Entreciencias
DIÁLOGOS EN LA SOCIEDAD DEL CONOCIMIENTO

Entreciencias 2 (3): 23–33, Abr. 2014
ISSN: 2007–8064

Ciencias Exactas e Ingenierías

www.entreciencias.enes.unam.mx

Codificación de red y sus aplicaciones

Network Codificatin and its applications

Recibido: 31 de agosto de 2013; aceptado: 7 de marzo de 2014

Francisco de Asís López Fuentes[1]
Universidad Autónoma Metropolitana - Unidad Cuajimalpa

Resumen

Este documento presenta una revisión general de una nueva técnica en el campo de la teoría de la información, llamada "codificación de red". La codificación de red se presenta como una técnica prometedora y de activa investigación en la teoría de redes. Diversos beneficios relacionados al flujo de información, tales como un óptimo aprovechamiento del ancho de banda y la reducción de retardos en redes de extremo a extremo han sido reportados en la literatura. Nuestro trabajo en este documento se enfoca principalmente a los siguientes aspectos de codificación de red: planteamiento del modelo, áreas de aplicación y beneficios obtenidos al usar esta técnica. Los aspectos discutidos en este trabajo cubren tanto a las redes fijas como móviles. El objetivo de este artículo es mostrar al lector la relevancia y potencial de esta técnica y las aplicaciones que se están desarrollando a su alrededor.

Palabras clave: teoría de la información, redes de computadoras, codificación de red, rendimiento

Abstract

This paper presents an overview of a new technique in the field of information theory called network coding. Network coding has become a promising and active research topic in networking. Several benefits related to the flow of information such as the optimal use of bandwidth and reduced delays in end-to-end networks have been reported in literature. Our work in this paper focuses mainly on the following aspects of network coding: model approach, application areas and benefits obtained by using this technique. The issues discussed in this paper cover both fixed and mobile networks. The aim of this paper is to show the reader the importance and potential of this technique and the applications being developed around it.

Keywords: Information theory, computer networks, network coding, throughput.

Introducción

Desde que Ahlswede *et al*., (2000) introdujeron la técnica de codificación de red en el campo de la teoría de la información, diversos avances en las redes de comunicación se han desarrollado basados en estos principios. La codificación de red permite a los nodos intermedios codificar los paquetes recibidos, y no únicamente reexpedirlos. Este avance resulta deseable ya que introduce diversos beneficios, principalmente la mejora del rendimiento, la escalabilidad y la robustez del sistema (Tuninetti y Fragouli, 2004). Esto ha generado un gran debate entre la codificación de red y la técnica tradicional de almacenamiento y reexpedición. Diversas investigaciones que muestran los beneficios de la codificación de red han sido publicadas en la literatura. Las áreas en las que se ha estudiado codificación de red son: Mesh, VANET, MANET, Ad-Hoc, redes de sensores, almacenamiento distribuido, seguridad, etc. A pesar de esta amplia gama de aplicaciones, la codificación de red todavía es un área emergente.

La intención de este documento es ofrecer una descripción de la parte teórica de la codificación de red, así como las diversas aplicaciones que han emergido para explotar

[1] Doctor en Ingeniería Eléctrica y Tecnologías de la Información por la Universidad Técnica de Munich (TUM). Es Maestro en Ciencias Computacionales con especialidad en Redes de Computadoras e Ingeniero Industrial en Eléctrica. Actualmente es Profesor-Investigador en la Universidad Autónoma Metropolitana-Unidad Cuajimapa. Sus áreas de interés actual son redes de computadoras, tecnología multimedia y sistemas distribuidos.

sus beneficios, tanto para redes fijas como móviles.

Este documento se encuentra organizado en cuatro secciones.En la primera se introduce la parte teórica de codificación de red. Un análisis sobre los trabajos realizados, que incluyen los retos, resultados y beneficios obtenidos se muestran en la sección 2. En el apartado 3 se cuestiona acerca de sobre qué nodos se puede aplicar codificación de red para obtener un mejor desempeño de la red. Finalmente se presentan las conclusiones.

Codificación de red

Idea principal

"Codificación de red" fue originalmente propuesto por Ahlswede *et al.* (2000). En este trabajo, los autores discuten un nuevo problema en las redes de comunicaciones relacionado con el flujo de información. Se declara que no es óptimo considerar una distribución *multicast* como un simple flujo, sino que se debe permitir la codificación en los nodos intermedios de la red, con el fin de aumentar el flujo, sin sobrepasar la capacidad del canal. Para este estudio, la red es representada como un grafo dirigido, $G = (V; E)$ donde los vértices V representan los nodos, mientras que los enlaces E representan a los canales de comunicación. Los autores inspiran su trabajo en el teorema de máximo flujo-mínimo corte de la teoría de grafos, que enuncia Bollobás (1979:47): "El valor del flujo máximo de una fuente a un destino , es igual al valor mínimo de las capacidades de los cortes que separa la fuente del destino."

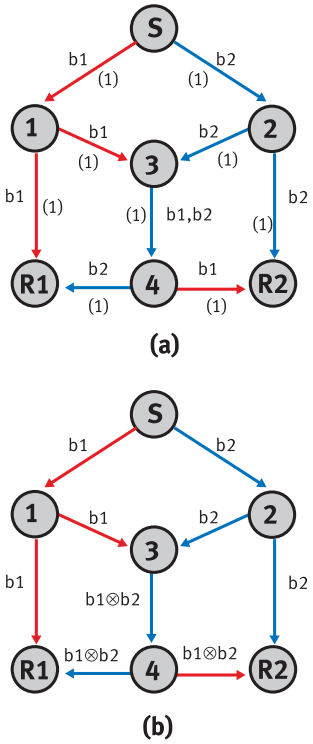
Para comprender mejor este teorema Ahlswede *et al.* (2000) (figura 1(a)) presentan un escenario formado por un nodo fuente y dos nodos receptores, donde la capacidad de cada canal de comunicación (indicado entre paréntesis) es de 1 bit/unidad de tiempo. Se puede observar que los valores del máximo flujo de S a cualquier receptor, ya sea a R1 o $R2$ es igual a dos, pero de manera independiente. Por lo tanto, cuando se quieren transmitir dos bits simultáneamente a $R1$ y $R2$, no es posible porque el canal de comunicación entre el nodo 3 y nodo 4 solamente puede transmitir un bit.

