TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 18, No. 3, Septiembre-Diciembre, 2019, p.1- 10 ISSN 1729-3804

DESEMPEÑO DE CÓDIGOS CORRECTORES DE ERROR EN LA TÉCNICA SECURE SKETCH PARA LA RECONCILIACIÓN DE LA INFORMACIÓN

Mario Ramírez Méndez[1], Yaime Fernández Jiménez[1], Vitalio Alfonso Reguera[1], An Braeken[2]

[1]University "Marta Abreu" of Las Villas, Road to Camajuaní Km. 5 ½, CP 54830, Santa Clara, Villa Clara, Cuba,
[2]Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Brussel, Belgium
[1]e-mail: riomarezamir@gmail.com

RESUMEN

El proceso de reconciliación de la información permite corregir las diferencias entre las claves generadas en los extremos de una transmisión. La técnica secure sketch para garantizar la reconciliación mediante el uso de códigos correctores de error, logra mitigar el daño ocasionado por el ruido y la naturaleza inalámbrica de las redes de comunicación. Un desafío en este contexto es la implementación de códigos correctores de error que permitan el éxito de la reconciliación, manteniendo la seguridad de este proceso ante la observación de un adversario. En esta investigación se evalúa el desempeño de los códigos correctores de error: Low-Density Parity-Check (LDPC), Bose-Chaudhuri-Hocquenghem (BCH) and Hamming, en la técnica secure sketch, y en distintos escenarios, considerando la presencia o no de ruido. Las evaluaciones se realizan en términos de la tasa de error de bit y la reconciliación exitosa de la clave. Los resultados obtenidos muestran que en un canal sin ruido el desempeño de los códigos BCH y LDPC es superior al de los códigos Hamming. Con la adición de ruido, los códigos LDPC son más robustos y presentan el mejor desempeño. Basado en estos resultados, se propone la utilización de códigos BCH y LDPC en la técnica secure sketch para canales con ruido.

PALABRAS CLAVES: Reconciliación de la información, secure sketch, códigos correctores de error

PERFORMANCE OF ERROR CORRECTING CODES IN SECURE SKETCH TECHNIQUE FOR INFORMATION RECONCILIATION

ABSTRACT

The information reconciliation process allows to correct the differences between the keys generated at both ends of a transmission. The secure sketch technique to guarantee the reconciliation through the use of error correcting codes, manages to mitigate the damage caused by noise and the wireless nature of communication networks. A challenge in this context is the implementation of error correcting codes that allows the success of reconciliation, maintaining the security of this process before the observation of an adversary. In this research the performance of the error correcting codes, Low-Density Parity-Check (LDPC), Bose-Chaudhuri-Hocquenghem (BCH) and Hamming, in the secure sketch technique for different scenarios, is evaluated considering the presence or absence of noise. The evaluations are made in terms of the bit error rate and the successful key reconciliation. The results obtained show that in a noise-free channel the performance of the BCH and LDPC codes is superior to the Hamming codes. With the addition of noise, the LDPC codes are more robust and present the best performance. Based on these results, the combination of BCH and LDPC codes in the secure sketch technique for noisy channels is proposed.

KEY WORDS: Information reconciliation, secure sketch, error correcting codes.

1. INTRODUCCIÓN

Uno de los aspectos fundamentales en la seguridad de la capa física en redes inalámbricas es la generación de claves físicas para cifrar la información de los mensajes. El aprovechamiento de las propiedades físicas del canal permite generar una clave en cada uno de los extremos legítimos de la comunicación, mediante el intercambio de señales piloto que contienen información de CSI, RSSI, fase u otro. Posteriormente, estas mediciones se cuantifican

obteniendo dos secuencias de bits en los extremos, que serán usadas como claves. Sin embargo, aunque estas claves están altamente correlacionadas, presentan ligeras diferencias debido a la variabilidad de los factores en el proceso de extracción. Para llevar a cabo el acuerdo de estas claves, y considerando un adversario computacionalmente ilimitado, se añade al modelo de la generación de claves físicas un mecanismo proveniente de la criptografía: la reconciliación de la información.

La reconciliación de la información, o reconciliación de la clave, es un proceso encargado de corregir los errores en las mediciones efectuadas al extraer las claves en cada uno de los extremos transmisor (Alice) y receptor (Bob). El principal obstáculo para realizar esta tarea es que debe hacerse a través de un canal con carácter público [3], lo que ocasiona que una parte de la información se "fugue" al adversario (Eve). La figura 1 muestra las distintas etapas del proceso.

