MASKAY 7(1), Nov 2017
ISSN 1390-6712

Recibido (Received): 2017/06/19
Aceptado (Accepted): 2017/07/27

Evaluación Estadística de Generadores de Secuencias Pseudoaleatorias para Aplicaciones de Dispersión de Energía

Statistical Evaluation of Pseudorandom Sequence Generators for Energy Dispersion Applications

Karla Rivas, Pablo Lupera Morillo, Christian Tipantuña

***Abstract*—A set of statistical tests is proposed, and with them it is evaluated three pseudorandom number generators PRNGs and two pseudorandom bit sequence generators PRBSs, which could be applied in the process of energy dispersion. With the generators analyzed is reached to the conclusion that none exceeds all statistical tests proposed.**

***Index Terms*— Energy dispersion, frequency selective fading, PRNG, PRBS, statistical tests.**

***Resumen*—Se propone un conjunto de pruebas estadísticas para evaluar tres generadores de números pseudoaleatorios y dos generadores de secuencias binarias pseudoaleatorias, que se podrían aplicar en el processo de dispersión de energía. Se concluye que ninguno de los generadores cumple todas las pruebas estadísticas propuestas.**

***Palabras Claves*— Dispersión de energía, desvanecimiento selectivo en frecuencia, PRNG, PRBS, pruebas estadísticas.**

I. Introducción

LOS generadores de secuencias pseudoaleatorias (PRNG, siglas en inglés) se usan en los sistemas de comunicaciones con diversos objetivos, entre ellos: simulación de canales de ruido, encriptación, ecualización, compresión, aleatorización de bits, etc. Por eso, constantemente se investigan métodos de generación de secuencias con características más aleatorias y eficientes para su implementación. Para la evaluación de aleatoriedad de generadores de secuencias se utilizan pruebas estadísticas.

En el caso de que la investigación presentada requiera de una revisión exhaustiva del estado del arte.

Respecto al estudio del canal inalámbrico Sklar en su trabajo de investigación afirma que el comportamiento del canal produce desvanecimientos selectivos en frecuencia que pueden ser contrarrestados con alguna técnica de dispersión de energía [1].

En algunos sistemas de comunicaciones inalámbricos la dispersión de energía se ejecuta multiplicando la señal digital de información con una secuencia pseudoaleatoria de bits, proceso que permite obtener una señal aleatoria. De esta manera en los sistemas de radio digital DRM y TV ISDBT-b se utilizan PRNGs de grado 9 y 15 respectivamente [2], [3].

En [4] se realiza la implementación de una forma caótica de aleatorizar una señal analógica de video en tiempo real. La señal de video se transmite por un canal inalámbrico y se reporta que se recupera la señal en el receptor con una claridad razonable.

En su trabajo Marinova y Tchobanova realizaron la evaluación estadística de secuencias con pruebas de monobit, runtest y espectral de circuitos generadores de números pseudoaleatorios utilizando secuencias de 1000 bits en base a la norma 800-22 de la NITS (National Institute of Standards and Technology). En este trabajo se evaluaron generadores de secuencias binarias pseudoaleatorias (PRBS, siglas en inglés) de grado 9, 16 y 21, y se implementaron sobre FPGA [5].

En el estudio realizado por Goretti, Campo y Echanobe se utiliza para la evaluación estadística la norma FIPS-140 y 141 del NITS considerando varios generadores, entre ellos los generadores congruenciales lineales (LCG) de Fibonacci, Green y Mitchell Moore [6].

En otro estudio realizado por Katti, Kavasseri y Sai se propone un generador lineal congruencial comparativo (CLCG) que se evalúa con la normativa 800-22. El CLCG está conformado por dos LCG que determinan su salida. Según el estudio este tipo de generador supera todas las pruebas de la norma 800-22, pero requiere dos LCG como fuente de aleatoriedad [7].

Considerando que la generación de secuencias pseudoaleatorias se aplica en los sistemas de transmisión inalámbrica para ejecutar la dispersión de energía, surge la necesidad de estabelecer una forma estadística para evaluar dichos generadores de secuencias pseudoaleatorias con la finalidad de estabelecer cuál de los generadores presenta mejores características para la aplicación de técnicas de dispersión de energía.