Por otro lado, la figura 1 (b), muestra la misma configuración de red, sólo que ahora utilizando codificación de red, donde el operador "⊗", denota la suma módulo 2. De esta forma, el receptor $R1$ puede recuperar los dos bits, $b1$ y $b2$. Solo que $b2$ se debe recuperar de $b1 \otimes b2$. De la misma manera, $R2$ puede recuperar los dos bits. En este ejemplo, codificación de red es aplicado en el nodo 3. Otro punto importante a observar es que la tasa *multicast* se incrementa, ya que para la transmisión tradicional es de 1 bit/unidad de tiempo, mientras que utilizando codificación de red la tasa aumenta a 2 bits/unidad de tiempo.

Basados en este análisis, los autores sugieren que cuando existe más de un receptor, los paquetes deben ser codificados por los nodos intermedios. Esto se debe a que la codificación de red optimiza la difusión. Ahlswede *et al.* (2000) declaran que en la teoría clásica de información, si las fuentes de información son independientes entre sí, lo óptimo se puede lograr realizando codificación de las fuentes por separado, este método es conocido como "codificación por superposición". Sin embargo, el método de superposición no es el mejor y mucho menos cuando dos fuentes de información son generadas en el mismo nodo.

Entre las ventajas que se reportan del uso de codificación de red, se encuentra el ahorro de ancho de banda, incremento del *throughput* y la reducción en los retardos.

Figura 1. Red de comunicaciones (a) tradicional y (b) aplicando codificación de red



Fuente: elaboración propia con base en Ahlswede, *et al*,2000

Codificación

La codificación de red ha generado diversas propuestas de esquemas de codificación. Algunas de estas propuestas consideran una codificación lineal sobre un campo finito, mientras que otras realizan una codificación lineal aleatoria, además de proponer un nuevo formato de paquete y un nuevo modelo del buffer. Li, Yeung y Cai (2003) muestran un esquema de codificación lineal sobre un campo finito. Este esquema asume que sobre los flujos de entrada de un nodo se realiza una combinación lineal, para así obtener los flujos de salida. Los coeficientes de la combinación son obtenidos de un campo finito. Este esquema de codificación ofrece un costo computacional bajo y puede ser aplicado tanto para redes cíclicas como acíclicas.

Un esquema donde no es necesario el conocimiento centralizado de la red, es el propuesto en Chou, Wu y Jain (2003). Para este fin, un nuevo formato de paquete es introducido, el cual consiste de un vector de codificación global y la carga útil, que se encuentra dividido en campos de tamaño de 2^8 o 2^{16}, es decir cada símbolo es de 8 o 16 bits. Este esquema considera un grafo acíclico, donde cada enlace es de capacidad unitaria, con una fuente y un conjunto de receptores. Cada nodo recibe paquetes que son combinaciones lineales de los paquetes fuente y los almacena en una matriz. Dentro de cada paquete se incluye un vector de codificación, de tal manera que cualquier receptor puede recuperar los vectores fuente usando eliminación gaussiana sobre el vector de los paquetes recibidos. Los paquetes que van llegando a los nodos receptores sobre los enlaces de entrada, podrían encontrarse con paquetes con el mismo vector fuente. A estos paquetes se les conoce como "paquetes de la misma generación", y son etiquetados con un mismo número de generación. Esto, con el propósito de sincronizarlos, y así afrontar problemas de retardo o encolado cuando los paquetes viajan sobre diferentes enlaces. Los autores emplean la política de "vaciar la generación actual antes de que llegue la siguiente", la cual nos indica que se tienen que atender los paquetes de la misma generación existentes antes de poder atender a otros paquetes de otras generaciones. Este esquema reporta diferentes beneficios, tales como que los nodos receptores puedan decodificar sin conocer la topología de la red, y los vectores de codificación son aleatorios y variables en el tiempo. Sin embargo, este esquema requiere transmitir símbolos extras en cada paquete para realizar la decodificación.

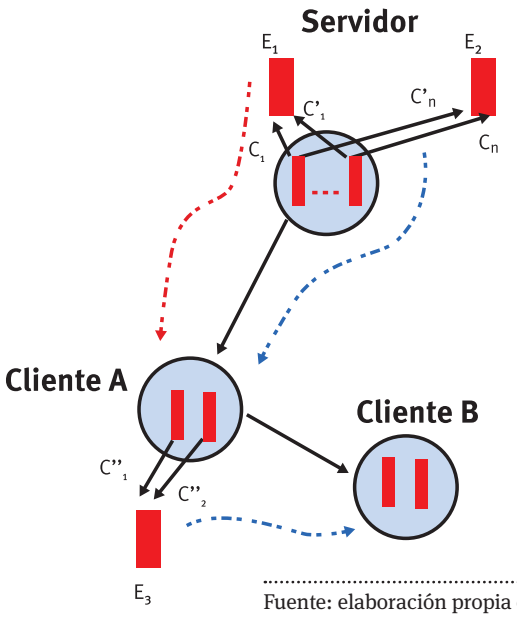
Aplicaciones de codificación de red

La codificación de red ha impactado en diversas áreas de las redes de comunicación. En este documento, hemos clasificado estas áreas como: distribución de contenidos, redes inalámbricas, redes de sensores y seguridad en la red.