Al igual que en la criptografía, el transmisor envía al receptor legítimo, utilizando el canal principal, cierta información sobre la clave. El receptor compara esta información con su versión de la clave y a su vez envía una respuesta similar, o confirma la recepción, dependiendo de la técnica empleada. En un principio tales técnicas se basaban en el envío de información sobre la paridad de las secuencias, subdivididas convenientemente en bloques [3]. El objetivo era disminuir el contenido secreto fugado hacia Eve, para lo cual se requería no solo la transmisión directa de Alice a Bob, sino también la confirmación de parte de Bob, haciendo uso de la reciprocidad del canal. Esta dificultad alentó la idea de emplear códigos correctores de error, sin llegar a subdividir las cadenas de bits de la clave, y sin la necesidad de una respuesta de Bob [4].

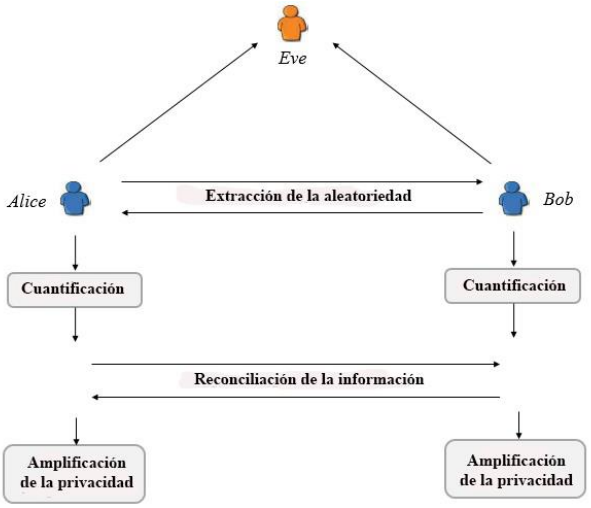

Figura 1: Modelo de generación de una clave física.

En los últimos años ha alcanzado popularidad una técnica proveniente de las mediciones biométricas, la cual emplea los códigos correctores de error para evitar la fuga de información parcial hacia el adversario: la *secure sketch* [5, 6]. Su funcionamiento se basa en la idea de un mecanismo de *one-time pad*, sustituyendo la fuente aleatoria por una palabra de código válida. La tarea del receptor se limita a implementar un algoritmo de decodificación y añadir a la secuencia decodificada su versión de la clave, mediante otro OR-exclusivo. Sin embargo, uno de los desafíos actuales de la implementación de la técnica *secure sketch* es la selección de los códigos correctores de error con un desempeño favorable.

2. SECURE SKETCH

En [6] es propuesta la técnica secure sketch para reconciliar las discrepancias entre las cadenas de bits. Por lo general, esta técnica se emplea en la transmisión de carácter público de una información *s* obtenida sobre una entrada K (clave), la cual no es revelada, y que permite aun así reconstruir dicha K, a partir de una medición aproximada a K en el otro extremo. Asumiendo que Alice y Bob han hecho una estima de canal por alguno de los métodos conocidos, posteriormente cuantificada para ser usada como clave en ambos extremos y que se designan como K_a y K_b, respectivamente, la técnica de secure sketch exige que:

$$d(K_a, K_b) \leq t \qquad (1)$$

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 18, No. 3, Septiembre-Diciembre, 2019, p.1- 10 ISSN 1729-3804

donde $d(K_a, K_b)$ designa la distancia de Hamming o la cantidad de bits en los que difieren las dos secuencias, y t es un valor umbral, correspondiente a la capacidad correctora de los códigos empleados.

Lo que plantea el mecanismo de secure sketch es, en esencia, la elección de un código corrector de errores $C(n, k)$, que permita obtener K_a, a partir de K_b, aun cuando ninguna de estas claves pertenezca a dicho código. La generación aleatoria de una palabra de código c perteneciente a C, permite computar la información denominada secure sketch, $SS(K) = s = K \oplus c$. Esta es enviada a Bob, que al recibirla efectúa la sustracción del error introducido para obtener $Rec(K', s) = c' = K' \oplus s$. Luego Bob decodifica c', si se cumple la condición expuesta en (1), para tener c y determinar el valor de K, mediante $K = c \oplus s$. El proceso puede ser resumido en el siguiente esquema (Fig. 2), siendo r la palabra de código generada aleatoriamente del código C.

Alice:

1. $s = K_a \oplus C(r)$
2. Envía s a Bob.

Bob:

3. $r' = Decod(K_b \oplus s)$
   $= Decod(K_b \oplus K_a \oplus C(r))$
   $= Decod(C(r) \oplus e)$
   $= r, \quad (si\ d(e,0) < t)$
4. $K_b = C(r') \oplus s$

Figura 2: Pasos en la técnica secure sketch.

