(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 681 681**

(51) Int. CI.:

H04L 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.02.2007 PCT/EP2007/051917**

(87) Fecha y número de publicación internacional: **07.09.2007 WO07099130**

(96) Fecha de presentación y número de la solicitud europea: **28.02.2007 E 07726553 (6)**

(97) Fecha y número de publicación de la concesión europea: **02.05.2018 EP 1989807**

(54) Título: **Procedimiento y sistema que permite transmitir un mensaje expresado por medio de un polinomio**

(30) Prioridad:

28.02.2006 FR 0601775

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.09.2018

(73) Titular/es:

THALES (100.0%)
45 RUE DE VILLIERS
92200 NEUILLY SUR SEINE, FR

(72) Inventor/es:

PAINCHAULT, PHILIPPE;
AGAGLIATE, SANDRINE y
GARRIDO, ERIC

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y sistema que permite transmitir un mensaje expresado por medio de un polinomio

La invención se refiere, en particular, a un procedimiento y a un sistema de gestión de interrupciones durante la recepción de una señal en un sistema de transmisión.

Uno de los problemas planteados en los sistemas de transmisión de información es la manera de gestionar las pérdidas de información debidas a interrupciones en la comunicación, interrupciones que pueden ser erráticas.

Después de una emisión o una recepción "errática", un receptor puede no tener acceso a varios paquetes del mensaje transmitido y es posible que no pueda emitir una solicitud en dirección al emisor para solicitar los paquetes ausentes.

Al no ser las pérdidas de paquetes predecibles, el mensaje puede transmitirse varias veces para evitar la pérdida de información. Un procedimiento simple consiste, por ejemplo, en repetir el mensaje. El receptor que pierde varios paquetes debe escuchar, eventualmente varias veces, la totalidad del mensaje. Para mensajes largos y/o en el caso de bajo ancho de banda, esta manera de operar puede volverse problemática. En todos los casos, conduce a una pérdida de tiempo importante.

El documento de Stephen B. Wickler titulado "An introduction to Reed-Solomon codes"; En: Wicker, Bhargava: "Reed-Solomon Codes and their Applications", septiembre de 1999 (1999-09), Wiley -IEEE Press, ISBN: 9780780353916, páginas 1-16, XP7918388 describe el uso de un código de Reed Solomon para efectuar correcciones de errores.

La invención se refiere a un procedimiento para gestionar interrupciones erráticas en un sistema de transmisión en el que los mensajes M que han de transmitirse están compuestos por paquetes de datos y están representados por un polinomio de grado t-1, conteniendo un mensaje una señalización CO, compartiendo los emisores y los receptores una información que permite referenciar cada paquete de datos, tal como una página o una referencia temporal, siendo el procedimiento tal que comprende al menos las siguientes etapas:

- durante la transmisión de un mensaje C representado por un polinomio P, generar t' puntos Ai a partir de dicha información, haciendo posible referenciar los paquetes de datos y las evaluaciones P (Ai) del polinomio P para los puntos Ai con t' superior o igual a t,
- transmitir un mensaje que contiene una señalización CO, estando la señalización compuesta por T0*N0 bits y considerándose como un polinomio de grado (T0-1),
- en la recepción, recopilar TO paquetes de datos que no contienen errores y, usando cada paquete de datos un punto diferente del resto de paquetes de datos, reconstituir la señalización CO a partir de estos paquetes de datos usando una interpolación polinómica,
- deducir, a partir de la señalización CO, la longitud del mensaje C y la manera en la que se ha cortado el mensaje C en F tramas, cortándose cada trama en q palabras, estando cada una de las palabras representada por un polinomio de grado (T-1),
- para cada polinomio correspondiente a una palabra, recopilar T evaluaciones P(Ai) sin errores, y
- a partir de las P(Ai) y los puntos Ai, reconstituir el mensaje C usando la interpolación polinómica.

Se puede usar una función de interpolación para determinar el polinomio.

El mensaje, por ejemplo, se divide en varias partes y se aplican las etapas del procedimiento descrito anteriormente en cada parte.

Durante la detección de errores, las evaluaciones P(Ai) contenidas en un paquete de datos erróneo, por ejemplo, se eliminan y el receptor permanece a la escucha de nuevos paquetes de datos. Estos paquetes de datos son, por ejemplo, páginas.

Las etapas del procedimiento se aplican en un sistema de transmisión comprende un satélite de comunicación.

La invención se refiere también a un sistema para gestionar interrupciones erráticas en un sistema de transmisión que comprende uno o varios emisores Ej y uno o varios receptores Rk, en el que los mensajes que han de transmitirse están compuestos por paquetes de datos y se expresan por medio de un polinomio de grado t-1, compartiendo los emisores y los receptores una información que permite referenciar paquetes de datos, caracterizado porque comprende al menos los siguientes elementos: un centro de formateo y estando los receptores provistos de medios adaptados para ejecutar las etapas del procedimiento enunciado.