Karla Rivas, Estudiante Escuela Politécnica Nacional, Departamento de Electrónica, Telecomunicaciones y Redes de Información, (e-mail: krivasp1504@hotmail.com).

Pablo Lupera Morillo, Escuela Politécnica Nacional, Departamento de Electrónica, Telecomunicaciones y Redes de Información, (e-mail: pablo.lupera@epn.edu.ec).

Christian Tipantuña, Escuela Politécnica Nacional, Departamento de Electrónica, Telecomunicaciones y Redes de Información, (e-mail: christian.tipantuna@epn.edu.ec).

DOI: 10.24133/maskay.v7i1.334

El presente artículo se halla estructurado de la siguiente manera. En la sección II se describe el comportamiento del canal inalámbrico y la aplicación de la dispersión de energía como técnica para mitigar el efecto del desvanecimiento selectivo en frecuencia. En la sección III se proponen las pruebas estadísticas para evaluar los generadores de secuencias pseudoaleatorias. En la sección IV se muestran los resultados de la evaluación de los tres generadores LCG (Fibonacci, Green y Mitchell-Moore) y dos PRBS (grado 9 y 15) con LFSR (registro de desplazamiento con realimentación lineal). Para la evaluación estadística se aplican seis pruebas seleccionadas de la norma 800-22 En la sección V se describen las conclusiones del trabajo desarrollado y se proponen los trabajos futuros a realizar.

II. Comportamiento del Canal Inalámbrico y la Aplicación de la Dispersión de Energía

El comportamiento del canal inalámbrico es totalmente impredecible por los fenómenos de reflexión, refracción, difracción y dispersión de las señales que pueden producirse en la propagación de las ondas electromagnéticas. Estos fenómenos producen réplicas de las señales que se manifiestan con cambios de la amplitud, fase, frecuencia y ángulo de llegada de la señal al receptor, produciendo desvanecimientos selectivos en frecuencia de la señal. El desvanecimiento de Rayleigh es muy utilizado como modelo del canal inalámbrico [8].

A. Desvanecimiento selectivo en frecuencia

Se pueden identificar dos tipos de desvanecimientos: desvanecimiento a gran escala y desvanecimiento a pequeña escala. El desvanecimiento a gran escala produce la atenuación de la señal como consecuencia de la propagación de la onda en áreas extensas y de la interacción con cuerpos grandes en relación a la longitud de onda de la señal, tales como bosques, edificios, etc. Por otro lado, el desvanecimiento a pequeña escala se produce por el movimiento de las estaciones enlazadas y por los obstáculos en el canal, cuyas dimensiones son comparables con la longitud de onda de la señal, y que afectan a su amplitud y fase.

Una de las manifestaciones del desvanecimiento a pequeña escala se produce cuando el tiempo que tarda la componente de la multitrayectoria en llegar al receptor, T_m, es mayor en relación al tiempo de duración del símbolo, T_s, es decir bajo la condición de $T_m > T_s$ [1]. En el dominio del tiempo, el desvanecimiento selectivo en frecuencia se manifiesta principalmente como distorsión por la interferencia entre símbolos ISI. Las componentes que se reciben son derivaciones de una señal principal, por lo que guardan un alto grado de similitud. Sin embargo, el desvanecimiento se puede analizar considerando la potencia de cada componente de frecuencia de señal original de manera independiente [1].

Se establece entonces una banda de coherencia, que es el rango de frecuencias donde el canal afecta por igual a las componentes. Fuera de la banda de coherencia, las atenuaciones de las componentes espectrales de la señal sufren degradaciones independientes y diferentes a las que están dentro del mismo. Los efectos de este tipo de desvanecimiento son "independientes del rango de frecuencias de la señal y ocurren todo el tiempo en el canal"

B. Dispersión de energía para mitigar el desvanecimiento selectivo en frecuencia

Para mitigar los efectos del desvanecimiento selectivo en frecuencia se utilizan varias técnicas como la ecualización, el ensanchamiento espectral, la multiplexación por división de frecuencia ortogonal (OFDM), y la dispersión de energía [1]. En este proyecto se estudió la dispersión de energía mediante la aleatorización de la señal.