Códigos correctores de error

Como se muestra en la figura 2, la implementación de la técnica secure sketch requiere de un proceso de corrección de errores para reconciliar la información de la clave. Para llevar a término este proceso se necesita seleccionar adecuadamente los códigos correctores de error que se adapten al problema en cuestión.

La elección de los códigos depende de diversos criterios como pueden ser el tamaño requerido de la clave, la capacidad correctora, la robustez ante el ruido, y la complejidad de diseño, entre otros [5, 7]. Por ejemplo, el código de Hamming es fácil de implementar, con respecto a otros de mayor intensidad de fuente como en el caso de los códigos LDPC. Por otro lado, mientras la capacidad correctora de los códigos de Hamming se subordina al umbral $t = (d_{mín} - 1)/2$, donde $d_{mín}$ es la distancia de Hamming mínima, los códigos LDPC pueden corregir un mayor número de errores a medida que el tamaño de la clave aumenta, aunque consumiendo más recursos debido a su proceso de decodificación iterativa [7].

Por tanto, uno de los criterios de fundamental cuidado en la implementación de la técnica se refiere a la capacidad correctora. Los códigos seleccionados deben ser capaces de corregir errores, pero no un número excesivo de errores. Si la capacidad correctora alcanza grandes cantidades de errores, el adversario, Eve, tiene la posibilidad de reconciliar su medición de canal cuantificada, o su información de clave K_e, implementando un algoritmo decodificador similar al del extremo receptor. Esto último representa una ventaja para los códigos de Hamming y los polinomiales, cuya capacidad correctora es conocida de antemano y prefijada en los límites de un umbral.

Por otro lado, la criptografía determina un valor teórico de tamaño mínimo de clave estipulado en 128 bits para los actuales estándares de potencia computacional [8]. Esto exige establecer una relación de compromiso entre la capacidad correctora, el tamaño de la clave (que coincide con el de las palabras de código) y el tamaño de los mensajes a cifrar, según este criterio códigos robustos como los LDPC, estarían en desventaja con respecto a los códigos de baja corrección, como los mencionados Hamming y la familia de códigos polinomiales, en general. Sin embargo, mediante vías como la transmisión de múltiples mensajes de forma simultánea, o el anidado de códigos de distinta matriz de chequeo de paridad, se consigue "confundir" al adversario Eve, tanto como es requerido para alcanzar la reconciliación exitosa, sin pérdida alguna de la confidencialidad.

Un criterio que otorga prevalencia a los códigos polinomiales y cíclicos, sobre los más robustos LDPC, es la complejidad de diseño [7]. Como estos códigos no persiguen corregir un alto número de errores, sus algoritmos de codificación y decodificación son simples, y utilizan bajos recursos de cómputo. La capacidad correctora de los códigos BCH, perteneciente a la familia de códigos cíclicos, puede ser limitada a unos pocos bits, tanto como se consiga disminuir su distancia de Hamming mínima. Esta propiedad garantiza una complejidad de diseño baja, aun cuando se trabaja con grandes cadenas de bits, a la vez que un control sobre la capacidad correctora de estos códigos. Por su parte, en la utilización de códigos LDPC se necesita construir una matriz dispersa para lograr la codificación eficiente, lo que conlleva a algoritmos iterativos de mayor complejidad computacional.

Teniendo en cuenta los criterios mencionados, los códigos LDPC, Bose-Chaudari-Hocquenghem (BCH) y Hamming fueron seleccionados para el propósito de implementar la técnica secure sketch.

3. EVALUACIÓN DEL DESEMPEÑO

Modelo del sistema

Se asumen dos escenarios, atendiendo a los parámetros de evaluación mencionados en el epígrafe anterior. En ambos escenarios se considera que las secuencias binarias K_a y K_b, usadas como claves, han sido obtenidas exitosamente en cada uno de los extremos transmisor y receptor. Además, se asume que las secuencias están correlacionadas con un factor de correlación de Pearson superior a 0.85, lo cual ha demostrado ser realista en [3, 7]. Se considera la presencia de un adversario pasivo (Eve), es decir, su actividad se limita a la observación del intercambio de información por el canal principal. Para este adversario, tomamos factores de correlación que oscilan entre -0.1 y 0.2, similares a los obtenidos en la práctica [7].