El procedimiento según la invención presenta, en particular, las siguientes ventajas:

- Ofrece una resistencia a las posibles interrupciones durante la transmisión de información,
- Permite aumentar el ancho de banda aparente teniendo en cuenta la diversidad de los emisores.

Otras características y ventajas de la presente invención se pondrán mejor de manifiesto tras la lectura de la

descripción que sigue de un ejemplo de realización dado a título ilustrativo y en ningún caso limitativo y con las figuras adjuntas, que representan:

- la figura 1 un ejemplo de arquitectura de un sistema para el cual se aplica la invención, y
- la figura 2 la multiplexación de la información relacionada con el mensaje y la señalización cuando existe.

Con el fin de hacer entender mejor el principio implementado en la invención, la descripción se da a título ilustrativo para un sistema que comprende uno o varios emisores Ej, un centro 1 de gestión o de formateo de los mensajes y uno o varios receptores Rk. El centro 1 de formateo está equipado con un procesador 2 adaptado para ejecutar las etapas del procedimiento según la invención detalladas a continuación y para generar señales. Los receptores también están provistos de medios tales como microprocesadores (no representaros por razones de simplificación) adaptados para ejecutar los cálculos implementados en el procedimiento.

El centro 1 de gestión formatea los mensajes en paquetes de datos llamados "páginas". Transmite los paquetes de datos o páginas a uno o varios emisores, los emisores que transmiten estos a los receptores.

En el ámbito del ejemplo, se supone que los emisores y los receptores comparten una información llamada "[page ref]", permitiendo referenciar de este modo cada página. Esta información puede ser, por ejemplo, una referencia temporal conocida por cada uno (emisores y receptores) o un campo específico incluido en la página, como un número de página. De manera general, cualquier información que permite referenciar un paquete de datos podrá usarse.

De manera simplificada, el procedimiento según la invención se basa en el siguiente principio: un mensaje M que debe transmitirse a uno o varios receptores también se descompone por el centro de formateo en t símbolos $s_0,s_1,...,s_{t-1}$.

Cada símbolo s_i está representado por un elemento en un cuerpo finito GF, es decir, en un conjunto GF que tiene un número finito de elementos y provisto de 2 operaciones + (suma) y * (multiplicación). Por motivos de simplificación, se supone que este cuerpo finito es $GF(2^n)$, es decir, el cuerpo que tiene 2^n elementos (sin salir del ámbito de la invención cualquier cuerpo finito puede ser adecuado). De este modo, los símbolos están compuestos por n bits y el tamaño del mensaje M es de n*t bits.

El mensaje M está representado por el polinomio:

$$P(X)=s_0 + s_1 X + s_2 X^2 + ...+s_{t-1}X^{t-1}$$

con coeficientes en $GF(2^n)$.

La idea de la presente invención usa, en particular, evaluaciones del polinomio P en t puntos distintos A_0, A_1, A_{t-1}, es decir, $P(A_0)$, $P(A_1)$, ...,$P(A_{t-1})$, para determinar los t coeficientes $s_0,s_1,...,s_{t-1}$.. del polinomio que representa el mensaje. Estas evaluaciones $P(A_i)$ son símbolos de n bits en $GF(2^n)$. El centro de formateo llenará las páginas (o paquetes de mensaje) con evaluaciones del polinomio P en varios puntos Ai diferentes. El número de evaluaciones de polinomio $P(A_i)$ en particular, se selecciona en función del grado del polinomio.

Esta forma de proceder no afecta al número total de bits (n*t) que le receptor memoriza para reconstituir el conjunto del mensaje M.

El centro 1 de formateo genera varios puntos Ai a partir del parámetro [page ref] de una página. Durante toda la sesión de la transmisión del mensaje, (toda la sesión que corresponde a la transmisión del mensaje de un emisor hacia un receptor) el centro de formateo genera puntos que son diferentes para cada página (o que tienen una gran probabilidad de ser diferentes). En particular, el centro genera más de (n*t) puntos Ai y evaluaciones del polinomio P(Ai) para los puntos Ai correspondientes. El número de puntos generados depende de la longitud de la sesión. El (los) emisor(es) envía(n) las evaluaciones P(Ai) al (a los) receptor(es).

De este modo, un receptor Ri tiene únicamente que memorizar t diferentes evaluaciones P(Ai) para ser capaz de reconstituir la totalidad del mensaje M, esto, independientemente de cuáles sean los momentos en que los recibe (haya o no interrupciones en la recepción de las páginas). El número mínimo t que un receptor debe memorizar depende del grado del polinomio usado para el mensaje. El indicador [page ref] permite al receptor calcular los puntos Ai correspondientes a las evaluaciones P(Ai) que recibe.