Distribución de contenidos

La distribución de contenido ha migrado recientemente de un enfoque centralizado hacia un enfoque distribuido. En este nuevo enfoque, las computadoras personales son utilizadas en forma de red cooperativa, con el fin de compartir recursos, tales como memoria, ancho de banda, etc. Estos sistemas son conocidos como "sistemas finales", porque todas las funciones del sistema recaen en los extremos. Existen diversos esquemas sobre distribución de contenido basado en los sistemas finales. Un ejemplo es BitTorrent (Cohen, 2003), que divide el archivo en bloques pequeños y permite a los usuarios descargar los bloques de forma paralela de diferentes nodos. Aunque BitTorrent es un esquema prometedor, todavía tiene cierta limitante, tal como la disminución del desempeño del sistema. Algunos investigadores ven

Figura 2. Esquema de la propuesta de Gkantsidis y Rodríguez (2005)



Fuente: elaboración propia con base en Gkantsidis y Rodríguez

en la codificación de red una herramienta para mejorar el *throughput* además de aumentar la probabilidad de recepción de los paquetes.

Gkantsidis y Rodríguez (2005) introducen un novedoso esquema de distribución de contenidos a gran escala basado en codificación de red. En este esquema, el archivo original es dividido en *k* bloques, y cada bloque es cargado a diferentes clientes, de manera aleatoria. En seguida se eligen coeficientes aleatorios $c_1,\ldots,c_n$, los cuales se multiplican con el bloque *i* correspondiente. De esta forma, los nodos clientes funcionan como servidores de otros nodos que requieran el bloque para reconstruir el archivo original. Este escenario se muestra en la figura 2. Al inicio, se asume que los clientes no contienen ningún bloque. El cliente *A* contacta al servidor para solicitar un bloque. Entonces el servidor combina todos los bloques del archivo y crea un bloque codificado E_1, donde primero se crean coeficientes aleatorios $c_1,\ldots,c_n$ y se multiplica cada elemento del bloque *i* con c_1. Entonces, el servidor envía al usuario *A* el resultado de la suma y el vector de coeficientes $j = c\ i$. En seguida el mismo cliente *A*, requiere de otro bloque codificado E_2, entonces se realiza la misma operación anterior. Si el cliente A requiere transmitir el bloque codificado E3 al usuario *B*, en seguida se hace una combinación lineal de los bloques *E1* y E2, entonces el cliente A genera coeficientes aleatorios c''_1 y c''_2, multiplica el bloque *E1* con c''_1 y de manera similar hace lo mismo con el bloque E2 y suma el resultado de las multiplicaciones. Si un nodo conoce los coeficientes de sus vecinos, puede saber qué nodos le pueden proporcionar nuevos bloques. También un nodo puede recuperar el archivo original después de recibir *k* bloques. El modelo es evaluado bajo un ambiente con nodos dinámicos. El modelo propuesto incrementa el *throughput* del sistema en alrededor de 30%, hay mayor probabilidad de reusar los bloques y la velocidad de distribución mejora. En este trabajo los autores no involucran el costo de codificar/ decodificar durante la codificación de red.

Un esquema que involucra los costos de codificar y decodificar es el propuesto en SmartCode (Ma *et al.*, 2009). Este esquema cuenta con un novedoso módulo de pre-control, el cual funciona de la siguiente manera. Supongamos que se tienen el *peer A* y el *peer B*. El *peer B* envía un mensaje de petición al *peer A*, entonces el *peer A* genera un paquete código, que cuenta con un vector de coeficientes y un paquete codificado. Primero el vector de coeficientes es enviado al *peer B*, el cual cuenta con una matriz de todos los vectores de coeficientes de los paquetes recibidos. En seguida, el vector de coeficientes recibido se compara con los vectores de la matriz, si es linealmente dependiente, se elimina este nuevo vector de coeficientes, en otro caso, el *peer B* envía otro mensaje al *peer A*, para indicarle que le puede enviar el paquete codificado. SmartCode es evaluado en la infraestructura PlanetLab (Planet-Lab, 2007) y comparado con otros esquemas. Los resultados muestran que SmartCode mejora el tiempo promedio de descarga en alrededor de 15% comparado con otros esquemas. Sin embargo, SmartCode también requiere enviar paquetes extras que son el vector de coeficientes. Asimismo, el *peer* que actúa como servidor tiene que esperar cierto tiempo antes de enviar el paquete codificado, y el envío de paquetes pequeños incrementan los tiempos de descarga.

Nguyen, Nguyen y Cheung (2010b) presentan Chameleon, un algoritmo para video en red P2P que combina codificación de red y codificación de video escalable (SVC). SVC da prioridad a los paquetes de video y maneja diferentes niveles de calidad de video. Por otra parte, la codificación de red trata a los paquetes por igual, para facilitar su entrega. Combinar ambas técnicas no es una tarea sencilla. Para este propósito, los autores aplican codificación de red de forma aleatoria sobre las diferentes capas de video. Chameleon es evaluado y comparado con FABALAM (Liu, Dou y Liu, 2004), en términos de tasa de repetición de saltos y calidad promedio obtenida. Para esta evaluación, se utilizan diferentes capacidades de ancho de banda, que identifican diferentes niveles de calidad. Los autores encuentran que si la codificación de red no es usada, entonces cuando un *peer* envía un paquete al receptor, este paquete debe ser recibido exactamente por el nodo al que fue enviado. Por otro lado, si la codificación de red es usada, el receptor puede recibir cualquier bloque, siempre y cuando dicho bloque sea linealmente independiente con los bloques que ha recibido hasta ese momento. También observan que el desempeño del sistema mejora.