En el primer escenario se siguen los pasos descritos en la figura 2. Además, se implementan los códigos LDPC, BCH y Hamming cuyas palabras de código, también generadas aleatoriamente, son mezcladas con la secuencia correspondiente a la clave de Alice, K_a. Esta mezcla es enviada por un canal libre de ruido hasta llegar el extremo receptor, donde se realiza la recuperación mediante un OR-exclusivo con la clave de Bob. Posteriormente se decodifica para obtener la palabra de código válida que permite la reconciliación de las claves.

En el segundo escenario se añade ruido aditivo blanco gaussiano (AWGN, *Additive White Gaussian Noise*) al canal por el que es enviada la mezcla del mecanismo secure sketch. Esta mezcla se modula para atravesar el canal. La modulación elegida fue la de desplazamiento de fase (PSK, *Phase Shift Keying*) por su aplicación en métodos de extracción de la aleatoriedad mediante el intercambio de valores de RSSI [9] o CSI [10], y por ser la modulación usual en el tratamiento de señales digitales. Además, en este escenario, la relación señal a ruido (SNR, *Signal to Noise Ratio*) es disminuida para evaluar el desempeño de los códigos ante el deterioro del canal.

Luego se produce la decodificación, convirtiéndose en una secuencia confiable para la reconciliación. Sin embargo, ante la presencia de ruido, se requiere aumentar la potencia para mantener la cantidad de errores en dependencia únicamente de las diferencias en la correlación de las secuencias. El objetivo de implementar la técnica en este escenario es determinar cuánto afecta la adición de ruido a la tasa de errores para los distintos códigos.

Tasa de error de bit

A medida que el tamaño del bloque en la codificación, y por consiguiente el tamaño de la clave aumente, el éxito de la técnica se verá amenazado, a menos que se implementen estrategias como el aumento en la potencia de la señal, o de la SNR. Además, cuando la correlación entre las secuencias medidas es baja [11], los errores introducidos artificialmente en el mecanismo secure sketch pueden ser irrecuperables. Por la tanto, un mecanismo secure sketch totalmente seguro se logra cuando la tasa de error de bit (BER, *Bit Error Rate*) es igual a cero.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 18, No. 3, Septiembre-Diciembre, 2019, p.1- 10 ISSN 1729-3804

Si el ruido presente en el canal también aumenta, es necesario incrementar la potencia, o la correlación entre las secuencias. Cuando esto último no es posible, porque los mecanismos de extracción de la aleatoriedad han sido explotados al máximo, se recurre a disminuir el tamaño de los mensajes, o sub-bloques en los que viaja la información acerca de la clave.

Teniendo en cuenta estos parámetros, una medida de la tasa de error de bit con respecto a varias muestras de la clave, puede ofrecer una evaluación de la técnica durante la transmisión. El comportamiento de la BER en escenarios donde son variados otros parámetros como la SNR o la potencia de la señal, permite establecer una región de trabajo para la técnica de reconciliación empleada [12].

Reconciliación exitosa de la clave

La reconciliación exitosa de la clave (SKR, *Successful Key Reconciliation*) es un parámetro de evaluación frecuente en los procesos de reconciliación de la información [7]. Usualmente es medida con respecto a otros parámetros, propios de la tecnología o de la transmisión, en una aplicación determinada. Así, por ejemplo, en [7] la SKR en una red de sensores inalámbricos tiene lugar frente a variaciones de la distancia entre los nodos, para distintos niveles de cuantificación. El éxito de la reconciliación se alcanza cuando SKR=1, lo que equivale a la corrección de un 100% de los errores entre las secuencias.

Para contabilizar la reconciliación exitosa de la clave, se repite el proceso de reconciliación y luego se calcula la cantidad de errores entre las secuencias que han sido corregidos al final de cada proceso, y este resultado se divide por la cantidad total de errores que se tenía al principio.

4. RESULTADOS DE LA SIMULACIÓN

Las simulaciones han sido llevadas a cabo para determinar el desempeño de los códigos seleccionados en las secciones previas. Se asumen los siguientes parámetros para los códigos LDPC, BCH y Hamming:

- Para todos los casos el tamaño de la clave es de 127 bits.
- La tasa de bit es la misma para todos: $1/3$.
- La tolerancia de error (t/n):
  - Para los códigos LDPC se emplea la matriz DVB-S.2, con tolerancia de error superior al 10%.
  - Los códigos BCH empleados tienen una tolerancia de error de 4,72%.
  - Los códigos Hamming corrigen un solo error, pero aplicando *interleaving* (sobre la clave) estos códigos alcanzan una tolerancia de error superior al 1%.