Si el receptor es capaz de escuchar en paralelo varios emisores y cada uno de ellos envía evaluaciones diferentes, entonces, el tiempo de recepción necesario para recuperar t evaluaciones corresponde a los tiempos de repetición si hubiera un solo receptor, dividido por el número de receptores.

Etapas de reconstitución del mensaje

Para reconstituir el mensaje, un receptor debe haber adquirido al menos t evaluaciones de un polinomio P válido correspondiente a t puntos distintos A_0, $A_1,...,A_{t-1}$ con, $z_0= P(A_0)$, $z_1= P(A_1),...$, $z_{t-1}= P(A_{t-1})$, que son elementos del cuerpo finito GF.

La validez de los puntos está controlada, por ejemplo, usando procedimientos conocidos por el experto en la materia cuyos ejemplos se dan a continuación.

Conociendo los puntos y las evaluaciones correspondientes, se usa, por ejemplo, la interpolación del polinomio de Lagrange $L_i(X)$ para el polinomio P de la siguiente manera:

$$P(X)=z_0 * L_0(X) + z_1 * L_1(X) + ...+ z_{t-1} * L_{t-1}(X)$$

donde, para 0 <= j <= t-1, $L_j(X)$ es el único polinomio de grado (t-1) tal que $L_j(A_k)=1$ para j=k et $L_j(A_k)=0$ para j<>k. Concretamente, el polinomio $L_j(X)$ se calcula de la siguiente manera:

$$Lj(X)=B(j)*(\text{el producto de t-1 monomios } (X-A_k), \text{ tal que } 0<= k <= t-1 \text{ y } k<>j)$$

B(j) es el elemento de $GF(2^n)$ que es la inversa en $GF(2^n)$ del producto de los elementos t-1 (A_j - A_k) para 0<= k <= t-1 y k<>j.

Conociendo el polinomio, un receptor conoce entonces el mensaje.

Las etapas de tratamiento descritas anteriormente se aplican para mensajes suficientemente cortos.

Para los mensajes largos, es posible cortar este mensaje en partes que tiene una longitud "adecuada" y aplicar el principio de base n cada una de las partes. La descripción detallada de un ejemplo de realización a continuación indica, entre otros, una manera para seleccionar los diferentes parámetros para tener una longitud adecuada de las partes del mensaje.

Por otra parte, el receptor debe ser capaz de detectar los posibles errores debidos a una mala transmisión o recepción de las páginas. Un mecanismo de corrección de errores no es obligatorio, una simple detección de errores es suficiente. Las páginas erróneas simplemente se borrarán por el receptor y este deberá permanecer a la escucha del (de los) emisor(es) para recuperar otras páginas (cualesquiera).

La siguiente descripción proporciona un ejemplo aplicado a un mensaje C transmitido a un receptor durante una sesión, sin que el receptor tenga información predefinida en el mensaje C (longitud, naturaleza, etc.)

Por lo tanto, es necesario transmitir también una señalización CO que contenga la información útil sobre C.

El formato de la página es, por ejemplo, el siguiente:

[Page ref] [campo de Señalización] [campo de mensaje útil] [MAC/CRC].

Donde

- [Page ref] indica el número de página que identifica la página. Este parámetro también puede usarse para cifrar la página en modo "contador",
- [Campo de Señalización] proporciona una información acerca de la señalización CO,
- [campo de mensaje útil] proporciona una información acerca del mensaje C,
- [MAC/CRC] contiene un MAC ("Message Authentication Code") o un CRC ("Cyclic Redundancy Check") que permite detectar los errores al nivel de la página. También puede usarse para la autentificación.

Una forma simple de implementar el principio de diversidad comprende, por ejemplo, las siguientes etapas:

- el dato útil de una página está compuesto por N_p=N0+q*N bits, es decir, compuesto por N0 bits para el campo [Campo de Señalización] y q paquetes de N bits para el campo [campo de mensaje útil]. Los parámetros (N0, N, a) se tratan después en la descripción,
- la señalización CO está compuesta, por ejemplo, de T0*N0 bits y se ve como un polinomio de grado (TO-1) en $GF(2^{N0})$. El campo [campo de señalización] de una página contiene una evaluación del polinomio en un punto, estando este punto calculado a partir de [page ref],
- el mensaje C está compuesto por F tramas, cada trama está compuesta por q palabras, cada palabra está compuesta por T*N bits y se ve como un polinomio de grado (T-1) en $GF(2^N)$. El campo [campo de señalización] de una página contiene q paquetes que dan una información acerca de una trama de C seleccionada gracias al parámetro [Page ref]. Cada uno de estos paquetes es una evaluación de un polinomio y un punto calculado a partir del parámetro [Page ref],
- para una sesión dada y un mensaje dado C, el centro calcula las páginas que dan la información acerca de C como se describió anteriormente. Un modo de transmisión, por ejemplo, se obtiene cuando el centro transmite páginas a varios emisores y cada emisor trasmite al receptor de las páginas que son diferentes de las

transmitidas por los otros emisores.