Debido a la naturaleza de la información, las secuencias binarias que son transmitidas en los sistemas de comunicaciones pueden contener patrones repetitivos, produciendo consecuentemente una concentración de potencia en ciertas regiones del espectro, tal como se observa en la Fig. 1. Por lo tanto, en el dominio de la frecuencia, se puede observar que la energía de la señal se concentra en unas frecuencias más que en otras. A diferencia de estas secuencias de información, las secuencias de bits aleatorias tienen una distribución equitativa de la potencia en el espectro de frecuencias [9]. La dispersión de energía consiste en "aleatorizar" una señal binaria mediante la suma lógica de la misma con una secuencia aleatoria [10].

Mediante la aleatorización se distribuye la potencia de la señal en todo el espectro, reduciendo el efecto del desvanecimiento selectivo en frecuencia [9] [10]. En la Fig. 1 se muestra el efecto de la aplicación de la dispersión de energía, al combinar una secuencia binaria de audio MP3 con un generador PRBS de grado 15. En la Fig. 1 se visualiza como disminuyen ciertos picos de potencia de la señal después de la dispersión de energía, lo que reduciría el efecto de los desvanecimientos selectivos en frecuencia.

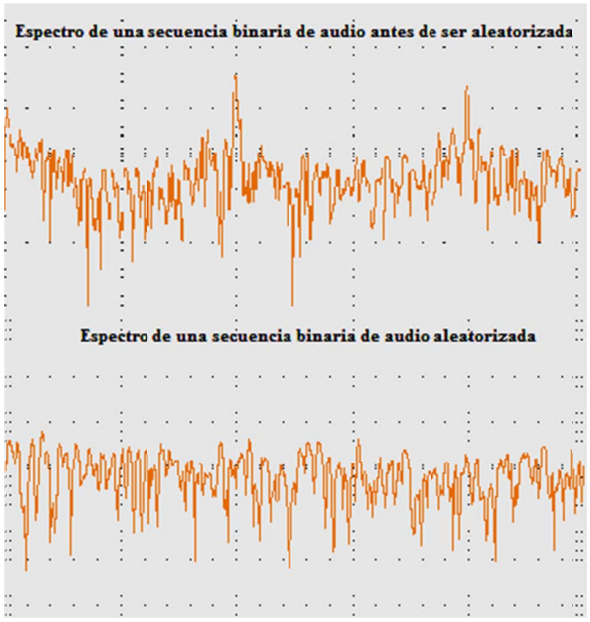

Fig. 1. Espectro de frecuencia de la secuencia binaria de audio antes y después de ser aleatorizada.

III. Propuesta de Pruebas Estadísticas

La evaluación del grado de aleatoriedad de los generadores se realiza en base a conjuntos de pruebas estadísticas. De los trabajos previos estudiados se establece que los conjuntos de pruebas más populares son las normas: 800-22, FIPS-140 y FIPS-141. En la evaluación de un generador se puede utilizar una parte o la totalidad de las pruebas propuestas de acuerdo a la profundidad de análisis que se requiera realizar. En [11] se enuncia que de acuerdo a la aplicación se deben establecer ciertas condiciones particulares para las pruebas estadísticas, como: longitud de la secuencia, condición mínima para superar la prueba, entre otros.

Para la evaluación de los generadores de secuencias pseudoaleatorias en aplicaciones de dispersión de energía se ha escogido un conjunto de pruebas estadísticas para evaluar el nivel de aleatoriedad de 6 generadores. El conjunto de pruebas se seleccionó de la norma 800-22 del NIST [11] y se muestran en la Tabla I con la propiedad estadística que permiten comprobar.

TABLA I
Conjunto de Pruebas Estadísticas

#	Prueba	Propiedad que se comprobará
1	Frecuencia Monobit	Uniformidad de valores y distribución uniforme en secuencia global
2	Frecuencias en bloques de M-bits	Uniformidad de valores y distribución uniforme en subsecuencias
3	Ráfagas (Runtest)	Aleatoriedad Global en secuencia global
4	Ráfagas largas (Longest Runtest)	Aleatoriedad Global en subsecuencias
5	Rango de matriz binaria	Independencia lineal de valores en secuencia global
6	Transformada de Fourier	Repetición de patrones y autocorrelación[1].

Para evaluar la aleatoriedad, en MatlabTM se programaron los generadores y se ejecutaron las pruebas estadísticas con los parámetros que se muestran en la Tabla II.