Otro esquema que busca minimizar la redundancia de almacenamiento y utilizar al máximo el ancho de banda es "codificación de red jerárquico" propuesto por (Nguyen, Li y Eliassen, 2010a). Este esquema utiliza un flujo de video escalable y además trabajan sobre el

protocolo de transporte TCP. Este esquema aumenta la probabilidad de que la información más importante se encuentre disponible en los servidores, en este caso, la capa base del video es considerada como la información más importante. Esto se logra primero dividiendo el flujo de video en un número extenso de pedazos, donde cada uno contiene bits de todas las capas, después, dentro de cada pedazo se generan paquetes que contienen bits de la misma capa. Usando este esquema de codificación, la probabilidad de recuperar los paquetes de la capa base es mayor en comparación con otras capas. Aunque este esquema es prometedor, está lejos de ser óptima ya que solo logra ser eficiente para ciertos escenarios.

Redes inalámbricas

Otra área de aplicación de codificación de red han sido las redes inalámbricas. Este tipo de redes, presentan aún grandes retos, tales como pérdidas debido al ruido, al desvanecimiento de la señal y por la obstrucción con objetos, etc. Codificación de red ha emergido como una solución prometedora para esta área y diversos beneficios han sido reportados en la literatura. Ejemplos de algunos beneficios son el aumento del *throughput*, el incremento en la probabilidad de entrega, es decir las pérdidas disminuyen y existe una mayor velocidad de entrega.

Al Hamra, Barakat y Turletti (2006) han investigado acerca de los beneficios de usar codificación de red en redes Mesh inalámbricas. Para este fin, los autores desarrollaron diferentes estrategias de reenvío entre nodos, tales como: reenvío a ciegas, reenvío a ciegas con codificación de red, reenvío selectivo y reenvío selectivo con codificación de red. Para evaluar estas estrategias, los autores implementaron su modelo en un simulador basado en C++, el cual permite observar paso a paso la distribución del archivo. El esquema es evaluado en términos de tiempo de servicio, paquetes transmitidos y paquetes no útiles. Entre los resultados importantes de este trabajo, se concluye que hay que considerar varios factores dentro de la red, para que la codificación de red muestre beneficios. Por ejemplo, si se utiliza una buena estrategia de cooperación como reenvío selectivo y existen buenas condiciones de la red, entonces la codificación de red no es necesaria. En contraste, si la estrategia de cooperación es mala y las condiciones de la red también, entonces codificación de red resulta ser una excelente herramienta para mejorar el desempeño del sistema.

Codificación de red también se ha implementado sobre las redes MANET (Mobile Ad-Hoc Network). Este tipo de redes son sistemas autónomos de nodos móviles conectados por enlaces inalámbricos. Cada nodo no sólo opera como un sistema final, sino que también como un enrutador para retransmitir los paquetes. Los nodos son libres de moverse y se organizan entre ellos mismos en la red. Las MANET no requieren de una infraestructura fija tales como estaciones base y entre sus características sobresalientes, se encuentran lo dinámico de sus topologías y la capacidad reducida de ancho de banda. Sin embargo, son particularmente vulnerables a ataques por negación de servicio lanzado por un nodo intruso.

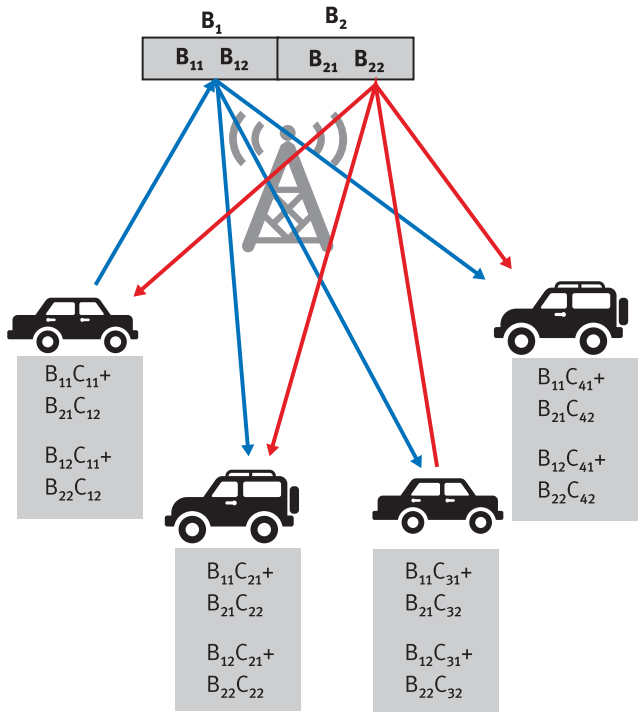
Un proyecto realizado sobre este tipo de redes es presentado por Park *et al.*, 2006 que proponen un nuevo protocolo llamado "CodeCast". Este esquema propone un modo de seleccionar subgrafos que son adecuados para las redes MANET bajo el estándar *IEEE* 802.11. El principal objetivo de CodeCast es controlar las pérdidas mientras que conserva la latencia *multicast*, esto con ayuda de la recuperación de pérdidas y la diversidad de rutas existentes. En este proyecto el término "latencia *multicast*" es considerado como la suma de los retardos dentro de la red. CodeCast es evaluado usando el simulador de redes (Qual-Net, 2000). En esta evaluación, los autores ponen una especial atención sobre el protocolo ODMRP (*On Demand Multicast Routing Protocol*), debido a que este protocolo ha demostrado tener un buen desempeño para canales móviles (Park *et al.*, 2006). Los resultados muestran que CodeCast realiza una razón de entrega cerca de 100%, mientras que ODMRP se encuentra en 94%, donde "razón de entrega" es definida como la relación entre los paquetes recibidos y los paquetes enviados. Con respecto a los retardos de extremo a extremo, CodeCast muestra un incremento debido a que a la fuente le toma tiempo realizar la codificación sobre un conjunto de paquetes. Cuando diferentes receptores son considerados, CodeCast alcanza una tasa de entrega cercana a 100%, mientras que ODMRP se encuentra muy por debajo de este umbral.

