 3G Communication, satellite communication (http://www.eas.uccs.edu/wickert/ece2610/).

Turbo code Encoding:

Turbo code encoding sends 3 sub blocks of bits. First sub block represents m bit block of payload data, second sub block represents n/2 parity bits for payload data and third sub block represents n/2 parity bits for a known permutation of payload data. Then the complete block has m + n bits and the code rate is m / (m + n).

Hardware wise the turbo code encoder consists of 2 identical RSC Coders connected to each other using concatenation scheme called "Parallel Concatenation" (Bernard Sklar,).

Here M is the memory region, interleaver is the force input bits d_k to appear indifferent sequence and RSC coders respectively used n1 and n2 iterations.

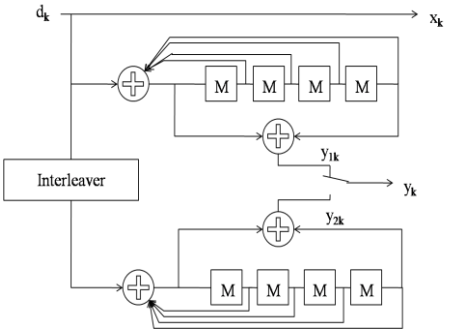

Fig. 3: Turbo code encoding Process.

Interleaver:

Coding techniques such as convolutional codes are suitable for channels with random errors like binary symmetric channel or AWGN (Additive White Gaussian Noise) channel. But there are many errors occur continuously in many channels.

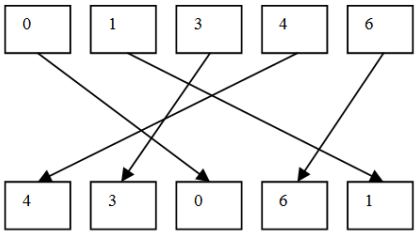

Fig. 4: Interleaver Procedure.

A burst of errors raises large number of errors in code words. So, there appears a need of strong correction capability. In this case, order deal with these bursty channels, inter-leaver is introduced. Inter-leaver works by taking an input sequence and permuting it randomly or according to a prescribed method (https://en.wikipedia.org/wiki/).

Inter-leaver proves to be very effective in dealing with bursty channels by permuting the data at the receiver side. There are various types of inter-leavers like block inter-leaver and convolutional inter-leaver. In turbo codes inter-leaver that permutes the data randomly is preferred. In Fig. 4, below working of random interleaver is shown. Suppose our input is (0,1,3,4,6) and after passing through inter-leaver we obtain (4,3,0,6,1).

Turbo code Decoding:

Turbo code decoding is similar way of encoding. Two elementary decoders interconnected each other. This is a serial way connection (Nabeel Arshad, Abdul Basit).

DEC1 operates lower speed. DEC2 is for second RSC coder respectively. DEC1 yields a soft decision which causes L1 delay.

An interleaver installed between 2 decoders to scatter error bursts coming from DEC1 output. "DI" block is demultiplexing and insertion module. It works as a switch. Redirecting input bits to DEC1 at one moment and to DEC2 at another. In off state it feeds both y1k and y2k inputs with padding bits (zeros).

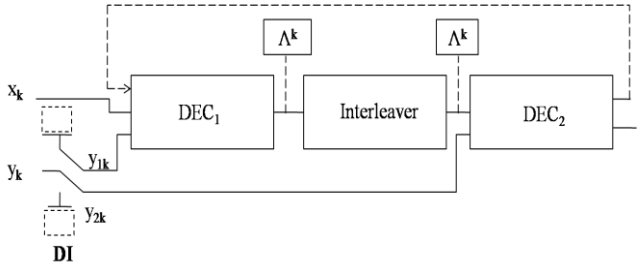

Fig. 5: Turbo code Decoding Process.

Consider a memory as AWGN Channel.

$Xk = (2dk - 1) + ak$ (3)

$Yk = 2(yk - 1) + bk$ (4)

ak, bk are independent noise components have same variance σ2. 'Yk' is a kth bit from yk encoder output.

Redundant information is demultiplexed and sent through DI to DEC1 (when yk = y1k) and DEC2 (when yk = y2k). DEC1 yields a soft decision i.e.,

$\Lambda dk = \log (p(dk = 1) / p(dk = 0))$ (5)

and delivers it to DEC2.

Λdk is Logarithm of Likelihood Ratio (LLR)

p (dk = i), i ϵ {0, 1} is the posteriori probability of dk data bits. Probability of received dk bits as 'i' and taking LLR

DEC1 yields a soft decision and DEC2 yields a hard decision. Both DEC1 and DEC2 are the stream of bits takes input as 1 or 0.

"Viterbi" algorithm is a dynamic programming algorithm for finding the most likely sequence of hidden states.

DEC1 is BCJR (Bahl, Cocke, Jelinek, Raviv) algorithm is used for posteriori probability and DEC2 is Viterbi algorithm is used for posteriori probability. These two are not optimal, because DEC1 uses only a proper fraction of available redundant information. In order to improve feedback loop is used.