Una manera simple de obtener esta diversidad de señales es forzar el centro a distribuir diferentes páginas a diferentes emisores.

El tratamiento de la página al nivel de un receptor comprende, por ejemplo, las siguientes etapas:

- el tamaño N0*T0 de la señalización está predefinido y es conocido por el receptor. El receptor recopila TO páginas, de modo que cada página no contenga ningún error (control con [MAC/CRC]) y cada página usa un punto diferente de las otras páginas (punto calculable a partir de [page ref]). El receptor reconstituye la señalización CO a partir de estas páginas usando la interpolación polinómica de Lagrange, como se explica a continuación,
- gracias a CO, el receptor conoce la longitud del mensaje C. Recopila T páginas de cada trama C (páginas sin errores y usando puntos distintos). Después, reconstituye el mensaje C usando la interpolación polinómica de Lagrange.

El resto de la descripción detalla la elección de los parámetros, la señalización CO, la multiplexación detallada de C y CO en las páginas usando el principio de diversidad y un procedimiento para que el receptor reconstituya la totalidad del mensaje a partir de las páginas.

Elección de parámetros

Se señala:

- **N_p** como el número de bits por página que están reservados exclusivamente para los datos reales, es decir, para los campos [Campo de Señalización] y [campo de mensaje útil],
- **N** como un número inferior o igual al número de bits de [Page ref],
- **N0** y **q** son números tales como **N_p=q*N +N0**.

Para tener un parámetro de eficacia cercano a 1, los parámetros N y N0 se elegirán, por ejemplo, para verificar:

$$2^{\frac{N}{2}} \geq \frac{|Palabra|}{N} = T \text{ y } 2^{\frac{N0}{2}} \geq \frac{|C0|}{N_0} = T0$$

donde |C0| es el tamaño de CO y |Palabra| es el tamaño de una palabra contenida en C.

Estas dos condiciones no son obligatorias, pero aseguran que no haya colisión entre los puntos seleccionados de [Page ref], con una alta probabilidad. La condición más importante es la primera. La segunda puede relajarse fácilmente (TO puede ser un poco mayor que $2^{N0/2}$) ya que la señalización CO es en su mayoría más corta que el mensaje C.

En todos los casos, es imperativo que $2^N \geq T$ y $2^{N0} \geq T0$ para garantizar que el número de símbolos del mensaje es inferior al número total de puntos. Para un número dado N_p, estas condiciones ajustan los parámetros N y N0, así como el resto de parámetros, es decir, TO si |C0| es fijo, |Palabra| y T.

Formato del mensaje C y señalización C0

El mensaje C está dividido en una o varias tramas de q*T*N bits. Para garantizar este tamaño de formato, el mensaje C, por ejemplo, se formatea con un campo de "relleno" de tamaño variable que sirve de atasco. Un encabezado que da el tamaño del "relleno" puede estar incluido en el mensaje C o en la señalización CO.

Señalización C0

La longitud |C0| de CO es un múltiplo de N0. Se señala **T0** como el número de partes de N0 de bits en CO, es decir, tal que **|C0|=T0*N0.**

Este mensaje puede contener, por ejemplo, la información siguiente:

Campos C0	Descripción
[Tipo de mensaje]	Codifica varios tipos predefinidos de mensaje
[Longitud de C]	Codifica la longitud del mensaje C (ver a continuación)
[Información temporal sobre C]	Indica la fecha de inicio y finalización (o la hora) de la sesión durante la cual se emite el mensaje C

(continuación)

Campos C0	Descripción
[Relleno]	Atasco (si hay alguno) que permite tener un tamaño |**C0**| que es un múltiplo de N0
[MAC]	MAC que permite que el receptor verifique que el CO se haya recibido correctamente

Campo [Longitud de C]

Un mensaje C está dividido en F tramas de q*T*N bits. Los parámetros N y q son fijos y conocidos por el receptor. La longitud del mensaje C viene dada por los dos campos siguientes:

- [tamaño de una palabra en C (N/2 bits)]: valor de T-1, donde T es el número de símbolos de N bits en una palabra, $1 \leq T \leq 2^{N/2}$.
- [número de tramas en C]: valor de F.

Definición de multiplexación

Los bits de información de CO y C se multiplexan en los N_p bits de las páginas en curso.

El paquete útil de N_p bits se descompone en (1+q) partes señaladas como:

M(0), M(1), M(2), …, M(q).