Otra aplicación de codificación de red, en el campo de las comunicaciones inalámbricas, apunta a la tecnología automotriz llamada "VANET" (Vehicular Ad-Hoc Networks). El objetivo de esta tecnología es desarrollar plataformas de comunicación entre vehículos en movi-

miento. Para lograr esto se explotan las capacidades de cómputo, además de las comunicaciones inalámbricas con que cuentan actualmente los automóviles. Las redes cooperativas sobre VANET son un gran desafío, debido a que los nodos se encuentran en constante movimiento, lo que provoca su frecuente desconexión.

Ahmed y Kanhere (2006) presentan un esquema de distribución de contenido sobre VANET, llamado "VANETCODE". Este novedoso esquema se encuentra basado en codificación de red. Este esquema asume que el archivo se encuentra en una puerta de enlace estática. La puerta de enlace actúa como un servidor, el cual divide al archivo en *k* bloques. Este servidor produce una combinación lineal de los k bloques, usando coeficientes aleatorios. Esta técnica de codificación es tomada de Gkantsidis y Rodríguez (2005). El funcionamiento de este protocolo se muestra en figura 3. Dentro del rango de comunicación de la puerta de enlace se encuentran los vehículos A, B, C y D. La puerta de enlace se dispone a compartir los bloques B_1 y B_2, los cuales han sido divididos en dos elementos, que son B_{11}, B_{12} y B_{21}, B_{22}. Suponemos que los vehículos requieren de estos bloques, para ello la puerta de enlace selecciona aleatoriamente los coeficientes para codificar todos los bloques, en este caso los coeficientes son C_{11} y C_{12}. Para generar los bloques codificados se multiplica B_{11} con C_{11} y B_{21} con C_{11}, en seguida se suma el resultado para crear el primer elemento del bloque codificado. Se realiza la misma operación para los demás elementos. Una vez que los bloques han sido codificados, la puerta de enlace envía los bloques a los vehículos correspondientes. Para la decodificación de los bloques, se requiere que los nodos obtengan suficientes bloques con coeficientes linealmente independientes, con el fin de resolver el conjunto de ecuaciones lineales. Otros puntos importantes a considerar es el tiempo de conexión entre los nodos y la puerta de enlace debe ser sumamente pequeño, asimismo se debe considerar un tiempo pequeño para la codificación de los bloques. Esto es con el objetivo de que cada nodo obtenga los bloques necesarios, y pueda recuperar el archivo.

Figura 3. Codificación y decodificación de la compuerta de enlace



Fuente: elaboración propia en base en Ahmed *et al.*, 2006

Otro ejemplo de codificación de red sobre redes inalámbricas es el propuesto por Sundararajan *et al.* (2009) para incidir en el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol). En este modelo los autores introducen una nueva capa, entre la capa de transporte (TCP) y la capa de red (IP). Aquí el control de congestión no es modificado. Un cambio importante introducido radica en la fuente, ya que cuando se encuentre lista para transmitir, envía una combinación lineal aleatoria de todos los paquetes que se encuentren en la ventana de congestión. No obstante, existe un gran problema, TCP opera con paquetes que tienen un orden específicamente definido. Sin embargo, cuando se realiza la codificación de todos los paquetes en la ventana de congestión, se pierde el orden. Para afrontar este problema, los autores proponen un novedoso algoritmo que involucra codificación de red en la fuente y el receptor. Los autores evalúan su protocolo en términos de equidad, *throughput* y tasa de pérdidas. Los resultados muestran que el *throughput* tiene un ligero incremento cuando se aplica TCP con codificación de red. Otro punto importante, es que TCP falla cuando las pérdidas se incrementan, mientras que TCP con codificación de red muestra una mayor robustez.

Redes de sensores

Actualmente, la tecnología nos ha permitido crear redes de sensores inalámbricos. Este tipo de red inalámbrica

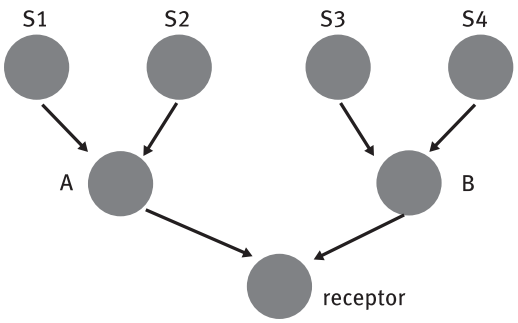
consiste en dispositivos autónomos que se encuentran distribuidos y que utilizan sensores para un estudio frecuente de las condiciones de cierto sistema en particular. Los nodos distribuidos se comunican de manera inalámbrica con un nodo central, al cual se le entregan los datos obtenidos para ser analizados. Esta es otra de las áreas en la cuales se ha aplicado codificación de red. Entre los beneficios reportados se encuentra una excelente técnica para la recuperación de errores, disminución sobre el consumo de energía y aumento del *throughput*, etc.

Un esquema de codificación de red para redes de sensores bajo el agua es presentado en Guo *et al.* (2006). En este tipo de redes, se busca tener un eficiente esquema de recuperación de errores, sólo que esto se dificulta, existen en gran tasa, además de grandes retardos de propagación. Otro problema está relacionado con la batería de los sensores, ya que se debe conservar la energía de los nodos para mantenerlos activos en la red. El esquema de codificación de red que se necesita para este tipo de redes debe encontrar un balance entre la cantidad de redundancia y la conservación de la potencia de los nodos de la red.