Primer escenario

En la figura 3 se muestra el comportamiento de los códigos LDPC, BCH y Hamming en un canal sin ruido, en lo referente a la tasa de error de bits de las transmisiones simuladas. Como se observa, los códigos BCH aventajan a los códigos LDPC y Hamming, al requerir de una menor correlación para alcanzar la condición de $\mathrm{BER} = 0$. Por otro lado, los códigos Hamming necesitan de mecanismos alternos para obtener valores de correlación lo suficientemente altos como para alcanzar la condición anterior [13]. Sin embargo, considerando la región en la que opera el adversario descrito en este trabajo, los códigos BCH y Hamming presentan un desempeño óptimo con respecto a los códigos LDPC, pues la tasa de error de bit en estos casos es la peor posible para el propósito de corregir los errores.

Por otro lado, en la figura 4 se observa la reconciliación exitosa de la clave en este mismo escenario. Para valores de correlación en correspondencia con los obtenidos en la práctica para la transmisión legítima, la reconciliación exitosa de la clave presenta valores aceptables para los tres códigos. Debe destacarse el caso de los códigos BCH y LDPC, los cuales realizan el cien por ciento de la reconciliación ($\mathrm{SKR} = 1$) para valores de correlación de poco menos de 0.8 y 0.9, respectivamente. Desde el punto de vista de un adversario, la reconciliación tendría un éxito a medias ($\mathrm{SKR} = 0.5$) para los tres códigos, siendo el peor de los casos el de los códigos LDPC.

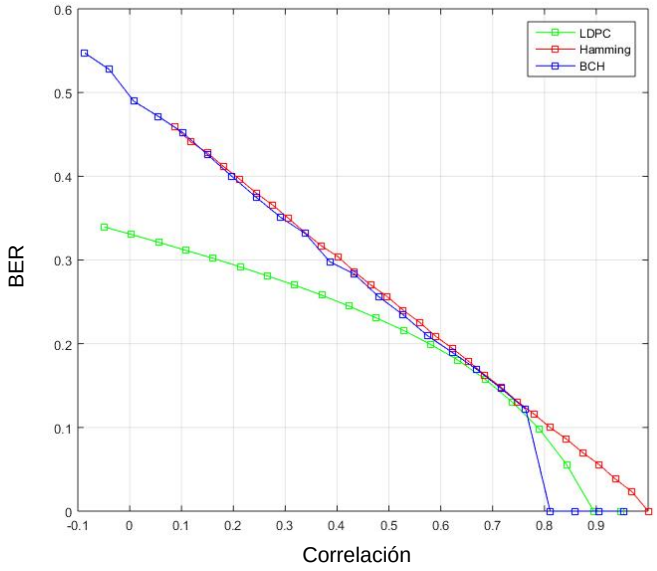

Figura 3: Comparación de los códigos simulados, en términos de BER, en un canal sin ruido.

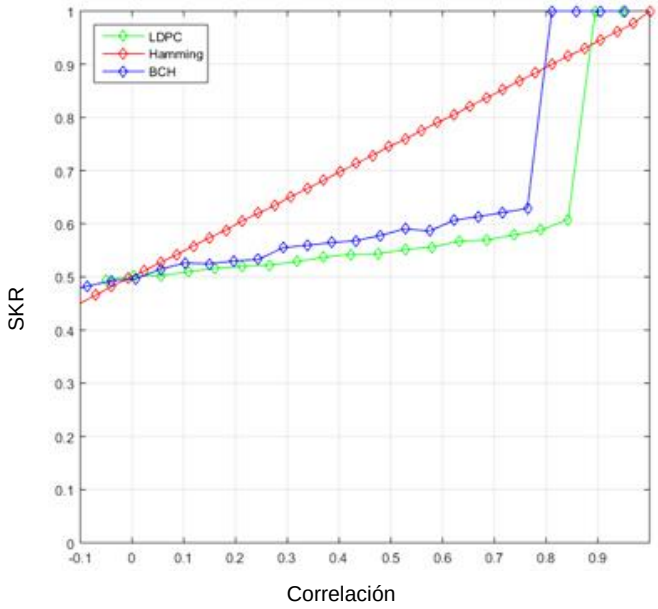

Figura 4: Comparación de los códigos simulados, en términos de SKR, en un canal sin ruido.