En el resto del documento, se llama "N-símbolo" a un símbolo de N bits, pudiendo este verse como un elemento del cuerpo finito $GF(2^N)$. Se define también un "NO-símbolo" como un símbolo de N0 bits, pudiendo verse como un elemento del cuerpo finito $GF(2^{N0})$.

La primera parte M(0) es un NO-símbolo calculado a partir de CO.

Las q otras partes se calculan a partir de una trama seleccionada de un mensaje C y siendo cada parte un N-símbolo.

El número de bits útiles por página, por lo tanto, es N_p=N0+q*N.

El mensaje CO se descompone en TO partes de N0 bits señaladas como: W(0), W(1), …, W(T0-1).

El mensaje C se descompone en F tramas, cada trama en q palabras, cada palabra en T N-símbolos.

Señalando:

f siendo el índice de la trama en el mensaje, 0 <= f <= F-1,

w el índice de las palabras en una trama, 0 <= w <= q-1,

b el índice de los N-símbolos en una palabra, 0 <= b <= T-1

Entonces, a un N-símbolo actual en el mensaje C se hace referencia por C[f][w][b].

La figura 2 resume la multiplexación definida en el resto de la descripción.

La extracción de la información de C0 en la página actual

Sea CO la señalización actual que incluye TO NO-símbolos señalada como:

W(0), W(1), …, W(T0-1)

Sea A' = HO([Page ref]) un NO-símbolo calculado a partir de [Page ref] con una función HO. La función HO es, por ejemplo, tal que HO([Page ref]) se distribuye aproximadamente de manera equidistante en el conjunto de los NO-símbolos cuando [page ref] cambia de manera aleatoria. El NO-símbolo M(0) en la señalización incrustado en la página actual es:

$$M(0) = W(0) + W(1) * A' + W(2) * A'^{2} + ...+ W(T0-1) * A'^{T0-1}$$

Donde todos los NO-símbolos son considerados como elementos $GF(2^{N0})$ y operaciones (+, *) se definen en este cuerpo finito.

Nota: Señalando P(X) como el polinomio definido por $P(X) = W(0) + W(1) X + W(2) * X^2 + ... + W(TO-1) X^{T0}$ se

define, en realidad, M(0) como siendo la evaluación P(A') del polinomio P en el punto A'.

Reconstitución de la señalización C0 al nivel del receptor:

Al nivel del receptor, la señalización actual CO se recupera usando los NO-símbolos de información M(0) proporcionados en cada página.

Tan pronto como las TO páginas están disponibles y los valores HO[(Page ref]) son distintas, CO se recupera de la siguiente manera:

A) Entrada para la recuperación C0

- j, 0 <= j <= TO-1 un índice para las TO páginas seleccionadas usadas para la recuperación de la señalización actual CO;
- A'_0, A'_1, ...,A'_{T0-1}, los valores distintos de HO([Page ref]) asociados a cada página seleccionada (j); 0 <= j <= T0-1;
- Z(0), Z(1), …, Z(T0-1) los TO NO-símbolos M(0) en una página seleccionada actual j, 0 <= j <= TO-1.

B) salida C0

A partir de los datos anteriores, se recuperan los TO NO-símbolos de CO señalados como:

- W(0), …, W(T0-1)

C) cálculo de la salida a partir de la entrada

El vector de TO NO-símbolos (W(0), W(1), ...W(TO-1)) a recuperar también es considerado como un polinomio $GF(2^N0)[X]$ de grado TO-1:

$$P(X) = W(0) + W(1)\,X + ... + W(T0\text{-}1)\,X^{T0-1}$$

P(X) se recupera por medio de una interpolación como siendo el único polinomio de grado TO-1 tal que $P(A'_j) = Z(_j)$, para 0<=j <= TO-1.

1) con la familia de TO puntos (A'_0 A'_{T0-1}) se calcula la familia de puntos TO asociados al polinomio de Lagrange. Para 0 <= j <= TO-1, Lj(X) es el único polinomio de grado TO-1 tal que $Lj(A'_k) = 1$ para k = j y $Lj(A'_k) = 0$ para k <> j.

$$Lj(X) = B(j) * (\text{el producto de T0-1 monomios } (X - A'_k), \text{ tal que } 0 <= k <= T0\text{-}1 \text{ y } k <> j.)$$

B(j) es el elemento de $GF(2^{N0})$ que es la inversa de $GF(2^{N0})$ del producto de TO-1 elementos (A'_j - A'_k), 0 <= k<=TO-1 y k<> j.
2) el vector de TO N0-símbolos (W(0), …,W(T0-1)), considerados como el polinomio P(X), se calcula entonces de la siguiente manera:

$$P(X) = Z(0) * L_0(X) + Z(1) * L_1(X) + ... + Z(T0\text{-}1) * L_{T0-1}(X).$$

Extracción de la información de C en la página actual:

Sea F el número de trama en C, q el número de palabras en una trama y T el número de N símbolos en una palabra.