El esquema de codificación de red que los autores proponen se encuentran inspirado por un trabajo realizado por Ho *et al.* (2003), principalmente por su simplicidad. Por "simplicidad", los autores consideran una red con una fuente y un receptor. Las rutas son determinados por el protocolo de enrutamiento *vector-based forwarding* (VBF). En un principio, la fuente cuenta con k paquetes, definidos como $X_1,...,X_k$. La fuente realiza una combinación lineal de estos paquetes, para obtener los paquetes de salida k', definidos como $Y_1,...,Y_k$' . El conjunto de coeficientes es conocido como el vector de codificación para los paquetes Y_i. Usando esta estrategia, la decodificación en el receptor es sumamente sencilla, ya que el receptor recibe k paquetes, además de los vectores de codificación que son linealmente independientes. Los k paquetes originales pueden ser recuperados por medio de una matriz de inversión. Cuando existen múltiples fuentes y múltiples receptores, a cada nodo se le asigna un ID (identificador), el cual indica la generación. De esta manera los nodos intermedios sólo aplican codificación de red a los paquetes de la misma generación. Los autores evalúan el desempeño de su modelo en términos de calidad de recuperación del sistema ante errores y el consumo de energía. Los autores concluyen que la codificación de red es una técnica eficiente para la recuperación de errores.

SenseCode es otro trabajo en redes de sensores, presentado por (Keller *et al.*, 2009), en el que se involucra codificación de red. En este trabajo los autores muestran que codificación de red proporciona una medida de balance entre la eficiencia de la energía y confiabilidad. El término confiabilidad, los autores lo definen como la fracción promedio de los mensajes que son enviados correctamente al receptor en cada ronda. En este modelo codificación de red es usado como una nueva forma de comunicación de múltiples caminos, en donde cada nodo difunde su información a través de los caminos disponibles, sin tener que descubrir o monitorear estos caminos. La operación del modelo es ilustrada en figura 4.

Figura 4. (a) Esquema SenseCode, (b) paquetes a enviar por cada nodo.



(a)

Nodo	Información a enviar
S_1	$X_{1_i}+X_1+X_2+X_3$
S_2	$X_{2_i}+X_1+X_2$
S_3	$X_{3_i}+X_1+X_3+X_4$
S_4	$X_{4_i}+X_3+X_4$
A	$X_{1_i}+X_{2_i}+X_{3_i}+X_1+X_4$
B	$X_{3_i}+X_{4_i}+X_1+X_2+X_3$

(b)

Fuente: elaboración propia con base en Keller *et al.*, 2009)

En este escenario se considera una red con varias fuentes, en donde cada fuente Si requiere de enviar un mensaje x_i al receptor (figura 4(a)). La forma en la que las fuentes envían los paquetes a los receptores, son resumidos en la figura 4(b). Supongamos que los paquetes, que llegan al nodo A se pierden, por alguna razón. Entonces, en el receptor tan sólo llegan los cuatro paquetes enviados por el nodo B, los cuales contienen cuatro com-

binaciones linealmente independientes, de los cuatro mensajes x_i. De esta forma, el receptor genera un sistema de ecuaciones, de donde se pueden recuperar los cuatro mensajes originales. En este ejemplo, la confiabilidad es de uno, ya que los mensajes son recuperados, a pesar de que los paquetes en el nodo *A* son perdidos. Existe un costo en este esquema, que es el envío extra de paquetes en la red, esto se puede ver en el ejemplo, ya que para lograr cierta confiabilidad se tuvieron que enviar 2x4 paquetes extras. SenseCode es evaluado y comparado con el protocolo CTP (Collection Tree Protocol) (Gnawali *et al*., 2009), sobre la plataforma TOSSIM (Levis *et al*., 2003). Los parámetros a evaluar son la confiabilidad y la energía de transmisión. La confiabilidad se refiere a la información útil que llega al receptor, mientras que la energía de transmisión se refiere a la cantidad de energía gastada durante la transmisión de paquetes de cada nodo. SenseCode demuestra poder alcanzar un nivel mayor de robustez, además de una gran confiabilidad comparada a CTP.

Seguridad en la red

Un área donde apunta la codificación de red actualmente es la seguridad en las redes. Diversos trabajos han intentado aplicar codificación de red para ofrecer una mayor seguridad en los datos, además de reducir el encabezado de los paquetes. Un esquema donde se usa codificación de red para diseñar una arquitectura de seguridad en la transmisión de video sobre redes inalámbricas es propuesto por Lima *et al.* (2010). En términos generales, este esquema consiste en lo siguiente. Por cada grupo de imágenes (GOP), se genera una matriz triangular *A*, de tamaño *n x n*, que sirve para codificar en la fuente. El valor de *n* representa el número de cuadros existentes en el GOP. Los elementos de esta matriz son generados sobre un campo finito. En seguida cada GOP es dividido en vectores llamados *plaintext*, en donde el primer elemento de cada vector pertenece a cada uno de los cuadros. El término *plaintext* es considerado como los datos originales a enviar, en este caso corresponden a los GOP. En seguida los vectores *plaintext* son encriptados, con el fin de obtener una mayor seguridad, además de ser un estándar en la seguridad multimedia. El siguiente paso es obtener la carga útil, realizando el producto de la matriz triangular *A* con el vector *plaintext*. Los coeficientes de la matriz *A* son encriptados para después colocarlos en la cabecera de los paquetes, seguidos de una matriz identidad *I* que indican el orden de las capas. Esta matriz *I* se encuentra desencriptada. Al final de cada paquete se encuentra la carga útil. Los autores evalúan su modelo para un escenario inalámbrico con pérdidas. Los resultados reportan que se tiene un menor tamaño de los paquetes encriptados en comparación con el método de encriptación tradicional, la probabilidad de pérdida es menor, lo que permite obtener una mejor calidad del video.