Cryptography:

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense (https://en.wikipedia.org/wiki/).

In modern field cryptography had added different fields. First, the Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key can be used to authenticate the hash value upon receipt; this additional complication blocks an attack scheme against bare digest algorithms, and so has been thought worth the effort. Second, in public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption.

Third, Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size.

An abelian group G sometimes denoted by {G, •}, is a set of elements with a binary operation, denoted by •, that associates to each ordered pair (a, b) of elements in G an element (a • b) in G, such that the following axioms are obeyed (William Stallings,):

(1) Closure: If a and b belong to G, then a • b is also in G.

(2) Associative: a • (b • c) = (a • b) • c for all a, b, c in G.

(3) Identity element: There is an element e in G such that a • e = e • a = a for all a in G.

(4) Inverse element: For each a in G there is an element a' in G such that a • a' = a' • a = e.

(5) Commutative: a • b = b • a for all a, b in G.

An elliptic curve is defined by an equation in two variables with coefficients. For cryptography, the variables and coefficients are restricted to elements in a finite field, which results in the definition of a finite abelian group.

An elliptic curve over real numbers may be defined as the set of points (x, y) which satisfy an elliptic curve equation of the form:

$y2 = x3 + ax + b$ (6)

Where x, y, a, b are real numbers.

All the curves are given in the above form and defines over finite field Fp, where p>3 is prime and a, b ϵ Fp.

Elliptic curve can be defined over any base field. However, a common choice for hardware implementations is extensions of the galois field of characteristic two, GF (2m). The structure of galois field is such that addition and multiplication can be implemented by XOR and AND gates.

Diffie-Hellman key Exchange:

Diffie-Hellman key exchange has done in following manner. First pick the large integer value q, which is either prime p or an integer of the form 2m and elliptic curve parameter a and b for equation

$y2 \bmod p = (x3 + ax + b) \bmod p$ (7)

and

$y2 + xy = x3 + ax2 + b$ (8)

A key exchange between users 'A' and 'B' can be accomplished as follows (Fig. 6) (Joppe, W.,).

- A selects an integer na less than n. This is A's Private Key. A then generates a public key PA = nA * G, the public key is a point in Eq (a, b).
- B similarly selects a private key nB and computes a public key PB.
- A generates the secret key k = nB * PA.

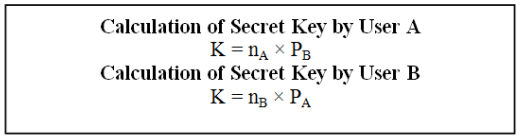

Fig. 6: ECC Diffie-Hellman Key Exchange.

ECC Encryption / Decryption:

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom (Mohammad Ghamgosar,).

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 - (n-1)].

Two cipher texts will be generated let it be C1 and C2.

C1 = k*P

C2 = M + k*Q

C1 and C2 will be sending.

Decryption

We have to get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that we have send.

How does we get back the message,

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1′

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P (canceling out k * d * P)

= M (Original Message)

Conclusion:

In this, we have been advised a new approach that provides security for MELP – compressed speech transmission in noisy channels in conjunction with a forward error control scheme. In this method by using ECC algorithm is encrypting, decrypting the data and over the unsecured channel .The decrypted output will got through the MELP decoding to shown us output as clean and neat voice with securely.

ACKNOWLEDGMENTS

Our sincere thanks to who guided us done this project and toward the development of this project. Our sincere thanks to supporter to development this project.

REFERENCES

Victor Demjanenko, David Satterlee, 2014. "RTP Payload Format for MELPe Codec draft-demjanenko-payload-melpe-01" in Vocal Technologies Ltd.

Weiran Lin, Soo Ngee Koh, Xiao Lin, "Mixed Excitation Linear Prediction Coding of Wideband speech at 8kbps".

Lynn, M., Supplee, Ronald, P. Cohn, John, S. Collura, "MELP: The New Federal Standard at 2400 bps".

https://en.wikipedia.org/wiki/Forward_error_correction.

Nabeel Arshad, Abdul Basit, "Implementation and Analysis of Turbo codes using MATLAB".

http://www.eas.uccs.edu/wickert/ece2610/lecture_notes/ece2610_chap7.pdf.

Bernard Sklar "Fundamentals of Turbo Codes."

https://en.wikipedia.org/wiki/Turbo_code

Nabeel Arshad, Abdul Basit "Implementation and Analysis of Turbo Codes Using MATLAB".

https://en.wikipedia.org/wiki/Cryptography.

William Stallings "Cryptography and Network Security Principles and Practice" Fifth Edition.

Joppe, W., Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig and Eric Wustrow "Elliptic Curve Cryptography in Practice".

Mohammad Ghamgosar, Farshad Akbari, Mehregan Mahdavi "Application of Elliptic Curves Cryptography in Wireless Communication Security".