Los parámetros F y T se calculan a partir del campo "longitud del mensaje" incluido en la señalización CO. El parámetro q es fijo (independiente del mensaje) y conocido por el receptor.

Los q N-símbolos M(1)...M(q) de la página actual son respectivamente información acerca que las q palabras incrustadas en una trama específica de C. El índice de la trama seleccionada y la naturaleza del N-símbolo de la información acerca de sus palabras están definidos sin ambigüedad con el parámetro [page ref].

Cualquier N-símbolo (N bits) es considerado también como un elemento del cuerpo finito que tiene 2^N elementos $GF(2^N)$.

Un N-símbolo de información acerca de una palabra que contiene T N-símbolos será una combinación lineal de sus T N-símbolos considerados en $GF(2^N)$.

Más precisamente:

El índice de la trama seleccionada en M es: f=H5[page ref].

La función de H5 es, por ejemplo, tal que f=H5([page ref]) se distribuye de manera equitativa aproximadamente en [0,... F-1] cuando [page ref] cambia de manera aleatoria. Planteemos A=H2([Page ref]) como un N-símbolo calculado a partir de [Page Ref] con una función H2. La función H2 es, por ejemplo, tal que H2([Page ref]) se distribuye aproximadamente de manera equidistante en el conjunto de los N-símbolos cuando [page ref] cambia de manera aleatoria.

Siendo:

- W(0,0), W(0,1),…, W(0,T-1), los T N-símbolos de la palabra TRAMA[f][0] en la trama correspondiente f;
- W(1,0), W(1,1),…, W(1,T-1), los T N-símbolos de la palabra TRAMA[f][1] en la trama correspondiente f;
- …
- W(q-1,0),…, W(q-1,T-1), los T N-símbolos de la palabra TRAMA[f][q-1] en la trama correspondiente f

Para 1 <= j<= q, los N-símbolos M(j) son:

$$M(j)=W(j-1,0) + W(j-1,1) * A + W(j-1,2) * A^2 + ...+ W(j-1, T-1) * A^{T-1}$$

Donde todos los N-símbolos son considerados como elemento de $GF(2^N)$ y operación (+, *) se efectúan en ese cuerpo finito.

Como se describe a continuación, tan pronto como un receptor recupera T páginas relacionadas con la trama y cuyos contenidos (M(0),…,M(q-1)) son distintos, será capaz de recuperar fácilmente la trama completa independientemente de la manera en la que las páginas han sido recibidas por el receptor:

- escuchando una sola señal,
- escuchando varias señales en paralelo,
- con varios huecos en la señal escuchada o no.

Reconstitución de una trama al nivel del receptor:

Al nivel del receptor, una trama actual de q*T N-símbolos, señalada como TRAMA[f], 0 <= f <= F-1, se recupera usando las páginas tales como H5([Page ref])=f.
Tan pronto como las T páginas están disponibles y los valores de H2([Page ref]) son diferentes, la trama se recupera usando una función de interpolación como se describió anteriormente:

A) Entradas para la recuperación de la trama actual:

- j, 0 <= j <= T-1 es un índice para las T páginas seleccionadas usadas para recuperar la trama actual;
- A_0, A_1, ...,A_{T-1} son los valores distintos de H2([Page ref]) asociados a cada página seleccionada (j); 0 <= j <= T-1;
- Z(j,0), Z(j,1), …,Z(j,q-1) son los q N-símbolos M(1), ... M(q) de la página actual seleccionada j, 0 <= j <= T-1.

B) Salida: la trama actual

De los atos anteriores, recuperamos los q*T N-símbolos siguientes en la trama actual TRAMA[f]:

- (W(0,0), …, W(0,T-1)), los T N-símbolos de la palabra TRAMA[f][0] en la trama relacionada f,
- (W(k,0), …, W(k,T-1)), los T N-símbolos de la palabra TRAMA[f][k] en la trama relacionada f,
- …
- (W(q-1,0), …, W(q-1T-1)) son los T N-símbolos de la palabra TRAMA[f][q-1] en la trama correspondiente f.

C) cálculo de la salida a partir de la entrada

Cada palabra de T N-símbolos (W(k,0), W(k,1), ...W(k,T-1)) a recuperar también se considera como un polinomio de $GF(2^N)[X]$ de grado T-1:

$$P_k(X) = W(k,0) + W(k,1)\, X + ... + W(k,T-1)\, X^{T-1}$$

$P_k(X)$ se recupera por la interpolación como siendo el único polinomio de grado T-1 tal que $P_k(Aj) = Z(j,i)$, para 0<=j <= T-1.