Segundo escenario

Cuando se añade AWGN al canal de transmisión, los resultados varían. En la figura 5 se observa como solo los códigos LDPC alcanzan la condición BER $= 0$, mientras que la capacidad correctora de los códigos BCH y Hamming se ha agotado ante el número de errores introducidos por el ruido. La robustez de los códigos LDPC les permite corregir un número considerable de errores, de ahí su buen desempeño con grandes cadenas de bits. Aun así, a un adversario le resultaría más arduo enfrentar las codificaciones BCH y Hamming, debido a sus mayores razones de errores de bits.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 18, No. 3, Septiembre-Diciembre, 2019, p.1- 10 ISSN 1729-3804

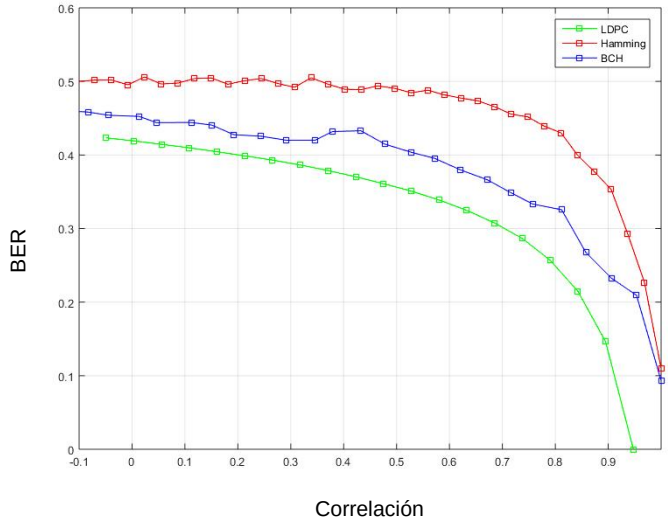

Figura 5: Comparación de los códigos simulados, en términos de BER, en un canal con ruido.

Algo similar se observa en la figura 6 con respecto a la reconciliación exitosa de la clave en este escenario. Aunque para una correlación muy alta (de 0.95 aproximadamente), los códigos LDPC consiguen el cien por ciento de reconciliación. El ruido introducido, sin embargo, impide este proceso en los códigos Hamming, y requiere de la total identidad de las claves, en el caso de los códigos BCH. De igual forma que en el primer escenario, un adversario puede extraer apenas la mitad de la información contenida en las claves.

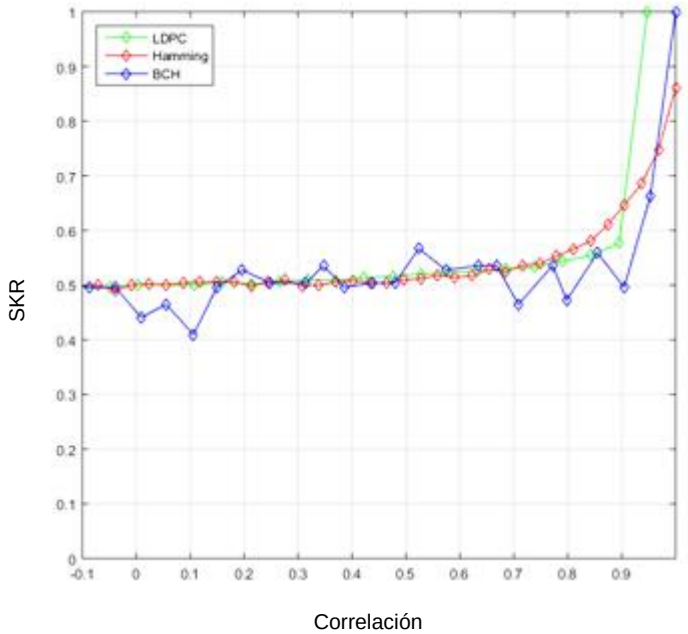

Figura 6: Comparación de los códigos simulados, en términos de SKR, en un canal con ruido.

Propuesta

Considerando estos resultados, y tomando en cuenta el segundo de los escenarios descritos, se realiza la propuesta de combinar los códigos BCH y LDPC dentro de la técnica secure sketch. Exactamente, el esquema consiste en emplear los códigos BCH durante las fases de mezclado secure sketch (paso 1 en figura 2) y de recuperación (pasos 2 y 3 en figura 2). Los códigos LDPC se emplearían aquí como una codificación adicional para enfrentar los errores introducidos por el ruido del canal. Las figuras 7 y 8 muestran los resultados de las simulaciones para este esquema.