Otro trabajo que usa codificación de red para cuestiones de seguridad, es el presentado por Oliveira y Barros (2008). Este trabajo presenta un esquema de distribución de claves secretas, sobre una red de sensores, en donde explotan la existencia de un nodo móvil. Las ventajas de este esquema son las siguientes: un número pequeño de claves son almacenadas en cada nodo, un número pequeño de transmisiones son requeridas y baja complejidad de procesamiento. Este esquema garantiza la seguridad con probabilidad de uno (Oliveira y Barros, 2008). El esquema basa su operación en el nodo móvil. Antes de que el nodo sea implementado, se generan K_i claves cada una con su respectivo identificador *i*. Enseguida, se produce una secuencia binaria llamada *R*, que tiene un tamaño igual a la clave. Después, los datos generados son almacenados en el nodo *S*, sobre una lista, usando todos los identificadores *i* y la encriptación de la clave $K_i \otimes R$. Por último, a cada nodo se le asignan *c* claves, las cuales indican el número de claves que el nodo utilizará durante toda su vida. Cada clave tiene asociado su correspondiente identificador *i*. Después de que el nodo móvil es implementado, este se encarga de enviar un mensaje de "hola", a los nodos que se encuentran a su alcance, los cuales responden con su identificador. De esta manera el receptor obtiene los identificadores. Así, el identificador *i(A)* corresponde al nodo *A* y el *i(B)* corresponde al nodo *B*. Después el nodo *S* realiza las operaciones de codificación de red sobre las correspondientes claves protegidas. De esta manera se cancelan las secuencias binarias R's y sólo son se envía $K_i(A) \otimes K_i(B)$, permitiendo que los receptores puedan recuperar las claves fácilmente. Una vez terminado este proceso, los nodos *A* y *B*, pueden comunicarse por medio de las claves obtenidas. El nivel de seguridad del sistema es determinado por medio de la vulnerabilidad, considerando si el nodo móvil es el único de un posible ataque.

Además, los requerimientos generales del sistema son determinados en función de la memoria.

Un esquema donde se explota la interacción entre codificación de red y la criptografía tradicional es Secure Practical Network Coding (SPOC) (Vilela, Lima y Barros, 2008). Entre algunas de las ventajas de SPOC se encuentran la reducción del encabezado de los paquetes en comparación con los métodos de encriptación tradicionales. El esquema SPOC propone lo siguiente. Primero, se generan dos tipos de coeficientes que son: *a)* coeficientes abiertos, los cuales son obtenidos de una matriz identidad, y *b)* coeficientes cerrados, que se utilizan para la codificación/decodificación, y son encriptados con las claves que se encuentran en el destino. Estos dos tipos de coeficientes son concatenados a la cabecera de cada paquete. La generación de coeficientes es ejecutado sobre los nodos intermedios de la red, siguiendo el mismo patrón sobre la mezcla de paquetes propuesta por Ho *et al.* (2006). El nodo fuente genera los coeficientes cerrados aleatoriamente y los encripta con las claves que comparte con los nodos receptores. Sobre los nodos intermedios, se realiza la operación de codificación de red, los cuales no distinguen entre coeficientes libres o cerrados. Cuando en los nodos receptores llega suficiente información, recuperan los coeficientes cerrados, teniendo en cuenta la transformación que estos sufrieron y se desencriptan. Finalmente los nodos receptores obtienen el mensaje original por medio de eliminación Gaussiana. SPOC reporta una mejor eficiencia en comparación con la encriptación tradicional de extremo a extremo, también se reduce el volumen de datos a ser encriptados, esto se debe a que los coeficientes cerrados son incluidos en cada paquete.

¿Dónde usar codificación de red?

Es importante saber en qué nodos de la red se puede implementar codificación de red, debido a que en algunos escenarios podría perjudicar más que beneficiar, de manera que exista un incremento en los retardos, decrezca el *throughput*, etc.

Motivados por esta cuestión, Cleju, Thomos y Frossard (2010) han propuesto un algoritmo, para la efectiva implementación de codificación de red en los nodos de la red. El objetivo es la reducción de los retardos y la cantidad de paquetes duplicados, así como la maximización de la cantidad de paquetes innovadores en la red. Los autores manejan como paquetes innovadores, los paquetes que llevan información nueva. Este problema de seleccionar los nodos que implementan codificación de red, es conocido como un problema NP-complejo (Cleju, Thomos y Frossard, 2010). Los autores proponen dos algoritmos que son: información global e información local. El algoritmo de información global es completamente centralizado, está diseñado para calcular el número de paquetes duplicados en el nodo cliente. Este algoritmo calcula los cambios que permiten aprovechar al máximo el incremento de la tasa innovadora de paquetes en los clientes. De esta forma, se seleccionan k nodos que pueden implementar codificación de red. En el algoritmo de información local, cada nodo tiene una vista local de la red. El objetivo de este algoritmo es calcular los beneficios obtenidos al reemplazar los nodos de almacén a reexpide por nodos que implementen codificación de red. Esto lo hace ejecutando el algoritmo en cada nodo vecino. Los autores concluyen que para ambos algoritmos, se puede alcanzar el mismo *throughput* en comparación con una red en donde todos los nodos implementan codificación de red, con tan sólo elegir adecuadamente algunos nodos que lo implementen.

El uso de codificación de red se ha extendido a otras aplicaciones tales como flujo de video en redes de comunicación inalámbricas (Gheorghiu *et al.*, 2010), (Oh y Kim, 2013), o para almacenamiento distribuido (Dimakis *et al.*, 2010). Recientemente, en noviembre de 2013, la IRTF (Internet Research Task Force) constituyó el NWCRG (Network Coding Research Group). Este grupo tiene como objetivo investigar principios y métodos de codificación de red que puedan ser benéficos a las comunicaciones en Internet (IRTF, 2014).

Conclusiones

Desde el surgimiento de codificación de red, diversos trabajos han sido propuestos. En la mayoría de los casos, el uso de codificación de red permite que los sistemas de comunicación alcancen un mejor desempeño en parámetros tales como el incremento del *throughput*, la disminución en la pérdida de paquetes, la eliminación de retardos, así como el incremento de la seguridad en las redes. Este artículo pretende mostrar al lector la re-

levancia de la codificación de red, así como de algunas aplicaciones potenciales que se están desarrollando alrededor de esta técnica. A pesar de que esta nueva técnica ha logrado introducirse en diferentes áreas, resulta de suma importancia el seguir realizando diversos estudios, ya que codificación de red promete muchos beneficios. Una de estas direcciones a considerar podría ser sobre la transmisión de paquetes multimedia en tiempo real en dispositivos móviles. También la aplicación de codificación de red en cuestiones de seguridad presente una prometedora área de oportunidad.