Para evaluar si un generador supera la prueba se utilizó el parámetro estadístico del p-valor. Como resultado de cada prueba realizada sobre las muestras analizadas se obtiene un conjunto de p-valores. Para interpretar los resultados considerando el conjunto de p-valores se utilizan dos métodos: el del intervalo de confianza y el del histograma.

En el primer método de interpretación de los resultados se analiza si el conjunto de p-valores se encuentra dentro del intervalo de confianza, para ello se utiliza la siguiente ecuación [11].

$$intervalo\ confianza = \dot{p} \pm \sqrt{\frac{\dot{p}\cdot(1-\dot{p})}{m}} \qquad (1)$$

En donde $p = 1 - \alpha$ y m representan el número de secuencias por muestra que se van a probar. En el caso de una muestra con 1000 secuencias el límite inferior del intervalo de confianza según la ecuación anterior sería 0.9806. Este primer método se utiliza para establecer los generadores con mejores características de aleatoriedad.

En el segundo método de interpretación se evaluaron los histogramas obtenidos de los p-valores en las pruebas con los generadores. Este segundo método de interpretación complementa al primero para establecer el generador con mejores características de aleatoriedad.

TABLA II
Parámetros para las Pruebas Estadísticas Realizadas sobre las Secuencias

Parámetro	Valor
Bits por muestra	Para cumplir con el requisito de la prueba de Rango de Matriz Binaria se generan secuencias de 5000 bits por cada muestra en los modelos.
Secuencias por muestra	Mínimo 1000 para ambos métodos de interpretación.
Cantidad de muestras probadas	10 muestras por cada generador.
Valor crítico α	0,01 para la batería de pruebas y métodos de interpretación.

IV. Resultados de Evaluación de los Generadores

Mediante el método de interpretación del intervalo de confianza, se obtuvieron los resultados de la Tabla III. En el análisis se considera que se supera la prueba si el valor estadístico es mayor a 0,9806. Analizando los resultados, se tiene que los PRNG de Fibonacci, Green y Mitchell-Moore superaron solo la prueba de frecuencia en bloques de M-bits. Por otro lado, el PRBS de grado 9 supera las tres primeras pruebas, siendo el modelo que más pruebas supera, seguido por el PRBS de grado 15 que supera la primera y tercera prueba.

TABLA III
Resultados de las Pruebas Estadísticas

# de Prueba		1	2	3	4	5	6
Generador de secuencias pseudoaleatorias	Fibonacci	0.955	0.990	0.959	0	0	0.070
	Green	0.962	0.992	0.965	0	0	0
	Mitchell Moore	0.961	0.992	0.959	0	0	0
	PRBS grado 9	1	1	1	0	0.77	0
	PRBS grado 15	0.993	0.843	0.998	0	0.40	0

El segundo método de interpretación se utiliza para evaluar la característica de aleatoriedad de los PRBS de grado 9 y grado 15. Este método se divide en dos partes, en la primera se evalúan los generadores en todo el período de los mismos, y la segunda es la evaluación de la secuencia generada con la "semilla" que establecen las normas de radiodifusión.

De los resultados de las pruebas estadísticas sobre el período completo de los PRBS de grado 9 y 15, se observan los mismos resultados para los dos generadores, obteniéndose

[1] En el contexto, significa que se compara la señal con sí misma para identificar los patrones repetidos.