1) con la familia de T puntos (A_0, ..., A_{T-1}) se determina la familia de los T polinomios de Lagrange asociados. Para 0 <= j <= T-1, Lj(X) es el único polinomio de grado T-1 tal que Lj(Ak) = 1 para k = j y Lj(Ak) = 0 para k <> j.

$$Lj(X) = B(j) * (\text{el producto de T-1 monomios}(X - Ak), \text{ tal que } 0 <= k <= T-1 \text{ y } k <> j.)$$

B(j) es el elemento de $GF(2^N)$ que es la inversa en $GF(2^N)$ del producto de T-1 elementos (Aj-Ak), 0 <= k<=T-1 y k<> j.

2) La palabra actual de T N-símbolos (W(k,0), …,W(k,T-1)), considerado como el polinomio $P_k(X)$ 0 <= k <= q-1, se calcula entonces de la siguiente manera:

$$P_{k(}X) = Z(0,k) * L_0(X) + Z(1,k) * L_1(X) + ... + Z(T-1,k) * L_{T-1}(X).$$

$P_k(X)$ se recupera por la interpolación como siendo el único polinomio de grado T-1 tal que $P_k(Aj) = Z(j,i)$, para 0<=j <= T-1.

1) con la familia de T puntos (A_0, ...,A_{T-1}) se determina la familia de los T polinomios de Lagrange asociados. Para 0 <= j <= T-1, Lj(X) es el único polinomio de grado T-1 tal que Lj(Ak) = 1 para k = j y Lj(Ak) = 0 para k <> j.

$$Lj(X) = B(j) * (\text{el producto de T-1 monomios}(X - Ak), \text{ tal que } 0 <= k <= T-1 \text{ y } k <> j.)$$

B(j) es el elemento de $GF(2^N)$ que es la inversa en $GF(2^N)$ del producto de T-1 elementos (Aj - Ak), 0 <= k<=T-1 y k<> j.

2) La palabra actual de T N-símbolos (W(k,0), ...,W(k,T-1)), considerado como el polinomio $P_k(X)$ 0 <= k <= q-1, se calcula entonces de la siguiente manera:

$$P_k(X) = Z(0,k) * L_0(X) + Z(1,k) * L_1(X) + ... + Z(T-1,k) * L_{T-1}(X).$$

REIVINDICACIONES

1. Procedimiento para gestionar interrupciones erráticas en un sistema de transmisión en el que los mensajes que han de transmitirse están compuestos por paquetes de datos y están representados por un polinomio de grado t-1, compartiendo los emisores y los receptores una información que permite referenciar cada paquete de datos, tal como una página o una referencia temporal, siendo el procedimiento tal que comprende al menos las siguientes etapas:

- durante la transmisión de un mensaje C representado por un polinomio P, generar t' puntos Ai a partir de dicha información que permite referenciar los paquetes de datos y las evaluaciones P(Ai) del polinomio P para los t' puntos Ai, con t' superior o igual a t,
- transmitir un mensaje que contiene una señalización CO, estando la señalización compuesta por T0*N0 bits y considerándose como un polinomio de grado (T0-1),
- en la recepción, recopilar TO paquetes de datos que no contienen errores, usando cada paquete de datos un punto diferente del resto de paquetes de datos, reconstituir la señalización CO a partir de estos paquetes de datos usando una interpolación polinómica,
- deducir, a partir de la señalización CO, la longitud del mensaje C y la manera en la que se ha cortado el mensaje C en F tramas, cortándose cada trama en q palabras, estando cada una de las palabras representada por un polinomio de grado (T-1),
- para cada polinomio correspondiente a una palabra, recopilar T evaluaciones sin errores del polinomio, y
- a partir de las evaluaciones P(Ai) y los puntos Ai, reconstituir el mensaje C usando la interpolación polinómica.

2. Procedimiento según la reivindicación 1, **caracterizado porque** se usa una función de interpolación para determinar el polinomio.

3. Procedimiento según la reivindicación 1, **caracterizado porque** se divide el mensaje en varias partes y se aplican las etapas de la reivindicación 1 en cada parte.

4. Procedimiento según la reivindicación 1, **caracterizado porque**, durante la detección de errores, las evaluaciones P(Ai) contenidas en un paquete de datos erróneo se eliminan y el receptor permanece a la escucha de nuevos paquetes de datos.

5. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado porque**, durante la detección de errores, las evaluaciones P(Ai) contenidas en una página errónea se eliminan y el receptor permanece a la escucha de nuevas páginas.

6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado porque** el sistema de transmisión comprende un satélite de comunicación.

7. Sistema para gestionar interrupciones erráticas en un sistema de transmisión que comprende uno o varios emisores Ej y uno o varios receptores Rk, en el que los mensajes que han de transmitirse están compuestos por paquetes de datos y se expresan por medio de un polinomio de grado t-1, compartiendo los emisores y los receptores una información que permite referenciar paquetes de datos, **caracterizado porque** comprende al menos los siguientes elementos: un centro (1) de formateo, y estando los receptores provistos de medios (2) adaptados para ejecutar las etapas del procedimiento según una de las reivindicaciones 1 a 6.