Referencias

Ahlswede, R., Cai, N., Li, S. y Yeung, R. W. (2000). Network Information Flow. *IEEE Trans. on Information Theory*, 46, 1204-1216.

Ahmed, S. & Kanhere, S. S. (2006). VANETCODE: Network coding to enhance cooperative downloading in vehicular ad hoc networks. *International Conference on Wireless communications and mobile computing (IWCMC 2006)*. 527-532.

Al Hamra, A., Barakat, C. y Turletti, T. (2006). Network Coding for Wireless Mesh Networks: A Case Study, *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 103-114.

Bollobás, B. (1979). *Graph Theory, An Introductory Course*. Nueva York: Springer-Verlag.

Chou, P., Wu, Y. y Jain, K. (2003). Practical Network Coding. *51st Allerton Conf. Communication, Control and Computing*. Monticello..

Cleju, N., Thomos, N. & Frossard, P. (2010). "Network coding node placement for delay minimization in streaming overlays", *IEEE International Conference on Communications (ICC)*. pp. 1-5. Cape Town, South Africa.

Cohen, B. (2003). Incentives build robustness en BitTorrent. *1st Workshop on Economics of Peer-to-Peer Systems*. Berkeley.

Dimakis, A., Godfrey, P., Wu, Y., Wainwright, M. y Ramchandran, K. (2010). Network Coding for Distributed Storage Systems. *IEEE Transaction on Information Theory*, *56* (9), 4539-4551.

Gheorghiu, S., Lima, L., López, A. L., Barros, J. y Medard, M. (2010). On the Performance of Network Coding in Multi-Resolution Wireless Video Streaming. *IEEE International Symposium on Network Coding (NetCod 2010)*. 1-6.

Gkantsidis, C. y Rodriguez, P. (2005). Network Coding for Large Scale Content Distribution. *IEEE INFOCOM*, *4*, 2235-2245.

Gnawali, O., Fonseca, R., Jamieson, K., Moss, D. y Levis, P. (2009). Collection tree protocol. *7th ACM Conf. on Embedded Networked Sensor Systems (SenSys)*. Berkeley.

Guo, Z., Xie, P., Cui, J. y Wang, B. (2006). On Applying Network Coding to Underwater Sensor Networks. *1st ACM international workshop on Underwater networks (WUWNet)*. 109-112.

Ho, T., Koetter, R., Médard, M., Karger, D. y Effros, M. (2003). The benefits of coding over routing in a randomized setting. *IEEE International Symposium on Information Theory*. 442.

Ho, T., Médard, M., Koetter, R., Karger, D., Effros, M., Shi, J. y Leong, B. (2006). A random linear network coding approach to multicast. *IEEE Transactions on Information Theory*, *52* (10), 4413-4430.

IRTF - Internet Research Task Force (2014). Recuperado de https://irtf.org/nwcrg.

Levis, P., Lee, N., Welsh, M. y Culler, D. (2003). TOSSIM: Accurate and scalable simulation of entire TinyOS applications. *1st ACM Conference on Embedded Networked Sensor Systems (SenSys)*, 126-137.

Li, S., Yeung, R. y Cai, N. (2003). Linear Network Coding. *IEEE, Transaction on Information Theory*, *49* (2), 371-381.

Lima, L., Gheorghiu, S., Barros, J., Médard. M. y Toledo, A. (2010). Secure Network Coding for Multi-Resolution Wireless Video Streaming. *IEEE Journal of Selected Areas in Communications*, 28 (3), 377-388.

Liu, Y., Dou, W. y Liu, Z. (2004). Layer Allocation Algorithms in Layered Peer-to-Peer Streaming, *IFIP International Conference on Network and Parallel Computing (NPC)*. 167-174.

Ma, G., Xu, Y., Ou, K. y Luo, W. (2009). How Can Network Coding Help P2P Content Distribution? *IEEE International Conference on Communications (ICC)*. 1-5.

Nguyen, K., Nguyen, T. y Cheung, S.-C. (2010). Video Streaming with Network Coding. *Springer Journal of Signal Process System, 59* (3), 319-333.

Nguyen, A. T., Li, B. & Eliassen, F. (2010). "Chameleon:

Adaptative Peer-to-Peer Streaming with Network Coding", *IEEE INFOCOM 2010*, pp. 1-5, San Diego, CA, USA.

Oh, H. & Kim, C. (2013). Network Coding-Based Mobile Video Streaming over Unreliable Wireless Links. *IEEE Communications Letters*, *17* (2), 281-284.

Oliveira, P. y Barros, J. (2008). A Network Coding Approach to Secret Key Distribution. *Transactions on Information Forensics and Security*, *3* (3), 414-423.

Park, J., Lun, D., Yi, Y., Gerla, M. y Médard, M. (2006). CodeCast: A Network Coding Based Ad Hoc Multicast Protocol. *IEEE Wireless Communications*, *13* (5), 76-81.

Planet-lab (2007). Disponible en http://www.planet-larb.org

Qual-Net (2010). Scalable Network Technologies. Disponible en http://www.qualnet.com, consultado el 10 de febrero de 2014.

Sundararajan, J., Shah, D., Médard, M. Mitzenmacher, M. y Barros, J. (2009). Network Coding meets TCP. *IEEE INFOCOMM 2009*, 280-288.

Tuninetti, D. y Fragouli, C. (2004). Processing along the way: Forwarding vs. Coding. *International Symposium on Information Theory and its Applications (ISITA)*. Parma: ISITA.

Vilela, J. P., Lima, L. y Barros, J. (2008). Lightweight Security for Network Coding. *IEEE International Conference on Communications (ICC 2008)*. 1750-1754.

.