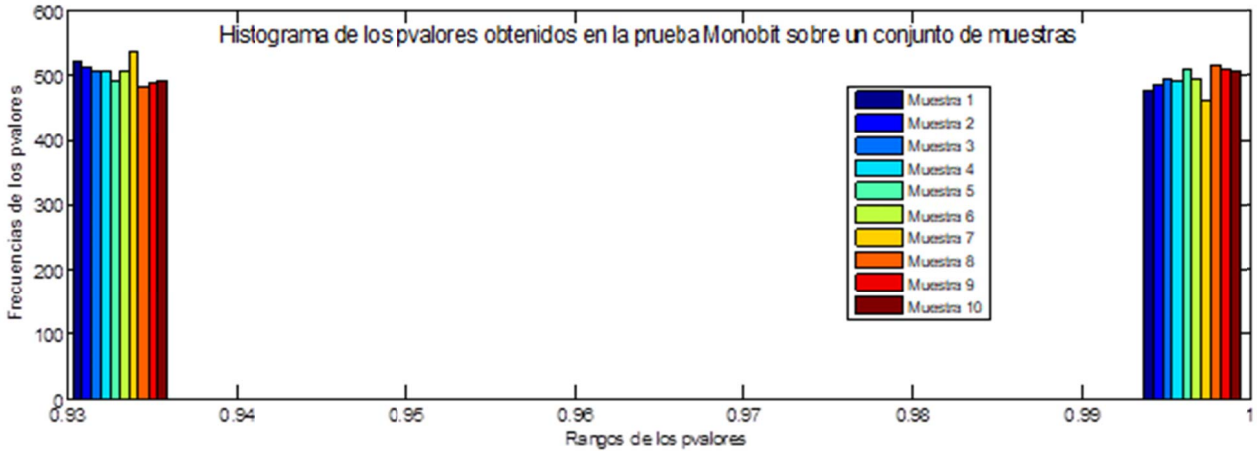

Fig. 2. Histograma de p-valores obtenidos para el PRBS grado 9.

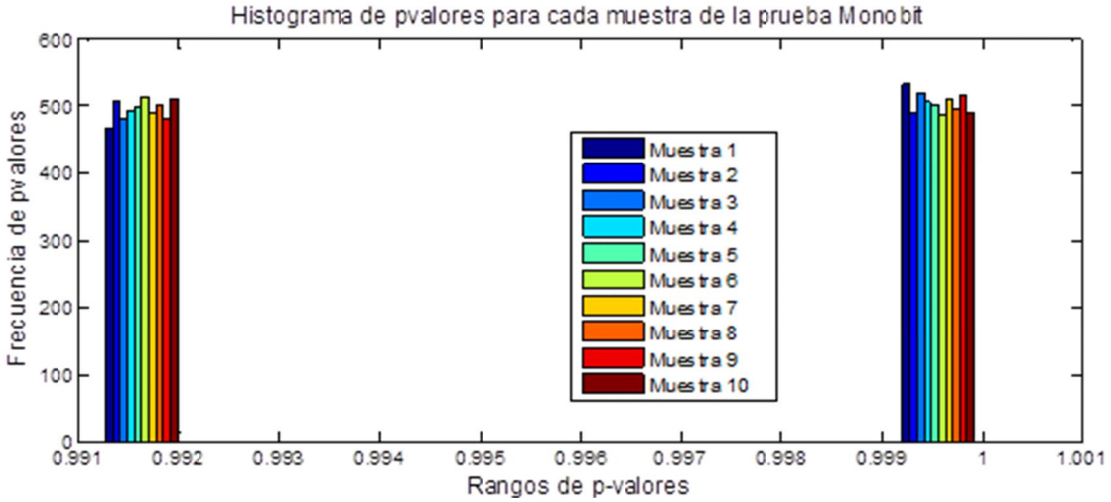

Fig. 3. Histograma de p-valores obtenidos para el PRBS grado 15.

que los dos superan las tres primeras pruebas con p-valores de 1 y que las tres últimas pruebas no son superadas con p-valores de 0. Por los resultados obtenidos se analizan los histogramas de los p-valores.

En las Fig. 2 y 3 se muestran los histogramas de los p-valores obtenidos de la prueba monobit para el PRBS de grado 9 y 15 respectivamente. La prueba monobit se toma como referencia para comparar el comportamiento de los dos generadores analizados. De los histogramas se observa que el PRBS de grado 15 concentra los p-valores en un rango más pequeño y más cercano a 1 que el PRBS de grado 9, interpretándose que el primero muestra mejores características de aleatoriedad.

Los resultados de la evaluación de la influencia de la "semilla" sobre los PRBS de grado 9 y 15 se presentan en la Tabla IV. En este caso se observan mejores efectos de aleatoriedad en el modelo del PRBS de grado 15 con la semilla de la norma ISDB-Tb. La quinta prueba de matriz de rango binario no se realizó sobre el PRBS de grado 9 debido a los requerimientos de longitud de secuencia