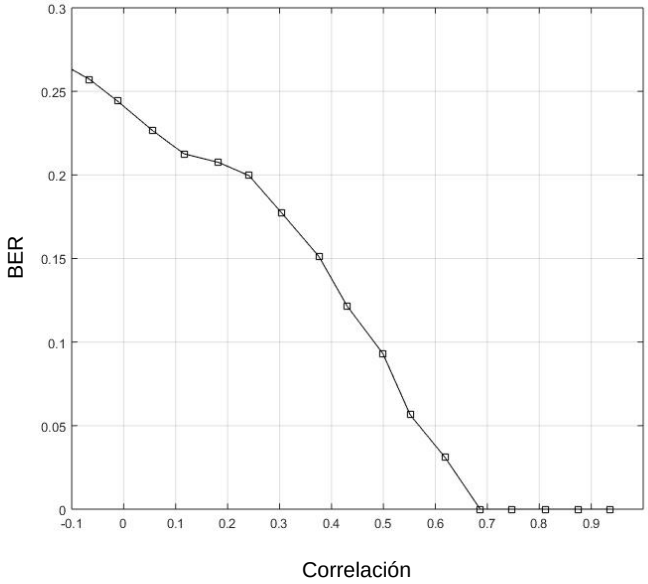

Figura 7: Desempeño del esquema de la propuesta en términos de BER.

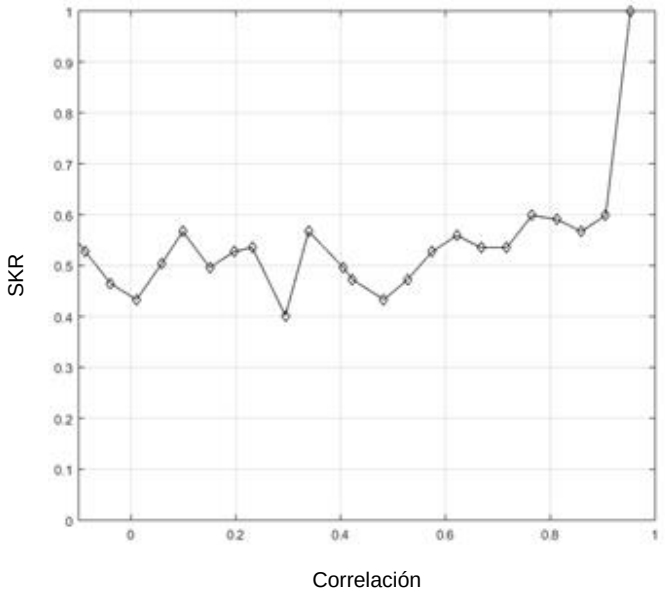

Figura 8: Desempeño del esquema de la propuesta en términos de SKR.

Como se aprecia en la figura 7, el factor de correlación para alcanzar $\mathrm{BER} = 0$ disminuyó a poco menos de 0.7. Como contraparte, se obtiene una tasa de error de bits entre 0.2 y 0.3 para la región considerada del adversario, facilitándole el proceso de corrección con respecto a lo mostrado en las figuras 3 y 5. En la figura 8 se observa como es necesaria una correlación superior a 0.95 para obtener una reconciliación aceptable de la clave. Mientras tanto, el comportamiento en correspondencia con el accionar de un adversario no varía demasiado con respecto al mostrado en la figura 6, para los códigos BCH.

Revista Telemática. Vol. 18, No. 3, Septiembre-Diciembre, 2019, p.1- 10 ISSN 1729-3804

5. CONCLUSIONES

En este trabajo se muestra cómo es el desempeño de los códigos LDPC, BCH y Hamming en la implementación de la técnica secure sketch. Estos códigos pertenecen a tres familias de códigos distintas: lineales, cíclicos y polinomiales, respectivamente; por lo que su utilización confiere generalidad a la evaluación del desempeño de la técnica. Los principales parámetros empleados para evaluar dicho desempeño son: la tasa de error de bit, la reconciliación exitosa de la clave y la aleatoriedad de la clave reconciliada. Los resultados obtenidos muestran una proporcionalidad directa entre los valores de BER y SKR.

El desempeño de los códigos BCH y LDPC en un canal libre de ruido es superior al de los códigos Hamming, al corregir un mayor número de errores para altos valores de correlación, sin la necesidad de incrementar estos valores por la intervención de otros mecanismos en las etapas precedentes. La reconciliación exitosa de la clave en este escenario favorece la utilización de los códigos BCH sobre los códigos LDPC, debido a su velocidad para realizar este proceso. En un canal contaminado con AWGN, los códigos LDPC muestran un desempeño mayor en relación a los códigos BCH y Hamming, debido a su robustez ante el ruido. Esta característica les permite obtener una mayor eficiencia en términos de BER y SKR. La combinación de los códigos BCH y LDPC para implementar la técnica *secure sketch* en un canal contaminado con AWGN, muestra una reducción de la BER y una aproximación al comportamiento de los códigos BCH en un canal libre de ruido, con respecto a la SKR.