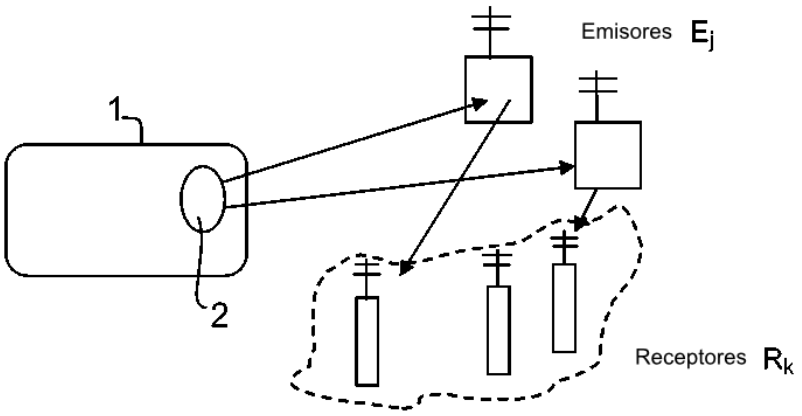
Emisores E_j
1
2
Receptores R_k

FIG.1

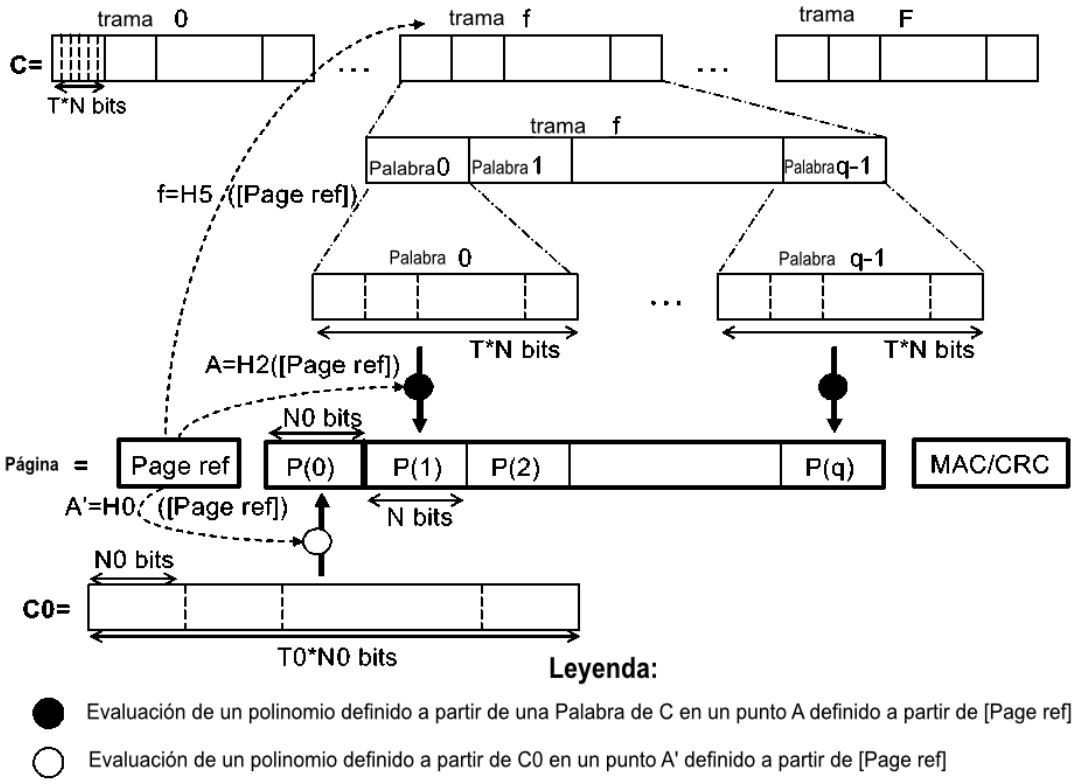
trama 0
trama f
trama F
C=
T*N bits
trama f
Palabra0
Palabra 1
Palabra q-1
f=H5 ([Page ref])
Palabra 0
Palabra q-1
T*N bits
T*N bits
A=H2([Page ref])
N0 bits
Página =
Page ref
P(0)
P(1)
P(2)
P(q)
MAC/CRC
A'=H0 ([Page ref])
N bits
N0 bits
C0=
T0*N0 bits
Leyenda:
Evaluación de un polinomio definido a partir de una Palabra de C en un punto A definido a partir de [Page ref]
Evaluación de un polinomio definido a partir de C0 en un punto A' definido a partir de [Page ref]

FIG.2