TABLA IV
EVALUACIÓN DE LOS PRBS 9 Y 15 CON LA SEMILLA DE LAS NORMAS DE RADIODIFUSIÓN DRM E ISDB-TB RESPECTIVAMENTE

# de Prueba	1	2	3	4	5	6
PRBS grado 9	0.929	0.280	0.929	0	NA*	0
PRBS grado 15	0.991	0.351	0.991	0	0	0

*NA - no aplica

V. CONCLUSIONES

Para la evaluación estadística de secuencias pseudoaleatorias en dispersores de energía se propone la aplicación de 6 pruebas planteadas en la norma 800-22. Para los parámetros establecidos en las pruebas estadísticas se observó que los PRBS de grado 9 y 15 tienen mejores características de aleatoriedad que el resto de generadores propuestos, porque superaron la mayor cantidad de pruebas estadísticas planteadas. Sin embargo, estos generadores no poseen las siguientes propiedades: distribución uniforme de unos y ceros en subsecuencias (Prueba de ráfagas en

subsecuencias), independencia lineal entre subsecuencias (Rango de matriz binaria), y distribución aleatoria entre los valores de las potencias en el espectro de frecuencia (Prueba espectral). Este incumplimiento de ciertas propiedades se debe principalmente a que los generadores mantienen patrones repetitivos, ya que utilizan una fórmula de recurrencia. En las condiciones establecidas en el presente análisis se comprobó que la utilización de las semillas de las normas DRM e ISDB-Tb no mejora los resultados de las pruebas estadísticas.

Resta por ejecutar un estudio del efecto del dispersor de energía en un canal inalámbrico mediante simulaciones y pruebas en ambiente real para comprobar el efecto del incumplimiento de ciertas propiedades de aleatoriedad.

REFERENCIAS

[1] B. Sklar, "Rayleigh Fading Channels in Mobile Digital Communication Systems. Part I: Characterization.", *IEEE Communication Magazine,* vol. 1, nº 0163-6804, pp. 90-100, 1997.

[2] ETSI, "Digital Radio Mondiale (DRM). System Specification" Enero 2014. [En línea]. Disponible: http://www.drm.org/wp-content/uploads/2014/01/DRM-System-Specification-ETSI-ES-201-980-V4.1.1-2014-01.pdf. [Último acceso: 21 Octubre 2014].

[3] Asociación Brasileña de Normas Técnicas, "NBR 15601", 11 Noviembre 2007. [En línea]. Disponible: http://www.upjet.org.ar/archivos_noticias/356-1.pdf. [Último acceso: 21 Octubre 2014].

[4] Ned, Corron; Billy Reed; Blakely Jonathan; Krishna Myneni; Shawn Pethel; "Chaotic scrambling for Wireless analog video"; Communications in Nonlinear Science and Numerical Simulation, vol. 15, Issue 9, pp. 2504-2513, 2010.

[5] Galia, Marinova; Zdravka, Tchobanova; "Simulation, Measurement and Test Environment for Pseudo Random Number Generator Circuits", Research on Electric and Electronic Measurement for the Economic Upturn, vol. 20, pp. 15-17, 2014.

[6] Goretti, Campo, Echanobe; "Circuitos digitales basados en FPGA para generación de números aleatorios", [En línea]. Disponible: http://gtts.ehu.es/dEyE/Actualizable/Anual/Curso05-06/VI_Jornadas_IE/trabajos_dirigidos/Goreti_Sevillano.pdf [Último acceso: 27 Octubre 2014].

[7] Raj, Katti; Rajesh, Kavasseri; Vyasa, Sai, "Pseudorandom bit generation using coupled congruential generators", Transactions on Circuits and Systems II, vol. 57, nº 3, pp. 203-207, 2010.

[8] Xinjia, Chen; Guoxiang, Gu; Kemin, Zhou; "Measurement complexity of Rayleigh Fading Channels", IEEE Transactions on Vehicular Technology, vol. 58, issue: 7, pp. 3776-3781, 2009.

[9] S. Morris y A. Smith-Chaigneau, Interactive TV Standars. A guide to MHP, OCAP and JavaTV., Burlington, USA: Focal Press, 2013, p. 28.

[10] H.-J. Zepernick y A. Finger, Pseudo ramdom signal processing. Theory and applications., Primera ed., Chischester, Inglaterra: John Wiley & Sons, Ltd., 2005.

[11] A. Rukhin, J. Soto, J. Nechvatal, M. Smid y E. Barker, "A Statistical Test Suite for Random and Pseudorandom Number Generators forCryptographic Applications.", Abril 2010. [En línea]. Disponible: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf. [Último acceso: 9 Octubre 2014].