RECOMENDACIONES

A pesar de que los códigos usados en este trabajo ofrecen cierta generalidad en la evaluación de la técnica, es recomendable el uso de otros códigos, como pudieran ser los códigos Reed-Solomon. Otro aspecto de interés es el relacionado con las etapas de extracción de la aleatoriedad y cuantificación, para obtener claves reales en los extremos de la trasmisión, con el objetivo de implementar la etapa de reconciliación de la información mediante la técnica secure sketch, en un ambiente más realista. En adición, otros escenarios pudieran ser considerados, tales como diferentes tipos de canales (ej. canales simétricos), distintos tipos de ruido (ej. ruido negro, multiplicativo).

REFERENCIAS

[1] BRASSARD, Gilles and SALVAIL, Louis, "Secret-key reconciliation by public discussion," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 410-423, 1993.

[2] FRAGKIADAKIS, Alexandros; TRAGOS, Elias and TRAGANITIS Apostolos, "Lightweight and secure encryption using channel measurements," in *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014 4th International Conference on*, pp. 1-5, 2014.

[3] WANG, Qian; SU, Hai; REN, Kui and KIM, Kwangjo, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *INFOCOM, 2011 Proceedings IEEE*, pp. 1422-1430, 2011.

[4] ISLAM, Nazia; GRAUR, Oana; FILIP, Alexandra and HENKEL, Werner, "LDPC code design aspects for physical-layer key reconciliation," in *Global Communications Conference (GLOBECOM), 2015 IEEE*, pp. 1-7, 2015.

[5] DODIS, Yevgeniy; REYZIN, Leonid and SMITH, Adam, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International conference on the theory and applications of cryptographic techniques*, pp. 523-540, 2004.

[6] LI, Nan; GUO Fuchun; MU, Yi; SUSILO, Willy and NEPAL, Surya, "Fuzzy Extractors for Biometric Identification," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*, pp. 667-677, 2017.

[7] MOARA-NKWE, Kemedi; SHI, Qi; LEE Gyu Myoung and EIZA, Mahmoud Hashem, "A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks," *IEEE Access*, vol. 6, pp. 11374-11387, 2018.

[8] LINDELL, Y. and KATZ, J., *Introduction to modern cryptography*: Chapman and Hall/CRC, 2014.

[9] CASTEL, Thijs; VAN TORRE, Patrick and ROGIER, Hendrik, "RSS-based secret key generation for indoor and outdoor WBANs using on-body sensor nodes," in *International Conference on Military Communications and Information Systems (ICMCIS 2016)*, pp. 1-5, 2016.

[10] MCGUIRE, Michael, "Channel estimation for secret key generation," in *Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on*, pp. 490-496, 2014.

[11] GHOSAL, A.; HALDER, S. and CHESSA, S., "Secure key design approaches using entropy harvesting in wireless sensor network: A survey," *Journal of Network and Computer Applications*, vol. 78, pp. 216-230, 2017.

[12] YANG, Zhiliang; FAN, Yuanzhang and WANG, Aihua, "Artificial noise and LDPC code aided physical layer security enhancement," 2014.

[13] WEI, Yunchuan; ZENG, Kai and MOHAPATRA, Prasant, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Transactions on Mobile Computing*, vol. 12, pp. 1842-1852, 2013.

SOBRE LOS AUTORES

Mario Ramírez Méndez. Ingeniero en Telecomunicaciones y Electrónica, su área de investigación está enfocada en protocolos de comunicaciones y seguridad de la capa física, riomarezamir@gmail.com.

Yaime Fernández Jiménez. Ingeniera en Telecomunicaciones y Electrónica, M.Sc., Prof. Asistente del Departamento de Electrónica y Telecomunicaciones de la Universidad Central "Marta Abreu" de Las Villas, Villa Clara, Cuba, yaimefj@uclv.cu.

Vitalio Alfonso Reguera. Ingeniero en Telecomunicaciones y Electrónica, D.Sc., Jefe del Departamento de Electrónica y Telecomunicaciones de la Universidad Central de Las Villas, Villa Clara, Cuba, vitalioar@gmail.com.

An Braeken. M.Sc. en Matemáticas por la Universidad de Gent, 2002, D.Sc. en Ciencias de la Ingeniería por la Universidad KULeuven, en el grupo investigativo COSIC (Computer Security and Industrial Cryptography), Prof. en Universidad de Vrije, Departmento de Ciencias Industriales, Bruselas, Bélgica, an.braeken@vub.be.